



IBM® i integration with BladeCenter® and System x®

# IBM i iSCSI Solution Guide

Last updated: 3 March 2016

Category	Fast Path TOC	Page
Support Matrices	<a href="#">iSCSI solution capabilities</a>	<a href="#">19</a>
	<a href="#">Blade server models</a>	<a href="#">32</a>
	<a href="#">Blade iSCSI initiators</a>	<a href="#">35</a>
	<a href="#">System x server models</a>	<a href="#">37</a>
	<a href="#">System x iSCSI initiators</a>	<a href="#">40</a>
	<a href="#">IBM i iSCSI targets</a>	<a href="#">42</a>
Concepts	<a href="#">Concepts</a>	<a href="#">50</a>
Installation and Configuration	<a href="#">Server installation road map and checklist</a>	<a href="#">140</a>
	<a href="#">Server cloning road map and checklist</a>	<a href="#">222</a>
	<a href="#">BladeCenter and System x configuration</a>	<a href="#">241</a>
Additional Topics	<a href="#">Installing IBM i integration service packs</a>	<a href="#">319</a>
	<a href="#">Configuring multipath I/O for integrated servers</a>	<a href="#">324</a>
	<a href="#">Using hot spare hardware</a>	<a href="#">338</a>
	<a href="#">Implementing IBM i clustering for integrated servers</a>	<a href="#">344</a>
	<a href="#">Expanding a disk drive for an integrated server</a>	<a href="#">353</a>
	<a href="#">Managing iSCSI target and initiator usage</a>	<a href="#">362</a>
	<a href="#">Additional integrated Windows server topics</a>	<a href="#">367</a>
<a href="#">Additional integrated VMware ESX server topics</a>	<a href="#">397</a>	

**3 March 2016**

This edition applies to version 5, release 4, modification 0 of IBM i (product number 5722-SS1) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright International Business Machines Corporation 2012. All rights reserved.**

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

# Table of Contents

<b>1</b>	<b>About this guide</b>	<b>11</b>
1.1	What's new	11
1.2	How to use this guide	15
1.2.1	Chapter overview	15
1.2.2	Use this guide in soft copy form, rather than hard copy (printed) form	16
1.2.3	Common notation used throughout this guide	17
1.2.3.1	IBM i (i5/OS) and machine code version combinations	17
1.2.3.2	iSCSI target and initiator types	17
1.2.4	Alternative task navigation	18
<b>2</b>	<b>iSCSI solution support matrices</b>	<b>19</b>
2.1	iSCSI solution capabilities	19
2.1.1	Integrated Server Operating System (Server OS) Versions	20
2.1.1.1	Microsoft service packs	21
2.1.2	Server Installation Capabilities	22
2.1.3	Configuration and Management Capabilities	22
2.1.4	Server Discovery and Power Control Capabilities	23
2.1.5	Virtual Storage Capabilities	24
2.1.6	Backup and Recovery Capabilities	25
2.1.7	iSCSI Network Capabilities	26
2.1.8	Virtual Ethernet Capabilities	27
2.1.9	Server OS Integration Capabilities	27
2.1.10	User Enrollment Capabilities	28
2.1.11	Miscellaneous Capabilities	28
2.2	Ordering channels	29
2.3	IBM i products and options	30
2.4	BladeCenter chassis models	31
2.5	Blade server models	32
2.5.1	Blade iSCSI initiators	35
2.6	System x server models	37
2.6.1	System x iSCSI initiators	41
2.7	IBM i iSCSI targets	42
2.7.1	Power Server IBM i iSCSI target support	43
2.8	iSCSI supported limits	44
2.9	IBM i tape and optical device access by integrated servers	45
2.9.1	IBM i tape devices for Windows Server 2012/2008	46
2.9.2	IBM i tape devices for Windows Server 2003	47
2.9.3	IBM i tape libraries	49
2.9.4	IBM i tape media	50
<b>3</b>	<b>Concepts</b>	<b>51</b>
3.1	Integrated server overview	53
3.2	Attaching servers to IBM i using iSCSI	54
3.2.1	Typical iSCSI-attached server installation	56
3.2.2	Single-server environment	58
3.2.3	Multiple-server environment	59
3.2.4	Integrated server service processor connection	60
3.2.5	Booting over the iSCSI network	61
3.3	IBM i configuration objects for integrated servers	62
3.4	Server management for integrated servers	67
3.4.1	IBM i management interfaces	67
3.4.2	Additional management interfaces	68
3.4.3	Integrated server installation	68

3.4.4	Integrated server cloning.....	69
3.4.5	Integrated server management infrastructure .....	72
3.4.5.1	Integrated Windows server management infrastructure .....	72
3.4.5.1.1	Windows services for IBM i integration with Windows servers .....	72
3.4.5.1.2	Windows utilities for IBM i integration with Windows servers .....	73
3.4.5.2	Integrated VMware ESX server management infrastructure.....	74
3.4.5.2.1	Windows services for IBM i integration with ESX servers.....	77
3.4.5.2.2	Windows utilities for IBM i integration with ESX servers.....	77
3.4.5.2.3	Service console programs for IBM i integration with ESX servers.....	78
3.4.6	Integrated server console.....	78
3.4.7	Software updates .....	79
3.5	Storage management for integrated servers .....	81
3.5.1	Virtual storage .....	81
3.5.2	IBM i storage management .....	82
3.5.2.1	IBM i and disk drives .....	82
3.5.2.2	Storage pools (ASPs).....	83
3.5.2.3	Disk protection .....	84
3.5.3	Predefined virtual storage and naming.....	85
3.5.4	Create user-defined virtual storage.....	87
3.5.4.1	Storage alignment considerations when creating virtual storage.....	88
3.5.5	Copy virtual storage .....	90
3.5.6	Extend the size of virtual storage .....	90
3.5.7	Virtual storage linking.....	91
3.5.7.1	Dynamic virtual storage linking while server is active .....	92
3.5.8	Virtual storage formatting .....	93
3.5.9	Virtual storage unlinking.....	94
3.5.9.1	Dynamic virtual storage unlinking while server is active .....	94
3.6	IBM i tape and optical devices shared with integrated Windows servers .....	95
3.7	Networking concepts for integrated servers .....	96
3.7.1	iSCSI network.....	96
3.7.2	Integrated iSCSI DHCP server.....	99
3.7.2.1	Advanced integrated iSCSI DHCP server concepts .....	99
3.7.3	Ethernet switches for the iSCSI solution .....	100
3.7.3.1	External switch considerations.....	100
3.7.3.2	BladeCenter switch module considerations .....	101
3.7.4	Service processor connection .....	102
3.7.4.1	Supported functions by service processor type .....	103
3.7.4.2	Service processor addressing methods .....	104
3.7.4.3	Service processor connection methods .....	105
3.7.4.4	Considerations for connecting service processors to IBM i .....	105
3.7.5	Networking for IBM i administration of integrated servers.....	107
3.7.5.1	Point-to-point virtual Ethernet network for integrated Windows servers .....	107
3.7.5.2	Multiple networks for integrated VMware ESX servers .....	108
3.7.6	Virtual Ethernet networks for integrated Windows servers.....	108
3.7.7	Physical networks.....	111
3.7.8	Network security.....	112
3.8	Performance concepts.....	114
3.8.1	Virtual storage performance .....	114
3.8.2	IBM i memory requirements .....	116
3.8.2.1	Machine pool.....	116
3.8.2.2	iSCSI virtual storage I/O memory pool.....	116
3.8.3	Virtual Ethernet performance for integrated Windows servers.....	117
3.8.4	MTU considerations for the iSCSI network .....	118
3.9	Backup and recovery concepts .....	119
3.9.1	What objects to save and their location on IBM i .....	123

3.10	High availability concepts.....	125
3.10.1	Multipath I/O (MPIO) .....	125
3.10.2	Hot spare support for integrated servers.....	128
3.10.2.1	Hot spare support for System x or blade hardware.....	128
3.10.2.2	Hot spare support for IBM i iSCSI target adapters.....	129
3.10.3	IBM i clustering for integrated servers.....	130
3.11	User and group enrollment concepts for integrated Windows servers .....	131
3.11.1	Enrolled user account options for integrated Windows servers .....	134
3.11.2	User enrollment templates for integrated Windows servers .....	136
3.11.3	Password considerations for integrated Windows servers.....	137
3.11.4	QAS400NT user and integrated Windows servers.....	138
3.12	IBM i NetServer for integrated servers.....	138
3.13	IBM i Access for Windows and integrated servers.....	139
<b>4</b>	<b>Server installation road map and checklist .....</b>	<b>140</b>
4.1	Prerequisites.....	142
4.1.1	Review iSCSI solution concepts.....	142
4.1.2	Ensure that you have access to the required documentation .....	142
4.1.3	Verify that you have access to the required IBM i products .....	143
4.1.4	Load required IBM i products .....	143
4.1.4.1	Install System i (iSeries) Navigator on a PC .....	144
4.1.5	Load latest required fixes (each time servers are installed).....	145
4.2	Prepare for the hardware installation.....	146
4.2.1	Obtain required hardware.....	146
4.2.1.1	Obtain IBM i iSCSI target adapter.....	146
4.2.1.2	Obtain BladeCenter or System x server and associated hardware .....	147
4.2.2	Obtain firmware updates and drivers for your integrated server hardware .....	148
4.2.3	Obtain the integrated server operating system .....	149
4.3	Plan the iSCSI network and integrated server installation.....	150
4.3.1	Planning work sheets overview .....	150
4.3.2	Configuration objects.....	151
4.3.3	Planning for the service processor connection.....	152
4.3.3.1	Identifying a BladeCenter or System x service processor type.....	153
4.3.3.2	Selecting a service processor connection method.....	153
4.3.3.3	Recording the system serial number and type/model .....	155
4.3.3.4	Selecting a name for the service processor configuration .....	155
4.3.3.5	Selecting a login ID and password for the service processor .....	156
4.3.4	Planning for the remote system configuration.....	157
4.3.4.1	Recording the blade system serial number and type/model .....	157
4.3.4.2	Selecting a name for the remote system configuration .....	158
4.3.4.3	Selecting a boot parameter delivery method.....	159
4.3.4.4	Selecting CHAP settings.....	160
4.3.4.4.1	Selecting parameters for target CHAP.....	160
4.3.4.4.2	Selecting parameters for initiator CHAP .....	161
4.3.4.5	Selecting the MTU for the iSCSI network.....	161
4.3.4.6	Recording iSCSI initiator (local adapter) MAC addresses .....	162
4.3.4.7	Selecting IP addresses for the System x or blade iSCSI initiator.....	164
4.3.4.7.1	Expanding on the iSCSI network addressing scheme for integrated servers .....	165
4.3.4.8	Selecting the initiator iSCSI Qualified Name (IQN) .....	166
4.3.4.9	Selecting the target iSCSI Qualified Name (IQN) .....	167
4.3.5	Planning for the network server host adapter (NWSH) object.....	168
4.3.5.1	Selecting a name for the NWSH .....	168
4.3.5.2	Selecting a hardware resource name .....	169
4.3.5.3	Selecting a connection type for the NWSH.....	169
4.3.5.4	Selecting IP addresses for the IBM i iSCSI target.....	170
4.3.5.5	Selecting line description values for a software target .....	172

4.3.6	Planning for the integrated server installation .....	173
4.3.6.1	Selecting the server operating system type .....	173
4.3.7	Choosing the system drive capacity and storage pool .....	174
4.3.7.1	Selecting a memory pool for iSCSI I/O .....	175
4.3.7.2	Selecting a name for the NWSD .....	176
4.3.7.3	Selecting a language version .....	176
4.3.7.4	Selecting IBM i tape and optical devices to allow (i 7.2 only) .....	177
4.3.7.5	Selecting IBM i tape and optical devices to restrict .....	177
4.3.7.6	Selecting point-to-point virtual Ethernet IP addresses .....	179
4.3.7.7	Selecting preferred storage unit to store virtual storage on (i 7.2 only) .....	180
4.3.7.8	Selecting additional INSxxxSVR command parameters .....	180
4.3.7.9	Planning for VMware ESX server management .....	182
4.4	Install the hardware .....	183
4.4.1	Install each new IBM i iSCSI target .....	183
4.4.2	Install the BladeCenter or System x hardware and iSCSI initiators .....	184
4.4.2.1	Update and configure the BladeCenter or System x hardware .....	185
4.4.2.1.1	Updating and configuring the BladeCenter chassis .....	185
4.4.2.1.2	Verifying blade information .....	186
4.4.2.2	Configure the iSCSI initiators .....	187
4.4.2.3	Configure the integrated server start options .....	187
4.4.3	Cable the network .....	187
4.5	Prepare IBM i for the integrated server installation .....	189
4.5.1	Create an NWSH for each new IBM i iSCSI target .....	189
4.5.1.1	Determining the hardware resource name for an iSCSI target adapter .....	191
4.5.2	Start the NWSH for each IBM i iSCSI target that the server uses .....	192
4.5.3	Create and initialize a service processor configuration .....	193
4.5.3.1	Configuring IBM i to use Service Processor Manager on i 6.1 and i 5.4 .....	194
4.5.4	Create a remote system configuration .....	195
4.5.5	Verify that the remote system is accessible and powered off .....	196
4.5.6	Create a QCNNSEC connection security configuration, if necessary .....	196
4.5.7	Prepare for IBM i memory requirements .....	197
4.5.8	Set the IBM i QRETSVRSEC system value for integrated servers .....	198
4.5.9	Ensure that NetServer is configured .....	199
4.5.10	WIN2003 only: Configure IBM i TCP/IP .....	200
4.6	Install the integrated server .....	201
4.6.1	Start the installation from IBM i .....	202
4.6.2	Continue the operating system installation from the integrated server console .....	205
4.6.2.1	Continuing the Windows Server 2012/2008 installation from the Windows console .....	205
4.6.2.2	Continuing the Windows Server 2003 installation from the Windows console .....	206
4.6.2.3	Continuing the VMware ESXi Embedded installation from the ESX console .....	207
4.6.2.4	Continuing the VMware ESX 5 installation from the ESX console .....	208
4.6.2.5	Continuing the VMware ESX 4 installation from the ESX console .....	208
4.6.2.6	Continuing the VMware ESX 3.5 installation from the ESX console .....	209
4.6.3	Complete the integrated server installation .....	210
4.6.3.1	Completing the Windows Server 2012/2008 installation .....	210
4.6.3.1.1	Completing the Windows Server 2012/2008 full installation .....	211
4.6.3.1.2	Completing the Windows Server 2012/2008 core installation .....	212
4.6.3.2	Completing the Windows Server 2003 installation .....	213
4.6.3.3	Completing the ESX installation – Management server based infrastructure .....	215
4.6.3.4	Completing the ESX installation – Service console based infrastructure .....	216
4.7	After the integrated server installation .....	218
4.7.1	Scale the iSCSI network .....	218
4.7.2	Create additional virtual storage for applications and data .....	218
4.7.3	Configure the integrated server to automatically start .....	218
4.7.3.1	Configuring a point-to-point virtual Ethernet port for an integrated ESX server .....	220

4.7.4	Windows only: Define additional virtual Ethernet LANs .....	221
4.7.5	Windows only: Enroll IBM i users to the Windows server or domain .....	221
4.7.6	Keep the IBM i Integrated Server Support software up to date .....	221
<b>5</b>	<b>Server cloning road map and checklist .....</b>	<b>222</b>
5.1	Prepare for server cloning .....	223
5.1.1	Review IBM i integrated server cloning concepts .....	223
5.1.2	Identify the base server to clone .....	223
5.1.3	Run sysprep to prepare the base server for cloning .....	223
5.1.4	Obtain necessary software licenses .....	226
5.1.5	Install and configure new server hardware, if necessary .....	227
5.1.5.1	Verify that the remote system is accessible from IBM i .....	228
5.2	Run the IBM i integrated server cloning Wizard .....	229
5.3	Configure the clone server .....	230
5.3.1	Verify or change the clone server NWSD properties .....	230
5.3.1.1	Checking NWSH resource usage .....	232
5.3.2	Start the clone server from IBM i .....	232
5.3.3	Complete the Windows Mini-Setup Wizard .....	232
5.3.4	Set the clone server point-to-point virtual Ethernet IP address .....	233
5.3.5	Change clone server properties on Windows .....	234
5.3.5.1	Change the clone server computer name (host name) .....	236
5.3.5.2	Change any clone server static IP addresses .....	237
5.3.6	Shut down and start the clone server from IBM i and regenerate path certificates .....	238
5.3.7	Verify that IBM i can manage the clone server .....	240
5.3.8	After the integrated server has been cloned .....	240
<b>6</b>	<b>BladeCenter and System x configuration .....</b>	<b>241</b>
6.1	Downloading and updating firmware and drivers .....	243
6.1.1	Using Bootable Media Creator (BoMC) .....	243
6.1.1.1	Downloading server updates with Bootable Media Creator (BoMC) .....	243
6.1.1.1.1	Updating Bootable Media Creator to latest version .....	244
6.1.1.2	Updating the server using Bootable Media Creator (BoMC) media .....	245
6.1.2	Firmware updates for the BladeCenter chassis .....	246
6.1.2.1	Downloading firmware updates for the BladeCenter chassis .....	246
6.1.2.2	Updating the BladeCenter management module firmware .....	247
6.1.2.3	Updating and configuring the BladeCenter I/O module .....	248
6.1.3	Windows drivers for iSCSI initiators .....	249
6.1.3.1	Downloading Windows Ethernet NIC software initiator driver .....	249
6.1.3.2	Downloading System x Windows Server 2012/2008 iSCSI HBA driver .....	250
6.2	Configuring the BladeCenter or System x service processor .....	250
6.2.1	Configuring the BladeCenter management module .....	250
6.2.2	Configuring the System x service processor .....	252
6.2.2.1	Configuring the System x IMM II .....	252
6.2.2.1.1	Configuring the IMM II IP address and DHCP settings .....	254
6.2.2.2	Configuring the System x IMM .....	255
6.2.2.2.1	Configuring the IMM IP address and DHCP settings .....	257
6.2.2.3	Configuring the System x RSA II .....	258
6.2.2.3.1	Configuring the RSA II IP address and DHCP settings .....	260
6.2.2.4	Configuring the System x BMC .....	261
6.2.3	Connecting to the service processor Web interface .....	263
6.2.3.1	Determining an IP address for the service processor Web interface .....	264
6.3	iSCSI Initiator Hardware Configuration .....	265
6.3.1	iSCSI initiator configuration methods .....	265
6.3.2	"iSCSI Mode" for booting UEFI-based servers .....	266
6.3.3	Starting the iSCSI initiator configuration utility .....	266
6.3.3.1	Starting the QLogic Fast!UTIL utility .....	267

6.3.3.2	Starting the UEFI Setup utility .....	268
6.3.3.3	Starting the iSCSI Configuration Manger utility (SWI-BladeBoot).....	268
6.3.3.3.1	Installing the iSCSI Configuration Manager application (SWI-BladeBoot).....	269
6.3.4	Configuring a boot iSCSI initiator port.....	270
6.3.4.1	Configuring a boot iSCSI initiator port (HWI-QLogic).....	270
6.3.4.1.1	Configuring a boot iSCSI initiator for dynamic addressing (HWI-QLogic).....	271
6.3.4.1.2	Configuring a boot iSCSI initiator for manual addressing (HWI-QLogic) .....	272
6.3.4.2	Configuring a boot iSCSI initiator port (SWI-UEFI) .....	275
6.3.4.2.1	Configuring a boot iSCSI initiator for dynamic addressing (SWI-UEFI) .....	275
6.3.4.2.2	Configuring a boot iSCSI initiator for manual addressing (SWI-UEFI).....	278
6.3.4.3	Configuring a boot iSCSI initiator port (SWI-BladeBoot).....	280
6.3.4.3.1	Configuring a boot iSCSI initiator for dynamic addressing (SWI-BladeBoot).....	280
6.3.4.3.2	Configuring a boot iSCSI initiator for manual addressing (SWI-BladeBoot) .....	282
6.3.5	Configuring advanced iSCSI initiator port settings.....	285
6.3.5.1	Configuring advanced iSCSI initiator port settings (HWI-QLogic).....	285
6.3.6	Configuring non-boot iSCSI initiator ports.....	286
6.3.6.1	Configuring non-boot iSCSI initiator ports (HWI-QLogic).....	286
6.3.6.2	Configuring non-boot iSCSI initiator ports (SWI-UEFI) .....	287
6.3.7	Configuring boot iSCSI initiator with manual addressing for MPIO target.....	288
6.3.7.1	Configuring boot iSCSI initiator with manual addr. for MPIO target (HWI-QLogic) ..	289
6.3.7.2	Configuring boot iSCSI initiator with manual addr. for MPIO target (SWI-UEFI) .....	290
6.3.8	Configuring additional boot iSCSI initiators for Windows MPIO .....	291
6.3.8.1	Configuring additional boot iSCSI initiators for Windows MPIO (HWI-QLogic).....	291
6.3.8.1.1	Configuring additional boot iSCSI initiators with dynamic addr. (HWI-QLogic).....	292
6.3.8.1.2	Configuring additional boot iSCSI initiators with manual addr. (HWI-QLogic) .....	293
6.3.8.2	Configuring additional boot iSCSI initiators for Windows MPIO (SWI-UEFI) .....	296
6.3.8.2.1	Configuring additional boot iSCSI initiators with dynamic addr. (SWI-UEFI) .....	296
6.3.8.2.2	Configuring additional boot iSCSI initiators with manual addr. (SWI-UEFI).....	298
6.3.9	Restoring factory defaults for an iSCSI initiator.....	301
6.3.9.1	Restoring factory defaults for an iSCSI initiator (HWI-QLogic) .....	301
6.3.10	Resetting cached iSCSI initiator configuration information .....	302
6.3.10.1	Resetting cached iSCSI initiator configuration information (HWI-QLogic) .....	302
6.3.11	Verifying the iSCSI connection using ping .....	303
6.3.11.1	Verifying the iSCSI connection using ping (HWI-QLogic) .....	303
6.3.12	Configuring target CHAP.....	304
6.3.12.1	Configuring target CHAP (HWI-QLogic).....	304
6.3.12.2	Configuring target CHAP (SWI-UEFI).....	305
6.3.13	Configuring initiator CHAP .....	306
6.3.13.1	Configuring initiator CHAP (HWI-QLogic) .....	306
6.3.13.2	Configuring initiator CHAP (SWI-UEFI).....	306
6.3.14	Changing the iSCSI initiator CHAP secret .....	308
6.3.14.1	Changing the iSCSI initiator CHAP secret (HWI-QLogic) .....	308
6.3.14.2	Changing the iSCSI initiator CHAP secret (SWI-UEFI).....	309
6.3.15	Changing the iSCSI initiator MTU .....	310
6.3.15.1	Changing the iSCSI initiator MTU (HWI-QLogic) .....	310
6.3.15.2	Changing the iSCSI initiator MTU (SWI-UEFI).....	311
6.3.16	Disabling iSCSI header and data digests.....	312
6.3.16.1	Disabling iSCSI header and data digests (HWI-QLogic).....	312
6.3.17	Ending the iSCSI initiator configuration utility.....	313
6.3.17.1	Ending the QLogic Fast!UTIL utility.....	313
6.3.17.2	Ending the UEFI Setup utility .....	313
6.3.17.3	Ending the iSCSI Configuration Manger utility (SWI-BladeBoot).....	313
6.4	Setting the integrated server start options.....	314
6.4.1	Setting the integrated server start options (UEFI).....	314
6.4.2	Setting the integrated server start options (BIOS).....	317



<b>7</b>	<b>Additional topics.....</b>	<b>319</b>
7.1	Installing IBM i integration service packs.....	319
7.1.1	Determining the integration software level .....	319
7.1.2	Updating the integration software running on Microsoft Windows .....	320
7.1.2.1	Updating the integration software: Windows server console .....	320
7.1.2.1.1	Updating the integration software: lvsync .....	321
7.1.2.2	Updating the integration software: IBM i GUI.....	322
7.1.2.3	Updating the integration software: remote command .....	322
7.1.3	Updating the integration software: ESX service console.....	323
7.2	Configuring multipath I/O for integrated servers.....	324
7.2.1	Configuring IBM i for multipath I/O .....	325
7.2.2	Configuring Windows Server 2012 for multipath I/O .....	327
7.2.3	Configuring Windows Server 2008 for multipath I/O .....	328
7.2.4	Configuring Windows Server 2003 for multipath I/O .....	329
7.2.5	Configuring ESXi 5 or ESXi 4 for multipath I/O with iSCSI software initiators.....	330
7.2.6	Configuring ESXi 4 or ESX 4 for multipath I/O with iSCSI HBAs .....	334
7.2.7	Configuring ESX 3.5 for multipath I/O with iSCSI HBAs .....	336
7.3	Using hot spare hardware .....	338
7.3.1	Using hot spare integrated server hardware .....	338
7.3.2	Using hot spare iSCSI hardware target adapters.....	340
7.3.3	Using hot spare iSCSI software target adapters .....	341
7.4	Implementing IBM i clustering for integrated servers .....	344
7.4.1	Mirroring virtual storage (NWSSTG) .....	345
7.4.1.1	Moving virtual storage between ASPs .....	347
7.4.2	Mirroring the network server description (NWSD).....	348
7.4.3	Mirroring network server configurations (NWSCFGs).....	349
7.4.4	Mirroring the NWSH for an iSCSI target.....	350
7.4.5	Recommended settings for geographic mirroring in an iSCSI environment.....	351
7.4.6	Switching an iSCSI-attached VMware ESX server from one node to another .....	351
7.5	Expanding a disk drive for an integrated server .....	353
7.5.1	Expanding a storage space from IBM i .....	353
7.5.2	Expanding a data drive for ESX Server.....	355
7.5.3	Expanding a data drive for Windows Server 2012 or 2008 or 2003.....	357
7.5.4	Expanding a system drive for Windows Server 2012/2008.....	358
7.5.5	Expanding a system drive for Windows Server 2003.....	359
7.6	Managing iSCSI target and initiator usage .....	362
7.6.1	Sharing an iSCSI target among multiple integrated servers .....	362
7.6.2	Distributing iSCSI network traffic between multiple iSCSI targets.....	363
7.6.3	Managing iSCSI initiator allocation at the Windows side of the iSCSI network.....	364
7.6.3.1	Display information about iSCSI initiator allocation.....	366
7.7	Additional integrated Windows server topics.....	367
7.7.1	Formatting storage for Windows servers.....	368
7.7.2	Enabling Windows share names for file level backup from IBM i .....	369
7.7.3	Managing virtual Ethernet networks .....	371
7.7.3.1	Display information about virtual Ethernet adapters .....	371
7.7.3.2	Configuring IP address, gateway, and MTU values for integrated servers .....	371
7.7.3.2.1	Configuring VE for applications that support frame sizes larger than 1500 bytes .....	371
7.7.3.2.2	Configuring VE for iSCSI networks with a frame size less than 1500 bytes .....	372
7.7.3.2.3	Configuring VE to support non-TCP applications that do not negotiate MTU .....	372
7.7.3.3	Configuring virtual Ethernet networks between integrated Windows servers .....	373
7.7.3.4	Configuring inter-partition virtual Ethernet for integrated Windows servers .....	374
7.7.3.5	Managing point-to-point virtual Ethernet networks for integrated Windows servers .....	375
7.7.3.5.1	Viewing point-to-point (PTP) virtual Ethernet connections from IBM i .....	375
7.7.3.5.2	Viewing PTP virtual Ethernet connections from the integrated Windows server console .....	376
7.7.4	Sharing tape and optical devices between IBM i and integrated Windows servers .....	377

7.7.4.1	Using IBM i tape devices with integrated Windows servers .....	377
7.7.4.1.1	Installing tape device drivers on Windows .....	377
7.7.4.1.2	Formatting an IBM i tape for use with an integrated Windows server.....	378
7.7.4.1.3	Transferring an IBM i tape device to an integrated Windows server .....	378
7.7.4.1.4	Transferring a tape device from integrated Windows server to IBM i .....	379
7.7.4.1.5	Identifying IBM i tape devices to Windows applications.....	380
7.7.4.2	Using IBM i optical devices with integrated Windows servers .....	381
7.7.4.2.1	Transferring an optical device from IBM i to an integrated Windows server.....	381
7.7.4.2.2	Transferring an optical device from an integrated Windows server to IBM i.....	382
7.7.4.3	Transferring IBM i tape and optical devices between integrated Windows servers .....	382
7.7.4.4	Restricting IBM i tape and optical devices from integrated Windows servers.....	383
7.7.5	Printing to IBM i printers from integrated Windows servers .....	384
7.7.6	Running integrated Windows server commands remotely .....	385
7.7.6.1	Guidelines for running remote commands on an integrated Windows server.....	386
7.7.6.1.1	SBMNWSCMD and file level backup support for Kerberos V5 and EIM .....	388
7.7.7	Configuring time synchronization for integrated Windows server .....	389
7.7.8	Firewall considerations for Windows servers .....	390
7.7.9	Windows Server 2003 topics.....	392
7.7.9.1	Integrating a service pack with Windows Server 2003.....	392
7.7.9.2	Windows Server 2003 Service Pack 1 .....	393
7.7.9.3	Using IBM i virtual optical support for Windows Server 2003 installations.....	393
7.7.9.4	Creating a Windows Server 2003 install CD image in IFS.....	395
7.7.9.5	Using the Windows Server 2003 Backup utility with integrated servers .....	396
7.7.9.6	Migrating IXS/IXA Windows Server 2003 to iSCSI .....	396
7.8	Additional integrated VMware ESX server topics .....	397
7.8.1	VMware ESX documentation and management tools.....	398
7.8.2	Tasks for ESX Management server based infrastructure.....	398
7.8.2.1	Configuring the QVMWINT user for integrated VMware ESX server management .....	398
7.8.2.2	Managing connections for integrated VMware ESX servers.....	400
7.8.2.2.1	Adding connection information.....	401
7.8.2.2.2	Listing connection information .....	402
7.8.2.2.3	Verifying connection information.....	402
7.8.2.2.4	Changing connection information .....	403
7.8.2.2.5	Overriding management of a connection .....	403
7.8.2.2.6	Deleting connection information.....	404
7.8.3	Switching between ESX 4 server management infrastructures on i 6.1.....	405
7.8.4	Save While Active (SWA) for integrated VMware ESX servers on i 7.1 or higher .....	406
7.8.4.1	Reverting to a consistent SWA virtual machine snapshot after restore .....	406
7.8.4.2	Deleting the SWA virtual machine snapshot without reverting.....	407
7.8.5	ESX migration and upgrade scenarios.....	408
7.8.5.1	Migrating VMware ESX servers to i 7.1 or higher .....	408
7.8.5.2	Migrating VMware ESX servers to i 6.1 .....	412
7.8.5.3	Upgrading VMware ESX 3 to VMware ESX 4.....	414
7.8.5.3.1	Upgrading an existing VMware ESX 3.x server to VMware ESX 4.....	415
<b>Notices</b>	.....	<b>417</b>

# 1 About this guide

This guide and the associated *IBM i iSCSI Solution Work Sheets* provide the information you need to plan for and install an IBM BladeCenter blade or System x server that is attached to an IBM i system using an iSCSI network (iSCSI).

This guide focuses primarily on the initial installation and configuration of an iSCSI-attached server.

This guide does not address all server management tasks for iSCSI-attached servers. Refer to the [IBM i Information Center](#) for post-installation tasks such as virtual storage management, backup and recovery, user and group enrollment, and implementing high availability.

## 1.1 What's new

### 3 March 2016

Information that has been updated in this revision:

1. Removed the port number limitation for **Power System Ethernet NIC** in chapter **2.7 IBM i iSCSI targets**. See [IBM i iSCSI Targets](#) section.

### 19 January 2015

Information that has been added or updated in this revision:

2. New Installs of WIN2003 are not supported. Existing installations should continue to work on an "as is" basis. See the [Integrated Server Operating System \(Server OS\) Versions](#) section.
3. Power8 systems are supported. See [Power Server IBM i iSCSI target support](#) for the Power systems that are supported.
4. Migration of pre-7.2 virtual disk to 7.2 formats is described. See the [Create user-defined virtual storage](#) for more information.
5. Add Notes about Enrolling to multiple domains. See the [User and group enrollment concepts for integrated Windows servers](#) for more information.

### 2 April 2014

Information that has been added or updated in this revision:

1. Virtual disk with 4K sector size is supported. See the [Create user-defined virtual storage](#) for more information.
2. Support to specify a preference to create virtual disk on solid-state drives. See the [Create user-defined virtual storage](#) for more information.
3. Add a new parameter of the Install Integrated Server command (INSINTSVR) and the Create NWS Storage Space command (CRTNWSSTG ) to customize the priority of IBM i resources allocated to format the client storage space. See the [Create user-defined virtual storage](#) for more information.
4. Additional server models are supported. See [System x server models](#) for the server models that are supported.

## 1 February 2013

Information that has been added or updated in this revision:

1. iSCSI direct connect is supported when using an IBM i software target (Ethernet NIC) on i 7.1. See the [Direct connect](#) capabilities matrix for more information.
2. Windows Server 2012 is now supported on selected System x and blade servers when connected to IBM i 7.1. See [Blade server models](#) and [System x server models](#) for the server models that are supported.
3. ESX 5.1 is now supported on selected System x and blade servers when connected to IBM i 7.1 and 6.1. See [Blade server models](#) and [System x server models](#) for the server models that are supported.

## 29 May 2012

Information that has been added or updated in this revision:

1. Additional server models supported. See [Blade server models](#) and [System x server models](#) for the latest list of server models that are supported.
2. Additional iSCSI initiator adapters supported. See [Blade iSCSI initiators](#) and [System x iSCSI initiators](#) for the current list of iSCSI initiator adapters that are supported.
3. UEFI boot is supported for some configurations. See [“iSCSI Mode” for booting UEFI-based servers](#) for more information.

## 2 February 2012

Information that has been added or updated in this revision:

1. ESX 5.0 is now supported on selected System x and blade servers when connected to IBM i 6.1. See [Blade server models](#) and [System x server models](#) for the server models that are supported.
2. The i 7.1 and 6.1 [Web GUI](#) has been enhanced to make it easier to enable Windows file level backup from IBM i. See [Backup and recovery concepts](#) and [Enabling Windows share names for file level backup from IBM i](#).
3. Multipath I/O (MPIO) configuration tasks have been improved. See [Configuring multipath I/O for integrated servers](#).

## 11 August 2011

Information that has been added or updated in this revision:

1. Documentation for VMware ESXi Embedded 5 and ESXi Installable 5 support on IBM i 7.1.
2. Document navigation usability improvements. See [Use this guide in soft copy form, rather than hard copy \(printed\) form](#).

## 11 July 2011

Information that has been added or updated in this revision:

1. The [IBM i iSCSI Solution Work Sheets](#) that are used in conjunction with this guide have been enhanced so that they can be filled out and saved softcopy.
2. The procedure for expanding a disk drive has been documented in more detail. See [Expanding a disk drive for an integrated server](#).
3. Service pack 1 (SP1) on Windows Server 2008 R2 is now supported with integrated servers. See [Microsoft service packs](#).

## 23 May 2011

Information that has been added or updated in this revision:

1. The following i 7.1 [Web GUI](#) tasks are now available on i 6.1 systems:
  - Create Server, including the ability to clone Windows servers.
  - Delete Server.
  - Launch Web Console
  - Support for configuring IBM i iSCSI software target (SWT) network server host adapters (NWSHs).
2. Save while active (SWA) concepts and implementation for integrated VMware ESX servers.
3. IBM i High Availability (HA) concepts and implementation for integrated servers.
4. Additional IBM i integration with BladeCenter and System x Web pages have been migrated to this Guide:
  - Microsoft service packs
  - Firewall considerations for Windows servers
  - Windows Server 2003 Service Pack 1

## 10 April 2011

The initial version of this guide, which consolidates information that was previously documented in several locations:

1. IBM i integration with BladeCenter and System x Web pages:
  - iSCSI solution (iSCSI)
  - BladeCenter and System x models supported with iSCSI
  - Ethernet switches for iSCSI
  - Ordering channels for iSCSI
  - Various Web pages related to tape and optical device support
  - Various Web pages related to migration
2. iSCSI installation road map PDFs for i 7.1, i 6.1, and i 5.4
3. iSCSI Initiator Hardware Configuration PDF

4. Various IBM i Information Center articles related to:
  - Integrated server concepts
  - Integrated server installation and configuration
  - iSCSI Network Planning Guide
  - Integrated server operating system support

## 1.2 How to use this guide

### 1.2.1 Chapter overview

Chapter	Purpose
<a href="#">About this guide</a> (page <a href="#">11</a> )	This chapter introduces this guide and provides usage tips.
<a href="#">iSCSI solution support matrices</a> (page <a href="#">19</a> )	<p>Use this chapter to understand the capabilities that the IBM i iSCSI solution provides, including features that vary based on:</p> <ul style="list-style-type: none"> <li>• The IBM i release.</li> <li>• The System x or BladeCenter blade server model that is used.</li> <li>• The iSCSI target and initiator adapters that are used.</li> <li>• The integrated server operating system that is installed.</li> <li>• Other factors.</li> </ul> <p>Use this information to help you choose a supported hardware and software configuration that is appropriate for your needs.</p>
<a href="#">Concepts</a> (page <a href="#">50</a> )	<p>Use this chapter to gain a deeper understanding of the IBM i iSCSI solution.</p> <p>Many of the concepts described in this chapter are referenced in other chapters of this document, so you can refer back to this information as needed.</p>
<a href="#">Server installation road map and checklist</a> (page <a href="#">140</a> )	Use the checklist in this chapter to step through the process of installing an IBM BladeCenter or System x server that is attached to IBM i using an iSCSI network (iSCSI).
<a href="#">Server cloning road map and checklist</a> (page <a href="#">222</a> )	Use the checklist in this chapter to step through the process of cloning an existing integrated Windows® server that is attached to IBM i using an iSCSI network (iSCSI).
<a href="#">BladeCenter and System x configuration</a> (page <a href="#">241</a> )	This chapter contains configuration tasks for BladeCenter blade and System x servers.
<a href="#">Additional topics</a> (page <a href="#">319</a> )	<p>This chapter contains various topics related to the IBM i iSCSI solution:</p> <ul style="list-style-type: none"> <li>• <a href="#">Installing IBM i integration service packs</a></li> <li>• <a href="#">Configuring multipath I/O for integrated servers</a></li> <li>• <a href="#">Using hot spare hardware</a></li> <li>• <a href="#">Implementing IBM i clustering for integrated servers</a></li> <li>• <a href="#">Expanding a disk drive for an integrated server</a></li> <li>• <a href="#">Managing iSCSI target and initiator usage</a></li> <li>• <a href="#">Additional integrated Windows server topics</a></li> <li>• <a href="#">Additional integrated VMware ESX server topics</a></li> </ul>

## 1.2.2 Use this guide in soft copy form, rather than hard copy (printed) form

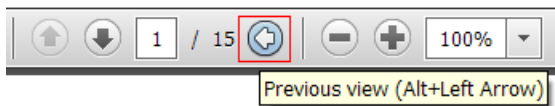
This guide is intended to be used in **soft copy** form, rather than in **hard copy** (printed) form for a couple of key reasons:

### 1. There are many hyperlinks between parts of this document.

For example, some tasks in this guide link to associated support matrices or concepts in this guide.

**Note:** With the exception of the table of contents (TOC), hyperlinks to another location within this document are shown with green underline highlighting. Here is an example link to the [iSCSI solution capabilities](#) section.

**Tip:** Enable the **Previous view** button in the **Page Navigation** tool bar of Adobe Reader or Adobe Acrobat:



Then, after following a link to another location within the document, you can use the **Previous view** button to easily return to the page that contained the link. This makes it easy to jump back and forth between sections of the document without keeping track of page numbers and doing a lot of scrolling.

To enable the **Previous view** tool bar button in **Adobe Reader X**, right click the tool bar and select **Page Navigation > Previous View**. Note that this option might be in a slightly different place in other versions of Adobe Reader or Adobe Acrobat.

### 2. There are many hyperlinks to information outside of this document.

For example, the support matrices for server models link to the Marketing Web pages for the newer server models. Likewise, various installation tasks link to external Web sites that are needed to complete the tasks, such as Web sites that provide the latest firmware to download.

**Note:** Hyperlinks to an external Web page or PDF are shown with blue underline highlighting. Here is an example link to the [IBM i PTFs](#) Web page.



### 1.2.3 Common notation used throughout this guide

The following sections show common notation that is used throughout this guide.

#### 1.2.3.1 IBM i (i5/OS) and machine code version combinations

The notation shown below is used in cases where it is necessary to distinguish which IBM i and machine code version combinations a particular feature or task applies to.

Notation	IBM i (i5/OS)		Machine Code	
	Product	Version	Product	Version
<b>i 5.4</b>	5722-SS1	V5R4M0	5722-999	V5R4M0 <i>or later</i>
<b>i 6.1</b>	5761-SS1	V6R1M0	5761-999	V6R1M0 <i>or later</i>
<b>i 6.1.1</b>	5761-SS1	V6R1M0	5761-999	<b>V6R1M1</b> <i>or later</i>
<b>i 7.1</b>	5770-SS1	V7R1M0	5770-999	V7R1M0 <i>or later</i>
<b>i 7.2</b>	5770-SS1	V7R2M0	5770-999	V7R2M0 <i>or later</i>
<b>All</b>	All of the above IBM i and machine code version combinations.			

Here is an **example** table showing support for features that vary based on the IBM i version:

Feature description	IBM i			
	i 7.2	i 7.1	i 6.1	i 5.4
This is the first feature	✓	✓	✓	
Another feature	✓	✓	✓	✓
One last feature			✓	✓

#### 1.2.3.2 iSCSI target and initiator types

Type	Description
<b>SWT</b>	iSCSI <b><u>S</u>oftware <u>T</u>arget</b> . For example, a Power Server Ethernet NIC port. With software targets, the iSCSI protocol is implemented in IBM i, rather than in the adapter hardware.
<b>HWT</b>	iSCSI <b><u>H</u>ardware <u>T</u>arget</b> . For example, a Power Server QLogic iSCSI HBA. With hardware targets, the iSCSI protocol is implemented in the adapter hardware, which offloads the iSCSI protocol processing from IBM i.
<b>SWI</b>	iSCSI <b><u>S</u>oftware <u>I</u>nitiator</b> . For example, a System x or blade server Ethernet NIC port. With software initiators, the iSCSI protocol is implemented in the integrated server operating system, rather than in the adapter hardware.
<b>HWI</b>	iSCSI <b><u>H</u>ardware <u>I</u>nitiator</b> . For example, a System x or blade server QLogic iSCSI HBA. With hardware initiators, the iSCSI protocol is implemented in the adapter hardware, which offloads the iSCSI protocol processing from the integrated server operating system.

## 1.2.4 Alternative task navigation

There are many cases in this guide where alternative task documentation is provided based on various criteria, such as:

- The IBM i version.
- The type of server (blade vs. System x).
- The server OS type or OS version (Windows vs. ESX).
- The iSCSI target or initiator type (HWT vs. SWT and HWI vs. SWI).

When alternative tasks are appropriate based on such criteria, this guide typically uses a table format to list the alternative tasks. The first column of the table lists the criteria choices and the second column lists the alternative tasks for each choice. Simply go to the table row that applies to your environment and then perform the alternative task that is documented in that table row.

Here is an **example** table with alternative tasks based on the [Server OS](#) version that is installed:

<b>Server OS</b>	<b>Tasks</b>
WIN2012 WIN2008	<a href="#">Continuing the Windows Server 2012/2008 installation from the Windows console</a>
WIN2003	<a href="#">Continuing the Windows Server 2003 installation from the Windows console</a>
<u>Embedded</u> ESXi5 ESXi4	<a href="#">Continuing the VMware ESXi Embedded installation from the ESX console</a>
<u>Non-embedded</u> ESXi5	<a href="#">Continuing the VMware ESX 5 installation from the ESX console</a>
<u>Non-embedded</u> ESXi4 ESX4	<a href="#">Continuing the VMware ESX 4 installation from the ESX console</a>
ESX3.5	<a href="#">Continuing the VMware ESX 3.5 installation from the ESX console</a>

## 2 iSCSI solution support matrices

### 2.1 iSCSI solution capabilities

The IBM i iSCSI solution provides the capabilities shown in the tables in the following sections.

#### Section Table of Contents

2.1.1	Integrated Server Operating System (Server OS) Versions.....	20
2.1.1.1	Microsoft service packs.....	21
2.1.2	Server Installation Capabilities .....	22
2.1.3	Configuration and Management Capabilities .....	22
2.1.4	Server Discovery and Power Control Capabilities.....	23
2.1.5	Virtual Storage Capabilities .....	24
2.1.6	Backup and Recovery Capabilities.....	25
2.1.7	iSCSI Network Capabilities .....	26
2.1.8	Virtual Ethernet Capabilities .....	27
2.1.9	Server OS Integration Capabilities .....	27
2.1.10	User Enrollment Capabilities .....	28
2.1.11	Miscellaneous Capabilities .....	28

**Note:** Some capabilities vary based on one or more of the following criteria:

- The IBM i version.
- The integrated server operating system type or version.
- The specific integrated server hardware that is used.

## 2.1.1 Integrated Server Operating System (Server OS) Versions

OS Type Notation	OS Version Notation	Server OS Versions	IBM i			
			i7.2	i7.1	i6.1	i5.4
Windows	WIN2012	Any of the following 64-bit x64 Microsoft® Windows Server 2012 versions (full and core installations): <ul style="list-style-type: none"> <li>Windows Server 2012 Foundation</li> <li>Windows Server 2012 Essentials</li> <li>Windows Server 2012 Standard</li> </ul>	✓	✓		
	WIN2008	Any of the following 64-bit x64 Microsoft® Windows Server 2008 versions (full and core installations): <ul style="list-style-type: none"> <li>Windows Server 2008 R2 Standard</li> <li>Windows Server 2008 R2 Enterprise</li> <li>Windows Web Server 2008 R2</li> <li>Windows Server 2008 Standard</li> <li>Windows Server 2008 Enterprise</li> <li>Windows Server 2008 Standard without Hyper-V</li> <li>Windows Server 2008 Enterprise without Hyper-V</li> <li>Windows Web Server 2008</li> </ul>	✓	✓	✓	
	WIN2003 <sup>1</sup>	Any of the following 32-bit x86 Microsoft Windows Server 2003 versions: <ul style="list-style-type: none"> <li>Windows Server 2003 R2 Standard</li> <li>Windows Server 2003 R2 Enterprise</li> <li>Windows Server 2003 Standard <b>plus</b> Service Pack 1 (SP1) or later</li> <li>Windows Server 2003 Enterprise <b>plus</b> Service Pack 1 (SP1) or later</li> <li>Windows Server 2003 Web <b>plus</b> Service Pack 1 (SP1) or later</li> </ul>	✓	✓	✓	✓
ESX	ESXi5	Any of the following VMware ESXi 5 versions: <ul style="list-style-type: none"> <li>VMware ESXi Installable 5.1</li> <li>VMware ESXi Embedded 5.1</li> <li>VMware ESXi Installable 5.0</li> <li>VMware ESXi Embedded 5.0</li> </ul>	✓	✓	✓	
	ESXi4	Any of the following VMware ESXi 4 versions: <ul style="list-style-type: none"> <li>VMware ESXi Installable 4.1</li> <li>VMware ESXi Embedded 4.1</li> <li>VMware ESXi Embedded 4.0</li> </ul>	✓	✓	✓	
	ESX4	VMware ESX 4.0	✓	✓	✓	
	ESX3.5	VMware ESX 3.5			✓	✓

**Notes:**

<sup>1</sup> WIN2003 is NOT supported except as is.

### 2.1.1.1 Microsoft service packs

IBM tests Windows operating system service packs on integrated servers shortly after they are released by Microsoft.

**Note:** When a new service pack for the operating system is released by Microsoft, the prior operating system service pack will continue to be supported for use with integrated servers for a minimum of 6 months. After that time, IBM might withdraw support for the prior operating system service pack on integrated servers.

The specific operating system service packs that are currently supported for each Windows version are listed below.

Server OS	Service Packs
WIN2012	No service packs are currently available for Windows Server 2012.
WIN2008 R2	<b>SP1:</b> IBM supports Microsoft Windows Server 2008 <b>R2</b> Service pack 1 (SP1) on iSCSI-attached BladeCenter and System x models.
WIN2008	<b>SP2:</b> IBM supports Microsoft Windows Server 2008 Service pack 2 (SP2) on iSCSI-attached BladeCenter and System x models.
WIN2003	<b>SP2:</b> IBM is supporting Microsoft Windows Server 2003 Service pack 2 (SP2) on iSCSI-attached BladeCenter and System x models.  <b>Note:</b> Since SP2 includes the SP1 security changes, additional configuration is required to enable SP2 on integrated Windows servers. See <a href="#">Windows Server 2003 Service Pack 1</a> for details.
	<b>SP1:</b> IBM is supporting Microsoft Windows Server 2003 Service pack 1 (SP1) on iSCSI-attached BladeCenter and System x models.  <b>Note:</b> Additional configuration is required to enable SP1 on integrated Windows servers. See <a href="#">Windows Server 2003 Service Pack 1</a> for details.

## 2.1.2 Server Installation Capabilities

Capability	Server OS	IBM i				More Information
		i7.2	i7.1	i6.1	i5.4	
Server installation road map	All	✓	✓	✓	✓	<a href="#">Integrated server installation</a> <a href="#">Server installation road map and checklist</a>
iSCSI solution planning work sheets	All	✓	✓	✓	✓	<a href="#">IBM i iSCSI Solution Work Sheets</a> <a href="#">Server installation road map and checklist</a>
Create Server Wizard	Windows	✓	✓	✓		<a href="#">Start the installation from IBM i</a>
	ESX	✓	✓	✓		
IBM i integrated server installation CL commands	All	✓	✓	✓	✓	<a href="#">Start the installation from IBM i</a>
Server cloning road map	Windows	✓	✓	✓		<a href="#">Integrated server cloning</a> <a href="#">Server cloning road map and checklist</a>
Server Cloning Wizard	Windows	✓	✓	✓		<a href="#">Run the IBM i integrated server cloning Wizard</a>

## 2.1.3 Configuration and Management Capabilities

Capability	Server OS	IBM i				More Information
		i7.2	i7.1	i6.1	i5.4	
IBM i management interfaces	All	✓	✓	✓	✓	<a href="#">IBM i management interfaces</a>
IBM Navigator for i Web GUI	All	✓	✓	✓		<a href="#">IBM i management interfaces</a>
System i Navigator client GUI	All	✓	✓	✓	✓	<a href="#">IBM i management interfaces</a> <b>Attention:</b> System i Navigator does <b>not</b> provide full support on i 7.2, 7.1 and 6.1, so use the <a href="#">Web GUI</a> with i 7.2, 7.1 and 6.1.
IBM i control language (CL) commands	All	✓	✓	✓	✓	<a href="#">IBM i management interfaces</a>
Windows management infrastructure	Windows	✓	✓	✓	✓	<a href="#">Integrated Windows server management infrastructure</a>
VMware ESX management using <b>management server</b> based infrastructure	ESXi5 ESXi4 ESX4	✓	✓	✓	N/A	<a href="#">Integrated VMware ESX server management infrastructure</a>
VMware ESX management using <b>service console</b> based infrastructure	ESX4			✓	N/A	<a href="#">Integrated VMware ESX server management infrastructure</a>
	ESX3.5	N/A	N/A	✓	✓	
Integrated server console	All	✓	✓	✓	✓	<a href="#">Integrated server console</a>
Updates to integration software	All	✓	✓	✓	✓	<a href="#">Software updates</a>
System x or BladeCenter service processor Web interface	All	✓	✓	✓	✓	<a href="#">Additional management interfaces</a>
Launch System x or BladeCenter service processor Web interface from IBM i Web GUI	All	✓	✓	✓		<a href="#">Additional management interfaces</a>

## 2.1.4 Server Discovery and Power Control Capabilities

Capability	Server OS	IBM i				More Information
		i 7.2	i 7.1	i 6.1	i 5.4	
Start the integrated server from IBM i	All	✓	✓	✓	✓	<a href="#">IBM i configuration objects for integrated servers</a>
Shut down the integrated server from IBM i	All	✓	✓	✓	✓	<a href="#">IBM i configuration objects for integrated servers</a>
Discovery and power control using Service Processor Manager	All	✓	✓	✓	✓	<a href="#">Integrated server service processor connection</a>
Discovery and power control using IBM Director Server running on IBM i	All	N/A	N/A	✓	✓	<a href="#">Integrated server service processor connection</a>

## 2.1.5 Virtual Storage Capabilities

Capability	Server OS	IBM i				More Information	
		i 7.2	i 7.1	i 6.1	i 5.4		
IBM i virtual storage	All	✓	✓	✓	✓	<a href="#">IBM i storage management</a>	
IBM i storage pools (ASPs)	All	✓	✓	✓	✓	<a href="#">Storage pools (ASPs)</a>	
IBM i disk data protection	All	✓	✓	✓	✓	<a href="#">Disk protection</a>	
IBM i virtual storage I/O capacity	All	✓	✓	✓	✓	<a href="#">Virtual storage performance</a> <i>Integrated BladeCenter and System x Performance</i> chapter of the <a href="#">IBM i Performance Capabilities Reference</a>	
"System" drive storage space	Windows	✓	✓	✓	✓	<a href="#">Predefined virtual storage and naming</a>	
	Non-embedded	ESXi5	✓	✓	✓		N/A
		ESXi4 ESX4	✓	✓	✓		N/A
	ESX3.5	N/A	N/A	✓	✓		
Embedded	ESXi5			✓	N/A		
	ESXi4						
"Install" drive storage space	Windows	✓	✓	✓	✓	<a href="#">Predefined virtual storage and naming</a>	
	ESXi5 ESXi4 ESX4			✓	N/A		
	ESX3.5	N/A	N/A	✓	✓		
Create user-defined storage spaces	Windows	62	62	62	62	<a href="#">Create user-defined virtual storage</a> <b>Note:</b> The number shown is the maximum number of user-defined storage spaces that can be linked to a server.	
	Embedded ESX	64	64	62	N/A		
	All other ESX	63	63	62	62		
Copy virtual storage	All	✓	✓	✓	✓	<a href="#">Copy virtual storage</a>	
Extend the size of virtual storage	All	✓	✓	✓	✓	<a href="#">Extend the size of virtual storage</a>	
Dynamic virtual storage linking	All	✓	✓	✓	✓	<a href="#">Dynamic virtual storage linking while server is active</a>	
Dynamic virtual storage unlinking	Windows	✓	✓	✓	✓	<a href="#">Dynamic virtual storage unlinking while server is active</a>	
Shared access to virtual storage	ESX	✓	✓	✓		<a href="#">Virtual storage linking</a>	
iSCSI I/O shared data memory pool	All	✓	✓	✓	N/A	<a href="#">iSCSI virtual storage I/O memory pool</a>	
iSCSI I/O private memory pool	All	N/A	N/A	N/A	✓	<a href="#">iSCSI virtual storage I/O memory pool</a>	
Virtual storage with 4K sector	All	✓				<a href="#">Create user-defined virtual storage</a>	
Allocate virtual storage on Solid State disk units	All	✓				<a href="#">Create user-defined virtual storage</a>	



## 2.1.6 Backup and Recovery Capabilities

Capability	Server OS	IBM i				More Information
		i 7.2	i 7.1	i 6.1	i 5.4	
Backup your entire IBM i system	All	✓	✓	✓	✓	<a href="#">Backup and recovery concepts</a>
Recover your entire IBM i system	All	✓	✓	✓	✓	<a href="#">Backup and recovery concepts</a>
Backup IBM i configuration objects	All	✓	✓	✓	✓	<a href="#">Backup and recovery concepts</a>
Restore IBM i configuration objects	All	✓	✓	✓	✓	<a href="#">Backup and recovery concepts</a>
Backup virtual storage from IBM i	While server is <u>shut down</u>	All	✓	✓	✓	<a href="#">Backup and recovery concepts</a>
	While server is <u>active</u> (storage space snapshot save while active – SWA)	Windows	✓	✓	✓	
		ESX	✓	✓		
Restore virtual storage from IBM i	All	✓	✓	✓	✓	<a href="#">Backup and recovery concepts</a>
File level backup and recovery	From IBM i	Windows	✓	✓	✓	<a href="#">Backup and recovery concepts</a>
	From Windows, using an IBM i tape device	Windows	✓	✓	✓	
	From integrated server, using native utilities	All	✓	✓	✓	
Shared IBM i tape and optical devices	Windows	✓	✓	✓	✓	<a href="#">IBM i tape and optical devices shared with integrated Windows servers</a>
Lock and unlock tape and optical devices from the integrated server OS	Windows	✓	✓	✓	✓	<a href="#">IBM i tape and optical devices shared with integrated Windows servers</a>

### Related information:

- [What objects to save and their location on IBM i](#)
- [IBM i tape devices for Windows Server 2008/2012](#)
- [IBM i tape devices for Windows Server 2003](#)

## 2.1.7 iSCSI Network Capabilities

Capability	Server OS	IBM i					More Information
		i7.2	i7.1	i6.1.1	i6.1	i5.4	
iSCSI hardware target (HWT)	All	✓	✓	✓	✓	✓	<a href="#">Attaching servers to IBM i using iSCSI iSCSI network</a>
iSCSI software target (SWT)	All	✓	✓	✓			<a href="#">Attaching servers to IBM i using iSCSI iSCSI network</a>
iSCSI hardware initiator (HWI)	WIN2012	✓	✓	N/A	N/A	N/A	<a href="#">Attaching servers to IBM i using iSCSI iSCSI network</a>
	WIN2008	✓	✓	✓	✓	N/A	
	WIN2003	✓	✓	✓	✓	✓	<a href="#">iSCSI network</a>
	ESXi4 ESX4	✓	✓	✓	✓	N/A	<a href="#">Blade server models</a> <a href="#">System x server models</a>
	ESX3.5	N/A	N/A	✓	✓	✓	<a href="#">System x server models</a>
iSCSI software initiator (SWI)	WIN2012	✓	✓	N/A	N/A	N/A	<a href="#">Attaching servers to IBM i using iSCSI iSCSI network</a>
	WIN2008	✓	✓	✓	✓	N/A	
	ESXi5 ESXi4	✓	✓	✓	✓	N/A	<a href="#">Blade server models</a> <a href="#">System x server models</a>
Connect with a switch from iSCSI initiator to IBM i iSCSI target	All	✓	✓	✓	✓	✓	<a href="#">Typical iSCSI-attached server installation</a> <a href="#">Ethernet switches for the iSCSI solution</a>
Direct connect (no switch) from iSCSI initiator to IBM i iSCSI target	IBM i iSCSI <b>hardware</b> target	All	✓	✓	✓	✓	<a href="#">Typical iSCSI-attached server installation</a>
	IBM i iSCSI <b>software</b> target	All	✓	✓			<a href="#">IBM i iSCSI targets</a>
iSCSI multipath I/O (MPIO)	Windows	✓	✓	✓	✓	✓	<a href="#">Multipath I/O (MPIO)</a>
	ESX	✓	✓	✓	✓	✓	
Maximum number of iSCSI initiator ports for MPIO	Windows	4	4	4	4	4	<b>Note:</b> Also limited by the number of initiator ports that are available for the particular server model.
	ESXi5 ESXi4 ESX4	4	4	4	4	N/A	
	ESX3.5	N/A	N/A	2	2	2	
Mixed iSCSI initiator types allowed for MPIO	Windows	✓	✓	✓	✓	✓	<b>Not</b> supported with ESX3.5.
	ESX	✓	✓	✓	✓	✓	
MPIO boot	Windows	✓	✓	✓	✓	✓	Multiple iSCSI initiator ports are configured as a boot device so that the boot process can proceed in case of an initiator port hardware failure.
	ESX						
DHCP boot mode	All	✓	✓	✓	✓	✓	<a href="#">Booting over the iSCSI network</a>
Manual boot mode	All	✓	✓	✓	✓	✓	<a href="#">Booting over the iSCSI network</a>
Target CHAP	All	✓	✓	✓	✓	✓	<a href="#">Network security</a>
Initiator (mutual) CHAP	All	✓	✓	✓	✓	✓	<a href="#">Network security</a>
View iSCSI initiator allocation	Windows	✓	✓	✓	✓	✓	<a href="#">View iSCSI initiator allocation (qvnimap.exe)</a>

## 2.1.8 Virtual Ethernet Capabilities

Capability	Server OS	IBM i				More Information
		i 7.2	i 7.1	i 6.1	i 5.4	
Virtual Ethernet connections provided through IBM i	Windows	✓	✓	✓	✓	<a href="#">Virtual Ethernet networks for integrated Windows servers</a>
Display information about virtual Ethernet adapters	Windows	✓	✓	✓	✓	<a href="#">Display virtual Ethernet information (qvndvimr.exe)</a>

## 2.1.9 Server OS Integration Capabilities

Capability	Server OS	IBM i				More Information
		i 7.2	i 7.1	i 6.1	i 5.4	
CPU statistics retrieval	Windows	✓	✓	✓	✓	<a href="#">Windows services for IBM i integration with Windows servers</a>
Disk statistics retrieval	Windows	✓	✓	✓	✓	<a href="#">Windows services for IBM i integration with Windows servers</a>
OS name and version retrieval	Windows	✓	✓	✓	✓	<a href="#">Windows services for IBM i integration with Windows servers</a>
	ESX	✓	✓	✓		
Submit remote commands from IBM i to Windows	Windows	✓	✓	✓	✓	<a href="#">Windows services for IBM i integration with Windows servers</a>
Propagate Windows event logs to IBM i	Windows	✓	✓	✓	✓	<a href="#">Windows services for IBM i integration with Windows servers</a>
Windows application access to DB2 for IBM i database	Windows	✓	✓	✓	✓	<a href="#">IBM i Access for Windows and integrated servers</a>
VMware VMotion, VMware HA, and VMware DRS	ESX	✓	✓	✓		<a href="#">Virtual storage linking</a>

## 2.1.10 User Enrollment Capabilities

Capability	Server OS	IBM i				More Information
		i7.2	i7.1	i6.1	i5.4	
Enroll IBM i users to Windows servers	Windows	✓	✓	✓	✓	<a href="#">User and group enrollment concepts for integrated Windows servers</a>
Enroll IBM i users to Windows domains	Windows	✓	✓	✓	✓	<a href="#">User and group enrollment concepts for integrated Windows servers</a>
Enroll IBM i groups to Windows servers	Windows	✓	✓	✓	✓	<a href="#">User and group enrollment concepts for integrated Windows servers</a>
Enroll IBM i groups to Windows domains	Windows	✓	✓	✓	✓	<a href="#">User and group enrollment concepts for integrated Windows servers</a>
Template user	Windows	✓	✓	✓	✓	<a href="#">User enrollment templates for integrated Windows servers</a>
Option to control which NWSDs are used to propagate domain users	Windows	✓	✓	✓	✓	<a href="#">User and group enrollment concepts for integrated Windows servers</a>
Support IBM i Enterprise Identity Mapping (EIM)	Windows	✓	✓	✓	✓	<a href="#">User and group enrollment concepts for integrated Windows servers</a>
Option to <u>not</u> disable Windows user profile when IBM i profile is disabled	Windows	✓	✓	✓		<a href="#">User and group enrollment concepts for integrated Windows servers</a>

## 2.1.11 Miscellaneous Capabilities

Capability	Server OS	IBM i				More Information
		i7.2	i7.1	i6.1	i5.4	
Hot spare integrated server hardware	All	✓	✓	✓	✓	<a href="#">Hot spare support for integrated servers</a>
Hot spare iSCSI target adapter hardware	All	✓	✓	✓	✓	<a href="#">Hot spare support for integrated servers</a>
High Availability via an IBM i cluster	All	✓	✓	✓		<a href="#">IBM i clustering for integrated servers</a>

## 2.2 Ordering channels

The IBM i iSCSI solution integrates components that are obtained from several channels:

Channel	Item	Additional Information
Power Systems channel	Power server	<a href="#">Power Server IBM i iSCSI target support</a>
	iSCSI target adapter	<a href="#">IBM i iSCSI targets</a>
	IBM i products and options	<a href="#">IBM i products and options</a>
	IBM i disk capacity	Plan IBM i virtual storage capacity for integrated Windows or VMware ESX servers as you would for stand-alone servers.
BladeCenter channel	BladeCenter hardware	<a href="#">BladeCenter chassis models</a> <a href="#">Blade server models</a>
	iSCSI initiator adapter	<a href="#">Blade iSCSI initiators</a>
	Keyboard/Mouse	
	Display	
	Additional processors	Optional
	Additional memory	Optional
System x channel	System x hardware	<a href="#">System x server models</a>
	iSCSI initiator adapter	<a href="#">System x iSCSI initiators</a>
	Keyboard/Mouse	
	Display	
	Additional processors	Optional
	Additional memory	Optional
Microsoft channel	Windows Server OS	See OS versions supported with your server model: <ul style="list-style-type: none"> <li><a href="#">Blade server models</a></li> <li><a href="#">System x server models</a></li> </ul>
VMware channel	VMware ESX Server OS	See OS versions supported with your server model: <ul style="list-style-type: none"> <li><a href="#">Blade server models</a></li> <li><a href="#">System x server models</a></li> </ul>
	VMware vSphere 5	Advanced or Enterprise editions (for use with ESXi 5 servers)
	VMware vSphere 4	Advanced or Enterprise editions (for use with ESXi 4 and ESX 4 servers)
	Virtual Infrastructure 3	Standard or Enterprise editions (for use with ESX 3 servers)
OEM channels	Ethernet switch	<a href="#">Ethernet switches for the iSCSI solution</a>
	Ethernet cables	Copper or fiber, as required by your iSCSI network
	Server applications	Contact your application provider

## 2.3 IBM i products and options

IBM i Product Description	IBM i				Product <sup>1</sup> or Option	Server OS	
	i 7.2	i 7.1	i 6.1	i 5.4		Windows	ESX
IBM i (i5/OS)	✓	✓	✓	✓	57xx-SS1	✓	✓
Extended Base Support	✓	✓	✓	✓	57xx-SS1 option 1	✓	✓
Online Information	✓	✓	✓	✓	57xx-SS1 option 2	✓	✓
Extended Base Directory Support (Includes IBM Navigator for i <a href="#">Web GUI</a> )	✓	✓	✓		57xx-SS1 option 3	✓	✓
Host Servers	✓	✓	✓	✓	57xx-SS1 option 12	✓	✓
Integrated Server Support <sup>2</sup>	✓	✓	✓	✓	57xx-SS1 option 29	✓	✓
Digital Certificate Manager	✓	✓	✓	✓	57xx-SS1 option 34	✓	✓
IBM HTTP Server for i <sup>3</sup>	✓	✓	✓	✓	57xx-DG1	✓	✓
IBM TCP/IP Connectivity Utilities for i <sup>3</sup>	✓	✓	✓	✓	57xx-TC1	✓	✓
IBM Developer Kit for Java <sup>3</sup>	✓	✓	✓		5761-JV1	✓	✓
				✓	5722-JV1		
Java Developer Kit 1.4 <sup>3</sup>	✓	✓	✓		5761-JV1 option 6	✓	✓
				✓	5722-JV1 option 6		
Java SE 6 32 bit (required by the <a href="#">Web GUI</a> )	✓	✓	✓		5761-JV1 option 11	✓	✓
IBM Extended Integrated Server Support for i5/OS <sup>3</sup>			✓		5761-LSV		✓
IBM i5/OS Integration for Linux® on xSeries <sup>3</sup>				✓	5722-LSV		✓
IBM System i Access for Windows (Includes <a href="#">System i Navigator</a> client GUI)	✓ <sup>4</sup>	✓ <sup>4</sup>	✓ <sup>4</sup>	✓	57xx-XE1	✓	✓

**Notes:**

<sup>1</sup> The specific **57xx** product IDs for each IBM i release are: **5770** for **i 7.2** and **i 7.1**, **5761** for **i 6.1**, and **5722** for **i 5.4**.

<sup>2</sup> The **Service Processor Manager** function of **Integrated Server Support** eliminates the requirement for the **IBM Director** (5722-DR1) and **Qshell** (57xx-SS1 option 30) products, which were originally required products for **i 6.1** and **i 5.4**. See [Configuring IBM i to use Service Processor Manager on i 6.1 and i 5.4](#).

<sup>3</sup> No charge licensed program product (LPP).

<sup>4</sup> [System i Navigator](#) is optional for i 7.2, i 7.1 and i 6.1. Note that some Integrated Server Administration GUI tasks and functions are available in the IBM Navigator for i [Web GUI](#), but are **not** in the System i Navigator client GUI.

## 2.4 BladeCenter chassis models

Chassis	Type	Number of Blades	Management Module <sup>1</sup>	Notes
<a href="#">BladeCenter S</a> (BC-S)	8886	1-6	AMM	2
<a href="#">BladeCenter E</a> (BC-E)	8677	1-14	AMM or MM	
<a href="#">BladeCenter H</a> (BC-H)	8852	1-14	AMM	3

**Notes:**

<sup>1</sup> There are two versions of the Management Module:  
**MM** Management Module  
**AMM** Advanced Management Module

<sup>2</sup> Blades that are integrated with an IBM i system via iSCSI do not use any of the disk drives that are installed in the BladeCenter S chassis. However, the BladeCenter S chassis disk drives can be used with blades that are not integrated with IBM i.

<sup>3</sup> This BladeCenter model has some special ordering considerations. See IBM Software Technical Document **453371664** titled [Ordering Blade Center Hardware for iSCSI Integrated Servers](#).

**Related information:**

➤ [Blade server models](#)

➤ [IBM System x Configuration and Options Guide](#)

## 2.5 Blade server models

Blade Server	Type	Number of Processors	Notes	Chassis	Initiator Type	Blade iSCSI initiators Option P/N <sup>1,6</sup>	Server OS <sup>2,6</sup>							
							WIN2012	WIN2008	WIN2003	ESXi5	ESXi4	ESX4	ESX3.5	
<a href="#">HS23</a>	7875	1-2	3	BC-S	SWI	LOM <sup>5</sup>	✓	✓		✓	✓			
					SWI	44W4475	✓	✓		✓	✓			
					SWI	44W4479	✓	✓						
				BC-H	SWI	46M6164	✓	✓		✓	✓			
					SWI	46M6168	✓	✓		✓	✓			
<a href="#">HX5</a>	7872	1-2	3	BC-S	SWI	LOM <sup>5</sup>		✓		✓	✓			
					SWI	44W4475		✓		✓	✓			
					SWI	44W4479		✓						
				BC-H	SWI	46M6164		✓		✓	✓			
					SWI	46M6168		✓		✓	✓			
					SWI	49Y4235		✓		✓	✓			
	7873	1-2	3		BC-S	SWI	LOM <sup>5</sup>	✓	✓		✓	✓		
					BC-E	SWI	44W4475	✓	✓		✓	✓		
					BC-H	SWI	44W4479	✓	✓					
<a href="#">HS22V</a>	7871	1-2	3	BC-S	SWI	LOM <sup>5</sup>	✓	✓		✓	✓			
					SWI	44W4475	✓	✓		✓	✓			
					SWI	44W4479	✓	✓						
				BC-H	SWI	46M6164	✓	✓		✓	✓			
					SWI	46M6168	✓	✓		✓	✓			
					SWI	49Y4235		✓		✓	✓			
					SWI	90Y3566		✓		✓	✓			
					SWI	44W4465		✓		✓	✓			
<a href="#">HS22</a>	7870	1-2	3	BC-S	SWI	LOM <sup>5</sup>	✓	✓		✓	✓			
					SWI	44W4475	✓	✓		✓	✓			
					SWI	44W4479	✓	✓		✓	✓			
				BC-H	SWI	46M6164	✓	✓		✓	✓			
					SWI	46M6168	✓	✓		✓	✓			
					SWI	49Y4235		✓		✓	✓			
					SWI	90Y3566		✓		✓	✓			
					SWI	44W4465		✓		✓	✓			
<b>The following server models have been withdrawn from Marketing:</b>														
<a href="#">HS12</a>	8028	1	3	BC-S	SWI	LOM <sup>5</sup>		✓						
					BC-E	SWI	44W4479		✓					
					BC-H		44W4465		✓					
<a href="#">HS21 XM</a>	7995	1-2	3	BC-S	HWI	32R1923		✓	✓				✓	
					BC-E	SWI	LOM <sup>5</sup>		✓					
					BC-H	SWI	44W4479		✓					
				BC-H	SWI	46M6164		✓						
					SWI	46M6168		✓						
<a href="#">HS21</a>	8853	1-2	3	BC-S	HWI	32R1923		✓	✓				✓	
					BC-E	SWI	LOM <sup>5</sup>		✓					
					BC-H	SWI	44W4479		✓					



Blade Server	Type	Number of Processors	Notes	Chassis	Initiator Type	Blade iSCSI initiators Option P/N <sup>1,6</sup>	Server OS <sup>2,6</sup>						
							WIN2012	WIN2008	WIN2003	ESXi5	ESXi4	ESX4	ESX3.5
				BC-H	SWI	46M6164		✓					
					SWI	46M6168		✓					
<a href="#">HS20</a>	8843	1-2	3	BC-S BC-E BC-H	HWI	32R1923			✓				✓
<a href="#">HS20</a>	7981	1-2	3	BC-S BC-E BC-H	HWI	32R1923			✓				
<a href="#">LS42</a>	7902	2-4	3	BC-S	HWI	32R1923 <sup>4</sup>		✓	✓				✓
				BC-E	SWI	LOM <sup>5</sup>		✓					
				BC-H	SWI	44W4479		✓					
				BC-H	SWI	46M6164		✓					
					SWI	46M6168		✓					
<a href="#">LS22</a>	7901	1-2	3	BC-S	HWI	32R1923		✓	✓				✓
				BC-E	SWI	LOM <sup>5</sup>		✓					
				BC-H	SWI	44W4479		✓					
					SWI	46M6164		✓					
					SWI	46M6168		✓					
<a href="#">LS41</a>	7972	2-4	3	BC-S	HWI	32R1923 <sup>4</sup>		✓	✓				
				BC-E	SWI	LOM <sup>5</sup>		✓					
				BC-H	SWI	44W4479		✓					
					SWI	46M6164		✓					
					SWI	46M6168		✓					
<a href="#">LS21</a>	7971	1-2	3	BC-S	HWI	32R1923		✓	✓				
				BC-E	SWI	LOM <sup>5</sup>		✓					
				BC-H	SWI	44W4479		✓					
					SWI	46M6164		✓					
					SWI	46M6168		✓					
<a href="#">LS20</a>	8850	1-2	3	BC-S BC-E BC-H	HWI	32R1923			✓				

**Notes:**

<sup>1</sup> The part number (P/N) shown for each adapter is the adapter option P/N. An adapter might also have an associated field replaceable unit (FRU) P/N and an adapter card assembly P/N (part number for the card itself). Make sure that you are using the adapter option P/N when looking up the iSCSI initiator in this table.

<sup>2</sup> Server operating system (OS) support also varies based on the IBM i version that is used.

IBM i	Server OS						
	WIN2012	WIN2008	WIN2003	ESXi5	ESXi4	ESX4	ESX3.5
i 7.2	✓	✓		✓	✓	✓	
i 7.1	✓	✓	✓	✓	✓	✓	
i 6.1		✓	✓	✓	✓	✓	✓
i 5.4			✓				✓

Refer to the Server OS notation on page [20](#) for the specific list of OS versions that correspond to the abbreviations shown in this table.

<sup>3</sup> With the IBM i iSCSI solution, all of the disk drives for the BladeCenter blade or System x model are provided as virtual storage by IBM i. When ordering BladeCenter blade or System x servers, do not order internal or external BladeCenter blade or System x controlled disk or disk controller adapters. Any disk drives and disk controller adapters that might be installed in the BladeCenter blade or System x server must be removed before the server installation process is started.

<sup>4</sup> There is room for two 32R1923 iSCSI HBAs in this blade, but only one is allowed when attaching to IBM i.

<sup>5</sup> **LOM** = LAN on Motherboard, which is also called embedded Ethernet or integrated Ethernet.

<sup>6</sup> Changes are made periodically to the IBM website, please refer to the [IBM Server Proven website](#) for tested combinations for Blade Servers.

**Related information:**

- [Blade iSCSI initiators](#)
- [BladeCenter chassis models](#)
- [IBM System x Configuration and Options Guide](#)
- [iSCSI supported limits](#)

## 2.5.1 Blade iSCSI initiators

Blade iSCSI initiators	Type	Feature Code	Option Part Number (P/N) <sup>1</sup>	Adapter Type	Ethernet Ports <sup>2</sup>	IBM i
LAN on Motherboard (LOM) <sup>4</sup>	SWI	N/A	LOM	N/A	2 ports (1 Gbps)	i 7.2 i 7.1 i 6.1
Broadcom Ethernet Expansion Card (CIOv)	SWI	5477 or 1039	44W4475	PCIe Ethernet NIC	2 ports (1 Gbps)	i 7.2 i 7.1 i 6.1
Broadcom 2/4 Port Ethernet Expansion Card (CFFh)	SWI	5476	44W4479	PCIe Ethernet NIC	2 ports (1 Gbps)	i 7.2 i 7.1 i 6.1
Broadcom 10Gb Gen2 4-port Ethernet Exp Cd (CFFh)	SWI	0098	46M6164	PCIe Ethernet NIC	4 ports (10 Gbps)	i 7.2 i 7.1 i 6.1
Broadcom 10Gb Gen2 2-port Ethernet Exp Cd (CFFh)	SWI	0099	46M6168	PCIe Ethernet NIC	2 ports (10 Gbps)	i 7.2 i 7.1 i 6.1
Emulex 10GbE Virtual Fabric Adapter (CFFh)	SWI	5755	49Y4235	PCIe Ethernet NIC	2 ports (10 Gbps)	i 7.2 i 7.1 i 6.1
Emulex 10GbE Virtual Fabric Adapter Advanced II (CFFh)	SWI	A1XH	90Y3566	PCIe Ethernet NIC	2 ports (10 Gbps)	i 7.2 i 7.1 i 6.1
<b>The following iSCSI initiators have been withdrawn from Marketing:</b>						
Broadcom 10Gb 4-port Ethernet Exp Card (CFFh)	SWI	5479	44W4465	PCIe Ethernet NIC	4 ports (10 Gbps)	i 7.1 i 6.1
QLogic iSCSI Expansion Card	HWI	1458	32R1923 <sup>3</sup>	PCI-X iSCSI HBA	2 ports (1 Gbps)	All
<p><b>Notes:</b></p> <p><sup>1</sup> The part number (P/N) shown for each adapter is the adapter <u>option</u> P/N. An adapter might also have an associated field replaceable unit (FRU) P/N and an adapter card assembly P/N (part number for the card itself). Make sure that you are using the adapter <u>option</u> P/N when looking up the iSCSI initiator in this table.</p> <p><sup>2</sup> Supports copper or fiber ports, depending on the BladeCenter I/O modules that are used. In order to use multiple ports for storage I/O, the associated I/O module bays must contain BladeCenter I/O modules and at least 2 IBM i iSCSI targets are required.</p> <p><sup>3</sup> Customers ordering part number <b>32R1923</b> should receive a card that shows part number <b>32R1925</b> on the adapter card sticker label. Only adapters with part number <b>32R1925</b> on the adapter sticker label are supported with this solution.</p> <p><b>Attention:</b> Adapters with part number <b>26K6489</b> on the adapter sticker label are not supported and will not work. They should be returned and replaced with adapters that have part number <b>32R1925</b> on the adapter sticker label.</p> <p><b>Note:</b> Adapters with part number <b>32R1925</b> on the adapter sticker label are supported, but may have a Vital Product Data (VPD) part number of either <b>32R1925</b> or <b>26K6489</b>. Both are valid VPD part numbers. The VPD can be viewed from the Management Module web interface. To identify a supported <b>32R1925</b> labeled adapter with the <b>26K6489</b> VPD, verify that the Manufacture Date (Manuf. Date) is 0806 or newer. Adapters with a VPD of <b>26K6489</b> with manufacturing dates of 0706 or earlier are not supported.</p> <p><sup>4</sup> Refer to the specific server model specifications for the LAN on Motherboard (LOM) port characteristics, such as number of ports, port speed, and port technology provider (for example, Intel or Broadcom). Note that LAN on Motherboard is also called embedded Ethernet or integrated Ethernet.</p>						

### Related information:

**Related information:**

➤ [Blade server models](#)

➤ [iSCSI supported limits](#)

## 2.6 System x server models

System x Server	Type	Number of Processors	Service Processor <sup>4</sup>	Notes	Initiator Type	System x iSCSI initiators Option P/N <sup>1,6</sup>	Server OS <sup>2,6</sup>						
							WIN2012	WIN2008	WIN2003	ESXi5	ESXi4	ESX4	ESX3.5
<a href="#">x3500 M4</a>	7383	1-2	IMM II	3	SWI	LOM <sup>5</sup>	✓	✓		✓	✓		
					SWI	49Y4220	✓	✓		✓	✓		
					SWI	42C1780	✓	✓		✓	✓		
<a href="#">x3550 M4</a>	7914	1-2	IMM II	3	SWI	LOM <sup>5</sup>	✓	✓		✓	✓		
					SWI	49Y4220	✓	✓		✓	✓		
					SWI	42C1780	✓	✓		✓	✓		
<a href="#">x3650 M4</a>	7915	1-2	IMM II	3	SWI	LOM <sup>5</sup>	✓	✓		✓	✓		
					SWI	49Y4220	✓	✓		✓	✓		
					SWI	42C1780	✓	✓		✓	✓		
	5460 <sup>7</sup>	1-2	IMM II	3	SWI	LOM <sup>5</sup>	✓	✓		✓			
					SWI	49Y4220	✓	✓		✓			
<a href="#">x3750 M4</a>	8722	1-4	IMM II	3	SWI	LOM <sup>5</sup>	✓	✓		✓	✓		
	8752	1-4	IMM II	3	SWI	90Y4600	✓	✓		✓	✓		
<a href="#">x3690 X5</a>	7148	1-4	IMM	3	SWI	LOM <sup>5</sup>		✓		✓	✓		
					SWI	49Y4220		✓		✓	✓		
					SWI	42C1780		✓		✓	✓		
<b>The following server models have been withdrawn from Marketing:</b>													
<a href="#">x3550 M3</a>	7944	1-2	IMM	3	HWI	39Y6146	✓	✓	✓		✓	✓	
					HWI	42C1770	✓	✓	✓		✓	✓	
					SWI	LOM <sup>5</sup>	✓	✓		✓	✓		
					SWI	49Y4220	✓	✓		✓	✓		
					SWI	42C1780	✓	✓		✓	✓		
<a href="#">x3650 M3</a>	7945	1-2	IMM	3	HWI	39Y6146	✓	✓	✓		✓	✓	
					HWI	42C1770	✓	✓	✓		✓	✓	
					SWI	LOM <sup>5</sup>	✓	✓		✓	✓		
					SWI	49Y4220	✓	✓		✓	✓		
					SWI	42C1780	✓	✓		✓	✓		
<a href="#">x3500 M3</a>	7380	1-2	IMM	3	HWI	39Y6146	✓	✓	✓		✓	✓	
					HWI	42C1770	✓	✓	✓		✓	✓	
					SWI	LOM <sup>5</sup>	✓	✓		✓	✓		
					SWI	49Y4220	✓	✓		✓	✓		
					SWI	42C1780	✓	✓		✓	✓		
<a href="#">x3620 M3</a>	7376	1-2	IMM	3	SWI	LOM <sup>5</sup>		✓		✓	✓		
					SWI	49Y4220		✓		✓	✓		
					SWI	42C1780		✓		✓	✓		
<a href="#">x3400 M3</a>	7378 7379	1-2	IMM	3	HWI	39Y6146	✓	✓	✓		✓	✓	
					HWI	42C1770	✓	✓	✓		✓	✓	
	7379	1-2	IMM	3	SWI	LOM <sup>5</sup>	✓	✓		✓	✓		
					SWI	49Y4220	✓	✓		✓	✓		
					SWI	42C1780	✓	✓		✓	✓		

System x Server	Type	Number of Processors	Service Processor <sup>4</sup>	Notes	Initiator Type	System x iSCSI initiators Option P/N <sup>1,6</sup>	Server OS <sup>2,6</sup>							
							WIN2012	WIN2008	WIN2003	ESXi5	ESXi4	ESX4	ESX3.5	
<a href="#">x3400 M2</a>	7836	1-2	IMM	3	HWI	39Y6146		✓	✓		✓	✓	✓	
					HWI	42C1770		✓	✓		✓	✓	✓	
					SWI	LOM <sup>5</sup>		✓		✓				
	7837	1-2	IMM	3	HWI	39Y6146		✓	✓		✓	✓	✓	
					HWI	42C1770		✓	✓		✓	✓	✓	
					SWI	LOM <sup>5</sup>		✓		✓				
<a href="#">x3500 M2</a>	7839	1-2	IMM	3	HWI	39Y6146		✓	✓		✓	✓	✓	
					HWI	42C1770		✓	✓		✓	✓	✓	
					SWI	LOM <sup>5</sup>		✓		✓				
<a href="#">x3550 M2</a>	7946	1-2	IMM	3	HWI	39Y6146		✓	✓		✓	✓	✓	
					HWI	42C1770		✓	✓		✓	✓	✓	
					SWI	LOM <sup>5</sup>		✓		✓				
<a href="#">x3650 M2</a>	7947	1-2	IMM	3	HWI	39Y6146		✓	✓		✓	✓	✓	
					HWI	42C1770		✓	✓		✓	✓	✓	
					SWI	LOM <sup>5</sup>		✓		✓				
<a href="#">x3850 M2</a>	7141 7233	1-4	RSA II Included	3	HWI	39Y6146		✓	✓			✓	✓	
					HWI	42C1770		✓	✓			✓	✓	
<a href="#">x3950 M2</a>	7141 7233	1-4	RSA II Included	3	HWI	39Y6146		✓	✓			✓	✓	
					HWI	42C1770		✓	✓			✓	✓	
<a href="#">x3500</a>	7977	1-2	RSA II P/N 39Y9566 Required	3	HWI	39Y6146		✓	✓			✓	✓	
					HWI	42C1770		✓	✓			✓	✓	
					HWI	30R5201		✓	✓				✓	✓
					HWI	30R5501		✓	✓					✓
<a href="#">x3550</a>	7978	1-2	BMC (RSA II P/N 39Y9566 Optional)	3	HWI	39Y6146		✓	✓			✓	✓	
					HWI	42C1770		✓	✓			✓	✓	
					HWI	30R5201 (requires riser P/N 32R2816)		✓	✓				✓	
					HWI	30R5501 (requires riser P/N 32R2816)		✓	✓				✓	
<a href="#">x3650</a>	7979	1-2	BMC (RSA II P/N 39Y9566 Optional)	3	HWI	39Y6146		✓	✓			✓	✓	
					HWI	42C1770		✓	✓			✓	✓	
					HWI	30R5201 (requires riser P/N 40K1908)		✓	✓				✓	
					HWI	30R5501 (requires riser P/N 40K1908)		✓	✓				✓	
<a href="#">x3850</a>	8863	1-4	BMC (RSA II P/N 39Y9566 Optional)	3	HWI	30R5201			✓					
					HWI	30R5501			✓					

System x Server	Type	Number of Processors	Service Processor <sup>4</sup>	Notes	Initiator Type	System x iSCSI initiators Option P/N <sup>1,6</sup>	Server OS <sup>2,6</sup>						
							WIN2012	WIN2008	WIN2003	ESXi5	ESXi4	ESX4	ESX3.5
<a href="#">x3850</a>	8864	1-4	BMC (RSA II P/N 39Y9566 Optional)	3	HWI	30R5201		✓	✓				✓
					HWI	30R5501		✓	✓				✓
<a href="#">x3950</a>	8872	2-4	RSA II Included	3	HWI	30R5201			✓				
					HWI	30R5501			✓				
<a href="#">x3950</a>	8878	2-4	RSA II Included	3	HWI	30R5201		✓	✓				✓
					HWI	30R5501		✓	✓				✓
<a href="#">x236</a>	8841	1-2	RSA II P/N 39Y9566 or 73P9341 Required	3	HWI	30R5201			✓				
					HWI	30R5501			✓				
<a href="#">x336</a>	8837	1-2	RSA II P/N 39Y9566 or 73P9341 Required	3	HWI	30R5201			✓				
					HWI	30R5501			✓				
<a href="#">x346</a>	8840	1-2	RSA II P/N 39Y9566 or 73P9341 Required	3	HWI	30R5201			✓				
					HWI	30R5501			✓				
<a href="#">x366</a>	8863	1-4	BMC (RSA II P/N 39Y9566 or 73P9341 Optional)	3	HWI	30R5201			✓				
					HWI	30R5501			✓				
<a href="#">x460</a>	8872	2-4	RSA II Included	3	HWI	30R5201			✓				
					HWI	30R5501			✓				

**Notes:**

<sup>1</sup> The part number (P/N) shown for each adapter is the adapter option P/N. An adapter might also have an associated field replaceable unit (FRU) P/N and an adapter card assembly P/N (part number for the card itself). Make sure that you are using the adapter option P/N when looking up the iSCSI initiator in this table.

<sup>2</sup> Server operating system (OS) support also varies based on the IBM i version that is used.

IBM i	Server OS						
	WIN2012	WIN2008	WIN2003	ESXi5	ESXi4	ESX4	ESX3.5
i 7.2	✓	✓		✓	✓	✓	
i 7.1	✓	✓	✓	✓	✓	✓	
i 6.1		✓	✓	✓	✓	✓	✓
i 5.4			✓				✓

Refer to the Server OS notation on page 20 for the specific list of OS versions that correspond to the abbreviations shown in this table.

<sup>3</sup> With the IBM i iSCSI solution, all of the disk drives for the BladeCenter blade or System x model are provided as virtual storage by IBM i. When ordering BladeCenter blade or System x servers, do not order internal or external BladeCenter blade or System x controlled disk or disk controller adapters. Any disk drives and disk controller adapters that might be installed in the BladeCenter blade or System x server must be removed before the server installation process is started.

<sup>4</sup> System x service processor types:

- IMM II** Integrated Management Module II
- IMM** Integrated Management Module
- RSA II** Remote Supervisor Adapter II SlimLine
- BMC** Baseboard Management Controller (use RSA II SlimLine service processor option, if available)

<sup>5</sup> **LOM** = LAN on Motherboard, which is also called embedded Ethernet or integrated Ethernet.

<sup>6</sup> Changes are made periodically to the IBM website, please refer to the [IBM Server Proven website](#) for tested combinations for System x Servers.

<sup>7</sup> Testing Status for this server is **Compatible**: IBM has performed limited testing of a representative subset of the Integrated Server solution on this server, IBM is reasonably confident that it will work effectively in a customer environment. However, problems may or may not be present. Problems, if present, may not be resolvable.

**Related information:**

- [System x iSCSI initiators](#)
- [iSCSI supported limits](#)
- [IBM System x Configuration and Options Guide](#)



## 2.6.1 System x iSCSI initiators

System x iSCSI initiators	Type	Feature Code	Option Part Number (P/N) <sup>1</sup>	Adapter type	Ethernet ports	IBM i
LAN on Motherboard (LOM) <sup>2</sup>	SWI	N/A	LOM	N/A	2-4 <b>Copper</b> ports (1 or 10 Gbps)	i 7.2 i 7.1 i 6.1
NetXtreme II 1000 Express Quad Port Ethernet Adapter	SWI	5766	49Y4220	PCIe Ethernet NIC	4 <b>Copper</b> ports (1 Gbps)	i 7.2 i 7.1 i 6.1
NetXtreme II 1000 Express Dual Port Ethernet Adapter	SWI	2995	42C1780	PCIe Ethernet NIC	2 <b>Copper</b> ports (1 Gbps)	i 7.2 i 7.1 i 6.1
QLogic iSCSI Single Port PCIe HBA	HWI	2976	39Y6146	PCIe iSCSI HBA	1 <b>Copper</b> port (1 Gbps)	All
QLogic iSCSI Dual Port PCIe HBA	HWI	2977	42C1770	PCIe iSCSI HBA	2 <b>Copper</b> ports (1 Gbps)	All
<b>The following iSCSI initiators have been withdrawn from Marketing:</b>						
QLogic QLA4050C	HWI		30R5201	PCI-X iSCSI HBA	1 <b>Copper</b> port (1 Gbps)	All
QLogic QLA4050	HWI		30R5501	PCI-X iSCSI HBA	1 <b>Fiber</b> port (1 Gbps)	All
<b>Notes:</b>						
<p><sup>1</sup> The part number (P/N) shown for each adapter is the adapter <u>option</u> P/N. An adapter might also have an associated field replaceable unit (FRU) P/N and an adapter card assembly P/N (part number for the card itself). Make sure that you are using the adapter <u>option</u> P/N when looking up the iSCSI initiator in this table.</p> <p><sup>2</sup> Refer to the specific server model specifications for the LAN on Motherboard (LOM) port characteristics, such as number of ports, port speed, and port technology provider (for example, Intel or Broadcom). Note that LAN on Motherboard is also called embedded Ethernet or integrated Ethernet.</p>						

### Related information:

➤ [System x server models](#)

➤ [iSCSI supported limits](#)

## 2.7 IBM i iSCSI targets

IBM i iSCSI targets	Type	Feature Code	Adapter type	Ethernet ports	Power Servers	IBM i				
						i7.2	i7.1	i6.1.1	i6.1	i5.4
Power System Ethernet NIC <sup>1</sup>	SWT	Any 1 or 10 Gbps Ethernet NIC Feature	PCIe or PCI-X <sup>4</sup> Ethernet NIC	(1 or 10 Gbps)	Any that run IBM i	✓	✓	✓		
Power System <i>Embedded</i> Ethernet port <sup>2</sup>	SWT	N/A	N/A	1 port (1 or 10 Gbps)	Any that run IBM i	✓	✓	✓		
Power System <i>Virtual</i> Ethernet port <sup>3</sup>	SWT	N/A	N/A	1 port (1 or 10 Gbps)	None					
Power System 1 Gigabit iSCSI TOE PCI-X Adapter	HWT	5713	PCI-X <sup>4</sup> iSCSI HBA	1 <b>Copper</b> port (1 Gbps)	720, 740, 750, 770, 780, 795, 520, 550, 560, 570, 595	✓	✓	✓	✓	✓
Power System 1 Gigabit iSCSI TOE PCI-X Adapter	HWT	5714	PCI-X <sup>4</sup> iSCSI HBA	1 <b>Fiber</b> port <sup>5</sup> (1 Gbps)	720, 740, 750, 770, 780, 795, 520, 550, 560, 570, 595	✓	✓	✓	✓	✓
System i iSCSI Host Bus Adapter	HWT	5783	PCI-X <sup>4</sup> iSCSI HBA	1 <b>Copper</b> port (1 Gbps)	i515, i520, i525, i550, i570, i595		✓	✓	✓	✓
System i iSCSI Host Bus Adapter	HWT	5784	PCI-X <sup>4</sup> iSCSI HBA	1 <b>Fiber</b> port <sup>5</sup> (1 Gbps)	i515, i520, i525, i550, i570, i595		✓	✓	✓	✓

**Notes:**

<sup>1</sup> See your Power Server model features list for the available Ethernet NIC feature codes. All 1 Gbps and 10 Gbps Ethernet NICs for your Power Server model are supported as IBM i iSCSI software targets.

<sup>2</sup> Power Server *embedded* Ethernet ports should be avoided as iSCSI software targets due to performance. See *Integrated BladeCenter and System x Performance* in the [IBM i Performance Capabilities Reference](#).

<sup>3</sup> Power Server *virtual* Ethernet ports are **not** supported as iSCSI software targets.

<sup>4</sup> PCI-X target adapters require a PCI-X slot either in the system CEC or in an expansion drawer.

<sup>5</sup> Use LC duplex connectors for the iSCSI adapter fiber ports.

### Related information:

➤ [Power Server IBM i iSCSI target support](#)

➤ [iSCSI supported limits](#)

## 2.7.1 Power Server IBM i iSCSI target support

Power Server (running IBM i)	Software Targets <sup>1</sup>	Hardware Targets <sup>2</sup>
POWER8 systems <sup>4</sup>	✓	
Power 710 Express	✓	
Power 720 Express	✓	✓
Power 730 Express	✓	
Power 740 Express	✓	✓
Power 750 Express	✓	✓
Power 770	✓	✓
Power 780	✓	✓
Power 795	✓	✓
Power 520 Express	✓	✓
Power 550 Express	✓	✓
Power 560 Express	✓	✓
Power 570	✓	✓
Power 595	✓	✓
System i 515	✓	✓ <sup>3</sup>
System i 520	✓	✓ <sup>3</sup>
System i 525	✓	✓ <sup>3</sup>
System i 550	✓	✓ <sup>3</sup>
System i 570	✓	✓ <sup>3</sup>
System i 595	✓	✓ <sup>3</sup>
<b>Notes:</b> <sup>1</sup> Software targets require IBM i 6.1.1 or later. <sup>2</sup> Hardware targets require a PCI-X slot either in the system CEC or in an expansion drawer. <sup>3</sup> The minimum server firmware required for the #5783 PCI-X iSCSI HBA Copper and #5784 PCI-X iSCSI HBA Fiber adapters are: <ul style="list-style-type: none"> <li>For Model 520 Power5+ (Processor Features 8325, 8327, and 8330) the server firmware level must be 240_219 or later.  <b>Note:</b> You can display the processor feature number of your Power server using the following IBM i command: DSPSYSVAL QPRCFEAT</li> <li>For all other supported Power5 and Power5+ models and other 520 processor features, the server firmware level must be the later of either 235_185 or the specific FW level required for your model/processor (which can be found at <a href="http://www-912.ibm.com/e_dir/eServerPrereq.nsf">http://www-912.ibm.com/e_dir/eServerPrereq.nsf</a>).</li> </ul> <sup>4</sup> Please refer to a complete listing of <a href="#">Power and System i model to operating system level mapping</a> to find out the supported hardware for a specific IBM i release.		

### Related information:

➤ [IBM i iSCSI targets](#)

➤ [iSCSI supported limits](#)

## 2.8 iSCSI supported limits

Description	Limit
IBM i iSCSI targets per Power Server (low end - high end). <sup>1,2,3</sup>	2 - 100+
Number of blade or System x servers per IBM i iSCSI target for storage access. <sup>3</sup>	8
Virtual Ethernet access points per IBM i iSCSI target. <sup>3,4</sup>	8
IBM i iSCSI targets per blade or System x server for storage access. <sup>5</sup>	4
IBM i iSCSI targets per blade or System x server for virtual Ethernet access. <sup>5</sup>	4
iSCSI initiator ports per System x server. <sup>5</sup>	4
iSCSI initiator ports per blade server. <sup>5</sup>	3
Cable length between a switch and an iSCSI adaptor: <b>Copper</b> (category 5e or 6) cables.	100m
Cable length between a switch and an iSCSI adaptor: 62.5/125 µm multimode <b>fiber</b> cables.	220m
Cable length between a switch and an iSCSI adaptor: 50/125 µm multimode <b>fiber</b> cables.	500m
<b>Notes:</b>	
<p><sup>1</sup> Power server models provide a range of iSCSI target attachment limits, from 2 iSCSI targets on low end models to over 100 iSCSI targets on high end models. You can use a mixture of iSCSI software and hardware targets if applicable. Your IBM sales representative or business partner can look up the iSCSI software and hardware target limits for a specific Power server model in the <b>Sales Manual</b>. Alternatively, you can use the <a href="#">IBM System Planning Tool</a> to determine the attachment capabilities for a particular Power server model.</p> <p><sup>2</sup> Each iSCSI-attached blade or System x server will consume IBM i resources. The actual number of blade or System x servers that an IBM i system can support will depend on the available IBM i resources and the applications on the blade or System x servers. See <i>Integrated BladeCenter and System x Performance</i> in the <a href="#">IBM i Performance Capabilities Reference</a> for more information.</p> <p><sup>3</sup> This is an attachment limit. The practical limit will depend on the cumulative amount of I/O for the attached blade or System x servers.</p> <p><sup>4</sup> Available virtual Ethernet access points could be used by multiple blade or System x servers using just one virtual Ethernet each, one blade or System x server using multiple virtual Ethernets, or some other combination.</p> <p><sup>5</sup> The specific blade or System x server model and the server OS that is installed might impose lower limits.</p>	

### Related information:

- [IBM i iSCSI targets](#)
- [Power Server IBM i iSCSI target support](#)
- [Ethernet switches for the iSCSI solution](#)
- [Blade server models](#)
- [System x server models](#)

## 2.9 IBM i tape and optical device access by integrated servers

iSCSI-attached blade and System x servers can access tested IBM i tape and optical devices as if they were local devices on those servers.

The table below summarizes the tested IBM i device types for each server OS:

IBM i device type <sup>1</sup>	Server OS			
	WIN2012	WIN2008	WIN2003	ESX
IBM i virtual tape devices	✓	✓	✓	
IBM i physical tape devices			✓	
IBM i virtual optical devices	✓	✓	✓	
IBM i physical optical devices	✓	✓	✓	
<b>Notes:</b>				
<sup>1</sup> The specific IBM i devices that are accessible by the integrated server vary by server OS version.				

### Related information:

- [IBM i tape devices for Windows Server 2008/2012](#)
- [IBM i tape devices for Windows Server 2003](#)
- [IBM i tape libraries](#)
- [IBM i tape media](#)

## 2.9.1 IBM i tape devices for Windows Server 2012/2008

The following table shows the IBM i tape devices and associated tape device driver versions that have been tested with the IBM i iSCSI solution on Windows Server 2012 and Windows Server 2008.

### Important:

- IBM i tape devices and tape libraries that are not listed in the table are not supported with the IBM i iSCSI solution.
- If you have an IBM i tape device that is not listed in the table, you can effectively backup to the tape device by doing a 2-step back up:
  1. First, backup from Windows to IBM i virtual tape media.
  2. Next, use IBM i to back up the virtual tape media in IBM i to your tape device.

Tape Device Name and/or Type-Model	Backup Application <sup>1</sup>	Tape Driver Provider <sup>2</sup>	Driver Version	Testing Status <sup>3</sup>
IBM i Virtual Tape <sup>4, 5</sup> (Virtual ULT3580-TD2) (IBM Ultrium 2)	Backup Exec 12	Symantec	5.1.37.0	Compatible

#### Notes:

<sup>1</sup> **Backup Application** lists the backup application that was tested:

Backup Exec 12: Symantec Backup Exec 12 for Windows Servers.

<sup>2</sup> **Tape Driver Provider** lists the providers of the tape device drivers. Tape device drivers must be installed on Windows in order to access IBM i tape devices. The first choice for tape drivers is to use drivers approved by your backup application. If the backup application does not provide or recommend tape device drivers, then use tape drivers appropriate for the type of tape drive you use. Use the following locations for obtaining device drivers that are appropriate for the tape drive:

**Symantec:** Tape drivers provided by Symantec are included with the Backup Exec application.

<sup>3</sup> **Testing Status** lists how extensively the listed application/driver combination has been tested by IBM.

**Tested:** IBM has performed extensive testing of the devices using the listed backup application and device driver version. IBM is confident that it will work in a customer environment.

Note: If a tape library type-model is also shown, then the tape device was tested within the specified tape library.

**Compatible:** IBM has performed limited testing of a representative subset of similar devices using the listed backup application and driver version. IBM is reasonably confident that it will work effectively in a customer environment. However, problems may or may not be present with this application and driver version combination. Problems, if present, may not be resolvable.

<sup>4</sup> **Tape spanning** is not supported with IBM i virtual tape devices. You must create IBM i virtual tape media that is large enough to hold the entire backup.

<sup>5</sup> With this device, you must disable Windows Automatic Data Path Failover. See Software Knowledge Base article [Ultrium Tape Devices Not Recognized by Windows Computer Management](#) for more information.

#### Related information:

➤ [IBM i tape libraries](#)

➤ [IBM i tape media](#)

## 2.9.2 IBM i tape devices for Windows Server 2003

The following table shows the IBM i tape devices and associated tape device driver versions that have been tested with the IBM i iSCSI solution on Windows Server 2003.

### Important:

- IBM i tape devices and tape libraries that are not listed in the table are not supported with the IBM i iSCSI solution.
- If you have an IBM i tape device that is not listed in the table, you can effectively backup to the tape device by doing a 2-step back up:
  1. First, backup from Windows to IBM i virtual tape media.
  2. Next, use IBM i to back up the virtual tape media in IBM i to your tape device.

Tape Device Name and/or Type-Model	Backup Application <sup>1</sup>	Tape Driver Provider <sup>2</sup>	Driver Version	Testing Status <sup>3</sup>
IBM i Virtual Tape <sup>4, 5</sup> (Virtual ULT3580-TD2) (IBM Ultrium 2)	Windows Backup	IBM	6.1.1.2	Tested
	Windows Backup	IBM	6.1.2.30	Compatible
	Windows Backup	IBM	6.1.5.4	Compatible
	Windows Backup	IBM	6.1.8.4	Compatible
	Backup Exec 9.1	Symantec	5.01	Tested
	Backup Exec 10d	Symantec	5.1	Tested
IBM ULT3580-TD1 <sup>5</sup> (IBM Ultrium) <a href="#">3580-001</a> , <a href="#">3580-H11</a> , <a href="#">3580-L11</a> , <a href="#">3580-H13</a> , <a href="#">3580-L13</a>	Backup Exec 11d	Symantec	5.1.25.0	Compatible
	Windows Backup	IBM	6.1.2.5	Tested (3581-L13)
	Windows Backup	IBM	6.1.2.30	Compatible
	Backup Exec 9.1	Symantec	5.1.1.1	Tested (3581-L13)
IBM ULT3580-TD2 <sup>5</sup> (IBM Ultrium 2) <a href="#">3580-002</a> , <a href="#">3580-H23</a> , <a href="#">3580-L23</a>	Backup Exec 10d	Symantec	5.1.1.1	Tested (3581-L13)
	Windows Backup	IBM	6.1.1.2	Tested (3581-L28)
	Windows Backup	IBM	6.1.2.30	Compatible
	Windows Backup	IBM	6.1.8.4	Compatible
	Backup Exec 9.1	Symantec	5.01	Tested (3581-L28)
	Backup Exec 10d	Symantec	5.1.1.1	Tested (3581-L28)
	Backup Exec 11d	Symantec	5.1.25.0	Compatible (3581-L28)
IBM ULT3580-003 <sup>5</sup> (IBM Ultrium 3) <a href="#">3580-003</a> , <a href="#">3580-L33</a>	Backup Exec 12	Symantec	5.1	Compatible (3581-L28)
	Windows Backup	IBM	6.1.1.2	Tested (3581-L38, 3582-L23)
	Windows Backup	IBM	6.1.3.5	Tested (3583-L72)
	Windows Backup	IBM	6.1.2.30	Compatible
	Windows Backup	IBM	6.1.2.50	Compatible (3581-L38)
	Windows Backup	IBM	6.1.7.8	Compatible (3581-L38)
	Windows Backup	IBM	6.1.4.8	Tested (3573-L2U)
	Windows Backup	IBM	6.1.8.4	Compatible (3573-L2U)
	Backup Exec 9.1	Symantec	5.01	Tested (3582-L23)
	Backup Exec 9.1	Symantec	5.1	Tested (3583-L72)
	Backup Exec 9.1	Symantec	5.1.1.1	Tested (3581-L38)
	Backup Exec 10d	Symantec	5.1	Tested (3582-L23, 3583-L72)
	Backup Exec 10d	Symantec	5.1	Tested (3573-L2U)
	Backup Exec 10d	Symantec	5.1.1.1	Tested (3581-L38)
Backup Exec 11d	Symantec	5.1.22.0	Compatible (3581-L38)	
Backup Exec 11d	Symantec	5.1.25.0	Compatible (3581-L38)	

Tape Device Name and/or Type-Model	Backup Application <sup>1</sup>	Tape Driver Provider <sup>2</sup>	Driver Version	Testing Status <sup>3</sup>
IBM 3590 (TotalStorage 3590H11) <a href="#">3590-011</a>	Backup Exec 9.1	Symantec	5.1.1.1	Tested (3590-H11)
	Backup Exec 10d	Symantec	5.1	Tested (3590-H11)
IBM 0359201A <a href="#">3592-J1A</a>	Windows Backup	IBM	6.1.2.30	Tested
	Backup Exec 9.1	Symantec	5.1.1.1	Tested
	Backup Exec 10d	Symantec	5.1	Tested
IBM TS1120 <a href="#">3592-E05</a>	Windows Backup	IBM	6.1.2.30	Tested
EXABYTE VXA-2 <a href="#">4685-001</a>	Windows Backup	IBM	1.8.4.0	Tested
	Backup Exec 10d	Symantec	5.1.1.1	Tested
IBM HHLTO2 5755-001	Windows Backup	IBM	1.0.0.2	Tested
EXABYTE VXA-3 (VXA-320) 6279-001	Windows Backup	IBM	1.10.1.1	Tested
	Backup Exec 10d	Symantec	5.1.1.1	Tested
	Backup Exec 11d	Symantec	5.1.25.0	Compatible
IBM 6330 DVD-RAM <sup>6</sup>	Windows Backup	Microsoft	5.2.3790.0	Tested
TANDBERG SLR60 6384-001	Windows Backup	Tandberg	1.6.0.0	Tested
	Backup Exec 10d	Symantec	5.1.1.1	Tested
TANDBERG SLR100 6387-001	Windows Backup	Tandberg	1.6.0.0	Tested
	Backup Exec 10d	Symantec	5.1.1.1	Tested
	Backup Exec 11d	Symantec	5.1.25.0	Compatible
	Backup Exec 12	Symantec	5.1.34.0	Compatible

**Notes:**

<sup>1</sup> **Backup Application** lists the backup application that was tested:

- Windows Backup: Microsoft Windows Backup.
- Backup Exec 9.1: VERITAS Backup Exec 9.1 for Windows Servers, now from Symantec.
- Backup Exec 10d: Symantec Backup Exec 10d for Windows Servers.
- Backup Exec 11d: Symantec Backup Exec 11d for Windows Servers.
- Backup Exec 12: Symantec Backup Exec 12 for Windows Servers.

<sup>2</sup> **Tape Driver Provider** lists the providers of the tape device drivers. Tape device drivers must be installed on Windows in order to access IBM i tape devices. The first choice for tape drivers is to use drivers approved by your backup application. If the backup application does not provide or recommend tape device drivers, then use tape drivers appropriate for the type of tape drive you use. Use the following locations for obtaining device drivers that are appropriate for the tape drive:

**Symantec:** Tape drivers provided by Symantec are included with the Backup Exec application.

**IBM:** Windows Backup tape drivers provided by IBM can be obtained from the following locations:

- For the IBM HHLTO2 5755-001 and EXABYTE VXA-3:  
<http://www.ibm.com/support/entry/portal/docdisplay?Indocid=TAPE-FILES&brandind=5000008>
- For all other tape devices listed in the table: <http://public.dhe.ibm.com/storage/devdrv>

**Tandberg:** Windows Backup tape drivers provided by Tandberg can be obtained from:

<http://www.tandbergdata.com>

**Microsoft:** Windows Backup tape drivers are provided by Microsoft.

<sup>3</sup> **Testing Status** lists how extensively the listed application/driver combination has been tested by IBM. If a tape library type-model is also shown, then the tape device was tested within the specified tape library.

**Tested:** IBM has performed extensive testing of the devices using the listed backup application and device driver version. IBM is confident that it will work in a customer environment.

**Compatible:** IBM has performed limited testing of a representative subset of similar devices using the listed backup application and driver version. IBM is reasonably confident that it will work effectively in a customer environment. However, problems may or may not be present with this application and driver version combination. Problems, if present, may not be resolvable.

<sup>4</sup> **Tape spanning** is not supported with IBM i virtual tape devices. You must create IBM i virtual tape media that is large enough to hold the entire backup.



Tape Device Name and/or Type-Model	Backup Application <sup>1</sup>	Tape Driver Provider <sup>2</sup>	Driver Version	Testing Status <sup>3</sup>
<sup>5</sup> With this device, you must disable <b>Windows Automatic Data Path Failover</b> . See Software Knowledge Base article <a href="#">Ultrium Tape Devices Not Recognized by Windows Computer Management</a> for more information.				
<sup>6</sup> <b>Media spanning</b> is not supported with the IBM 6330 DVD-RAM device.				

**Related information:**

- [IBM i tape libraries](#)
- [IBM i tape media](#)

### 2.9.3 IBM i tape libraries

The following table shows the IBM i tape libraries that have been tested with the IBM i iSCSI solution.

Tape Library Name and/or Type-Model	Tape Devices Used in Library
IBM <a href="#">TS3100</a> 3573-L2U	3580-003 (IBM Ultrium 3)
IBM <a href="#">TS3310</a> 3576-L5B	3580-003 (IBM Ultrium 3)
<a href="#">3581-H13, 3581-L13, 3581-H17, 3581-L17</a>	3580-001 (IBM Ultrium)
<a href="#">3581-H23, 3581-L23</a>	3580-002 (IBM Ultrium 2)
<a href="#">3581-F28, 3581-L28</a>	3580-002 (IBM Ultrium 2)
<a href="#">3581-F38, 3581-L38</a>	3580-003 (IBM Ultrium 3)
<a href="#">3582-L23</a>	3580-002 (IBM Ultrium 2), 3580-003 (IBM Ultrium 3)
<a href="#">3583-L72</a>	3580-002 (IBM Ultrium 2), 3580-003 (IBM Ultrium 3)
IBM 03590H11 <a href="#">3590-H11, 3590-H1A</a>	3590-011 (TotalStorage 3590H11)
<b>Notes:</b>	
<sup>1</sup> The Auto Cartridge Loader (ACL) feature is supported with all tape libraries listed in this table that support sequential access.	
<sup>2</sup> Random access of media is not supported for the IBM i iSCSI solution when accessing media through a Windows application. If multiple media backups are required by a Windows application, the library must be configured for sequential access of media.	
<sup>3</sup> Refer to the referenced <b>Related information</b> sections for the testing status of the specific tape devices that are used in the tape library.	

**Related information:**

- [IBM i tape devices for Windows Server 2003](#)
- [IBM i tape media](#)

## 2.9.4 IBM i tape media

The following table shows the tape media that is supported for each tape device.

<b>Tape Library Name and/or Type-Model</b>	<b>Tape Media<sup>1</sup></b>
IBM i Virtual Tape (Virtual ULT3580-TD2)	LTO Ultrium 2 (Virtual)
IBM ULT3580-TD1 (IBM Ultrium) <a href="#">3580-001</a> , <a href="#">3580-H11</a> , <a href="#">3580-L11</a> , <a href="#">3580-H13</a> , <a href="#">3580-L13</a>	LTO Ultrium
IBM ULT3580-TD2 (IBM Ultrium 2) <a href="#">3580-002</a> , <a href="#">3580-H23</a> , <a href="#">3580-L23</a>	LTO Ultrium 2
IBM ULT3580-003 (IBM Ultrium 3) <a href="#">3580-003</a> , <a href="#">3580-L33</a>	LTO Ultrium 1 (r), Ultrium 2 (rw), Ultrium 3 (rw)
IBM 3590 (TotalStorage 3590H11) <a href="#">3590-011</a>	IBM 3590 Magstar Extended High Performance Tape Cartridge
IBM 0359201A <a href="#">3592-J1A</a>	IBM Total-Storage Enterprise Tape Cartridge 3592
IBM TS1120 <a href="#">3592-E05</a>	IBM Total-Storage Enterprise Tape Cartridge 3592
IBM HHLTO2 5755-001	LTO Ultrium 2
<a href="#">EXABYTE VXA-3</a> (VXA-320) 6279-001	X23 (VXA-3)
TANDBERG SLR60 6384-001	SLR60 30G QIC
TANDBERG SLR100 6387-001	SLR100 50G QIC
<b>Notes:</b>	
<sup>1</sup> If a tape device supports more than one tape media type, use the default media for the device. All IBM testing is performed using the default media.	

### Related information:

- [IBM i tape devices for Windows Server 2003](#)
- [IBM i tape libraries](#)

# 3 Concepts

This chapter explains key concepts for integrated servers.

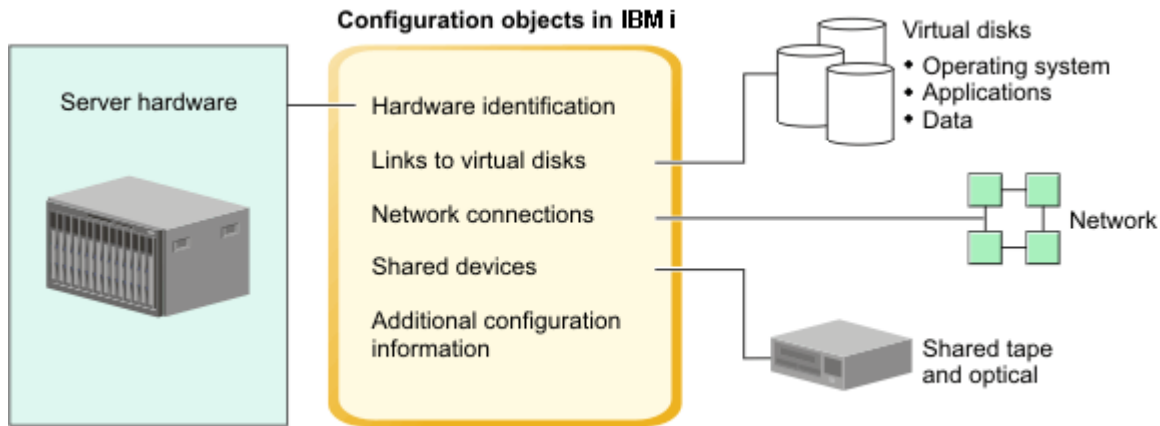
## Chapter Table of Contents

- 3.1 Integrated server overview .....53
- 3.2 Attaching servers to IBM i using iSCSI.....54
  - 3.2.1 Typical iSCSI-attached server installation.....56
  - 3.2.2 Single-server environment .....58
  - 3.2.3 Multiple-server environment.....59
  - 3.2.4 Integrated server service processor connection.....60
  - 3.2.5 Booting over the iSCSI network .....61
- 3.3 IBM i configuration objects for integrated servers .....62
- 3.4 Server management for integrated servers .....67
  - 3.4.1 IBM i management interfaces.....67
  - 3.4.2 Additional management interfaces .....68
  - 3.4.3 Integrated server installation .....68
  - 3.4.4 Integrated server cloning.....69
  - 3.4.5 Integrated server management infrastructure .....72
    - 3.4.5.1 Integrated Windows server management infrastructure .....72
      - 3.4.5.1.1 Windows services for IBM i integration with Windows servers .....72
      - 3.4.5.1.2 Windows utilities for IBM i integration with Windows servers .....73
    - 3.4.5.2 Integrated VMware ESX server management infrastructure.....74
      - 3.4.5.2.1 Windows services for IBM i integration with ESX servers .....77
      - 3.4.5.2.2 Windows utilities for IBM i integration with ESX servers .....77
      - 3.4.5.2.3 Service console programs for IBM i integration with ESX servers .....78
  - 3.4.6 Integrated server console.....78
  - 3.4.7 Software updates .....79
- 3.5 Storage management for integrated servers .....81
  - 3.5.1 Virtual storage .....81
  - 3.5.2 IBM i storage management .....82
    - 3.5.2.1 IBM i and disk drives .....82
    - 3.5.2.2 Storage pools (ASPs).....83
    - 3.5.2.3 Disk protection .....84
  - 3.5.3 Predefined virtual storage and naming.....85
  - 3.5.4 Create user-defined virtual storage .....87
    - 3.5.4.1 Storage alignment considerations when creating virtual storage .....88
  - 3.5.5 Copy virtual storage .....90
  - 3.5.6 Extend the size of virtual storage .....90
  - 3.5.7 Virtual storage linking.....91
    - 3.5.7.1 Dynamic virtual storage linking while server is active .....92
  - 3.5.8 Virtual storage formatting .....93
  - 3.5.9 Virtual storage unlinking .....94
    - 3.5.9.1 Dynamic virtual storage unlinking while server is active .....94
- 3.6 IBM i tape and optical devices shared with integrated Windows servers .....95
- 3.7 Networking concepts for integrated servers .....96
  - 3.7.1 iSCSI network.....96
  - 3.7.2 Integrated iSCSI DHCP server.....99
    - 3.7.2.1 Advanced integrated iSCSI DHCP server concepts .....99
  - 3.7.3 Ethernet switches for the iSCSI solution .....100
    - 3.7.3.1 External switch considerations.....100
    - 3.7.3.2 BladeCenter switch module considerations .....101
  - 3.7.4 Service processor connection .....102

3.7.4.1	Supported functions by service processor type .....	103
3.7.4.2	Service processor addressing methods .....	104
3.7.4.3	Service processor connection methods .....	105
3.7.4.4	Considerations for connecting service processors to IBM i .....	105
3.7.5	Networking for IBM i administration of integrated servers .....	107
3.7.5.1	Point-to-point virtual Ethernet network for integrated Windows servers .....	107
3.7.5.2	Multiple networks for integrated VMware ESX servers .....	108
3.7.6	Virtual Ethernet networks for integrated Windows servers.....	108
3.7.7	Physical networks.....	111
3.7.8	Network security.....	112
3.8	Performance concepts.....	114
3.8.1	Virtual storage performance .....	114
3.8.2	IBM i memory requirements .....	116
3.8.2.1	Machine pool.....	116
3.8.2.2	iSCSI virtual storage I/O memory pool.....	116
3.8.3	Virtual Ethernet performance for integrated Windows servers .....	117
3.8.4	MTU considerations for the iSCSI network .....	118
3.9	Backup and recovery concepts .....	119
3.9.1	What objects to save and their location on IBM i .....	123
3.10	High availability concepts.....	125
3.10.1	Multipath I/O (MPIO).....	125
3.10.2	Hot spare support for integrated servers .....	128
3.10.2.1	Hot spare support for System x or blade hardware.....	128
3.10.2.2	Hot spare support for IBM i iSCSI target adapters .....	129
3.10.3	IBM i clustering for integrated servers .....	130
3.11	User and group enrollment concepts for integrated Windows servers .....	131
3.11.1	Enrolled user account options for integrated Windows servers .....	134
3.11.2	User enrollment templates for integrated Windows servers .....	136
3.11.3	Password considerations for integrated Windows servers .....	137
3.11.4	QAS400NT user and integrated Windows servers .....	138
3.12	IBM i NetServer for integrated servers.....	138
3.13	IBM i Access for Windows and integrated servers.....	139

### 3.1 Integrated server overview

An integrated server is a combination of integrated server hardware, network components, virtual storage (virtual disks), shared devices, and IBM i integrated server configuration objects.



RZAHQ507-2

Figure 1: Integrated server overview

The key components of the iSCSI solution are summarized below.

Item	Description
<b>Server hardware</b>	The server hardware is the physical hardware (such as the processor and memory) that the integrated server runs on. There are several types of server hardware that can be used for integrated servers, depending on your needs. The integrated server hardware is an external System x or BladeCenter blade model that is attached to IBM i with iSCSI initiator and target adapters.
<b>iSCSI adapters</b>	Both IBM i and the integrated server contain iSCSI adapters, which are connected over an Ethernet network. The integrated server uses its iSCSI adapter to connect to the iSCSI adapter in IBM i. Using this connection, the integrated server can access virtual storage, shared tape and optical devices, and virtual Ethernet resources on IBM i. See <a href="#">Attaching servers to IBM i using iSCSI</a> for more information.
<b>Virtual storage</b>	Each integrated server uses virtual storage that contains the integrated server operating system, applications, and data. This virtual storage is allocated from IBM i disk storage. The integrated server treats these drives as physical disk drives that are contained within the server. However, the integrated server does not actually have any physical disk drives of its own. See <a href="#">Storage management for integrated servers</a> for more information about virtual storage.
<b>Shared tape and optical devices</b>	An integrated Windows server can share supported tape and optical devices that are connected to the hosting IBM i partition. Shared IBM i devices are accessed as if they were local to the integrated server. By default, IBM i tape and optical devices are automatically accessible by an integrated server. You can choose to restrict which of these IBM i devices the integrated server can access. A <u>subset</u> of IBM i tape devices are supported for use with various integrated server OS versions. See <a href="#">IBM i tape devices for Windows Server 2008/2012</a> and <a href="#">IBM i tape devices for Windows Server 2003</a> for more information.  <b>Note:</b> IBM i devices cannot be shared with integrated VMware ESX servers.

Item	Description
<b>Network</b>	Each integrated server has one or more connections to a network. Physical network connections with a network adapter are supported for all types of integrated servers. Power server virtual Ethernet network connections are supported by integrated Windows servers. See <a href="#">Networking concepts for integrated servers</a> for more information about the types of network connections that can be used with integrated servers.
<b>Configuration objects in IBM i</b>	Configuration objects in IBM i describe each integrated server. The IBM i configuration objects identify the hardware that the integrated server runs on, the virtual storage that the integrated server uses, the iSCSI target and initiator adapters that the integrated server uses, the virtual Ethernet connections that an integrated Windows server uses, and many other attributes of the server. See <a href="#">IBM i configuration objects for integrated servers</a> for more information.

**Related information:**

- [Blade server models](#)
- [System x server models](#)
- [IBM i iSCSI targets](#)

### 3.2 Attaching servers to IBM i using iSCSI

A basic iSCSI network consists of an IBM i iSCSI target adapter and a System x or IBM BladeCenter blade iSCSI initiator adapter.

The target and initiator devices are connected over an Ethernet local area network (LAN). The iSCSI target for IBM i provides the storage devices for the iSCSI initiator. For an integrated Windows server, the iSCSI target also provides removable media devices and virtual Ethernet connections for the iSCSI initiator. The following figure illustrates a basic iSCSI network.

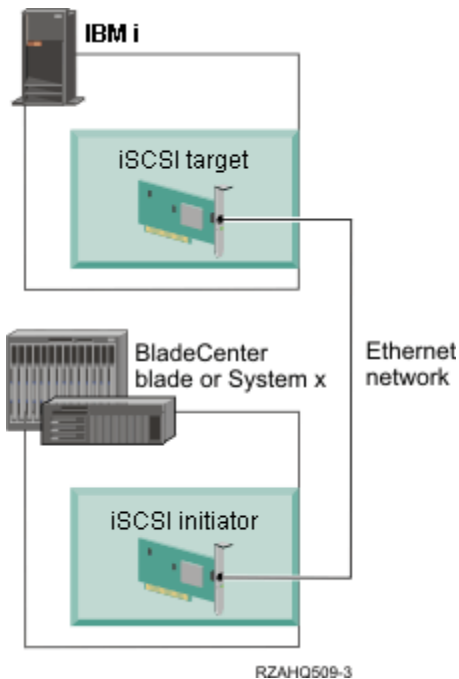


Figure 2: Basic iSCSI network

You need to configure both the iSCSI target and initiator adapters from IBM i. The iSCSI network is used for iSCSI traffic only.

There are two types of iSCSI target and initiator adapter implementations:

### **Software target (SWT) or software initiator (SWI)**

With a software target or initiator, the iSCSI protocol is implemented in the server operating system. Server resources (for example, CPU and memory) are used for the iSCSI protocol.

Standard Ethernet network interface cards (Ethernet NICs) are typically used as software targets and initiators.

### **Hardware target (HWT) or hardware initiator (HWI)**

With a hardware target or initiator, the iSCSI protocol is implemented in firmware on the iSCSI adapter. The iSCSI protocol is offloaded from the server.

iSCSI host bus adapters (iSCSI HBAs) are typically used as hardware targets and initiators.

### **Notes:**

1. Either type of iSCSI initiator adapter can connect to either type of iSCSI target adapter.
2. IBM i can use any combination of software-based or hardware-based iSCSI target adapters that are supported for the IBM i version.
3. The integrated server can use any combination of software-based or hardware-based iSCSI initiator adapters that are supported for the IBM i version, the specific integrated server model, and the operating system that is installed on the server.
4. Support information for specific configurations is documented in the related information below.

### **Related information:**

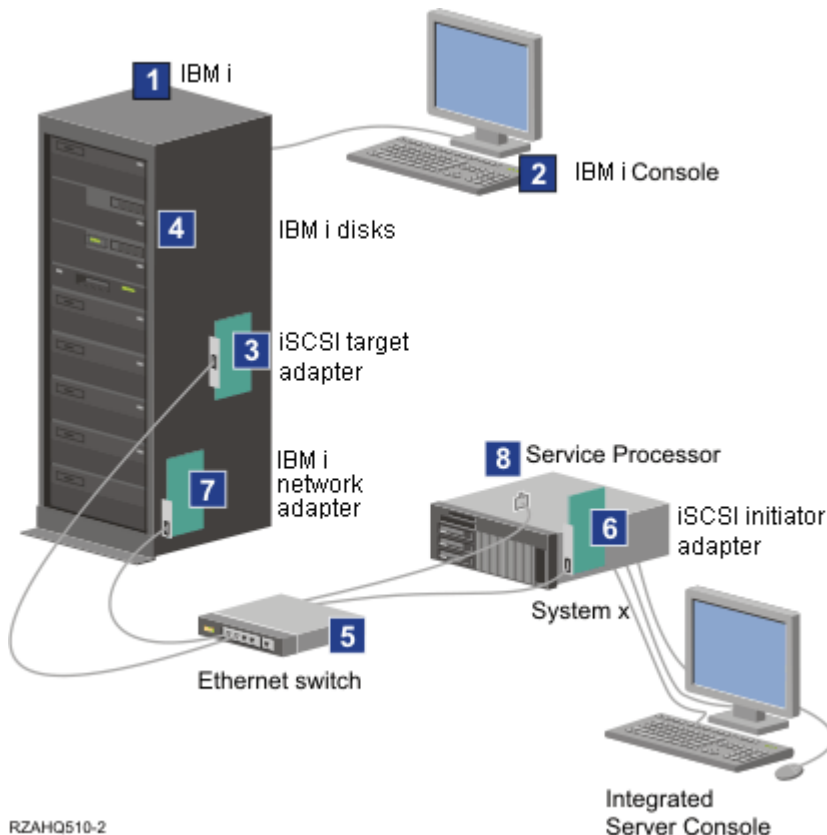
- [Blade server models](#)
- [System x server models](#)
- [IBM i iSCSI targets](#)

### 3.2.1 Typical iSCSI-attached server installation

iSCSI-attached integrated servers are standard System x or IBM BladeCenter blade models that have processors, memory, and expansion cards, but no physical disks. Integrated servers use virtual disks on IBM i that are managed by IBM i.

The installation procedure for an iSCSI-attached integrated server requires hardware to be installed and configured in both the IBM i and the System x or blade servers.

The following figure illustrates a typical iSCSI-attached server installation:



RZAHQ510-2

Figure 3: A typical iSCSI-attached integrated server installation

The items shown in the above figure are described below:

1. You need a compatible Power server model. See [Power Server IBM i iSCSI target support](#) for information about supported Power server models.
2. The IBM i console, from which you connect to IBM i using a graphical or character-based interface, is shown to make clear the distinction between it and the integrated server console.
3. An iSCSI target adapter is required in the IBM i system. Depending on the type of the physical network, copper or fiber iSCSI adapters (Ethernet NICs or iSCSI HBAs) are available. This iSCSI adapter installed in IBM i is the target device and connects to an Ethernet network using standard Ethernet cables.
4. An integrated server does not have its own physical disk drive. IBM i provides virtual hard disk space for it to use from IBM i disks. These disks and other IBM i storage devices are accessed



through the iSCSI target adapter.

5. The iSCSI adapter network cables are typically connected to a standard 1 Gigabit or 10 Gigabit Ethernet switch.
6. An iSCSI initiator adapter is required in the System x or blade server. This iSCSI initiator adapter provides the connection to the iSCSI target adapter in the Power server. This iSCSI initiator adapter can be viewed from the System x or blade server as the storage adapter, where the disks are found across the network.
7. A typical Power server has a network card. An IBM i LAN connection is required to connect to and manage the System x or BladeCenter hardware.
8. A System x or BladeCenter service processor allows IBM i to connect to and manage the system. The System x service processor might be an Integrated Management Module II (IMM II), Integrated Management Module (IMM), a Remote Supervisor Adapter II (RSA II), or a Baseboard Management Controller (BMC). A BladeCenter service processor might be a Management Module (MM) or an Advanced Management Module (AMM). The System x or BladeCenter service processor is connected to IBM i over an Ethernet network.

**Related information:**

- [Blade server models](#)
- [System x server models](#)
- [Power Server IBM i iSCSI target support](#)
- [IBM i iSCSI targets](#)

### 3.2.2 Single-server environment

A basic iSCSI-attached integrated server configuration requires iSCSI adapters and IBM i configuration objects.

The simplest form of the physical connection between an initiator system and IBM i is illustrated in the following figure.

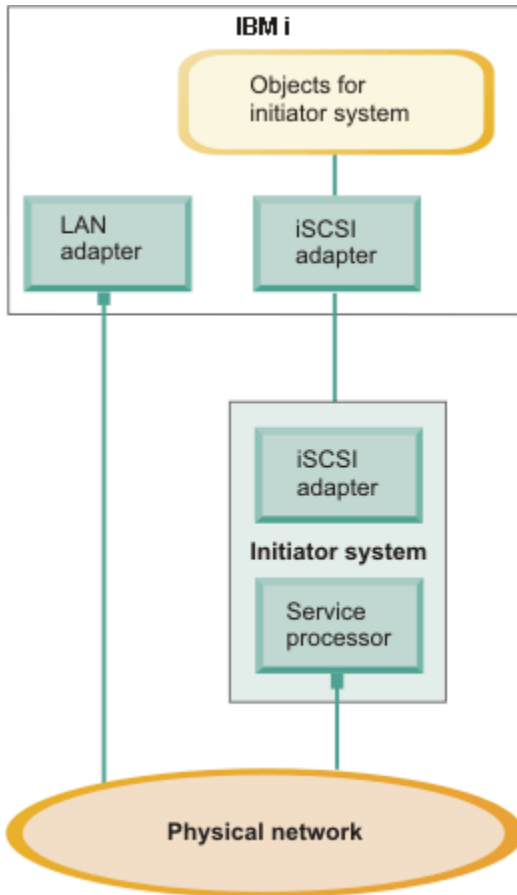


Figure 4: Single iSCSI-attached server

An iSCSI adapter is installed in each system. The Ethernet network between the iSCSI adapters is known as the iSCSI network. The initiator system (System x or BladeCenter system) uses this network to access storage through the IBM i iSCSI target adapter.

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

The iSCSI-attached servers are configured in IBM i objects. See [IBM i configuration objects for integrated servers](#).

IBM i can connect to and manage remote systems by sending commands to the service processor of the remote (initiator) system over an Ethernet network.

Two distinct networks are illustrated in the above figure. The iSCSI network uses an isolated switch or a direct connection. The service processor connection uses an external network (shared network).

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

Both types of networks should be secured. See [Network security](#).

**Related information:**

- [Blade server models](#)
- [System x server models](#)
- [Power Server IBM i iSCSI target support](#)
- [IBM i iSCSI targets](#)
- [IBM i configuration objects for integrated servers](#)

### 3.2.3 Multiple-server environment

You can use one IBM i iSCSI target adapter to host multiple initiator (System x or blade) systems.

This concept is illustrated in the following figure.

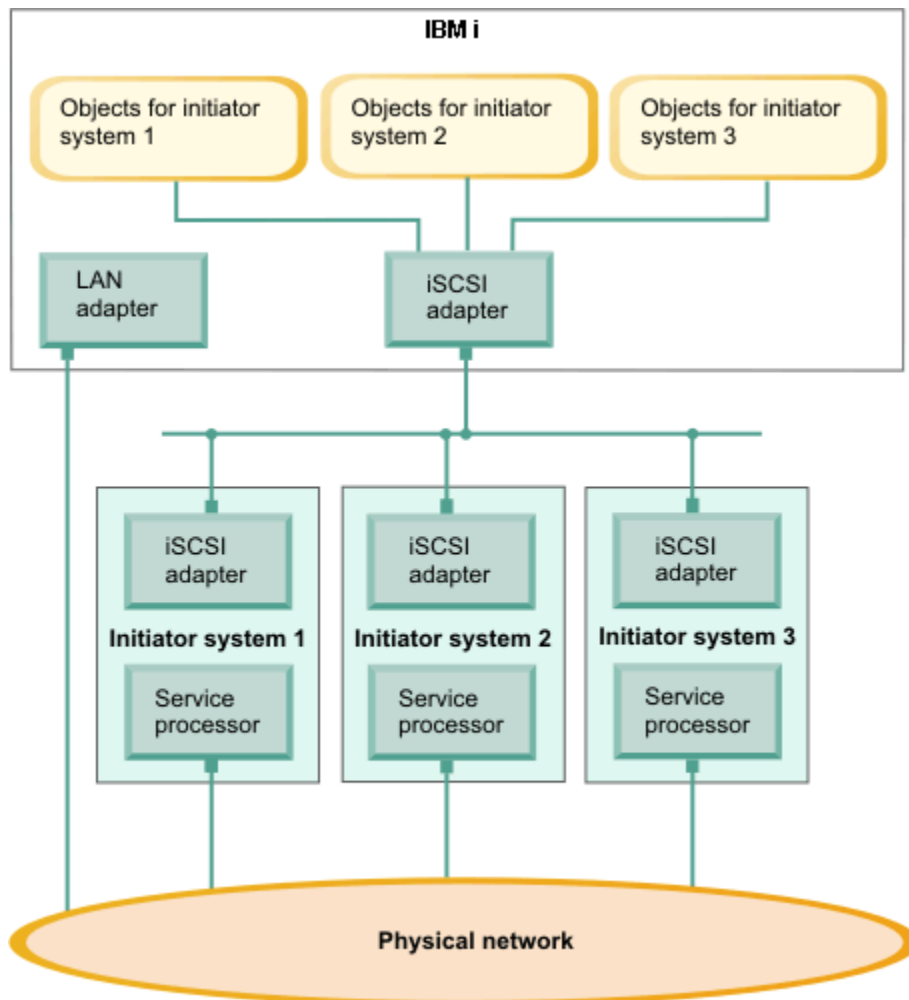


Figure 5 Multiple iSCSI-attached servers

RZAHQ502-4

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

You must install an iSCSI initiator adapter in each hosted System x or blade server. The iSCSI initiator adapters are connected by an Ethernet network. This network can be a physically secure or isolated network when a physically secure model is implemented. Each initiator system is represented by a set of IBM i objects. See [IBM i configuration objects for integrated servers](#).

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

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

**Related information:**

- [Blade server models](#)
- [System x server models](#)
- [Power Server IBM i iSCSI target support](#)
- [IBM i iSCSI targets](#)
- [IBM i configuration objects for integrated servers](#)

### 3.2.4 Integrated server service processor connection

IBM i uses the **Service Processor Manager** function of IBM i **Integrated Server Support** to connect to integrated System x or BladeCenter server hardware on the network, to turn the server hardware on and off, and to retrieve power status.

The integrated server hardware is identified by information stored in the remote system configuration and the service processor configuration in IBM i.

This is a different connection than the iSCSI network connection between the IBM i iSCSI target adapter and the iSCSI initiator adapter in the integrated server. The LAN adapter for the service processor of the integrated server must be attached to a network that is reachable by an IBM i LAN adapter.

Both the IBM i objects and the integrated server service processor must be configured. You configure the connection options in the IBM i network server configuration objects.

**Note:** With IBM i 5.4 and 6.1, **IBM Systems Director** was originally used for integrated server discovery and power control. However, the IBM Director version (5.20) that is available on i 5.4 and i 6.1 systems does not support newer System x and BladeCenter blade server models, so the **Service Processor Manager** function must be used for integrated server discovery and power control if you have a newer integrated server model. When using Service Processor Manager, most customers do not need to run an IBM Director server in their IBM i partition. Tasks described in this document assume that Service Processor Manager is used.

**Related information:**

- [IBM i configuration objects for integrated servers](#)
- [Configuring IBM i to use Service Processor Manager on i 6.1 and i 5.4](#)

### 3.2.5 Booting over the iSCSI network

iSCSI-attached integrated server hardware is diskless. Integrated servers that run ESXi Embedded boot from flash memory, so they do not boot over the iSCSI network. However, all other integrated server operating systems use the iSCSI network to boot, and the boot device is a port configured on the iSCSI initiator adapter installed in the System x or blade hardware.

Both the IBM i remote system configuration and the iSCSI initiator adapter must be configured before you install or use a new integrated server. See [IBM i configuration objects for integrated servers](#).

#### Boot modes and parameters

Boot parameters for an iSCSI initiator are configured with an iSCSI initiator configuration function. Boot parameter values, such as the initiator and target IP address and IQN values, must match the values in the IBM i remote system configuration (RMTSYS) and network server description (NWSD). The parameters vary depending on the selected boot mode.

You can use either dynamic or manual addressing to deploy iSCSI initiator configuration values.

Addressing Method	Description
<b>Dynamic</b> (Recommended)	<p>You can use dynamic addressing for most environments. This method requires fewer manual configuration steps and allows some configuration information to be automatically generated, such as iSCSI qualified names (IQNs).</p> <p>When the NWSD is varied on, an <a href="#">Integrated iSCSI DHCP server</a> in IBM i automatically deploys the target and initiator IP address and IQN values (configured in the RMTSYS and NWSD objects) to the integrated server.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"><li>1. Dynamic addressing does not require a general purpose DHCP server in your network.</li><li>2. The integrated iSCSI DHCP server is only used to deploy iSCSI boot parameters to iSCSI initiators. It is not a general purpose DHCP server, so it will <b>not</b> provide IP addresses to other systems in the network and it will <b>not</b> interfere with other DHCP servers in the network.</li></ol>
<b>Manual</b>	<p><b>Attention:</b> You should <b>not</b> use manual addressing unless you run into problems when using the dynamic method.</p> <p>If you use manual addressing method, you will need to specify significantly more parameters when configuring the iSCSI initiator.</p> <p>Also, with manual addressing some integrated server functions are more difficult to implement, such as the integrated server hot spare capability.</p>

See [Configure the iSCSI initiator](#) to configure the iSCSI initiator port as the iSCSI boot device.

#### Enabling the hosted server boot device

The iSCSI initiator adapter installed in the System x or blade hardware acts as a boot device during the boot process, based on the configured parameters. You must configure at least one port on an iSCSI initiator adapter as a boot device, unless you are using an embedded version of ESXi.

#### Related information:

➤ [IBM i configuration objects for integrated servers](#)

➤ [Integrated iSCSI DHCP server](#)

### 3.3 IBM i configuration objects for integrated servers

IBM i uses objects to represent and control integrated server hardware, software, and virtual storage.

The following figure shows the objects that IBM i uses to configure iSCSI-attached integrated servers.

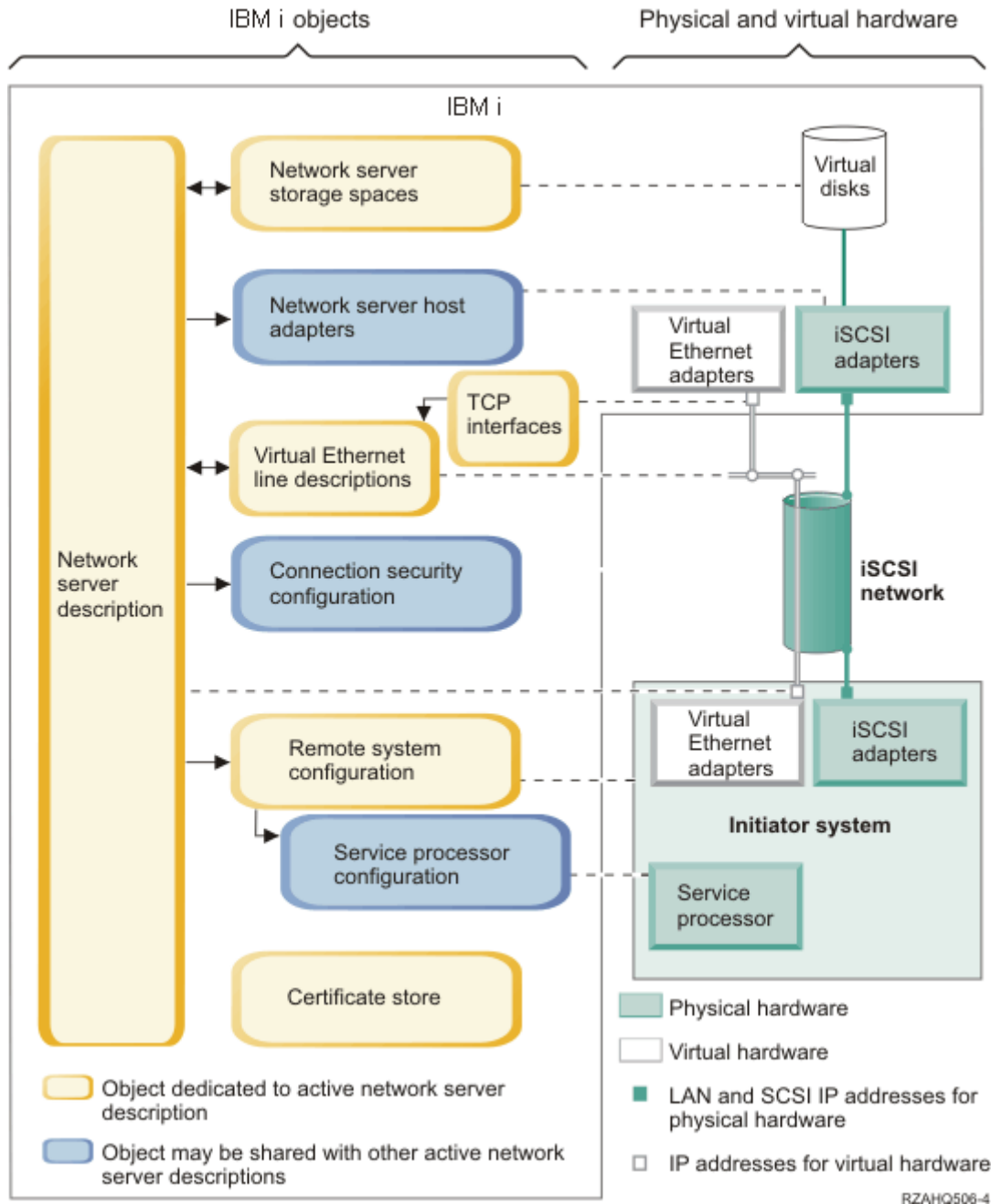


Figure 6: iSCSI configuration objects in IBM i

The key IBM i objects for iSCSI-attached servers are described below:

Objects	Description
Network server description (NWSD)	<p>An IBM i network server description (IBM i object type *NWSD) is the main configuration object for an integrated server.</p> <ul style="list-style-type: none"> <li>It contains a reference to a remote system configuration.</li> </ul> <p><b>Note:</b> In case of an integrated server hardware failure, you can change the remote system configuration name that is specified in the NWSD and restart the server using spare hardware. See <a href="#">Hot spare support for integrated servers</a>.</p> <ul style="list-style-type: none"> <li>It contains references to the iSCSI (storage) data paths for the integrated server. You can define one or more storage paths. These storage paths reference the network server host adapter (NWSH) objects that are associated with the iSCSI target adapters that are used by the integrated server. You can choose which storage path is used for the SCSI data flows for each virtual disk drive. By associating your virtual disk drives with different storage paths, you can spread the overall server SCSI data flow workload across the storage path iSCSI target adapters for greater bandwidth. See <a href="#">Multipath I/O (MPIO)</a>.</li> <li>It contains references to the virtual Ethernet data paths for the integrated server. You can define one or more virtual Ethernet paths. These virtual Ethernet paths also reference the NWSH objects that are used by the integrated server. You can choose which NWSH is used for each virtual Ethernet port that the integrated server uses. By associating different virtual Ethernet ports with different NWSHs, you can spread the overall server virtual Ethernet data flow workload across the virtual Ethernet path iSCSI target adapters for greater bandwidth.</li> </ul> <p>The iSCSI-attached System x or BladeCenter hardware is controlled by IBM i.</p> <ul style="list-style-type: none"> <li>You can <b>power on</b> the integrated server hardware and boot the server operating system by starting (varying on) the associated IBM i NWSD.</li> <li>You can <b>shut down</b> the integrated server operating system and power off the integrated server hardware by shutting down (varying off) the associated IBM i NWSD.</li> <li>IBM i uses an Ethernet network to communicate with the service processor for the System x hardware or the BladeCenter management module for a BladeCenter server to perform the start and shut down tasks.</li> </ul>
Network server host adapters (NWSH)	<p>An IBM i network server host adapter device description (IBM i object type *DEVD, subtype *NWSH) represents the iSCSI target adapter that is used by the IBM i side of the iSCSI connection.</p> <ul style="list-style-type: none"> <li>It identifies the iSCSI target adapter port. <ul style="list-style-type: none"> <li>For a hardware target (iSCSI HBA), it identifies the IBM i Network Server Host Port resource name (for example, CMNxx) for the iSCSI HBA port.</li> <li>For a software target (Ethernet NIC), the NWSH uses a virtual port and also identifies the IBM i TCP/IP interface that is associated with the line description for the Ethernet NIC port.</li> </ul> </li> <li>It defines how communications errors are logged and communications recovery information.</li> </ul>

Objects	Description
	<ul style="list-style-type: none"> <li>• It defines the IP addresses, ports, and so on, for the SCSI and LAN interfaces on the iSCSI target adapter.</li> </ul> <p>IBM i can have multiple iSCSI target adapters. Each port on an iSCSI target adapter has an associated NWSH object.</p> <ul style="list-style-type: none"> <li>• Each NWSH can be shared by multiple integrated servers. In configurations where bandwidth is not a concern, this results in a lower-cost solution.</li> <li>• Each integrated server can use multiple NWSHs. Multiple NWSHs allow multiple SCSI and virtual Ethernet data paths between IBM i and the System x or blade system. Multiple NWSHs can provide greater bandwidth and connection redundancy.</li> </ul> <p>Starting and stopping iSCSI target adapters.</p> <ul style="list-style-type: none"> <li>• An iSCSI target adapter is started and stopped using the NWSH for that iSCSI target adapter.</li> <li>• Alternatively, a software target (Ethernet NIC) can be started and stopped using the TCP/IP interface that is associated with the NWSH. The NWSH and the associated TCP/IP interface are started and stopped together.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Do <b>not</b> use the same TCP/IP interface for multiple NWSHs. Only one NWSH that uses a particular TCP/IP interface can be active at a time.</li> <li>• When starting a software target, the associated line description (LIND) is also started. However, when stopping a software target, the associated LIND remains active.</li> </ul>
Remote system configuration (RMTSYS)	<p>An IBM i remote system network server configuration (IBM i object type *NWSCFG, subtype *RMTSYS) contains information that identifies the System x or BladeCenter blade server hardware to IBM i.</p> <ul style="list-style-type: none"> <li>• It identifies the server hardware.</li> <li>• It contains configuration information for the iSCSI initiator adapters that are used by the System x or blade hardware.</li> <li>• It contains values required to boot the server.</li> <li>• It contains a reference to the service processor NWSCFG object that is used to control the System x or blade hardware.</li> <li>• It contains challenge handshake authentication protocol (CHAP) configuration values that are used to authenticate the remote system when it initially accesses storage.</li> </ul> <p>The System x or blade server can have multiple iSCSI initiator adapters. Multiple iSCSI initiators allow multiple SCSI and virtual Ethernet data paths between IBM i and the System x or blade hardware. Multiple iSCSI initiators can provide greater bandwidth and connection redundancy.</p>



Objects	Description
	<p>The remote system configuration for an integrated server is referenced from the NWSD.</p>
<p>Service processor configuration (SRVPRC)</p>	<p>An IBM i service processor network server configuration (IBM i object type *NWSCFG, subtype *SRVPRC) represents the System x service processor or the BladeCenter management module.</p> <p>The service processor configuration contains the following information:</p> <ul style="list-style-type: none"> <li>• It identifies the service processor or management module hardware by serial number and type and model.</li> <li>• It defines how to find the service processor or management module on the Ethernet network using an IP address or host name.</li> <li>• It contains a service processor user name and password that are used to sign on to the service processor.</li> </ul> <p><b>Note:</b> For a System x server, there is a one-to-one relationship between the service processor configuration and the remote system configuration. The service processor controls only one System x server. However, for BladeCenter systems, there can be a one-to-many relationship between the service processor configuration and the remote system configuration. Each management module can control any of the BladeCenter systems that are contained within the BladeCenter chassis. Therefore, with iSCSI-attached BladeCenter blade servers it is common for several remote system configurations to share (refer to) the same service processor configuration.</p>
<p>Connection security configuration (CNNSEC)</p>	<p>An IBM i connection security network server configuration (IBM i object type *NWSCFG, subtype *CNNSEC) is used by the system.</p> <ul style="list-style-type: none"> <li>• For i 7.2 and 7.1, the integrated server installation process normally creates a default connection security configuration named QCNNSEC that is shared by all integrated servers on the IBM i system.</li> <li>• For i 6.1 and 5.4, the user must create a connection security configuration named QCNNSEC that is shared by all integrated servers on the IBM i system.</li> </ul>
<p>Certificate stores</p>	<p>IBM i certificates are used to secure communications between IBM i and the initiator system for various functions. The certificates are kept in a certificate store that is associated with the network server description. This certificate store is created and maintained automatically for you. It is used to store certificates that are generated and used internally by the IBM i Integrated Server Support. For example, certificates that are used when enrolling users to the hosted system. The certificates in this certificate store are used only when communicating with hosted systems that use the corresponding network server description.</p>
<p>Network server storage spaces (NWSSTG) (virtual storage)</p>	<p>An IBM i network server storage space (NWSSTG) represents a virtual disk drive (virtual storage) for an integrated server. Virtual storage can vary in size from 1 MB to 1000 GB each. Up to 64 virtual storage spaces can be linked to a server, depending on the server configuration. The storage capacity of an integrated server can range from several gigabytes to many terabytes. The virtual storage spaces 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.</p> <p>Each server has up to two virtual disk drives that are automatically created by the server installation process. Each server can also have many user-defined virtual</p>

Objects	Description
	<p>disk drives.</p> <ul style="list-style-type: none"> <li>• The system drive (typically the C: drive for Windows servers) contains the integrated server operating system (such as Windows Server or VMware ESX Server).</li> <li>• The install drive (typically the D: drive for Windows servers), if present, is used every time the server is started to pass configuration information from IBM i to the server. It also contains the IBM i Integrated Server Support code that runs on the integrated server. For Windows Server 2003 servers, the installation drive also contains a copy of the Windows server installation media.</li> <li>• Additional user defined drives are typically used for server applications and data.</li> <li>• When linking the virtual disk drive to the NWSD, it is necessary to identify which of the NWSD storage paths to use for the SCSI data flows for that virtual disk drive. You can choose a specific storage path, the multipath group or let the default storage path be used.</li> </ul> <p>The actual disk storage for the virtual disks is allocated from the IBM i integrated file system. The virtual disk drives can be allocated from the default system storage pool (also known as the system auxiliary storage pool, or system ASP), from a user defined storage pool, or from an independent storage pool (independent ASP).</p> <p>See <a href="#">Storage management for integrated servers</a> for more information about virtual storage.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. Since virtual disks are objects in the IBM i integrated file system, an entire virtual disk drive image can be backed up and restored using the IBM i <a href="#">Save (SAV)</a> and <a href="#">Restore (RST)</a> commands. You can also do a file-level backup for the Windows operating system. For more information, see <a href="#">Backing up and recovering integrated servers</a>.</li> <li>2. Even though storage spaces are allocated out of the integrated file system, storage operations are not performed by IFS while the integrated server is varied on. Therefore, operations like journaling are not enabled.</li> </ol>

**Related information:**

- [Viewing or changing integrated server configuration information](#)
- [Managing storage for integrated servers](#)
- [Managing network server host adapters](#)
- [Managing remote system configurations](#)
- [Managing service processor configurations](#)
- [What objects to save and their location on IBM i](#)
- [Backing up the NWSD and other objects associated with integrated servers](#)
- [Restoring the NWSD and other objects associated with integrated servers](#)

### 3.4 Server management for integrated servers

#### 3.4.1 IBM i management interfaces

You can manage IBM i integration features using GUI or CL command user interfaces.

User Interface	Description
IBM Navigator for i (Web GUI)	<p>The <b>Web GUI</b> provides convenient access to management tasks from supported Web browsers without requiring that the user install special software on their PC. The Web GUI is included with IBM i 6.1, i 7.1 and i 7.2.</p> <p>To launch the <b>IBM Navigator for i</b> Web GUI, use URL:</p> <p style="text-align: center;"><a href="https://Ibmhostname:2005/ibm/console/logon.jsp">https://Ibmhostname:2005/ibm/console/logon.jsp</a></p> <p>where <i>Ibmhostname</i> is your IBM i system host name or IP address.</p> <p><b>Note:</b> The Web GUI includes tasks that are not in the System i Navigator client GUI.</p>
System i Navigator (Client GUI)	<p><b>System i Navigator</b> is a no-charge feature of System i Access for Windows.</p> <p>System i Access must be installed on a Windows PC, including at least the following System i Navigator components:</p> <ul style="list-style-type: none"> <li>• <b>Integrated Server Administration</b></li> </ul> <p>In addition, the following System i Navigator components might be useful when managing integrated servers:</p> <ul style="list-style-type: none"> <li>• Basic Operations</li> <li>• Work Management</li> <li>• Configuration and Service</li> <li>• Network</li> <li>• Users and Groups</li> </ul> <p>System i Navigator is launched from the Windows PC that it is installed on.</p> <p><b>Attention:</b> You should use the <a href="#">Web GUI</a> with i 7.2, 7.1 and 6.1 systems. The System i Navigator client GUI does <b>not</b> provide full support for integrated servers on IBM i 7.2, 7.1 and 6.1 systems. Most notably, software target network server host adapters and VMware ESX servers are not fully supported in System i Navigator.</p>
IBM i control language (CL) commands	<p>A set of <b>IBM i CL commands</b> is provided for integrated server management. The CL commands are included with IBM i.</p>

**Note:** Most integrated server management tasks in this document are described using the appropriate GUI, but links to the corresponding CL commands are also provided.

### 3.4.2 Additional management interfaces

You can use non-IBM i user interfaces to help manage your integrated servers.

User Interface	Description
IBM Systems Director	<p>IBM Systems Director, an integral component of IBM's Smarter Systems portfolio, provides systems management personnel with a single-point-of-control, helping reduce IT management complexity and cost. With IBM Systems Director, IT personnel are able to optimize compute and network resources, quickly respond to business requirements with greater delivery flexibility, and attain higher levels of services management with streamlined management of - physical, virtual, storage and network resources.</p> <p><b>Note:</b> The IBM i <a href="#">Web GUI</a> can be used from within the IBM Systems Director Web GUI. To access the IBM i <a href="#">Web GUI</a> from within IBM Systems Director, navigate to an IBM i system and then select the <b>IBM i management</b> task for that system.</p>
System x or BladeCenter service processor Web interface	<p>System x and BladeCenter service processors (except for a System x BMC service processor) support a Web interface for performing server management tasks.</p> <p>This Web interface is launched by simply typing the System x or BladeCenter service processor host name or IP address in your Web browser address field. Then you sign on to the Web interface and perform tasks as needed.</p> <p><b>Note:</b> The IBM i <a href="#">Web GUI</a> can also be used to launch the Web interface for a System x and BladeCenter service processor. Simply select the <b>Launch Web console</b> task from the appropriate server, remote system configuration, or service processor configuration object in the IBM i <a href="#">Web GUI</a>.</p>

**Related information:**

- [IBM Systems Director](#)
- [Launching the Web console for an integrated server](#)
- [Launching the Web console for a remote system](#)
- [Launching the Web console for a service processor](#)

### 3.4.3 Integrated server installation

When you install an integrated server, parts of the installation process are performed on IBM i and parts of the installation process are performed on the integrated server console. For example, IBM i creates configuration objects and virtual storage for the server and starts the server. Then you install the integrated server operating system from the integrated server console. Unlike a stand-alone server, the integrated server installation process is initiated from IBM i, rather than at the server console. You must also perform some other tasks both before and after the integrated server operating system is installed. See the [Server installation road map and checklist](#) for the entire process.

The [BladeCenter](#) or [System x iSCSI Installation Overview](#) Flash animation provides an overview of the iSCSI-attached server installation process. It also provides a conceptual overview of the various hardware and software components and shows how they work together in the IBM i iSCSI solution.

### 3.4.4 Integrated server cloning

With **IBM i 7.2, 7.1 and 6.1**, you can clone an existing integrated Windows server. This makes it easy to deploy multiple integrated Windows servers that support similar application environments and workloads.

When you clone an existing integrated Windows server, parts of the installation process is performed on IBM i and parts of the installation process are performed on the integrated server console. For example, you prepare the server for cloning from the Windows console, then you use an IBM i GUI cloning wizard to duplicate the IBM i configuration objects and virtual storage for the server, then you perform some final setup on the clone server to get it ready for production use. See the [Server cloning road map and checklist](#) for the entire process.

Concepts for cloning integrated Windows servers:

Concept	Description
Base NWSD (Base Server)	<p>The base NWSD (network server description) is the IBM i configuration object that represents the IBM i iSCSI-attached integrated server (base server) that will be cloned to deploy a new IBM i iSCSI-attached integrated server.</p> <p><b>Note:</b> Use the base server <b>only</b> as a template for cloning new servers. The base server should <b>not</b> be a production server.</p>
Clone Server	<p>The clone server is a copy of the base server. Objects copied include the base server IBM i configuration objects (NWSD, LINDs, TCP interfaces, etc.) and virtual storage.</p>
Base NWSD Requirements	<p><b>Base NWSD Types:</b></p> <p>The base NWSD must have a NWSD type of <b>*ISCSI</b>, with server operating system type <b>*WIN64</b> (for Windows Server 2008 and Windows Server 2012) or <b>*WIN32</b> (for Windows Server 2003).</p> <p><b>Software Installed on the Base Server:</b></p> <p><b>Windows Server 2012, Windows Server 2008 R2, Windows Server 2008, Windows Server 2003 R2 or Windows Server 2003</b> must already be installed on the base server. The specific Windows versions supported on servers attached to IBM i using iSCSI are listed in the <a href="#">Integrated Server Operating System (Server OS) Versions</a> section.</p> <p><b>Important:</b> Some Windows components <u>cannot</u> be cloned (for example, Active Directory). See the Microsoft TechNet articles referenced in the <a href="#">Microsoft System Preparation Tool (Sysprep)</a> concept below for more information.</p> <p><b>Other Software</b> and data can optionally be installed on the base server in addition to the server operating system.</p> <p><b>Important:</b> Some software products do <u>not</u> support cloning. Ensure that all software installed on the base server is enabled for cloning.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. The cloning process requires that the <b>Sysprep</b> tool (see below) is run on the base server. After sysprep is run, the base server is shut down and you should</li> </ol>

Concept	Description
	<p>then use the base server <u>only</u> as a template for cloning new servers. The base server should <u>not</u> be a production server.</p> <p>2. If a base NWSD that meets the above requirements is not available, then a new server cannot be created using the cloning process. Instead, use the normal server installation process and follow the <a href="#">Installation Checklist</a>.</p>
<p>Microsoft System Preparation Tool (Sysprep)</p>	<p>A tool called <b>sysprep</b> is used to reset key attributes of a Windows server, such as the system security ID (SID), so that it can be cloned. For detailed information on sysprep, see the Microsoft <a href="#">Sysprep Technical Reference</a> TechNet articles, and in particular, see the <a href="#">What is Sysprep?</a> article.</p> <p><b>Important:</b></p> <ul style="list-style-type: none"> <li>• Failure to use sysprep prior to cloning a Windows server might result in a server that does not start, does not function properly, or does not meet Microsoft licensing requirements.</li> <li>• Sysprep has restrictions on server roles, server components that are installed (for example, Active Directory), encrypted files and other items. For details, see the referenced TechNet articles. Ensure that the base server meets these restrictions before using sysprep.</li> <li>• Normally, once sysprep is run on the base server, the base server is shut down and you should then use the base server <u>only</u> as a template for cloning new servers.</li> </ul> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. The TechNet articles referenced above are for Windows 7, but also apply to Windows Server 2012 and Windows Server 2008 R2. Similar TechNet articles are available for Windows Vista (which also apply to Windows Server 2012 and Windows Server 2008) and Windows XP (which also apply to Windows Server 2003 and Windows Server 2003 R2).</li> <li>2. The sysprep documentation refers to <b>disk-imaging software</b> that is used to create binary images of the source computer disks. For the IBM i integrated server cloning process described in this document, there is no need to manually create a disk image after running sysprep. The IBM i virtual storage for the base server <u>is</u> the disk image. When the cloning Wizard is run, binary copies of the base server's virtual storage are automatically created for the clone server.</li> <li>3. A Mini-Setup runs when starting a clone server and system attributes such as the system security ID (SID) are regenerated.</li> </ol>
<p>Software Licenses</p>	<p><b>Important:</b></p> <ul style="list-style-type: none"> <li>• The user of the integrated server cloning support described in this document is responsible for complying with the licensing requirements for all software that is installed on the base server and copied to the clone server.</li> <li>• Check the licensing terms for all software that is installed on the base</li> </ul>

Concept	Description
	<p>server and prepare to comply with those licensing requirements <u>before</u> cloning the base server.</p> <p>For example, unless a volume license is used, the base server and the clone server typically require unique license keys for the Windows operating system and possibly for other software that is installed on the servers. Obtain any additional license keys that are needed <u>before</u> cloning the base server.</p>
Compatible Server Hardware	<p>When cloning a server, the clone server typically uses different server hardware (BladeCenter blade or System x server) than the base server.</p> <p>Server hardware is identified by a type-model number of the format TTTT-MMM, where TTTT is the type number and MMM is the model number. For example, one type-model number for a HX5 blade server is 7872-42Y.</p> <p>The BladeCenter blade or System x server hardware that is used for the clone server must have the <b>same type number</b> (TTTT) that was used for the base server. Note that the model number (MMM) does not need to match between the base and clone servers.</p> <p>For example, if the base server runs on an HX5 (7872) blade, then the clone server must also run on an HX5 (7872) blade. However, it does not matter if the two servers have different model numbers (for example 7872-42Y and 7872-61Y).</p> <p>In addition, the BladeCenter blade or System x models must have a similar configuration of adapters (iSCSI initiators, Ethernet NICs, etc.). In particular, the iSCSI initiator adapters used (iSCSI HBAs or Ethernet NICs) must be consistent between the two servers.</p> <p><b>Note:</b> The BladeCenter blade or System x server hardware is represented on IBM i with a remote system network server configuration (IBM i object type *NWSCFG, with subtype *RMTSYS). When you run the cloning Wizard, you will identify the server hardware to use for the clone server by selecting a previously configured IBM i remote system configuration.</p>
Cloning Wizard	<p>A Wizard is provided in the IBM Navigator for i <a href="#">Web GUI</a> to clone integrated servers.</p> <p>There are several methods to launch the cloning Wizard. The two most common methods to launch the cloning Wizard are as follows:</p> <ol style="list-style-type: none"> <li>1. Select the <b>Create Server</b> task from the <b>Integrated Server Administration</b> welcome page. Then select a base NWSD and click <b>Continue</b> to launch the cloning Wizard.</li> <li>2. Display the <b>Servers</b> list from the <b>Integrated Server Administration</b> welcome page. Then select a base NWSD from the list and click the <b>New Based On...</b> action to launch the cloning Wizard.</li> </ol> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• The cloning Wizard is <u>not</u> provided in the <a href="#">System i Navigator</a> client GUI.</li> <li>• An IBM i command line interface for cloning integrated servers is <u>not</u> provided.</li> </ul>

**Related information:**

- [Server cloning road map and checklist](#)

### 3.4.5 Integrated server management infrastructure

The IBM i management infrastructure for integrated servers varies based on the IBM i release and the server operating system (OS). See the following subsections for each type of server OS.

#### 3.4.5.1 Integrated Windows server management infrastructure

The IBM i management infrastructure for integrated Windows servers has the following key pieces:

Piece	Description
IBM i software	Most of the software for installing and managing an integrated server runs on IBM i. This software consists of IBM i base operating system functions and various IBM i options, such as Integrated Server Support (IBM i option 29). The IBM i software enables integrated server installation, IBM i configuration object management, virtual storage management, and much more. See <a href="#">IBM i products and options</a> .
IBM i configuration objects	On the IBM i side of server management, an integrated server is represented by a network server description (NWSD) and several other types of configuration objects. Among other things, you can stop and restart the server from IBM i by varying the NWSD off and on. See <a href="#">IBM i configuration objects for integrated servers</a> .
Integrated Windows server	The Windows Server 2012, Windows Server 2008 or Windows Server 2003 server that is integrated with IBM i.
Windows services	Windows services are used to perform many of the integration tasks for integrated Windows server. See <a href="#">Windows services for IBM i integration with Windows servers</a> .
Windows utilities	Windows utilities are used to access shared IBM i tape and optical devices. Windows utilities are also used to maintain the Integrated Server Support software that runs on the integrated Windows server. See <a href="#">Windows utilities for IBM i integration with Windows servers</a> .
QAS400NT user profile	This IBM i user profile is used when performing integrated Windows server administration tasks. See <a href="#">QAS400NT user and integrated Windows servers</a> .

##### 3.4.5.1.1 Windows services for IBM i integration with Windows servers

Some of the programs that provide the IBM i Integrated Server Support features are installed as Windows services that run on the integrated Windows server. The following Windows services are provided for integrated Windows server management:

Windows Service	Description
IBM i Integration Manager	Manages integrated server startup and shut down operations.
IBM i Shutdown Manager	Enables system shutdown from IBM i over the iSCSI network. <b>Important:</b> If this service is stopped, the computer might not respond to a shutdown request from IBM i, which might result in data corruption.
IBM i Administration	Supports the following functions:



Windows Service	Description
	<ol style="list-style-type: none"> <li>1. User enrollment. See <a href="#">User and group enrollment concepts for integrated Windows servers</a>.</li> <li>2. Windows event logs can be propagated to an IBM i message queue or job log. IBM i administrators can view the Windows event log entries from IBM i. The event logs to propagate and the destination for the event log entries are controlled by attributes stored in the network server description (NWSD).</li> <li>3. Retrieve the integrated server CPU statistics (for example, CPU percent) and show it on IBM i management interfaces (for example, in the IBM i Web GUI).</li> <li>4. Retrieve the integrated server disk statistics (for example, percent full) and show them on IBM i management interfaces (for example, in the IBM i Web GUI).</li> <li>5. Retrieve the integrated server operating system name and version and show them on IBM i management interfaces (for example, in the IBM i Web GUI).</li> </ol>
IBM i Remote Command	You can use IBM i to remotely submit integrated Windows server batch commands. Windows server commands that can run in batch mode without user interaction will work. See <a href="#">Running integrated Windows server commands remotely</a> .
IBM i Virtual Ethernet Manager	<p>Manages the connection status (link state) for iSCSI-based virtual Ethernet network adapters.</p> <p><b>Note:</b> If this service is stopped, the computer does not respond to any virtual Ethernet link state changes.</p>

**Related information:**

➤ [IBM i configuration objects for integrated servers](#)

### 3.4.5.1.2 Windows utilities for IBM i integration with Windows servers

Some of the utilities that provide the IBM i Integrated Server Support features are installed on the integrated Windows server. The following Windows utilities are provided:

Utility	Description
IBM i post-install utility for Windows Server 2012 or Windows Server 2008 (ibmsetup.exe)	<p>This utility is used to install Integrated Server Support on an integrated Windows Server 2012 or Windows Server 2008 server.</p> <p><b>Note:</b> Integrated Server Support is automatically installed on integrated Windows Server 2003 servers, so there is no equivalent utility for integrated Windows Server 2003 servers.</p>
Software Level (lv1sync.exe)	<p>View the level of IBM i Integrated Server Support software that is installed on IBM i and on the integrated Windows server. Optionally synchronize the Integrated Server Support software from IBM i to the integrated Windows server.</p> <p><b>Note:</b> This utility is provided in a Microsoft Management Console (MMC) plug-</p>

Utility	Description
	in named <b>IBM i Integrated Server Support</b> . You can also run it as a Windows command. Run: <code>lvlsync</code>
i5/OS Devices (as400dev.exe)	View the IBM i (i5/OS) tape and optical devices that can be shared with the integrated Windows server. Lock (allocate) an IBM i device so that it can be used by the integrated Windows server. Unlock (deallocate) the IBM i device when it is no longer needed by the integrated Windows server.  <b>Note:</b> This utility is provided in a Microsoft Management Console (MMC) plug-in named <b>IBM i Integrated Server Support</b> . You can also run it as a Windows command. To see the parameters, run: <code>as400dev /help</code>
View iSCSI initiator allocation (qvnimap.exe)	You can use the <code>qvnimap</code> command to display how iSCSI initiators are being used for a particular Windows server. The output consists of several tables.  To use this utility, see <a href="#">Display information about iSCSI initiator allocation</a> .
Display virtual Ethernet information (qvndvimir.exe)	Used to display information, such as UDP port numbers, for virtual Ethernet adapters on a particular Windows server.  To use this utility, see <a href="#">Display information about virtual Ethernet adapters</a> .

**Related information:**

- [IBM i configuration objects for integrated servers](#)

### 3.4.5.2 Integrated VMware ESX server management infrastructure

Depending on your IBM i version and the VMware ESX version you are using, there are two infrastructures that could be used for IBM i Integrated Server Support to administer VMware ESX servers, as described below.

Infrastructure	Description
Management server based infrastructure	This infrastructure requires an iSCSI-attached integrated Windows server to manage the administrative communication between IBM i and the VMware ESX server. This solution is available for ESX 4 or later servers when attached to IBM i 6.1 or later.  The management server based infrastructure provides the following benefits: <ul style="list-style-type: none"> <li>• Provides the ability to shut down VMware ESX servers from IBM i.</li> <li>• Dynamically linked storage spaces are automatically recognized by the ESX server.</li> <li>• VMware ESX server statistics (operating system version, build number, etc.) and status (Started, Shut down, etc.) are shown in IBM i management interfaces.</li> </ul> <b>Note:</b> Support for VMware ESXi versions require that this infrastructure is used.
Service console based infrastructure	This infrastructure requires integrated server programs to be installed on the service console of the VMware ESX server. With this solution, IBM i can communicate directly with the ESX server. This solution is available for ESX 3.x servers when attached to IBM i 5.4 or 6.1 and for ESX 4.0 servers when attached to IBM i 6.1.  The service console based infrastructure provides the following benefits: <ul style="list-style-type: none"> <li>• Provides the ability to shut down VMware ESX servers from IBM i.</li> <li>• Dynamically linked storage spaces are allowed, but manual intervention is</li> </ul>

Infrastructure	Description
	<p>required in order for the linked storage to be recognized by the ESX server.</p> <p><b>Note:</b> VMware ESXi versions do not have a service console partition, so this method cannot be used with ESXi servers.</p>

The IBM i management infrastructure for integrated VMware ESX servers has the following pieces that are common to both management infrastructures:

Piece	Description
IBM i software	<p>Most of the software for installing and managing an integrated server runs on IBM i. This software consists of IBM i base operating system functions and various IBM i options, such as Integrated Server Support (IBM i option 29). The IBM i software enables integrated server installation, IBM i configuration object management, virtual storage management, and much more.</p> <p>See <a href="#">IBM i products and options</a>.</p>
IBM i configuration objects	<p>On the IBM i side of server management, an integrated server is represented by a network server description (NWSD) and several other types of configuration objects. Among other things, you can stop and restart the server from IBM i by varying the NWSD off and on.</p> <p>See <a href="#">IBM i configuration objects for integrated servers</a>.</p>
Integrated VMware ESX server	<p>The VMware ESX server that is integrated with IBM i.</p>

Additional pieces that are used **only** with the [Management server based infrastructure](#):

Piece	Description
ESX platform manager (optional)	<p>Software that manages one or more VMware ESX servers and their virtual servers. VMware vCenter Server is one example of an ESX platform manager.</p>

Piece	Description
Management server (integrated Windows server)	<p>The IBM i Integrated Server Support software does not run directly on the VMware ESX server. Instead, an iSCSI-attached integrated Windows server serves as a management server for the VMware ESX server. IBM i management tasks, such as shutdown and dynamic virtual storage linking, are sent to the management server over the point-to-point virtual Ethernet connection. Then the task is sent from the management server to the integrated VMware ESX server over a physical Ethernet connection. If an ESX platform manager (for example, VMware vCenter) is configured, the task flows from the management server to the platform manager server and then to the VMware ESX server.</p> <p>The supported operating system versions on the iSCSI-attached integrated Windows server are as follows:</p> <ul style="list-style-type: none"> <li>• WIN2012 (see <a href="#">Server OS</a> for specific OS versions)</li> <li>• WIN2008 (see <a href="#">Server OS</a> for specific OS versions)</li> <li>• WIN2003 (see <a href="#">Server OS</a> for specific OS versions)</li> </ul> <p>An integrated Windows server can serve as the management server for any number of integrated VMware ESX servers within the same IBM i logical partition. At least one integrated Windows server is required in each IBM i logical partition that hosts integrated VMware ESX servers.</p> <p><b>Note:</b> Only a small portion of the integrated Windows server capacity is needed to manage integrated VMware ESX servers. The integrated Windows server can be used for other workloads as well.</p>
Windows services	Windows services are used to perform requests initiated from IBM i to integrated VMware ESX servers that are managed from the integrated Windows server. See <a href="#">Windows services for IBM i integration with ESX servers</a> .
Windows utilities	Windows utilities are used to define and manage connection information so that IBM i can manage integrated VMware ESX servers, as well as provide other functions. See <a href="#">Windows utilities for IBM i integration with ESX servers</a> .
QVMWINT user profile	<p>This IBM i user profile is used when performing integrated VMware ESX server administration tasks.</p> <ul style="list-style-type: none"> <li>• QVMWINT is automatically created on IBM i. This profile is initially disabled.</li> <li>• As part of the integrated VMware ESX server installation process, the QVMWINT profile must be enabled and then enrolled to the associated management server. The QVMWINT profile must also be created on either the integrated VMware ESX server or the associated ESX platform manager (if one is used). The QVMWINT user must have Administrator permissions on the management server and the VMware ESX server or ESX platform manager (vCenter) server.</li> <li>• The QVMWINT password must match on IBM i, the integrated Windows server, and the integrated VMware ESX server or the associated ESX platform manager (if one is used). Note that at IBM i password level (QPWDLVL) 0 or 1, the QVMWINT password is converted to all lower case characters when it is set on the integrated Windows server.</li> </ul>

Additional pieces that are used **only** with the [Service console based infrastructure](#):

Piece	Description
ESX service console programs	Some of the programs that provide the IBM i Integrated Server Support features are installed on the VMware ESX server service console. See <a href="#">Service console programs for IBM i integration with ESX servers</a> .

### 3.4.5.2.1 Windows services for IBM i integration with ESX servers

With the [Management server based infrastructure](#), some of the programs that provide the IBM i Integrated Server Support features are installed as Windows services that run on the management server. The following Windows services are provided for integrated VMware ESX server management:

Windows Service	Description
IBM i Virtual Server Administration	Perform requests initiated from IBM i to integrated VMware ESX servers that are managed from the integrated Windows server.  <b>Note:</b> This service uses the connection information that is defined by the <b>IBM i connection utility for virtualization hosts</b> . See <a href="#">Windows utilities for IBM i integration with ESX servers</a> .
Services shared with integrated Windows servers	Several of the Windows services that are used for integrating Windows servers are also used when integrating VMware ESX servers. See <a href="#">Windows services for IBM i integration with Windows servers</a> .

**Related information:**

- [IBM i configuration objects for integrated servers](#)

### 3.4.5.2.2 Windows utilities for IBM i integration with ESX servers

With the [Management server based infrastructure](#), some of the utilities that provide the IBM i Integrated Server Support features are installed on the management server. The following Windows utilities are provided:

Utility	Description
IBM i post-install utility for VMware ESX (ibmvmins.exe)	This utility runs on the integrated Windows server that serves as a management server for the integrated VMware ESX server. It is used to install Integrated Server Support for VMware ESX server.
IBM i connection utility for virtualization hosts (ibvmcon.exe)	This utility runs on the integrated Windows server that serves as a management server for the VMware ESX server. It is used to define and manage connection information so that IBM i can manage integrated VMware ESX servers. Connection information can be added, deleted, listed, verified, and managed from the connection utility.  <b>Note:</b> The connection information is used by the <b>IBM i Virtual Server Administration</b> service to establish connections between the integrated Windows server and the integrated VMware ESX servers that the integrated Windows server manages. See <a href="#">Windows services for IBM i integration with ESX servers</a> .
Software Level (lvlsync.exe)	View the level of IBM i Integrated Server Support software that is installed on IBM i and on the integrated Windows server. Optionally synchronize the Integrated Server Support software from IBM i to the integrated Windows server.  <b>Note:</b> This utility is provided in a Microsoft Management Console (MMC) plug-in named <b>IBM i Integrated Server Support</b> .

**Related information:**

- [IBM i configuration objects for integrated servers](#)

### 3.4.5.2.3 Service console programs for IBM i integration with ESX servers

With the [Service console based infrastructure](#), some of the programs that provide the IBM i Integrated Server Support features are installed on the VMware ESX server service console. The following service console programs are provided:

Program	Description
IBM i post-install utility for VMware ESX (i 6.1: <code>ibmsetup.sh</code> ) (i 5.4: <code>esxsetup.sh</code> )	This utility is used to install Integrated Server Support on an integrated VMware ESX server.
Update IBM i Integration Software Level (i 6.1: <code>ibmlsvupdt</code> ) (i 5.4: <code>ixsupdt</code> )	Update the level of IBM i Integrated Server Support software that is installed on the integrated VMware ESX server to match the level that is installed on IBM i.
Uninstall IBM i Integration Software (i 6.1: <code>ibmunins</code> )	Remove the IBM i Integrated Server Support software that is installed on the ESX service console. Used when migrating from the <a href="#">Service console based infrastructure</a> to the <a href="#">Management server based infrastructure</a> .

**Related information:**

- [IBM i configuration objects for integrated servers](#)

### 3.4.6 Integrated server console

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

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

Method	Description
Directly attached monitor, keyboard, and mouse	You can use a monitor, keyboard, and mouse that are directly connected to the System x or BladeCenter blade server. You interact with the integrated server through these devices exactly as you would with a regular stand-alone server.
Remote GUI desktop application	You can use an application such as Microsoft Terminal Services, Remote Desktop, or another third party application to display the integrated server graphical user interface (GUI) desktop on a remote workstation. Most administration tasks that are normally performed on the server directly attached console can be performed on the remote desktop. See the Microsoft or other third party application documentation for information about how to configure and use a remote desktop for the server console.
System x IMM II, IMM, or RSA II graphical console redirection	For System x servers equipped with an Integrated Management Module II (IMM II), Integrated Management Module (IMM), or Remote Supervisor Adapter II (RSA II) service processor, the service processor provides full hardware-based graphical console redirection. This redirection means that you can use a local desktop to access and control a System x server using a Web browser.
BladeCenter MM or AMM graphical console redirection	A BladeCenter chassis uses either a Management Module (MM) or an Advanced Management Module (AMM) which provides hardware-based graphical console redirection for the blade servers in the chassis. This redirection means that you can use a local desktop to access and control a blade server using a Web browser.

### 3.4.7 Software updates

There are several types of software and firmware updates for integrated servers.

Component	Description
IBM i, and related licensed products	<p>Updates and fixes for the IBM i and related products that provide support for integrated servers are distributed in IBM i program temporary fixes (PTFs).</p> <p>Use the normal IBM i service mechanisms to get, load and apply the PTFs.</p> <p><b>Note:</b> For each IBM i release, IBM provides a group PTF named <b>IBM i integration with BladeCenter and System x</b> that pulls together the required PTFs for the IBM i iSCSI solution.</p>
IBM i Integrated Server Support software that runs on the integrated server	<p>The code fixes to the IBM i integration code that runs on Windows or VMware ESX are in packages called <b>service packs</b>. Service packs are cumulative - the most recent service pack contains all the fixes from prior service packs in addition to new fixes. IBM distributes these service packs in IBM i PTFs.</p> <p>Use the normal IBM i service mechanisms to get, load and apply the service pack PTF on IBM i. Then, you must install or synchronize that service pack from IBM i to the integrated server.</p> <p>When you synchronize an integrated server, there are four things that can happen:</p> <ol style="list-style-type: none"> <li>1. If IBM i has been upgraded to a new release, for example, from i 6.1 to i 7.1, the integration software for the new release replaces that of the old release on the integrated server.</li> <li>2. If a new IBM i Integrated Server Support service pack PTF has been installed on IBM i, it is copied over to the integrated server.</li> <li>3. If an IBM i Integrated Server Support service pack PTF has been removed from IBM i, it is removed from the integrated server as well, and replaced with the integration software currently existing in IBM i.</li> <li>4. If the IBM i integration software and integrated server integration software are at the same level, the synchronization operation can still be performed. This allows for recovery of a deleted or damaged integration software file on the integrated server.</li> </ol> <p>In all cases the integrated server is brought to the same level of integration software which exists in IBM i.</p> <p><b>Note:</b> Server integration fixes can be provided either within a service pack or separate from a service pack. In either case, use the service pack installation process to load the fixes on the integrated server. When a service pack PTF is loaded on the integrated server, the service level will show the service pack PTF number. However, when a fix that is not part of a service pack PTF is loaded on the integrated server, the service level will continue to show the most recent service pack PTF number that has been loaded on the</p>

Component	Description
	<p>integrated server.</p> <p><b>Note:</b> The service packs for the IBM i Integrated Server Support software are separate from the updates for the server operating system itself, which you must get from the operating system provider (for example, get a Windows Server 2008 service pack from Microsoft).</p>
System x or BladeCenter updates	Before installing an integrated server, you must update the firmware for the System x, BladeCenter, and blade hardware, including the iSCSI initiator adaptors that are used.
Integrated server operating system	The operating system that is installed on the integrated server might have updates periodically. Apply any operating system updates using the normal procedures for the operating system.

**Related information:**

- [IBM i products and options](#)
- [IBM i PTFs](#)
- [Service pack PTFs](#)
- [Installing IBM i integration service packs](#)
- [Using Bootable Media Creator \(BoMC\)](#)
- [Firmware updates for the BladeCenter chassis](#)



## 3.5 Storage management for integrated servers

Integrated servers use virtual storage that is managed by IBM i.

### 3.5.1 Virtual storage

Integrated servers use virtual storage provided by IBM i instead of physical disk drives attached to the integrated server hardware.

Operating systems, such as Windows and VMware ESX, work with what they see as physical disk drives; there is little or no virtualization of storage at an operating system level. Because IBM i virtualizes all disk storage, you can use chunks of disk space from an IBM i storage pool to form virtual disk drives, which can then be allocated to the integrated server operating system. These virtual disks are also known as storage spaces or virtual storage. Integrated VMware ESX and Windows servers see these storage spaces as physical disk drives.

The IBM i object that is used to create virtual storage for an integrated server is called a Network Server Storage Space (NWSSTG), or storage space for short. These storage spaces are stored in the IBM i integrated file system (IFS) in a directory called /QFPNWSSTG. You can use the File Systems function of the [Web GUI](#), [System i Navigator](#), or the [Work with Object Links \(WRKLNK\)](#) command from an IBM i command line to view the contents of the /QFPNWSSTG directory. This storage space architecture is used by integrated Windows and VMware ESX servers.

The amount of disk storage that you create for your servers is taken directly from the IBM i available storage, and each virtual disk is physically scattered across the physical disks in the IBM i storage pool. You can create virtual disks as large as 1 TB if there is available storage in the storage pool.

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

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

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

Here is a summary of the operations that you can perform on integrated server virtual storage:

- Create new virtual storage (optionally copying preexisting virtual storage)
- Link virtual storage to an integrated server
- Unlink virtual storage from an integrated server
- Expand virtual storage
- Delete virtual storage

Virtual storage operations can be performed in these ways:

- Using the [Web GUI](#)
- Using [System i Navigator](#)
- Using IBM i CL commands

### 3.5.2 IBM i storage management

Integrated servers use virtual storage (virtual disks) that are managed by IBM i.

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

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

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

#### 3.5.2.1 IBM i and disk drives

The key to understanding how disk storage is allocated to integrated servers is an understanding of how IBM i storage management works. The heart of storage management on IBM i is a technology called single-level storage. Single-level storage is a revolutionary storage management architecture that not only gives IBM i outstanding disk I/O performance, but greatly reduces the amount of administration required. IBM i does not directly manage disk drives. Beneath the operating system a level of software (called Licensed Internal Code) "hides" the disk drives and manages the storage of objects on those disk drives. A virtual address space is mapped over the existing disk space and used for addressing objects rather than disk drive IDs, cylinders, and sectors. Needed objects are copied ("paged in") from this address space on disk into the address space of main memory.

The major features of single-level storage are:

- Storage pools

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

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

To increase the size of the pool, simply add disk drives to IBM i and they automatically become part of the system ASP.

You can create additional storage pools that are called user ASPs and independent ASPs.

- Scattering of data

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

IBM i disk management supports fully parallel disk I/O, which provides outstanding disk I/O performance because each object on the system is accessible by multiple disk arms concurrently. There is no need to be concerned about particular disk drives filling up, or moving data from one disk to another to improve performance because all data management is taken care of by the licensed internal code. Therefore, IBM i does not require a Database Administrator. Licensed internal code also ensures that there is no disk fragmentation.

- Single address space

Memory and disk on IBM i form a single 64-bit address space.

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

Because of the way IBM i 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 sends and receives disk data to and from the IBM i storage management subsystem. IBM i storage management handles the hard disks, including spreading the integrated server disk drive images across multiple hard disk drives and applying RAID and file mirroring (if configured). Disk defragmentation software manages logical file fragmentation of the hard disk images. Because IBM i 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.

### 3.5.2.2 Storage pools (ASPs)

In IBM i, 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 storage pool, and the new storage space will be available immediately. Every system has at least one storage pool, the system storage pool. The system storage pool is always ASP 1. You can configure additional user storage pools, numbered 2 - 255. You can use storage pools to distribute your IBM i 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.

### 3.5.2.3 Disk protection

Integrated servers that use IBM i virtual storage implicitly take advantage of superior data protection schemes which exist in IBM i such as RAID or drive mirroring.

IBM i disks can be protected in these ways:

Disk Protection	Description
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 on the other disks. When you replace a failing disk with a new one, IBM i can rebuild the information from the failed disk on the new (and therefore empty) disk.
Mirroring	<p>Mirroring keeps two copies of data on two different disks. IBM i 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, IBM i uses information from the second disk. When you replace the failing disk, IBM i copies the data from the intact disk to the new disk.</p> <p>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 Power server models, you can attach controllers to more than one bus. Attaching the two disk controllers that form a mirrored pair to two different buses increases availability even more.</p>
Cross-site mirroring	Cross-site mirroring, using the operating system geographic mirroring function for independent ASPs, mirrors data on disks at sites that can be separated by a significant distance.

You can define storage pools on IBM i to have different levels of protection or no protection at all. Then you can put applications and data into a storage pool with the right amount of protection, depending on how important their availability is. For more information about IBM i disk protection and availability options, see the [Recovering your system](#) topic collection in the IBM i Information Center.

### 3.5.3 Predefined virtual storage and naming

With the exception of embedded versions of VMware ESX, predefined virtual storage (virtual disk drives) are automatically created when you install the integrated server operating system. The system uses this virtual storage for the integrated server support code and the operating system.

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

The predefined disk naming convention and how they are used by the various integrated server operating systems are shown in the table below:

Predefined Disk	Naming Convention	Description	Server OS	IBM i			
				i7.2	i7.1	i6.1	i5.4
System (boot) Drive	nwsdname1  where nwsdname is the name of the NWSD	<p>This drive serves as the system drive for integrated server operating system (OS). Also:</p> <ul style="list-style-type: none"> <li>It is drive <b>C:</b> on Windows and <b>/dev/sda</b> on ESX.</li> <li>It resides in the integrated file system.</li> <li>It is automatically linked as the first drive.</li> <li>The size ranges from 15 GB to 1000 GB.</li> </ul> <p><b>Attention:</b></p> <ul style="list-style-type: none"> <li><b>ESX only:</b> Do not configure virtual machines on the system drive. Create additional storage spaces and link them to the server for your virtual machines. For most environments, you can configure one virtual machine per storage space to simplify backup and other administration tasks.</li> </ul>	Windows	✓	✓	✓	✓
			Embedded <sup>1</sup> ESXi5 ESXi4			2	N/A
			Non-embedded ESXi5 ESXi4 ESX4	✓	✓	✓	N/A
Install Drive	nwsdname2  where nwsdname is the name of the NWSD	<p>This drive contains integrated server support code and configuration information. Also:</p> <ul style="list-style-type: none"> <li>It is drive <b>D:</b> on Windows and <b>/dev/sdb</b> on ESX.</li> <li>It resides in the integrated file system.</li> <li>It is automatically linked as the second drive.</li> <li>The size ranges from 500 MB to 2 GB.</li> <li>IBM i formats this drive as a file allocation table (FAT or FAT32) disk.</li> </ul> <p><b>Attention:</b></p> <ul style="list-style-type: none"> <li>This drive must remain formatted as a FAT drive. Do not make any changes to this drive. IBM i uses this drive for administration functions and to perform code updates.</li> </ul>	Windows	✓	✓	✓	✓
			ESXi5 ESXi4			2	N/A
			ESX4			✓	N/A

Predefined Disk	Naming Convention	Description	Server OS	IBM i			
				i 7.2	i 7.1	i 6.1	i 5.4
		<ul style="list-style-type: none"> <li><b>Windows only:</b> Some third-party applications such as Citrix require that the drive letter (D:) for this drive be changed. This is supported as long as the drive remains linked to the server as the second drive and has a FAT or FAT32 file system to allow configuration files to be written when the server is started.</li> </ul>	ESX3.5	N/A	N/A	✓	✓
<b>Notes:</b> <sup>1</sup> Embedded versions of VMware ESX server are installed in flash memory and do not require a system drive. <sup>2</sup> The NWSD requires this disk on i 6.1, but it is not actually used for ESX, so a small (1-33 MB) disk is linked.							

**Related information:**

- [Virtual storage](#)

### 3.5.4 Create user-defined virtual storage

Before you can assign virtual storage to an integrated server, you must first create an IBM i network server storage space. This allocates the IBM i virtual storage.

Key attributes that you can specify when creating virtual storage for a server:

Attribute	Description
Capacity (Size)	<p>The amount of storage that is available to the integrated server. You can create a virtual disk with a capacity up to 1000 GB.</p> <p><b>Note:</b> The capacity available in the IBM i storage pool that the disk is allocated from might limit the capacity to less than 1000 GB.</p>
Source storage space	<p>You can optionally copy an existing storage space when creating a new one. This is useful if you want the two storage spaces to contain the same data, or if you want to make a backup copy of the source storage space.</p>
Planned file system (Format)	<p>This identifies the intended file system for the storage.</p> <p>Virtual storage format types allowed for iSCSI-attached servers are NTFS, ReFS (i 7.2 only), FAT, FAT32, and OPEN (open source). Although any of these formats can be used with any iSCSI-attached server, the following format types are most appropriate for each operating system type:</p> <p style="margin-left: 40px;"><b>Windows: NTFS</b> <b>ESX: OPEN</b></p> <p>Note that you can format the storage from the server OS differently than what is specified for this attribute. For example, even if you specify FAT32 as the intended format when you create the disk, you can later format the disk as NTFS.</p> <p>However, some default attributes of the disk (for example, the data offset, which affects performance) are chosen based on the format that is specified when the disk is created, so choose the format that most closely matches your intended use of the disk.</p>
Data offset (i 7.2, 7.1 and i 6.1 only)	<p>The data offset is used to logically align key on-storage structures with the IBM i system pages.</p> <p><b>Important note:</b> For optimal performance, this value must be set properly to align virtual storage I/O requests to IBM i pages. Incorrectly setting this parameter might adversely affect virtual storage performance.</p> <p>For more information, see <a href="#">Storage alignment considerations when creating virtual storage</a>.</p>
Sector size (i 7.2 only)	<p>The sector size is used to specify the number of bytes per sector for this virtual storage. Sector size 4096 is supported from i 7.2 and higher release.</p> <p><b>Note:</b> Sector size of 4096 is not supported when FORMAT(*FAT) or FORMAT(*FAT32) is specified.</p>

Attribute	Description
Preferred storage unit (i 7.2 only)	The preferred storage unit is used to specify whether the network server storage space should be allocated from solid-state drive storage media if available, or if no preference is specified, it will be allocated from any available storage media.
Resource allocation priority (i 7.2 only)	This specifies the relative resource allocation priority to be used by the hosting IBM i system to initialize the disk when the client operating system formats this storage space. This task can impact the hosting operating system performance. Higher priority will consume more resources but complete more quickly.

**Note:** After you create the virtual storage, you must link it to an integrated server and then partition and format the storage using the standard utilities provided by the integrated server operating system.

**Note:** Unexpected results will occur if a virtual storage participates in a Windows 2012 storage pool. For more information, see [What types of drives can I use with Storage Spaces](#).

**Note:** Since IBM i 7.2, the internal data structure of virtual storage is changed. After a LPAR is upgraded to 7.2, the virtual storage will be automatically converted to 7.2 format whenever the virtual storage is first touched, for example when commands such as WRKNWSSTG, CHGNWSSTG are executed, or its linked NWSD is varied on.

**Note:** During the format conversion for virtual storage created prior to 7.2, the parameter "Preferred storage unit" will be set to \*ANY by default. If you need to move virtual storage created prior to 7.2 into a Solid-state drive, you can create a new virtual storage, copy from the pre-7.2 storage and specify a different "Preferred storage unit". Alternatively you can save the pre-7.2 storage, delete it, and pre-create a storage with the same name but specify a different "Preferred storage unit". Then restore the storage, it will be moved into the preferred storage unit that is specified.

**Related information:**

➤ [Virtual storage](#)

➤ [Creating virtual storage for integrated servers](#)

### 3.5.4.1 Storage alignment considerations when creating virtual storage

**IBM i 7.2, 7.1 and i 6.1 only:** When you create virtual storage, the data offset that is chosen aligns the first partition that is created on the virtual storage. Incorrectly aligned storage might adversely affect virtual storage performance.

By default, the data offset is based on the planned file system (format) that is specified for the disk:

Format	Default Data Offset
ReFS	Align the first logical partition sector (*ALIGNLGLPTN)
NTFS	Align the first logical partition sector (*ALIGNLGLPTN)
FAT32	Align the first logical partition sector (*ALIGNLGLPTN)
FAT	Align the first logical partition sector (*ALIGNLGLPTN)
OPEN	Align the first logical storage (disk) sector (*ALIGNLGLDSK)



**Important note:** For optimal performance, the data offset must be set properly to align virtual storage I/O requests to IBM i pages. Incorrectly setting this parameter might adversely affect virtual storage performance.

However, virtual storage access might realize a performance improvement by specifying an offset value other than the default. Use the following data offset values when creating virtual storage:

Server OS	Format	Storage Usage	Data Offset Value to Use
WIN2012	ReFS	Any	Align the first logical storage (disk) sector (*ALIGNLGLDSK) <b>(NOT the default offset for ReFS)</b>
WIN2012 or WIN2008	NTFS	Any	Align the first logical storage (disk) sector (*ALIGNLGLDSK) <b>(NOT the default offset for NTFS)</b>
WIN2003	NTFS	Any	Align the first logical partition sector (*ALIGNLGLPTN) (Default offset for NTFS)
ESX	OPEN	ESX system disk	Align the first logical partition sector (*ALIGNLGLPTN) <b>(NOT the default offset for OPEN)</b>
		Storage for guest operating systems: <ul style="list-style-type: none"> <li>Windows Server 2012</li> <li>Windows Server 2008</li> <li>Windows Server 2008 R2</li> <li>Windows Vista</li> <li>Windows 7</li> </ul>	Align the first logical storage (disk) sector (*ALIGNLGLDSK) (Default offset for OPEN)
		Storage for guest operating systems: <ul style="list-style-type: none"> <li>Windows Server 2003</li> <li>Windows XP</li> <li>Windows 2000</li> <li>Windows NT® 4.0</li> <li>Linux</li> <li>Any other guest operating systems not previously listed</li> </ul>	Align the first logical partition sector (*ALIGNLGLPTN) <b>(NOT the default offset for OPEN)</b>

### Storage alignment considerations for multiple partitions

The data offset value aligns the first partition on the disk. To align additional partitions on the disk, all partitions on the disk (including the first partition) must use partition sizes that are a multiple of the values listed below. These values are based on the total size of the virtual storage space:

Storage Space Size	Partition Size Increments To Enable Storage Alignment
Less than 1024 MB	All partition sizes must be a multiple of 1 MB.
1025 MB to 511000 MB	All partition sizes must be a multiple of 63 MB.
511000 MB or greater	All partition sizes must be a multiple of 252 MB.

### 3.5.5 Copy virtual storage

Virtual storage can be copied or duplicated. For example, you can make a backup copy of a storage space. You can also move a storage space from one storage pool (ASP) to another one by first copying the storage space to the new ASP and then deleting it from the original ASP.

You can also expand the capacity of the virtual storage space while copying it. The additional capacity appears as unpartitioned space on the new disk. Use the server OS partitioning utilities to address the additional capacity by extending an existing partition or creating a new one.

**Note:** If a storage space is currently linked to an active server, it cannot be copied. Either the server must be shut down first or the storage space must be dynamically unlinked from the server before it can be copied.

**Related information:**

- [Copying virtual storage](#)

### 3.5.6 Extend the size of virtual storage

The capacity of an existing virtual storage space can be expanded. For example, if the disk is filling up, you can expand the disk to make additional capacity available to the server.

The storage space disk geometry (number of cylinders, sector size, etc.) limits how large a storage space can be expanded. The disk geometry for a storage space is set when the storage space is created, and is based on the original size of the storage space. The following table shows the maximum size a storage space can be expanded to, based on the original storage space size:

Original Storage Space Size	Maximum Size the Storage Space can be Expanded To
Less than 1024 MB	1024 MB
1025 MB to 511000 MB	511000 MB
511001 MB or greater	1024000 MB (1000 GB or 1 TB)

After expanding a disk, the additional capacity appears as unpartitioned space on the disk. Use the server operating system partitioning utilities to address the additional capacity by extending an existing partition or creating a new one.

**Note:** If a storage space is currently linked to an active server, it cannot be expanded. Either the server must be shut down before the storage space can be expanded or the storage space must be dynamically unlinked from the server before it can be expanded.

**Related information:**

- [Expanding virtual storage](#)
- [Expanding a disk drive for an integrated server](#)

### 3.5.7 Virtual storage linking

After you create virtual storage for an integrated server, you must link it to the NWSD associated with the server so that the server can access it.

Key attributes that you can specify when linking a disk to a server:

Attribute	Description	
Link type	iSCSI-attached integrated servers use only dynamic virtual storage links.  You must select <b>Dynamic</b> when using the GUI or specify DYNAMIC(*YES) when using the ADDNWSSTGL CL command.	
Sequence position	This attribute identifies the order that the integrated server sees the linked disk.  For example, a server normally sees a disk linked at sequence position 3 ahead of a disk that is linked at position 7.  However, when dynamically linking virtual storage to an <u>active</u> server, the new virtual storage appears following all other linked virtual storage. In this case, the link sequence position is not used until the server is restarted.  You can use the default (next available) link sequence position or specify a value (1-64).	
Storage path	The storage path identifies which iSCSI target network server host adapter (NWSH) or group of iSCSI targets (multipath group) are used when the integrated server accesses the virtual storage over the iSCSI network.  You can use the default storage path or specify a specific storage path or the multipath group.	
Access to storage	Exclusive - Update	The server has exclusive access to the disk and can update it. Only one server at a time is allowed to have the disk linked with this access type.  <b>Note:</b> If linking a predefined system or install drive, this access type is required.
	Shared - Update	The server can share access to the disk with other servers and can update it. Multiple (up to 50) servers at a time are allowed to have the disk linked with this access type.  <b>Note:</b> When sharing storage among multiple servers, the integrated server operating system (for example VMware ESX) is responsible for implementing protocols that ensure that multiple servers can access the storage without conflicts.  <b>Tip:</b> Use this access type with multiple ESX servers on i 7.2, 7.1 and 6.1 to enable VMware VMotion, VMware HA and VMware DRS.

**Note:** After you create virtual storage and link it to an integrated server, you must partition and format the storage using the standard utilities provided by the integrated server operating system.

**Related information:**

- [Virtual Storage Capabilities](#)
- [Virtual storage](#)
- [Predefined virtual storage and naming](#)

### 3.5.7.1 Dynamic virtual storage linking while server is active

IBM i virtual storage can be linked (added) to the integrated server while it is active. For example, if the server is running low on storage capacity, you can add virtual storage to the server without shutting it down.

Support for dynamically linking virtual storage to an active server is shown below:

Task	Storage Creation Type	Server OS	IBM i			
			i 7.2	i 7.1	i 6.1	i 5.4
Link virtual storage while the server is active	Predefined	All				
	User-defined	Windows	✓	✓	✓	✓
		ESX	✓	✓	✓ <sup>1</sup>	✓ <sup>1</sup>
<b>Notes:</b>						
<sup>1</sup> For ESX servers that use the <a href="#">Service console based infrastructure</a> , you must do a manual rescan of the iSCSI initiators in order for ESX to see the dynamically linked storage.						

**Related information:**

- [Virtual storage](#)
- [Predefined virtual storage and naming](#)

### 3.5.8 Virtual storage formatting

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

**Important:** The partitions on the disk must be properly aligned to avoid degraded performance. See [Storage alignment considerations for multiple partitions](#).

See the additional considerations for supported operating systems shown below:

<b>Server OS</b>	<b>Formatting Considerations</b>
WIN2012 or WIN2008	Use the Windows Server <b>Disk Management</b> function to format the disk. See <a href="#">Formatting storage for Windows servers</a> .
WIN2003	Use the Windows Server <b>Disk Management</b> function to format the disk. See <a href="#">Formatting storage for Windows servers</a> .  You can also use the Windows Server 2003 <b>DISKPART</b> tool to format the disk.
ESX	Format virtual storage based on the operating system that will use the storage.  Refer to VMware ESX documentation for information on partitioning and formatting storage for ESX and the associated virtual machines.  See White Paper <a href="#">Aligning storage partitions for VMware ESX Server on iSCSI attached integrated servers</a> for additional considerations to help you partition your storage for improved performance.

**Note:** For Windows Server 2012, the virtual storage can be formatted as ReFS, but it will show as NTFS on IBM i 7.1.

**Related information:**

- [Virtual storage](#)
- [Storage alignment considerations when creating virtual storage](#)

### 3.5.9 Virtual storage unlinking

IBM i virtual storage can be unlinked (removed) from an integrated server.

Once the virtual storage is unlinked:

- The storage is no longer accessible by the integrated server.
- You can link the storage to the same or a different integrated server.
- You can delete the storage if it is no longer needed.

Normally you would unlink virtual storage while the server is shut down. If you want to unlink virtual storage while the server is active, see [Dynamic virtual storage unlinking while server is active](#) for some considerations.

**Related information:**

- [Virtual storage](#)

#### 3.5.9.1 Dynamic virtual storage unlinking while server is active

IBM i virtual storage can be unlinked (removed) from an integrated server while it is active under some circumstances.

Support for dynamically unlinking virtual storage from an active server is shown below:

Task	Storage Creation Type	Server OS	IBM i			
			i 7.2	i 7.1	i 6.1	i 5.4
Unlink virtual storage while the server is active	Predefined	All				
	User-defined	Windows <sup>1</sup>	✓	✓	✓	✓
		ESX				
<b>Notes:</b>						
<sup>1</sup> The unlinked storage cannot be part of a volume set and cannot be a volume mounted in a directory. Also, no users can currently be using a volume on the storage space.						

**Related information:**

- [Virtual storage](#)
- [Predefined virtual storage and naming](#)

### 3.6 IBM i tape and optical devices shared with integrated Windows servers

Integrated Windows servers can use tested IBM i tape and optical devices. The IBM i devices can be used by the integrated Windows server as if they were local devices on Windows for such tasks as installing applications and backing up data.

A particular IBM i device can be used only by IBM i or one integrated Windows server at a time.

- In order for the Windows server to use a particular IBM i device, the device must be locked from Windows using a device locking utility that is provided by IBM i Integrated Server Support.
- Likewise, when the Windows server is done using a particular IBM i device, the device locking utility must be used to unlock the device so that it is available for use by IBM i or other integrated Windows servers.

For more information, see [Sharing tape and optical devices between IBM i and integrated Windows servers](#).

#### Attention:

- A subset of IBM i tape devices are supported for use with various Windows versions. For example, only IBM i **virtual** tape devices can be used with Windows Server 2008. See the support matrices in the [IBM i tape and optical device access by integrated servers](#) section and subsections for details.
- IBM i tape and optical devices cannot be used by iSCSI-attached VMware ESX servers.

#### Related information:

- [IBM i tape devices for Windows Server 2008/2012](#)
- [IBM i tape devices for Windows Server 2003](#)
- [Sharing tape and optical devices between IBM i and integrated Windows servers](#)
- [Microsoft Windows Batch Commands for Controlling Devices](#)

## 3.7 Networking concepts for integrated servers

iSCSI-attached integrated servers use several types of network connections, as described in the following sections.

### 3.7.1 iSCSI network

This physical network connects iSCSI target adapters in the hosting IBM i partition with iSCSI initiator adapters in the System x or BladeCenter system.

The iSCSI network is typically a simple, switched, 1 or 10 Gigabit Ethernet network. For some configurations, the iSCSI target and initiator adapters can be connected directly to each other without a switch. Two kinds of traffic flow over this connection: storage (SCSI) and virtual Ethernet (LAN).

#### iSCSI target adapters

On one side of the network is an iSCSI target adapter or adapters controlled by IBM i. Each iSCSI target adapter port has up to two IP addresses: one for SCSI and one for LAN. For a hardware target (iSCSI HBA), separate IP addresses are used for the SCSI and LAN connections. For a software target (Ethernet NIC), the LAN connection uses the same IP address as the SCSI connection. You configure the IP addresses and other attributes of an adapter in an IBM i device description object known as the network server host adapter (NWSH). Each iSCSI target adapter controlled by IBM i needs its own NWSH object. When you start (vary on) an NWSH, an iSCSI target adapter controlled by IBM i uses the values configured in the NWSH. If you want different values to be used, you must vary off the NWSH, change the NWSH configuration, and vary on the NWSH again.

The iSCSI protocol is implemented differently, depending on the type of iSCSI target adapter:

Type	Description
Software Target (SWT)	<p>The iSCSI protocol is implemented in IBM i, so IBM i resources (for example, CPU and memory) are used for the iSCSI protocol. The IBM i TCP/IP stack is aware of the IP address configured for the iSCSI target adapter.</p> <p>For the IBM i iSCSI solution, standard IBM i Ethernet NICs are used as iSCSI software target adapters.</p> <p><b>Note:</b> SWT support requires IBM i 6.1.1 or later.</p>
Hardware Target (HWT)	<p>The iSCSI protocol is implemented in firmware on the iSCSI adapter, so the iSCSI protocol is offloaded from IBM i. The TCP/IP stack is also implemented in hardware and is independent of the normal IBM i TCP/IP stack. The IBM i TCP/IP stack is unaware of the IP addresses configured for the iSCSI target adapter.</p> <p>For the IBM i iSCSI solution, QLogic iSCSI host bus adapters (iSCSI HBAs) are used as iSCSI hardware target adapters.</p>

#### iSCSI initiator adapters

On the other side of the network is an iSCSI initiator adapter or adapters for the integrated server. You configure the IP addresses and other attributes of these adapters in an IBM i object known as the



remote system configuration. This configuration differs from the IBM i network server host adapter object in several ways:

- You can configure an iSCSI initiator adapter port with 1 or 2 IP addresses: SCSI, LAN, or both. There must be at least one SCSI and one LAN IP address among all the configured adapters.
- Whenever you configure an IP address for an iSCSI initiator adapter, you must also configure the corresponding adapter MAC address. Be careful to configure MAC addresses correctly.
- You configure all the iSCSI initiator adapters for an initiator system in the same IBM i remote system configuration. When the integrated server is later varied on, IBM i automatically ensures that iSCSI initiator adapters in the initiator system use values in the IBM i remote system configuration. If you want different values to be used, you must change the remote system configuration and vary on the server again.

The iSCSI protocol is implemented differently, depending on the type of iSCSI initiator adapter:

Type	Description
Software Initiator (SWI)	<p>The iSCSI protocol is implemented in the integrated server operating system, so integrated server resources (for example, CPU and memory) are used for the iSCSI protocol. The integrated server operating system TCP/IP stack is aware of the IP addresses configured for the iSCSI initiator adapter.</p> <p>For the IBM i iSCSI solution, standard System x or blade server Ethernet NICs or LOM (LAN on Motherboard, which is also called embedded Ethernet or integrated Ethernet) ports are used as iSCSI software initiator adapters.</p>
Hardware Initiator (HWI)	<p>The iSCSI protocol is implemented in firmware on the iSCSI adapter, so the iSCSI protocol is offloaded from the integrated server. The SCSI traffic uses the iSCSI initiator adapter hardware TCP/IP stack, but LAN traffic uses the integrated server operating system TCP/IP stack. Consequently, the integrated server operating system TCP/IP stack is unaware of the iSCSI initiator adapter SCSI IP address, but is aware of the LAN IP address.</p> <p>For the IBM i iSCSI solution, QLogic iSCSI host bus adapters (iSCSI HBAs) are used as iSCSI hardware initiator adapters.</p>

**Notes:**

1. iSCSI initiator support varies by server model. See [Blade server models](#) and [System x server models](#).
2. In IBM i configuration objects, network interface information is labeled as local or remote. These terms are relative to IBM i. Local interface information is for the IBM i side. Remote interface information is for the integrated server side.
3. The NWSH and the remote system configuration define IP address information for opposite sides of the iSCSI network. When connected by a simple, switched network, the following rules apply:
  - The SCSI IP addresses in these two objects that are connected by a switch must be in the same subnet. For example, with IP addresses of the form a.b.x.y and 255.255.255.0 subnet masks, a.b.x must be the same value for both objects.
  - The LAN IP addresses in these two objects that are connected by a switch must be in the same subnet.

- In the NWSH, use the default value (none) for the gateway elements.
- In the remote system configuration, use the default value (none) for the gateway elements

### Additional considerations

See the following additional considerations for the iSCSI network:

Item	Considerations
Scaling the iSCSI Network	<p>After you have installed an integrated server, you can scale the iSCSI network.</p> <p>The basic installation process addresses integrated servers that use one IBM i iSCSI target and one System x or blade iSCSI initiator. After the server is installed, you can configure additional iSCSI targets or initiators if needed. See <a href="#">Multipath I/O (MPIO)</a>.</p>
Integrated iSCSI DHCP server	<p>There are multiple methods for delivering boot information to the integrated server. The default method of delivering IP and storage information to boot the integrated server uses an integrated iSCSI Dynamic Host Configuration Protocol (DHCP) server on the IBM i side of the iSCSI network. See <a href="#">Integrated iSCSI DHCP server</a>.</p> <p>Even with DHCP, the IP address might be considered static because the DHCP server associates a single IP address with a MAC address.</p>
Managing IBM i iSCSI target adapter function	<p>Paths configured in the network server description control what storage and virtual Ethernet traffic, if any, can flow over an IBM i iSCSI target adapter. For more information, see:</p> <ul style="list-style-type: none"> <li>• <a href="#">Sharing an iSCSI target among multiple integrated servers</a></li> <li>• <a href="#">Distributing iSCSI network traffic between multiple iSCSI targets</a></li> </ul> <p>Multiple initiator systems can use an IBM i iSCSI target adapter simultaneously if multiple network server descriptions use the same NWSH object.</p>
Managing iSCSI initiator adapter function	<p>You can configure an iSCSI initiator adapter with a SCSI IP address, a LAN IP address, or both. A SCSI IP address enables storage traffic, and a LAN IP address enables virtual Ethernet traffic.</p> <p>Use of the iSCSI initiator adapter as a general-purpose external network connection is not supported. For more information about external network connections, see <a href="#">Physical networks</a>.</p> <p>For integrated Windows servers, each virtual Ethernet adapter is automatically assigned to an iSCSI initiator adapter. There is an option to select particular iSCSI initiator adapter on the advanced properties tab of each virtual Ethernet adapter. See <a href="#">Managing iSCSI initiator allocation at the Windows side of the iSCSI network</a>.</p>
Security	<p>For information about securing storage and virtual Ethernet traffic, see <a href="#">Network security</a>.</p>
Other considerations	<p>The following items are additional considerations for iSCSI adapters.</p> <ul style="list-style-type: none"> <li>• The iSCSI network only uses Internet Protocol version 4.</li> <li>• The frame format is Ethernet version 2.</li> <li>• The iSCSI network does not support Network Address Translation.</li> </ul>

#### Related information:

- [IBM i iSCSI targets](#)
- [Blade iSCSI initiators](#)
- [System x iSCSI initiators](#)
- [Integrated iSCSI DHCP server](#)
- [IBM i configuration objects for integrated servers](#)
- [Multipath I/O \(MPIO\)](#)
- [Implementing Integrated Windows Server through iSCSI to System i5](#)

## 3.7.2 Integrated iSCSI DHCP server

The IBM Integrated Server Support option provides an integrated iSCSI DHCP server that is used for communication with iSCSI initiators in integrated servers.

The integrated iSCSI DHCP server is used to deploy boot parameters to the hosted-server iSCSI initiator when the **Dynamically delivered to the remote system via DHCP** option is specified in the IBM i remote system configuration and when the corresponding option is specified in the hosted-server iSCSI initiator. The following parameters are deployed to the hosted-server iSCSI initiator when an NWSD is varied on:

- IP addresses for the IBM i iSCSI target boot devices and the BladeCenter blade or System x iSCSI initiator devices.
- iSCSI Qualified Names (IQNs) that represent the target and initiator devices.

Both of these sets of IP addresses and IQNs are in the IBM i configuration objects used to define the hosted server. The target IP address is defined in the NWSH object. The initiator IP address and initiator IQN are defined in the remote system configuration. The target IQN is automatically configured and defined in the NWSD object. For more information about these objects refer to [IBM i configuration objects for integrated servers](#).

### Notes:

1. The integrated iSCSI DHCP server is only used to deploy boot parameters to iSCSI initiators.
2. The integrated iSCSI DHCP server is **not** a general purpose DHCP server, so it will **not** provide IP addresses to other systems in the network and it will **not** interfere with other DHCP servers in the network.

### Related information:

- [Booting over the iSCSI network](#)

### 3.7.2.1 Advanced integrated iSCSI DHCP server concepts

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

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

You should use the default configuration for most environments. However, the scope that the vendor ID and MAC address provide can be changed. Advanced and sophisticated users can more specifically configure this setting, when required. The default vendor ID can be configured to other values. Configuration screens are available in the iSCSI initiator configuration function of the hosted server and the corresponding remote system configuration object. This advanced function is compliant with the RFC 2132 specification.

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

### 3.7.3 Ethernet switches for the iSCSI solution

Blade and System x servers that are attached to IBM i via an iSCSI network typically require the use of Ethernet switches.

An Ethernet switch is optional for simple one-to-one iSCSI networks when using an IBM i hardware target on i 6.1 or later. An Ethernet switch is **required** for all other IBM i iSCSI network configurations.

#### 3.7.3.1 External switch considerations

##### Minimum requirements

The Ethernet switch that is used for the iSCSI network must meet the following requirements:

1. 1 or 10 gigabit layer 2 switch, preferably dedicated to the iSCSI network and isolated from other networks.
2. Copper and/or fiber optic ports consistent with your iSCSI adapters.
3. Any copper cables and premises wiring involved should be category 5e or category 6.
4. Fiber optic connections might be preferred in environments with high electrical noise or longer cable length requirements. Fiber optic connections might cost considerably more than copper.
5. Enough ports to accommodate all iSCSI adapters.
6. Switch ports should be 'access ports' rather than 'trunk ports'. Access ports are for device connections. Trunk ports are for connections to other switches.

**Note:** For most environments, turn off **Spanning Tree Protocol (STP)**. If this is not done, the integrated server may fail to boot because STP typically introduces a large delay before the switch port goes into the forwarding mode. If Spanning Tree Protocol is still desired, then it may only be used if a special switch feature, such as Spanning Tree Portfast or STP Fast Start, is used so that the large delay is eliminated.

##### Optional features and considerations

The following Ethernet switch features are optional:

1. 9000 byte jumbo frame support: The iSCSI network normally uses standard 1500 byte frames. It is possible to configure iSCSI adapters to use larger frames on the iSCSI network. However, under heavy traffic, many switches do not perform well with larger frames, degrading performance of both storage and virtual Ethernet.

If you are not sure that your switch performs well with larger frames, you should use the default settings for 1500 byte frames.

As long as switch limitations are not affecting performance, setting the iSCSI adapter and switch MTU configuration to 9000 typically improves performance, especially virtual Ethernet performance.

If you plan to use jumbo frame support, you need to configure it on the switch, if not already enabled.

2. Extra ports to accommodate future growth (for example, additional iSCSI adapters per server or additional servers). iSCSI adapters and hosted systems involved in hot spare need to be on the same switched network.
3. Rack mounting capability.
4. Managed switch functions provide additional features, such as the following:
  - Port mirroring to accommodate a sniffer – recommended.
  - Statistics support – recommended.
  - VLAN packet tagging (IEEE 802.1q).  
If your switch supports IEEE 802.1q VLAN, ensure that the switch is configured to treat the iSCSI adapters as VLAN unaware (untagged) devices. This is also true for any service processor connection using the switch. This is generally the default behavior of new switches that support VLANs.
  - Special connections may be needed for the device providing the user interface.

### Ethernet switch requirements for the service processor connection

The Ethernet switch that is used for the BladeCenter or System x service processor connection must meet the following requirements:

1. Layer 2 switch with ports for copper cables.
2. Typically part of an existing network with an IBM i LAN connection.

See [Considerations for connecting service processors to IBM i](#) for some considerations that may affect how you decide to configure your network for IBM i to service processor communications.

### 3.7.3.2 BladeCenter switch module considerations

#### Ethernet switch modules

BladeCenter Ethernet switch modules are normally used to connect the blade iSCSI initiators to the iSCSI network. The Ethernet switch module that is used for the iSCSI network must meet the following requirements:

- Most of the considerations listed in the [External switch considerations](#) section above also apply to Ethernet switch modules.

**Note:** One of the available BladeCenter Ethernet switch modules does not meet the minimum requirements stated in the [External switch considerations](#) section, but can be used with restrictions. See the [Problems with Blades Connected to System i via Server Connectivity Module](#) software knowledge base article for more information.

- When Ethernet switch modules are used, a separate external Ethernet switch is **not** required. You can connect the Ethernet switch module directly to the IBM i iSCSI targets if your environment does not otherwise require an external Ethernet switch.
- You can optionally use both an Ethernet switch module and an external Ethernet switch.

**Note:** iSCSI initiator adapters in a BladeCenter system have two ports. A single switch module or pass-through module enables the use of one port of all iSCSI initiator adapters in the BladeCenter system. A

second switch module or pass-through module enables the use of the other port of all iSCSI initiator adapters in the BladeCenter system. A second switch module or pass-through module, along with multiple iSCSI target adapters, is useful for multipath I/O.

### Pass-through I/O modules

BladeCenter pass-through I/O modules can be used to connect the blade iSCSI initiators to the iSCSI network. There are no special requirements for pass-through I/O modules.

**Note:** When pass-through I/O modules are used, an external Ethernet switch **is** required except when the iSCSI network allows [Direct connect](#) support.

### 3.7.4 Service processor connection

This physical connection is required so that the hosting IBM i partition can communicate with the service processor of the integrated server (System x or BladeCenter blade). This connection is different than the connection between the IBM i iSCSI target adapter and the iSCSI initiator adapter in the integrated server.

The connection can consist of a simple and switched network or a more complex and routed network. IBM i Integrated Server Support uses this connection to manage the state of the integrated server.

At one end of the connection is a LAN adapter or adapters that are controlled by IBM i. This LAN adapter can be available for other uses. The IP address and other attributes of this adapter are controlled using standard IBM i configuration methods. IBM i can automatically connect to the service processor using one or more IBM i TCP interfaces that are already configured.

At the other end of the connection is the service processor. The service processor has its own Ethernet port and TCP/IP stack. This TCP/IP stack is active whenever the system power cord is plugged into a power source, even if the server hardware is not in a powered on state.

#### Connection

There are multiple options that IBM i offers for connecting to the service processor. For more information, see:

- [Service processor connection methods](#)
- [Considerations for connecting service processors to IBM i](#)

#### Security

- The security capabilities of your service processor hardware may affect your decision to use an isolated network or a shared network to provide the service processor connection. For more information, see [Considerations for connecting service processors to IBM i](#).

### 3.7.4.1 Supported functions by service processor type

The configuration options depend on the type of service processor. For information about identifying the type of service processor in your System x server or BladeCenter chassis, see [System x server models](#) and [BladeCenter chassis models](#).

The types of service processors are shown below:

Service Processor	Considerations
Management Module (MM) or Advanced Management Module (AMM)	<p>The MM and AMM service processors are available in IBM BladeCenter servers.</p> <p>To configure the MM or AMM, use the provided Web interface.</p> <p>The MM and AMM support connections using an IP address or host name. Use the method that is the most appropriate for your network. Parameters in the service processor configuration determine the MM or AMM connection method.</p> <p>The MM and AMM can obtain IP address information using either of the following methods.</p> <ul style="list-style-type: none"> <li>• Static IP addressing.</li> <li>• Dynamic IP addressing (using DHCP).</li> </ul> <p><b>Note:</b> Dynamic IP addressing is the factory default. If dynamic IP addressing is used, then a <b>host name</b> <u>must</u> be configured.</p> <p>The MM and AMM support security using a password.</p> <p>BladeCenter systems have additional considerations.</p> <ul style="list-style-type: none"> <li>• IBM i must connect to the MM or AMM service processor in the BladeCenter before any server blades can be managed.</li> <li>• After connecting to the MM or AMM, IBM i gathers information about the server blades contained in the enclosure. The remote system identity is used to identify the individual server blade.</li> <li>• The remote system identity in the remote system configuration must be set to the serial number of the IBM BladeCenter blade server (not the BladeCenter chassis). The blade serial number can be found on the label on the server.</li> <li>• The enclosure identity in the service processor configuration can be set to the IBM BladeCenter chassis (enclosure) serial number.</li> </ul>
Integrated Management Module II (IMM II), Integrated Management Module (IMM), or Remote Supervisor Adapter II	<p>The IMM II, IMM, and RSA II service processors are available in most System x servers.</p> <p>To configure the service processor, do one of the following.</p> <ul style="list-style-type: none"> <li>• Use the system BIOS or UEFI setup menu. This method cannot be used to configure a host name.</li> <li>• Use the provided Web interface.</li> </ul> <p>These service processors support connections using an IP address or host name. Use the method that is the most appropriate for your network. Parameters in the service processor configuration determine the connection method.</p> <p>The service processor can obtain IP address information using either of the following methods.</p>

Service Processor	Considerations
(RSA II)	<ul style="list-style-type: none"> <li>Static IP addressing.</li> <li>Dynamic IP addressing (using DHCP).  <b>Note:</b> Dynamic IP addressing is the factory default. If dynamic IP addressing is used, then a <b>host name</b> <u>must</u> be configured.</li> </ul> <p>These service processors support security using a password.</p>
Baseboard Management Controller (BMC)	<p>The BMC service processor is available in some System x models.</p> <p>To configure the BMC, use the system BIOS setup menu</p> <p>The BMC supports static IP addressing.</p> <p>The BMC supports connection by IP address.</p> <p>The BMC supports security using a password.</p>

**Related information:**

- [Changing a service processor password for an integrated server](#)
- [Changing service processor configuration properties](#)

### 3.7.4.2 Service processor addressing methods

The method used to address the service processor is configured both in the service processor itself and in the IBM i service processor configuration. See the considerations below:

Addressing Method	Considerations
Host name	The service processor is configured with a host name.
Static IP addressing	The service processor is configured with a specific IP address.
Dynamic IP addressing (DHCP)	<p>Dynamic IP addressing uses a DHCP server in your network to obtain the service processor IP address.</p> <p>Dynamic IP addressing is the factory default. If dynamic IP addressing is used, then a <b>host name</b> <u>must</u> be configured.</p> <p><b>Note:</b> If a specific IP address or host name has not been set yet for the service processor, the factory default for most service processors is to use DHCP to obtain an IP address. The service processor initializes immediately when the server receives power and starts the DHCP process. If a service processor IP address cannot be obtained with DHCP, the service processor uses the default static IP address of <b>192.168.70.125</b>. You can use the IP address obtained using DHCP, or the default IP address, to connect to the service processor Web interface and set a static IP address or host name for the service processor.</p>

**Related information:**

- [Changing service processor configuration properties](#)
- [Configuring service processor connection using IP address for integrated servers.](#)
- [Configuring service processor connection using host name for integrated servers.](#)



### 3.7.4.3 Service processor connection methods

IBM i connects to the BladeCenter or System x hardware on the network using either an IP address or a host name. Some considerations for these connection methods are listed below:

Connection Method	Advantages	Disadvantages	Compatible Service Processors
IP address	This connection method is simple if the service processor IP address is known and configured into the service processor.	The IP address must be configured into the service processor.	MM AMM IMM II IMM RSA II BMC
Host name	If a Domain Name System (DNS) server is available, a specific IP address need not be maintained in the IBM i service processor configuration.  <b>Note:</b> The DNS server must be on a system that does not require a DNS to be discovered.	The host name must be configured into the service processor using the service processor Web interface.  A Domain Name System (DNS) server is required.	MM AMM IMM II IMM RSA II

**Note:** On IBM i 5.4 and 6.1, multicast discovery using Service Location Protocol (SLP) could be used to discover the System x or BladeCenter service processor if using **IBM Systems Director** for integrated server discovery and power control. However, when using **Service Processor Manager** function of IBM i **Integrated Server Support** for integrated server discovery and power control, SLP discovery cannot be used. A specific IP address or host name must be used to connect to the service processor.

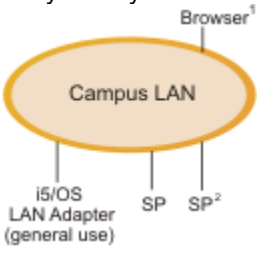
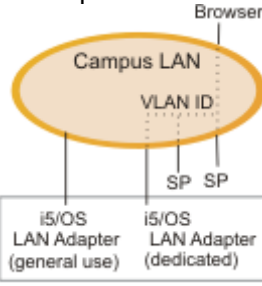
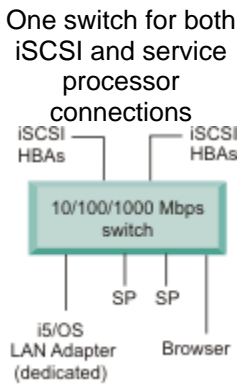
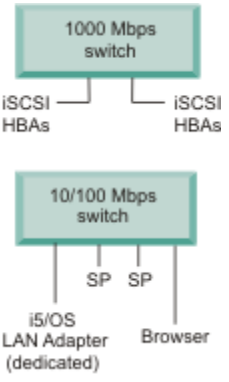
**Related information:**

- [Changing service processor configuration properties](#)
- [Configuring service processor connection using IP address for integrated servers.](#)
- [Configuring service processor connection using host name for integrated servers.](#)

### 3.7.4.4 Considerations for connecting service processors to IBM i

Use this information to compare configurations between IBM i and the service processor for the integrated server.

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

Aspect	Connection Method			
	Campus LAN or Intranet		Physically isolated network	
Network Hardware Configuration	<p>Any-to-any network</p> 	<p>Logically isolated network</p> <p>For example, use VLAN switches configured with a unique VLAN ID.</p> 	<p>One switch for both iSCSI and service processor connections</p> 	<p>Separate switches for iSCSI and service processor connections</p> 
Flexibility of remote management by using a Web Browser <sup>3</sup>	Better ←-----→ Worse			
	Browser can be anywhere on the campus LAN.	Browser must be connected to the logically isolated LAN.	Browser must be connected to the switch providing the service processor connection.	Browser must be connected to the switch providing the service processor connection.
Security <sup>4</sup>	Worse ←-----→ Better			
	Highest risk.	Lower risk than any-to-any network.	Low risk. Requires access to the switch providing the service processor connection.	Low risk. Requires access to the switch providing the service processor connection.
Multiple Management Server Coexistence <sup>5</sup> (Shared SP Login ID)	Worse ←-----→ Better			
	Any management server connected to the campus LAN might interfere.	Only management servers connected to the logically isolated LAN might interfere.	Only management servers connected to the switch providing the service processor connection might interfere.	Only management servers connected to the switch providing the service processor connection might interfere.
<p><b>Notes:</b></p> <p><sup>1</sup> Browser is a Web browser used for remote management.</p> <p><sup>2</sup> SP is a System x or a BladeCenter service processor.</p> <p><sup>3</sup> The web browser interface is not available for a System x model that has only a BMC service processor.</p> <p><sup>4</sup> For example, consider the possibility of a LAN sniffer attack seeking a service processor password.</p> <p><sup>5</sup> If your company has multiple management servers (Service Processor Managers or IBM Director Servers), be sure to change the default login ID of the service processor.</p> <ul style="list-style-type: none"> <li>• This row does <b>not</b> apply to you if you change the default login ID of the service processor.</li> <li>• If you do <b>not</b> change the default login ID of the service processor, this row shows which management servers might interfere with the ability of IBM i to access a service processor (especially for a BladeCenter).</li> </ul>				

**Related information:**

- [Selecting a login ID and password for the service processor](#)

### 3.7.5 Networking for IBM i administration of integrated servers

IBM i uses network connections to communicate with integrated servers for some administrative functions, such as linking storage and shutting down the server. Integrated Windows servers use a point-to-point virtual Ethernet network and integrated VMware ESX servers use multiple networks.

#### 3.7.5.1 Point-to-point virtual Ethernet network for integrated Windows servers

IBM i uses the point-to-point virtual network to communicate with integrated Windows servers. This type of virtual Ethernet network is specifically for integrated Windows servers and is different from the virtual Ethernet networks used for inter-partition communication on your Power server.

IBM i communicates with integrated Windows servers over a point-to-point virtual Ethernet network. When an integrated server is installed, a special virtual network is created between the integrated server and a controlling IBM i partition. This network is called point-to-point because it has only two end points (the integrated server, and the IBM i server). This point-to-point virtual Ethernet is emulated within IBM i and no additional physical network adapters or cables are used. In IBM i, it is configured as an Ethernet line description with Port Number value \*VRTETHPTP.

A point-to-point virtual Ethernet connection and a virtual Ethernet network are different in the following ways:

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

The point-to-point virtual Ethernet IP addresses take the form of 192.168.xxx.yyy, where xxx ranges from 100 to 254 and results in a unique class C network (using subnet mask 255.255.255.0). For example, the IBM i side of the point-to-point network is given the IP address 192.168.100.1, and the Windows operating system side has 192.168.100.2. As you create multiple integrated Windows servers, xxx is incremented so that the point-to-point network for each integrated Windows server is on a unique subnet.

You can allow IBM i to automatically assign these IP addresses when you install an integrated Windows server, or you can manually configure them to prevent TCP/IP address collisions with other hosts in your network.

**Related information:**

- [Virtual Ethernet networks for integrated Windows servers](#)

### 3.7.5.2 Multiple networks for integrated VMware ESX servers

The IBM i connection for ESX servers uses multiple networks and varies based on the IBM i management infrastructure that is used for the ESX server:

Management Infrastructure	Connection
<a href="#">Management server based infrastructure</a>	<p>IBM i does not communicate directly with a VMware ESX server to perform VMware ESX server management tasks (for example, to shut down the ESX server). Instead, IBM i uses an intermediate integrated Windows server that serves as a management server for the VMware ESX server.</p> <p>IBM i uses the point-to-point virtual Ethernet network to communicate with the integrated Windows server. The integrated Windows server then uses a physical network between the two integrated servers to communicate with the VMware ESX server or an ESX platform manager to perform administrative functions.</p>
<a href="#">Service console based infrastructure</a>	IBM i uses a physical network between IBM i and the integrated VMware ESX server to perform administrative functions.

**Related information:**

- [Virtual Ethernet networks for integrated Windows servers](#)
- [Physical networks](#)

### 3.7.6 Virtual Ethernet networks for integrated Windows servers

Integrated servers can use a virtual Ethernet network that is configured on a Power server to communicate with the hosting IBM i partition, another partition, or other integrated servers.

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

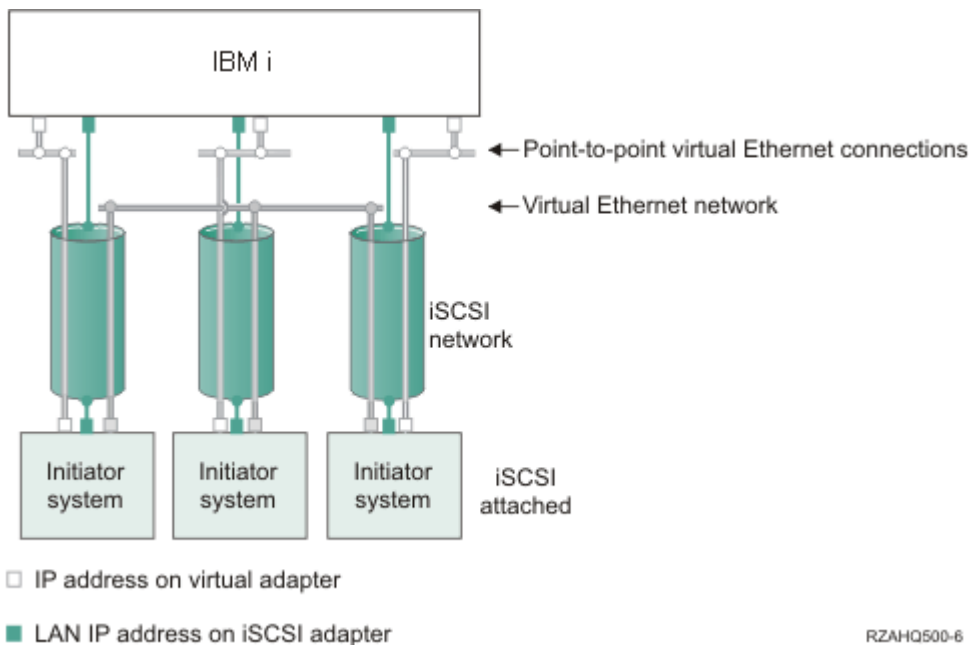


Figure 7: iSCSI network tunnels

iSCSI-attached systems can participate in virtual Ethernet networks and can communicate with each other. Virtual Ethernet traffic is tunneled through a physical iSCSI network. Virtual Ethernet is needed when an iSCSI network is present for several reasons:

- Virtual Ethernet can work with other virtual Ethernet support on your Power server.
- Virtual Ethernet can provide multiple isolated virtual networks through each iSCSI target adapter even when switches in the iSCSI network do not support IEEE 802.1Q VLANs
- Integrated servers can communicate with each other even if they are each attached by Ethernet switches that are not connected to each other.

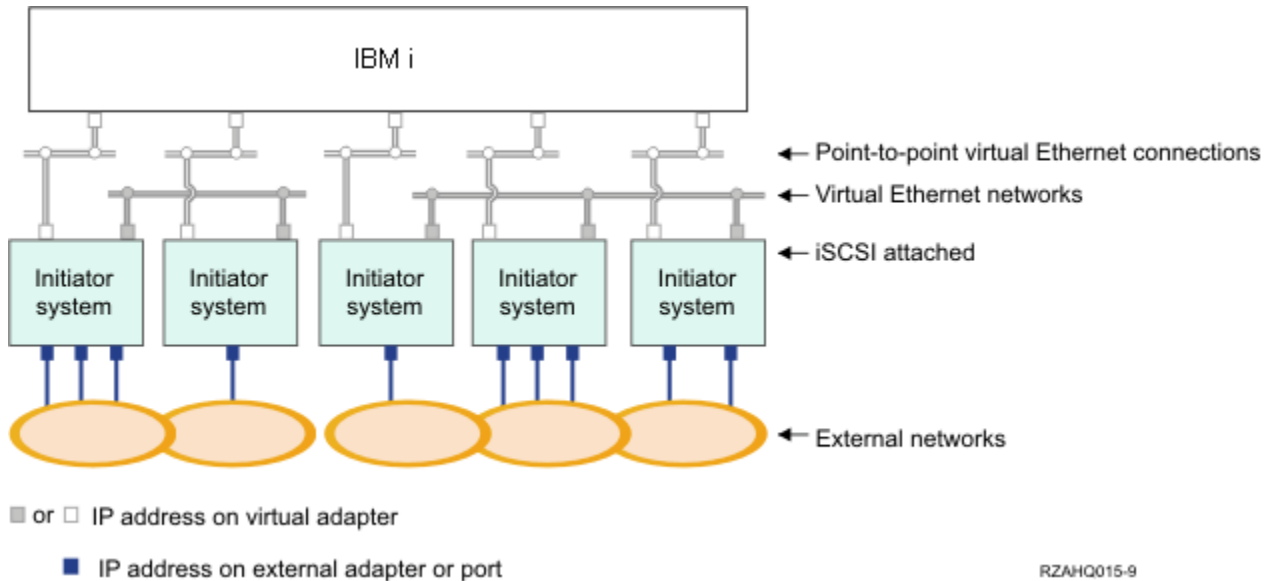
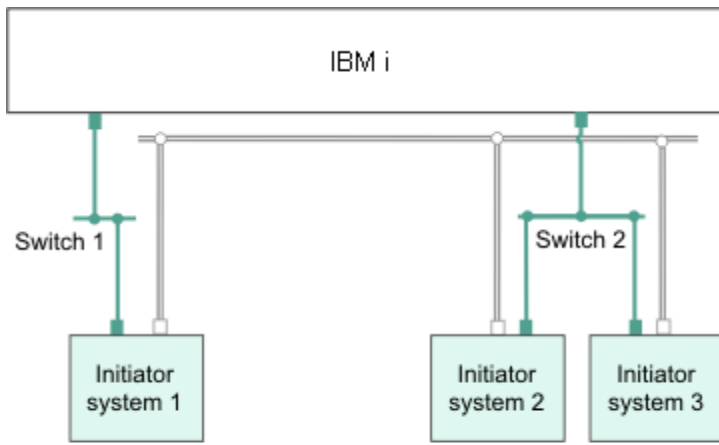


Figure 8: Two isolated groups of integrated Windows servers on the same Power server. Each group has its own virtual Ethernet network

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

Like point-to-point virtual Ethernet, virtual Ethernet networks are configured through Ethernet line descriptions. An integrated server is connected to a virtual Ethernet network when its IBM i configuration (NWSD) is configured to have an Ethernet line description port number with a value of \*VRTETH0 through \*VRTETH9. Integrated servers that have NWSDs configured with the same port number values are connected to the same virtual Ethernet network. In the figure, the IBM i side of the line descriptions is not shown. Unlike when you use point-to-point virtual Ethernet, you do not configure a TCP/IP address on the IBM i side of a line description that is used in a virtual Ethernet network.



□ IP address on virtual adapter

■ LAN IP address on an iSCSI adapter

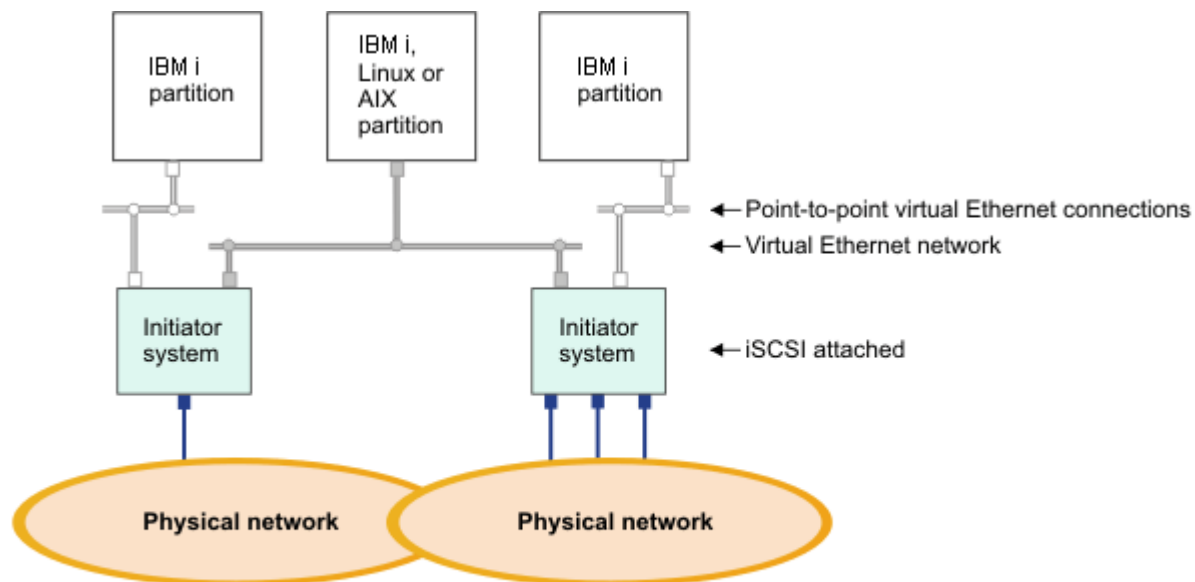
RZAHQ513-3

Figure 9: Virtual Ethernet tunneled through iSCSI networks

Virtual Ethernet tunneled through iSCSI networks has some special characteristics that are illustrated in the figure above.

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

### Virtual Ethernet networks that include more than one logical partition



■ or □ IP address on virtual adapter

■ IP address on external adapter or port

RZAHQ016-10

Figure 10: A simple, inter-partition virtual Ethernet network

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

Inter-partition connections exist between partitions or integrated servers that are assigned 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 that has a virtual LAN ID. To create the virtual adapter, see [Logical partitioning](#) in the IBM Systems Hardware Information Center. Note that within the same partition, Windows servers can communicate with each other by using the same virtual Ethernet port number.

**Related information:**

➤ [Managing virtual Ethernet networks](#)

➤ [Logical partitioning](#)

### 3.7.7 Physical networks

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

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

In an integrated server you can use any integrated network adapter or install a network adapter card as you would in a stand-alone server.

### 3.7.8 Network security

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

Network	Security Mechanisms
iSCSI network	<p>Consider the following two types of iSCSI network traffic.</p> <p><b>Storage</b> security can involve one or more of the following mechanisms:</p> <ul style="list-style-type: none"> <li>• Network isolation and physical security</li> <li>• Firewalls</li> <li>• Challenge Handshake Authentication Protocol (CHAP)</li> </ul> <p><b>Virtual Ethernet</b> security can involve one or more of the following mechanisms:</p> <ul style="list-style-type: none"> <li>• Network isolation and physical security</li> <li>• Firewalls</li> <li>• Secure Sockets Layer (SSL) connection for sensitive data during user enrollment and remote command submission</li> </ul>
Service processor connection	<p>Service processor security can involve one or more of the following mechanisms:</p> <ul style="list-style-type: none"> <li>• Service processor password</li> <li>• Network isolation and physical security</li> </ul>

The security mechanisms mentioned in the above table are described below:

Security Mechanism	Description
Network isolation and physical security	<p>Network isolation minimizes the risk that data might be accessed by unauthorized devices or that data that could be modified when it traverses the network. You can create an isolated network by using a dedicated Ethernet switch or a dedicated virtual local area network (VLAN) on a physical VLAN switch or network. Note that IBM i iSCSI target adapters do not support VLAN tagging. When you configure a VLAN switch, do <b>not</b> configure it to add a special VLAN tag to the frames.</p> <p>Physical security involves physical barriers that limit access to the network equipment and the network end points at some level (locked rack enclosures, locked rooms, locked buildings, and so on).</p>
Firewalls	<p>A firewall can be used between a shared network and IBM i to protect IBM i from unwanted network traffic. Similarly, a firewall can be used between a shared network and the initiator system to protect the initiator system from unwanted network traffic.</p> <p>iSCSI-attached system traffic has the following attributes that should be helpful when configuring a firewall:</p>



Security Mechanism	Description
	<ul style="list-style-type: none"> <li>• iSCSI target and initiator adapters have static IP addresses (there is a DHCP boot mode, but the IP addresses involved are statically pre-configured).</li> <li>• UDP and TCP ports that are deterministic and configurable. Each virtual Ethernet adapter on the hosted system uses a different UDP port to tunnel through the iSCSI network. Virtual Ethernet packets are encapsulated as follows, from outer header to inner header: <ul style="list-style-type: none"> <li>○ MAC and IP header for the iSCSI adapter using LAN (not SCSI) addresses.</li> <li>○ UDP header. See <a href="#">Configuring a firewall to allow integrated server connections</a> for information about optionally controlling UDP port selection.</li> <li>○ MAC and IP headers for the virtual Ethernet adapter.</li> </ul> </li> </ul>
Challenge Handshake Authentication Protocol (CHAP)	<p>CHAP protects against the possibility of an unauthorized system using an authorized system's iSCSI name to access storage. CHAP does not encrypt network traffic, but rather limits which system can access an IBM i storage path.</p> <p>CHAP involves configuring a secret that both IBM i and the hosted system must know. Short CHAP secrets may be exposed if the CHAP packet exchange is recorded with a LAN sniffer and analyzed offline. The CHAP secret should be random and long enough to make this method of attack impractical. IBM i can generate an appropriate secret. A hosted system uses the same CHAP secret to access all of its configured IBM i storage paths.</p> <p>You can configure two types of CHAP.</p> <ul style="list-style-type: none"> <li>• <b>Target CHAP</b> authenticates the iSCSI initiator adapters that connect to the iSCSI target adapter in IBM i.</li> <li>• <b>Initiator CHAP</b> authenticates the iSCSI target adapters that connect to the iSCSI initiator adapter in the System x or blade hardware.</li> </ul> <p><b>Note:</b> Target CHAP is a prerequisite for Initiator CHAP, so initiator CHAP is also called <b>bidirectional</b> or <b>mutual</b> CHAP.</p> <p><b>Note:</b> Initiator CHAP is only supported for the iSCSI initiator that is used as the boot device.</p>
Secure Sockets Layer (SSL) connection between IBM i and Windows	<p>The IBM i Integrated Server Support option includes user enrollment and remote command submission functions, which may transfer sensitive data over the point-to-point virtual Ethernet. These applications automatically set up an SSL connection to encrypt their sensitive network traffic, and to ensure that each side of the conversation is authentic, based on automatically installed digital certificates. This security feature is provided by default and is not configurable. File data, command results, and traffic for other applications are not protected by this SSL connection.</p>
Service processor password	<p>This password is managed by IBM i and is used when IBM i starts a conversation with the service processor of the integrated server. The service processor checks the password to ensure that the IBM i configuration is authentic. New service processors have a default name and password. IBM i provides a way to change the password.</p>

**Related information:**

- [Changing a service processor password for an integrated server](#)
- [Configuring CHAP for integrated servers](#)
- [Configuring target CHAP](#)
- [Configuring initiator CHAP](#)

## 3.8 Performance concepts

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

The iSCSI-attached systems have their own memory and one or more processors, but share the IBM i hard disk storage through virtual (simulated) disk drives (virtual storage). The disk drives are allocated to integrated servers by creating an IBM i virtual disk (network server storage space). The major difference between the integrated servers and stand-alone servers is that stand-alone servers tend to use dedicated disk drives and the integrated servers use IBM i storage spaces as virtual disks.

Integrated Windows servers also include optional features to share IBM i tape, CD and DVD drives. Integrated Windows servers can use high-speed virtual Ethernet networks to communicate with other integrated servers or Power server logical partitions.

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

### 3.8.1 Virtual storage performance

Virtual storage performance depends on the configuration of the integrated server environment.

For performing processor or memory intensive work on an integrated server, the performance characteristics are equivalent to a standalone server using dedicated disk drives. However, since the integrated server disk drives (virtual storage) are allocated out of IBM i storage, the disk performance is dependent on IBM i.

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

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

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

On an integrated server, the IBM i storage, CPU and memory are shared between the integrated server and IBM i applications. It is normal for disk response to swing through a larger range. Short periods might occur where I/O operations from multiple integrated servers, or other IBM i operations contend for the same disk. Some disk intensive IBM i applications (like SAV and RST) can reduce the disk

performance seen on the integrated server for a period of time. This can make it more difficult to choose a threshold value for short time periods.

### **Storage space balancing for integrated servers**

The disks in the IBM i storage pool (ASP) 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 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 IBM i storage architecture, regardless of how an ASP or independent ASP is configured.

IBM i 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.

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

You can monitor how well IBM i is fulfilling the integrated server's disk requirements by using the [Work with Disk Status \(WRKDSKSTS\)](#) and [Work with NWS Storage Spaces \(WRKNWSSTG\)](#) commands.

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

### **Consider the entire group of IBM i disks when you evaluate storage bottlenecks for integrated Windows servers**

The IBM 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 IBM i 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.

#### **Related information:**

- *Integrated BladeCenter and System x Performance* chapter of the [Performance Capabilities Reference](#)

## 3.8.2 IBM i memory requirements

Configuring IBM i with enough memory allocated to iSCSI-attached servers is very important for performance. iSCSI-attached integrated servers use a combination of memory in the IBM i machine, base, and optional memory pools.

See the *Integrated BladeCenter and System x Performance* chapter of the [Performance Capabilities Reference](#) for background information about iSCSI-attached integrated servers and IBM i memory pools.

**Note:** 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

### 3.8.2.1 Machine pool

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

### 3.8.2.2 iSCSI virtual storage I/O memory pool

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

To move the iSCSI virtual storage I/O out of the \*BASE memory pool into its own memory pool, configure a dedicated memory pool to use for iSCSI I/O. This change can prevent the iSCSI I/O from adversely affecting the performance of any process that runs in the \*BASE memory pool. This is especially important if you are planning to have an IBM i partition with multiple iSCSI-attached servers, or with an iSCSI-attached server that performs a large amount of disk activity.

The type of memory pool that is used for iSCSI I/O varies based on the IBM i version:

IBM i	Memory Pool Type	Considerations
i 7.2 i 7.1 i 6.1	Shared data memory pool	<p>There are a couple of ways to create the iSCSI memory pool:</p> <ol style="list-style-type: none"> <li>1. The <b>Create Server <a href="#">Web GUI</a></b> task provides an option to create a default iSCSI memory pool.</li> <li>2. Otherwise, you can use the IBM i <a href="#">Work with Shared Storage Pools (WRKSHRPOOL)</a> or <a href="#">Change Shared Storage Pool (CHGSHRPOOL)</a> command to create an iSCSI memory pool.</li> </ol> <p>See <a href="#">Prepare for IBM i memory requirements</a> for details.</p>
i 5.4	Private memory pool	<p>The private memory pool is enabled by creating a subsystem description named QGPL/QFPHIS and allocating a private memory pool of at least 4096 kilobytes. The amount of memory you want to allocate will depend on a number of factors, including number of iSCSI network servers, expected sustained disk activity for all servers, etc.</p> <p>See <a href="#">Prepare for IBM i memory requirements</a> for details.</p>

**Notes:**

1. Use the iSCSI memory pool when installing iSCSI-attached servers.
2. If you already have iSCSI-attached servers installed that use the \*BASE pool, configure those servers to use the iSCSI memory pool. Use the server properties in the IBM i GUI or the [Change Network Server Desc \(CHGNWSD\)](#) command.
3. The amount of memory required for the iSCSI memory pool depends on a number of factors, including the number of iSCSI-attached servers and the expected sustained disk activity for all servers. For most environments, you can use an iSCSI memory pool with a size of **512 MB**. This iSCSI memory pool can be shared among all the iSCSI-attached servers on your system. If you notice an excessive number of page faults in the iSCSI memory pool, you can increase the iSCSI memory pool size to see if that helps.

**Related information:**

- *Integrated BladeCenter and System x Performance* chapter of the [Performance Capabilities Reference](#)

### 3.8.3 Virtual Ethernet performance for integrated Windows servers

The Virtual Ethernet point-to-point connection is the default virtual network connection between the hosting IBM i 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 IBM 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 storage, tape and other integrated server operations. You can separate virtual Ethernet operations from storage operations by using another iSCSI target adapter.

A Virtual Ethernet connection between two or more integrated servers uses the IBM i CPU to switch the traffic between servers, even when IBM i is not an endpoint of the traffic. For most connections this utilization is not significant. If you expect high sustained network loads across the virtual Ethernet

connection between integrated Windows servers, you might want to balance the cost of using the Virtual Ethernet internal switch against external network adapters on the integrated servers.

### 3.8.4 MTU considerations for the iSCSI network

By default, iSCSI normally uses standard 1500 byte frames. You can configure the network to use other Ethernet frame sizes to adjust network performance.

High bandwidth and low latency is desirable for the iSCSI network. Storage and virtual Ethernet can take advantage of a maximum transmission unit (MTU) up to a 9000 byte 'jumbo' frame if the iSCSI network supports the larger MTU. As a rule of thumb, a larger MTU typically decreases the amount of CPU utilization that is required on IBM i and the integrated server.

- Jumbo frames significantly improve performance for a software initiator to software target iSCSI network. Therefore, if your iSCSI network uses all software initiators and all software targets, and the network switches support jumbo frames, then use jumbo frames.
- However, if your iSCSI network uses any hardware initiators or hardware targets, or if the network switches do not support jumbo frames, then use standard frames.

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

MTU considerations for each component of the iSCSI network:

Component	MTU Considerations
iSCSI target	IBM i iSCSI target adapters automatically negotiate an MTU, up to 9000 bytes, that is compatible with initiators using the TCP/IP protocol. Therefore, you do not need to configure an MTU for the iSCSI target.
iSCSI initiator	<p>iSCSI initiator adapters default to a frame size that can be transported in a standard 1500 byte Ethernet frame.</p> <p>Hardware initiators (iSCSI HBAs) can be configured to use up to 9000 byte MTUs.</p> <p>Some software initiators (Ethernet NICs) support larger MTUs and some do not. Check your Ethernet NIC documentation to determine if the Ethernet NIC can use a larger MTU.</p> <p>If you want to use an MTU larger than 1500 bytes, you must configure it at each iSCSI initiator adapter.</p>
Switch	<p>Network switches typically use a default 1500 byte MTU.</p> <p>Some switches support larger MTUs and some do not. Check your switch documentation to determine if the switch can use a larger MTU.</p> <p>If you want to use an MTU larger than 1500 bytes, you must configure it on the switch. See your switch documentation for more information.</p>

**Related information:**

- [Changing the iSCSI initiator MTU](#)
- *Integrated BladeCenter and System x Performance* chapter of the [Performance Capabilities Reference](#)

### 3.9 Backup and recovery concepts

You can back up and recover integrated server data from IBM i, from the integrated server operating system, or a combination of both.

When you are planning your backup strategy, refer to the following sources:

- [IBM i configuration objects for integrated servers](#)
- [What objects to save and their location on IBM i](#)
- [Backup and recovery](#) in the Information Center
- Microsoft or VMware documentation
- Chapter 7: **Backup and recovery** in Redbook [Implementing Integrated Windows Server through iSCSI to System i5](#) (SG24-7230-00)
- Chapter 5: **Backup and recovery** in Redbook [VMware VI3 on BladeCenter and System x Integrated with System i](#) (SG24-7408-00)

The following table summarizes the methods you can use to backup and recover data related to integrated servers:

Method	Description
Backup your entire IBM i system	<p>You can back up the entire IBM i system, including IBM i configuration objects and virtual storage spaces for integrated servers.</p> <p>See <a href="#">Backing up your system</a> in the Information Center.</p>
Recover your entire IBM i system	<p>You can restore the entire IBM i system, including IBM i configuration objects and virtual storage spaces for integrated servers.</p> <p>See <a href="#">Recovering your system</a> in the Information Center.</p>
Backup virtual storage from IBM i	<p>You can backup entire IBM i virtual storage spaces that the integrated server uses along with your other IBM i data. This is the fastest method for backing up large amounts of data.</p> <p>The virtual storage spaces for an integrated server are in the integrated file system. To save the virtual storage from IBM i, you use the <a href="#">Save (SAV)</a> command.</p> <p>This backup method provides a copy of the storage that can be used for <b>disaster recovery</b>. You can use this backup to restore the entire storage space, but <u>not</u> individual files and directories within the storage space.</p> <p><b>Note:</b> Treat the network server description, predefined virtual storage, and any user defined virtual storage linked to an integrated server as a unit. Save and restore them at the same time. Together they constitute a complete system, and should be treated as such. Otherwise, the integrated server might not start or run correctly after the data is restored.</p> <p>Storage spaces can be backed up under the following conditions:</p> <ol style="list-style-type: none"> <li>1. While the server is <b>shut down</b></li> </ol> <p>Any storage space can be backed up while the associated integrated server is shut down. This backup is consistent with the state of the storage when the server was most recently shut down.</p>

Method	Description	
	<p>2. While the server is <b>active</b> – save while active (SWA)</p> <p>A storage space can be backed up while the associated integrated server is <b>active</b> for the server OS and IBM i version combinations listed below.</p> <p>This SWA method implicitly uses the IBM i <b>storage space snapshot</b> support to do a concurrent save of the virtual storage spaces without requiring the server to be shut down or applications ended.</p> <p><b>Note:</b> This backup method uses a side file on IBM i to queue changes to the storage space while it is being backed up. Once the backup is finished, the queued changes in the side file are merged into the storage space.</p>	
	Server OS	Additional Considerations
	<p><b>Windows on i 6.1 or later</b></p>	<p>Since the server OS and applications are active when the side file processing is started, there is the potential that data on the disk is not consistent at that point. However, you can provide a <b>freeze</b> script to help get the server into a consistent state before the side file processing starts. You can also provide and <b>thaw</b> script to resume normal application processing once the side file is established. See <a href="#">Backing up virtual storage for active Windows servers</a> for additional considerations.</p>
	<p><b>ESX on i 7.1 or later</b></p>	<p>When saving a storage space that contains active VMware ESX virtual machines, the save process automatically uses VMware ESX utilities to create a virtual machine snapshot named <b>IBMi_NWSSTG_SWA</b> that can be used as a safe and consistent recovery point. The IBMi_NWSSTG_SWA snapshot is automatically deleted once the IBM i save processing is completed, which merges the changes made since the snapshot into the base.</p>
<p>Restore virtual storage from IBM i</p>	<p>You can restore entire IBM i virtual storage spaces that the integrated server uses. This is the fastest method for restoring large amounts of data.</p> <p>The virtual storage spaces for an integrated server are in the integrated file system. To restore virtual storage for integrated servers, use the <a href="#">Restore (RST)</a> command.</p> <p>The integrated server must be shut down in order to restore a storage space.</p> <p><b>ESX on i 7.1 or later (SWA):</b> Note that when saving active ESX servers, after the IBMi_NWSSTG_SWA snapshot is taken during the save operation, the virtual machine resumes normal operations while the storage space is being saved, so the save process could capture inconsistent data that is being written by the virtual machine after the snapshot is taken. Therefore, after restoring a VMware ESX storage space that was saved while the ESX server was active, any virtual machines that used the storage space will resume using the latest data that is on the storage space, which might <b>not</b> be in a consistent state. You must revert to the virtual machine IBMi_NWSSTG_SWA snapshot that was taken when the storage space was saved in order to ensure that the virtual machine data is in a consistent state.</p> <p>See <a href="#">Reverting to a consistent SWA virtual machine snapshot after restore</a>.</p>	



Method	Description
<p>File level backup and recovery from IBM i</p> <p><b>(Windows only)</b></p>	<p>You can save integrated Windows server data (files, directories, shares, and the Windows registry) to tape, optical or disk (*SAVF) along with other IBM i data and restore the data on an individual basis. This method uses the <a href="#">Save (SAV)</a> and <a href="#">Restore (RST)</a> commands.</p> <p>File-level backup and recovery of Windows data is enabled through the IBM i NetClient file system (<b>QNTC</b>) of the Integrated File System (IFS). The process involves the following tasks:</p> <ol style="list-style-type: none"> <li>From Windows, define file share names for the data that will be backed up from IBM i.</li> </ol> <p><b>Note:</b> Windows share names are visible from IBM i under the <code>/QNTC/servername</code> directory in the IFS, but only if the IBM i user profile has authority to access to the share name on Windows. For example, the share name could allow public access or the IBM i user profile could be explicitly authorized to the share name from Windows.</p> <p><b>Tip:</b> Enroll the IBM i user profile to Windows. See <a href="#">User and group enrollment concepts for integrated Windows servers</a>.</p> <ol style="list-style-type: none"> <li>Enable which share names under the <code>/QNTC/servername</code> directory can be saved from IBM i by adding a member to the QAZLCSAVL file in QUSRSYS and listing the share names to enable. See <a href="#">Enabling Windows share names for file level backup from IBM i</a>.</li> </ol> <p><b>Note:</b> By default, the directories and files under the QNTC share names are <b>not</b> savable from IBM i.</p> <ol style="list-style-type: none"> <li>Use the IBM i SAV and RST commands to address the IFS directories for those shares in order to save and restore the Windows data that is visible through those shares.</li> </ol> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This method implicitly uses the Windows <b>Volume Shadow-copy Service</b> to ensure that objects are saved in a consistent and complete manner.</li> <li>The integrated Windows server must be <b>active</b> for this backup and recovery method.</li> </ul>
<p>File level backup and recovery from Windows, using an IBM i tape device</p> <p><b>(Windows only)</b></p>	<p>You can save integrated Windows server data (files, directories, etc.) to an IBM i tape device and restore the data on an individual basis. This method uses a native Windows backup application, such as the Windows Server 2003 <b>Backup</b> utility or a third party Windows backup product.</p> <p><b>Note:</b> With this method, you must allocate (lock) the IBM i tape device from Windows before starting the backup and free (unlock) the IBM i tape device once the backup is complete. See <a href="#">IBM i tape and optical devices shared with integrated Windows servers</a>.</p> <p><b>Note:</b> The integrated Windows server must be <b>active</b> for this backup and recovery method.</p>

Method	Description
File level backup and recovery from the integrated server OS, using native utilities	<p>You can save integrated server data (files, directories, etc.) and restore the data on an individual basis using a native utilities provided by the integrated server operating system or a third party backup product. With this method, store the backup data on a network attached tape device or a network share.</p> <p>For example, you could map a network drive to another computer and backup the integrated server data to that location. Then you can use the other computer to back up the data to a physical tape device, if required. In this scenario, the network drive could be on an arbitrary server in the network, or even on an IBM i system (using a NetServer file system share).</p> <p><b>Note:</b> The integrated server must be <b>active</b> for this backup and recovery method.</p>
Backup IBM i configuration objects	<p>You can backup IBM i configuration objects using several methods, depending on the object type. See the following topics for details:</p> <ul style="list-style-type: none"> <li>• <a href="#">Backing up the NWSD of an integrated server</a></li> <li>• <a href="#">Backing up NWSH objects</a></li> <li>• <a href="#">Backing up NWSCFG objects and validation lists</a></li> </ul> <p><b>Note:</b> Treat the network server description, predefined virtual storage, and any user defined virtual storage linked to an integrated server as a unit. Save and restore them at the same time. Together they constitute a complete system, and should be treated as such. Otherwise, the integrated server might not start or run correctly.</p>
Restore IBM i configuration objects	<p>You can restore IBM i configuration objects using several methods, depending on the object type. See the following topics for details:</p> <ul style="list-style-type: none"> <li>• <a href="#">Restoring integrated server NWSDs</a></li> <li>• <a href="#">Restoring NWSH objects</a></li> <li>• <a href="#">Restoring NWSCFG objects and validation lists</a></li> </ul>
Saving user enrollment information	<p>You can save the enrollment definitions using options 8, 21 or 23 on the GO SAVE menu, the <a href="#">Save Security Data (SAVSECDTA)</a> command, or the <a href="#">Save Object List (QSRSAVO)</a> API.</p>
Restoring user enrollment information	<p>You can restore the user profiles using the <a href="#">Restore User Profiles (RSTUSRPRF)</a> command and specifying USRPRF(*ALL) or SECDTA(*PWDGRP) values.</p>

**Related information:**

- [Backup and Recovery Capabilities](#)
- [Backup and recovery](#)
- [IBM i configuration objects for integrated servers](#)
- [Backing up virtual storage for integrated servers](#)
- [Save While Active \(SWA\) for integrated VMware ESX servers on i 7.1 or higher](#)
- [Restoring virtual storage for integrated servers](#)
- [IBM i tape and optical devices shared with integrated Windows servers](#)
- [IBM i tape devices for Windows Server 2008/2012](#)
- [IBM i tape devices for Windows Server 2003](#)
- [Enabling Windows share names for file level backup from IBM i](#)

### 3.9.1 What objects to save and their location on IBM i

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 IBM i GO SAVE command. Option 21 saves the entire system. Option 22 saves system data. Option 23 saves all user data (which includes storage spaces).

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

Use this table to determine which objects need to be saved when you save your integrated server and the command to use.

Object	Object Name	Object Location	Object Type	Save command
Virtual disks	Various (Predefined <i>nwsdname1</i> , <i>nwsdname2</i> , and user-defined)	/QFPNWSSTG	Network server storage space	GO SAVE, option 21 or 23  SAV OBJ('/QFPNWSSTG/ <i>nwsstg</i> ') DEV('/QSYS.LIB/ <i>TAP01</i> .DEVD')
				<b>i 5.4 only:</b> If the disk is in a user ASP: SAV OBJ('/QFPNWSSTG/ <i>nwsstg</i> ') ( '/dev/QASP <i>nn</i> / <i>nwsstg</i> .UDFS')
				<b>i 5.4 only:</b> If the disk is in an independent user ASP: SAV OBJ('/QFPNWSSTG/ <i>nwsstg</i> ') ( '/dev/ <i>aspdev</i> / <i>nwsstg</i> .UDFS')
				DEV('/QSYS.LIB/ <i>TAP01</i> .DEVD')
Windows server files and directories	Various	/QNTC/ servername/ sharename	Directory	GO SAVE, option 21 or 22  SAV OBJ('/QNTC/...')
				DEV('/QSYS.LIB/ <i>TAP01</i> .DEVD')
IBM i device config. objects for integrated servers	Various	QSYS	NWSD, NWSH, LIND, etc.	GO SAVE, option 21, 22, or 23 SAVCFG DEV( <i>TAP01</i> )
iSCSI remote system, service processor, and connection security objects	Various	QUSRSYS	NWSCFG and associated VLDL	SAVOBJ LIB(QUSRSYS) OBJTYPE(*NWSCFG *VLDL) DEV( <i>TAP01</i> )
IBM i TCP interfaces	QATOCIFC	QUSRSYS	Physical file	GO SAVE, option 21 or 23  SAVOBJ LIB(QUSRSYS) OBJ(QATOCIFC QATOCLIFC) DEV( <i>TAP01</i> ) OBJTYPE(*FILE)
	QATOCLIFC	QUSRSYS	Logical file	<b>Note:</b> TCP/IP must be ended when you save the files.
iSCSI path certificate store	nwsdname.*	/QIBM/ UserData/ NWSDCert	Certificate store file	GO SAVE, option 21 or 23  SAV OBJ('/QIBM/UserData/ NWSDCert/nwsdname.*')
				DEV('/QSYS.LIB/ <i>TAP01</i> .DEVD')
User profile enrollment information	Various	QSYS	User profile	GO SAVE, option 8, 21, or 23 SAVSECDTA DEV( <i>TAP01</i> )

Object	Object Name	Object Location	Object Type	Save command
Messages from the integrated server	Various	Various	Message queue	GO SAVE, option 21 or 23 SAVOBJ OBJ( <i>msgq</i> ) LIB( <i>library</i> ) OBJTYPE(*MSGQ) DEV( <i>TAP01</i> )
IBM i Integrated Server Support	QNTAP	QSYS	Library	SAVLICPGM LICPGM( <i>57xxSSI</i> ) <sup>1</sup> OPTION(29) DEV( <i>TAP01</i> )
	NTAP and subdirectories	/QIBM/ ProdData/ NTAP	Directory	
<b>Notes:</b>				
<sup>1</sup> The specific <i>57xx</i> product IDs for each IBM i release are: <b>5770</b> for <b>i 7.2 and i 7.1</b> , <b>5761</b> for <b>i 6.1</b> , and <b>5722</b> for <b>i 5.4</b> .				

**Note:** The [Manually saving parts of your system](#) articles in the Information Center have more information about using the save commands.

### 3.10 High availability concepts

Integrated servers can be made highly available through multipath storage connections, hot spare hardware, or clustering.

#### 3.10.1 Multipath I/O (MPIO)

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

You can configure the iSCSI environment to support multiple iSCSI targets, multiple iSCSI initiators, and multiple storage connections.

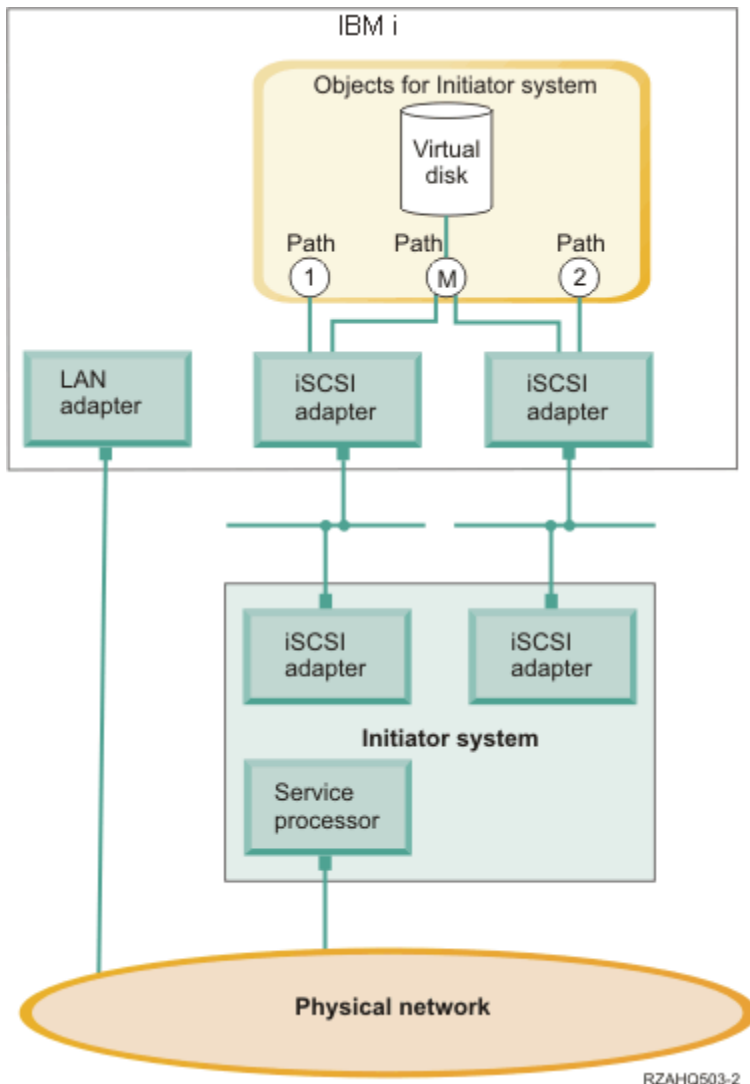


Figure 11: An environment with multiple iSCSI adapters installed in the target and initiator systems

#### Paths

Paths are connection points between virtual devices and iSCSI target adapters in IBM i. A virtual device being hosted by IBM i is said to be linked to a path. iSCSI initiator adapters access the virtual device through the path.

When the network server description (NWSD) for an integrated server is started, the associated IBM i virtual storage or devices are linked to a network server host adapter (NWSH) object. For example, a configured virtual disk (such as Drive C:) hosted in IBM i is linked to the NWSH that represents the iSCSI target adapter.

There are several storage paths defined in the above figure. The paths labeled **1** and **2** each represent a single iSCSI target adapter. The path labeled **M** represents the multipath group, which is a group of iSCSI target adapters.

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

Removable media and virtual Ethernet connections use a single path. Connections for these devices cannot use the multipath group.

### **Multipath I/O and storage connection redundancy**

An integrated server can use multiple iSCSI data paths to access virtual disks hosted by IBM i.

You can configure a multipath group of two or more iSCSI target adapters. Then specify that a virtual disk is accessed using the multipath group instead of a single iSCSI target adapter. With this configuration, the data on the virtual disk can be accessed using any of the iSCSI target adapters in the multipath group.

In the above figure, the multipath group is defined as path **M**. The virtual disks that are linked to the multipath group can be accessed by any of the iSCSI target adapters that are part of the multipath group. Only one multipath group can be defined per integrated server. This group can include up to four iSCSI target adapters.

For the most reliable storage network, do the following things:

- Configure multiple iSCSI targets in IBM i and define a multipath group that contains them.
- Configure multiple iSCSI initiators in the System x or blade server and configure them in the IBM i remote system configuration.
- Configure multiple switches to provide redundant network connections between the iSCSI targets and iSCSI initiators.
  - If you are using a BladeCenter system, configure multiple switch modules.
  - If you are using System x hardware, configure multiple switches in the iSCSI network.
- Link all storage to the multipath group.

**Note:** Removable media devices cannot use the multipath group.

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

For more information about installing the required software components and linking storage to the multipath group, as well as information about iSCSI initiator MPIO capabilities that vary by operating system type, see [Configuring multipath I/O for integrated servers](#).

## Virtual Ethernet and initiator connection redundancy

Virtual Ethernet does not have the same multipath I/O concept that storage does. Virtual Ethernet supports iSCSI initiator redundancy, but not iSCSI target redundancy:

- If the integrated server has multiple iSCSI initiator adapters, the iSCSI initiator that is used for a particular virtual Ethernet adapter is automatically selected. If there are no failures, the virtual Ethernet adapter continues to use the selected iSCSI initiator. However, if the iSCSI initiator connection fails (for example, an initiator cable is pulled or the initiator card fails), a different iSCSI initiator adapter is automatically selected for the virtual Ethernet adapter and is used until another failure occurs.

**Note:** In order for the automated selection process to work, the configured iSCSI target adapter must still be accessible by at least one iSCSI initiator adapter that is listed in the IBM i remote system configuration.

- There is no multipath group available for virtual Ethernet. A virtual Ethernet adapter is configured to use a specific iSCSI target and always uses that target. If the iSCSI target adapter fails or its cable is pulled, any virtual Ethernet adapters that are configured to use that iSCSI target adapter stop communicating. However, if the cable is plugged back in, communication automatically resumes.

For the most reliable virtual Ethernet network, do the following things:

- Configure multiple iSCSI initiators in the System x or blade server and configure them in the IBM i remote system configuration.
- Ensure that multiple iSCSI initiators can access the same IBM i iSCSI target.

## 3.10.2 Hot spare support for integrated servers

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

IBM i Integrated Server Support and storage virtualization provide innovative options that can enhance the reliability and recoverability of the integrated server environment. 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.

Hot spare support is available for System x or blade hardware as well as IBM i iSCSI target adapters. These hot spare types are described in the following subsections.

### Related information:

- [Using hot spare integrated server hardware](#)
- [Using hot spare iSCSI hardware target adapters](#)
- [Using hot spare iSCSI software target adapters](#)

### 3.10.2.1 Hot spare support for System x or blade hardware

If the System x or BladeCenter blade server hardware fails, you can quickly and easily switch the integrated server configuration to hot spare System x or blade hardware. Hot spare support also adds flexibility by enabling one spare server to be used to protect multiple production servers. This may reduce the overall number of servers needed to provide increased availability.

**Server hardware compatibility:** Switching a Windows or VMware ESX server from one set of server hardware to another is like migrating the Windows or ESX system drive from one PC to a second PC. Differences in the required hardware abstraction layer (HAL), the server firmware (UEFI or BIOS) level, or the devices that are installed on the two PCs can cause problems with the migration. During the initial boot of Windows or ESX on the second PC, hardware differences are detected and are handled in one of several ways:

- Some can be automatically handled using plug and play.
- Others might require manual intervention. For example a new device driver might need to be installed.
- If the hardware differences are great enough, they could prevent the second PC from booting. For example, the two PCs might require incompatible versions of the HAL.

These same hardware compatibility considerations apply when hot sparing between iSCSI-attached BladeCenter blade and System x servers. In order for the hot spare migration to work successfully, the hardware configurations of the two servers must be closely matched.

Therefore, in order to use hot spare server hardware in the IBM i iSCSI environment, it is strongly recommended that the two BladeCenter blade or System x models be the same type. For example, an HX5 type 7872 blade can be a hot spare for another HX5 type 7872 blade. In addition, the BladeCenter blade or System x models should have a similar configuration of PCI adapters, etc.

**Server operating system compatibility:** Server hardware that is **not** configured for an embedded version of VMware ESX can typically be used to provide hot spare support for both Windows and non-embedded versions of ESX. However, since embedded versions of VMware ESX boot from flash memory, they require a specific hardware configuration that is incompatible with Windows or non-



embedded versions of ESX. For example, the server boot options for embedded versions of ESX are different than for other types of servers. Therefore, server hardware that is configured for an embedded version of VMware ESX can only be used to provide hot spare support for another server with the same embedded version VMware ESX.

**Windows Server activation:** Each time a Windows server's storage spaces are switched to another hot spare server, Windows Activation might be triggered:

- **Windows Server 2012:** Activation might require either a phone or on-line activation. Volume Activation 2.0 allows for volume licensing and transparent activation using either the Multiple Activation Key (MAK) or the Key Management Service (KMS) key.
- **Windows Server 2008:** Activation might require either a phone or on-line activation. Volume Activation 2.0 allows for volume licensing and transparent activation using either the Multiple Activation Key (MAK) or the Key Management Service (KMS) key.
- **Windows Server 2003:** There are a limited number of free activations per license key. If activation is triggered enough times, this may require a phone call to Microsoft in order to re-activate. Volume licenses of Windows Server 2003 can help in this case, since there is no activation.

**Related information:**

- [Using hot spare integrated server hardware](#)

### 3.10.2.2 Hot spare support for IBM i iSCSI target adapters

If an IBM i iSCSI target adapter that the System x or blade server is using has a hardware failure, you can quickly switch the IBM i configuration for the System x or blade server to use a spare iSCSI target adapter and restart the System x or blade server. iSCSI adapters and hosted systems involved in hot spare need to be on the same switched network. The hot spare iSCSI target adapter must be on the same iSCSI network and subnet as the one that failed so that the System x or blade server can access the virtual storage using the hot spare IBM i iSCSI target adapter without needing to reconfigure the iSCSI network.

**Related information:**

- [Using hot spare iSCSI hardware target adapters](#)
- [Using hot spare iSCSI software target adapters](#)

### 3.10.3 IBM i clustering for integrated servers

You can include the disks and configuration information for integrated servers in an IBM i cluster.

See the following topics in the Information Center for an overview of IBM i clustering concepts:

- [High availability overview](#)
- [High availability technologies](#)

Some key items to note when integrated servers participate in an IBM i cluster:

Item	Notes
<b>Cluster Administrative Domain</b>	Used to replicate integrated server configuration objects between nodes in the IBM i cluster.
<b>Geographic mirroring</b>	Preferred method to replicate integrated server storage between nodes in the IBM i cluster.

**Related information:**

- [Implementing high availability](#)
- [Implementing IBM i clustering for integrated servers](#)

### 3.11 User and group enrollment concepts for integrated Windows servers

Learn about how IBM i users and groups interact with integrated Windows servers.

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

The key concepts for the enrollment function are described below:

Concept	Description
Enrollment	<p>Enrollment is the process by which an IBM i user or group profile is registered with the integration software.</p> <p>The enrollment process happens automatically when triggered by an event such as:</p> <ul style="list-style-type: none"> <li>• Using the IBM i GUI or the <a href="#">Change NWS User Attributes (CHGNWSUSRA)</a> command to enroll a user or group.</li> <li>• An enrolled Windows user updating their IBM i user profile password or user attributes.</li> <li>• Restarting the integrated server.</li> </ul> <p>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.</p>
Windows domains and local servers	<p>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 IBM i user accounts into the Windows domain.</p> <p>On the other hand, if you enroll IBM i 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.</p> <p><b>Note:</b> 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. IBM i user accounts cannot be enrolled to Windows workgroups.</p>
Special groups created by IBM i on an integrated Windows server	<p>Two groups of users are created in Microsoft Windows as part of the installation to an integrated Windows server.</p> <p><b>AS400_Users</b>            Every IBM i user, when first enrolled to the Windows server, is placed in the AS400_Users group. You can remove a user from this group in the Windows server; however, the next time an update occurs from IBM i, the user will be replaced. This group is a useful place to check which IBM i user profiles are enrolled to the Windows server.</p>

Concept	Description
	<p><b>AS400_Permanent_Users</b></p> <p>Users in this group cannot be removed from the Windows server by IBM i. It is provided as a way to prevent Windows users from being accidentally deleted by actions taken within IBM i. Even if the user profile is deleted from IBM i, the user will continue to exist in the Windows server. Membership in this group is controlled from the Windows server, unlike the AS400_Users group. If you delete a user from this group, it will not be replaced when an IBM i update is performed.</p>
<p>Using the IBM i user profile local password management (LCLPWDMGT) attribute</p>	<p>There are two ways to manage user profile passwords.</p> <p><b>Traditional user (password managed by IBM i)</b></p> <p>You may choose to have IBM i passwords and Windows passwords be the same. Enrolled Windows users manage their passwords in IBM i. This is configured by setting LCLPWDMGT(*YES) in the IBM i user profile. This is the default setting.</p> <p><b>Windows password-managed user</b></p> <p>You may choose to manage enrolled Windows profile passwords in Windows without IBM i overwriting the password. This is configured by setting LCLPWDMGT(*NO) in the IBM i user profile.</p> <p>For more information see <a href="#">Enrolled user account options for integrated Windows servers</a>.</p>
<p>Using IBM i Enterprise Identity Mapping (EIM)</p>	<p>Defining EIM associations allows IBM i to support Windows single sign-on using an authentication method such as Kerberos. There are two ways to take advantage of the IBM i EIM support:</p> <ol style="list-style-type: none"> <li>1. You can automatically create an EIM association using functions in the EIM Windows registry. Auto-creation and deletion of Windows EIM source associations are done when the IBM i Create, Change, or Delete user profile (CRTUSRPRF, CHGUSRPRF, or DLTUSRPRF) commands are used, specifying the EIMASSOC parameter values of *TARGET, *TGTSRC, or *ALL.</li> <li>2. You may manually define EIM associations in the EIM Windows registry. When an EIM IBM i target association and Windows source association is defined for an IBM i user profile, the enrolled IBM i user profile may be defined as a different user profile name in Windows.</li> </ol> <p><b>Note:</b> SBMNWSCMD, QNTC, and file level backup operations only work with EIM Kerberos associations. IBM i user profiles mapped to different Windows user names using an EIM Windows registry are not recognized. Those operations still attempt to use equivalent names.</p> <p>For more information see <a href="#">Enrolled user account options for integrated Windows servers</a> and <a href="#">Configuring Enterprise Identity Mapping for integrated Windows servers</a>.</p>
<p>Enrolling existing Windows user profiles</p>	<p>You can also enroll a user who already exists in the Windows server. The password for the user must be the same on IBM i as for the already existing Windows user or group.</p>

Concept	Description
User enrollment templates	<p>You can customize the authorities and properties a user receives during enrollment through the use of user enrollment templates. See <a href="#">User enrollment templates for integrated Windows servers</a>.</p> <p>If you do <b>not</b> use a template when you enroll users, they receive the following default settings:</p> <ul style="list-style-type: none"> <li>Users become members of the <b>AS400_Users</b> group and either the <b>Users</b> group in a local integrated Windows server or the <b>Domain Users</b> group on a Windows domain.</li> <li>IBM i keeps track of the user's IBM i password, password expiration date, description, and enabled or disabled status.</li> </ul>
Enrolling IBM i groups	<p>Up to this point, only the enrollment of individual IBM i user profiles to the Windows server has been discussed. You can also enroll entire IBM i groups. Then, when you add users to those IBM i groups that have been enrolled to the Windows server, you automatically create and enroll those users in the Windows server as well.</p>
Enrolling to multiple domains	<p>You may enroll users and groups to multiple domains, but typically this is unnecessary. In most Windows servers, multiple domains set up trust relationships with each other. In such cases, you only need to enroll the user in one domain because trust relationships automatically give the user access to other domains. See your Windows documentation for additional information about trust relationships.</p> <p><b>Note:</b> Although one windows server can host multiple domains in the same Active Directory, one integrated server instance (NWSD) is limited to enrolling users to one domain at a time. Attempts to enroll users or groups to additional domains will fail.</p>
Using the NWSD propagate domain user (PRPDMNUSR) parameter	<p>If you have multiple servers which are members of the same domain, you can prevent duplicate domain enrollment from occurring on each member server. Use the Propagate Domain User (PRPDMNUSR) parameter in the <a href="#">Change Network Server Desc (CHGNWSD)</a> command.</p> <p>See <a href="#">Preventing enrollment to an integrated Windows server</a> for more information.</p>
Using the NWSD disable user profile (DSBUSRPRF) parameter	<p>You can specify whether you want user profiles on integrated Windows servers to be disabled when the corresponding IBM i user profiles are disabled. Use the Disable User Profile (DSBUSRPRF) parameter on the <a href="#">Change Network Server Desc (CHGNWSD)</a> command.</p>

**Related information:**

- [User Enrollment Capabilities](#)
- [Enrolling IBM i users to integrated Windows servers](#)
- [Enrolling IBM i groups to integrated Windows servers](#)
- [Changing the local password management user profile attribute](#)
- [Configuring Enterprise Identity Mapping for integrated Windows servers](#)
- [Saving user enrollment information for integrated Windows servers](#)
- [Restoring user enrollment information for integrated Windows servers](#)

### 3.11.1 Enrolled user account options for integrated Windows servers

You can manage passwords for enrolled Windows users in either Windows or IBM i.

The types of user configurations for the enrollment function are described below:

User type	Description	User Profile Attributes
<p>Traditional user (password managed on IBM i)</p>	<p>This user works in both Windows and IBM i. The IBM i password and Windows password are synchronized. Each time that the integrated Windows server is restarted, the user password is reset to the IBM i password. Password changes can only be made in IBM i. This user type is recommended for running File Level Backup and remote Windows commands.</p> <p>By default, enrolled users are set to this type of user.  <b>Note:</b> If it is necessary to reset an IBM i user profile for a Windows user to this configuration, set the local password management (LCLPDMGT) user profile attribute to <b>Manage this password locally through IBM i</b>. See <a href="#">Changing the local password management user profile attribute</a> for instructions.</p> <p>Key functions provided by this type of enrollment configuration:</p> <ul style="list-style-type: none"> <li>• Both IBM i and Windows fully functional.</li> <li>• Easy to configure.</li> <li>• Password is changed from IBM i.</li> <li>• IBM i and Windows user ID and passwords are identical.</li> <li>• Recommended for system administrators, users who frequently use IBM i, or for systems which use IBM i for backup and restoration of user profiles.</li> </ul>	<p>LCLPDMGT (*YES) and no EIM Windows source associations defined</p>
<p>Windows password-managed user</p>	<p>This person does all or most of their work in Windows and might never, or rarely, sign on to IBM i. If the user signs-on to IBM i, they must use an authentication method such as Kerberos to access IBM i.</p> <p>When the user profile attribute LCLPDMGT(*NO) is defined for an IBM i user, the IBM i user profile password is set to *NONE. The IBM i enrollment password is saved until Windows enrollment is successfully completed. After the IBM i user is enrolled to Windows, the Windows user can change and manage their password in Windows without IBM i overwriting their password.</p> <p>Using this method allows for a more secure environment because there are fewer passwords being managed. To set an IBM i user profile for a Windows user to this configuration, set the local password management (LCLPDMGT) user profile attribute to <b>Manage this password remotely through some other platform</b>. See <a href="#">Changing the local password management user profile attribute</a> for instructions.</p> <p>Key functions provided by this type of enrollment configuration:</p>	<p>LCLPDMGT (*NO)</p>

User type	Description	User Profile Attributes
	<ul style="list-style-type: none"> <li>• Password can be changed from Windows.</li> <li>• Simple configuration.</li> <li>• Windows password administration makes this configuration more secure because the IBM i password is *NONE.</li> <li>• IBM i sign-on requires an authentication method such as System i Navigator provides with its support of IBM i sign-on using Kerberos.</li> </ul>	
Windows user with Enterprise Identity Mapping (EIM) associations automatically configured	<p>Specifying the EIMASSOC user profile attribute 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 <a href="#">Configuring Enterprise Identity Mapping for integrated Windows servers</a>.</p> <p>Key functions provided by this type of enrollment configuration:</p> <ul style="list-style-type: none"> <li>• Automatic creation of Windows source associations makes it easier to set up and configure to use Kerberos enabled applications.</li> </ul>	For example: EIMASSOC (*CHG *TARGET *ADD *CRTEIMID)
Windows user with Enterprise Identity Mapping (EIM) associations manually configured	<p>The user can choose to manually define EIM Windows source associations. This method can be used to set the IBM i user profile to be enrolled to a different Windows user profile name.</p> <p>The user must manually define an IBM i target association for the IBM i user profile and also a Windows source association for the same EIM identifier. See the <a href="#">Enterprise Identity Mapping</a> topic collection for details.</p> <p>Key functions provided by this type of enrollment configuration:</p> <ul style="list-style-type: none"> <li>• Allows the user to define EIM associations for enrolled IBM i user profiles to be different user profiles in Windows.</li> </ul>	Use the IBM i GUI to manually define EIM IBM i target associations and Windows source associations

**Related information:**

- [User Enrollment Capabilities](#)

### 3.11.2 User enrollment templates for integrated Windows servers

You can use templates to simplify the enrollment of new users to an integrated Windows server.

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

When you enroll users and groups from IBM i 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 MYGRP1 and MYGRP2. On IBM i, you could have a group called MGMT. You could decide to enroll the MGMT group and its members to a Windows server. If during the MGMT group enrollment process you specify USRTEMP as the user template, then all members of the MGMT group are automatically added to the MYGRP1 and MYGRP2 groups on Windows.

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 IBM i or not. You can enroll users with a template that is a member of a group that was not enrolled from IBM i. If you do this, the users become members of that non-enrolled group as well. IBM i does not know about groups that were not enrolled from IBM i. 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 IBM i counterpart, the template is ignored.

**Related information:**

➤ [User Enrollment Capabilities](#)



### 3.11.3 Password considerations for integrated Windows servers

You can change IBM i system values and Windows Server policies to configure the rules for passwords and ensure that they work correctly for your environment.

1. Enrolled users must use IBM i passwords containing only characters and password lengths allowed in Windows passwords.
2. IBM i and an integrated Windows server must enforce consistent password rules. If the password rules on the two systems are not consistent, then a password for an enrolled IBM i user might be rejected by the integrated Windows server. You can adjust the password rules either on IBM i or on the integrated Windows server to make them consistent:
  - IBM i password rules can be adjusted using the IBM i system values listed in the table below.
  - Refer to your Windows Server documentation for the methods to change Windows Server policies that control the rules for passwords.
3. When the IBM i 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 IBM i. Changing the IBM i password first automatically changes the Windows password.

IBM i uses system values to control password rules and other security-related items:

System Value	Considerations for User Enrollment
QRETSVRSEC	<p>Make sure that the IBM i QRETSVRSEC system value is set to <b>1</b>. You can set QRETSVRSEC using the <a href="#">Work with System Value (WRKSYSVAL)</a> command.</p> <p>If you do not set QRETSVRSEC to 1, you cannot enroll users on your integrated Windows server until they sign on to IBM i.</p> <p><b>Note:</b> Setting QRETSVRSEC to 1 is also required for other integrated server support functions, such as powering on an integrated server.</p>
QPWDLVL	<p>The IBM i password level can be set to allow user profile passwords of 1 - 10 characters or to allow user profile passwords of 1 - 128 characters. An IBM i password level change of the system value QPWDLVL requires an IPL.</p> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. The IBM i password level of 0 or 1 supports passwords of 1 - 10 characters and limits the set of characters.           <ul style="list-style-type: none"> <li>• At password level 0 or 1, the IBM i user enrollment support converts passwords to all lowercase for Windows.</li> <li>• 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 <a href="#">IBM i globalization</a> 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, variant characters can be used without causing any problems.</li> </ul> </li> <li>2. The IBM i 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, IBM i preserves password case sensitivity for Windows.</li> </ol>

System Value	Considerations for User Enrollment
QPWDMAXLEN	If system value QPWDLVL is set to allow user profile passwords of 1 - 128 characters, then system value QPWDMAXLEN also needs to be changed to allow passwords to be 128 characters in length.
QSECURITY	If the IBM i system value QSECURITY is 10, IBM i users do not require passwords to sign on. Note that you might not be able to enroll IBM i users without passwords to Windows due to Windows password policy restrictions. All other IBM i QSECURITY levels require that a user profile has a password to sign on. You can find more information about security levels in the <a href="#">Security reference</a> topic collection.

### 3.11.4 QAS400NT user and integrated Windows servers

IBM i uses the QAS400NT user to sign on to the integrated Windows server operating system.

The QAS400NT user is used to enroll IBM i users and groups to Windows domains and servers.

**Related information:**

- [Integrated Windows server management infrastructure](#)

### 3.12 IBM i NetServer for integrated servers

You must configure NetServer to enable updates to the IBM i Integrated Server Support software that runs on the integrated server and to enable communication for integrated VMware ESX server administration tasks. You can also configure print and file sharing.

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

**Notes:**

- To install Integrated Server Support service packs on an integrated server, you must be signed on to the integrated server with an account that corresponds to an IBM i user profile with the same password, or you must have a guest NetServer user profile configured.
- When you install a VMware ESX server that uses the [Management server based infrastructure](#), a NetServer file share is automatically created and used exclusively for integrated VMware ESX server administration. Access to this share requires that user **QVMWINT** exists on both IBM i and the integrated Windows server that manages the integrated VMware ESX server.

To set up NetServer for Integrated Server Support tasks, use the method found in the [Getting started with i5/OS® NetServer topic](#).

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

**Related information:**

- [i5/OS NetServer](#)

### **3.13 IBM i Access for Windows and integrated servers**

IBM i Access for Windows enables you to connect to IBM i.

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

IBM i Access for Windows also provides an Open Database Connectivity (ODBC) driver that can be used for server-to-server applications between integrated Windows servers and IBM i. You can enable Open Database Connectivity (ODBC) to run as a Windows service by installing IBM i Access for Windows on your integrated Windows server. This enables you to write server applications that call the ODBC device driver to access DB2 for IBM i.

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

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

**Related information:**

➤ [IBM i Access for Windows](#)

➤ [IBM i NetServer vs IBM i Access for Windows](#)

## 4 Server installation road map and checklist

Use the checklist in this chapter to step through the process of installing an IBM BladeCenter or System x server that is attached to IBM i using an iSCSI network (iSCSI).

### Notes:

1. The checklist in this chapter applies to IBM i **7.2, 7.1, 6.1, and 5.4**.
2. Use the checklist in this chapter when installing a new integrated server from scratch.  
  
Use the [Cloning Checklist](#) on page [222](#) when creating a new integrated Windows server based on a previously installed integrated Windows server.
3. The planning and installation process described in this chapter **overrides** information in the **IBM i Information Center**, so it is important to closely follow the checklist in this document.
4. The order of the tasks listed in the following sections is also important, so please resist the temptation to perform hardware installation or IBM i configuration tasks until you get to the step that instructs you to do those tasks.
5. You might want to **print** the checklist so that you can check off the tasks as you complete them.
6. If you run into problems while installing an iSCSI-attached server using this checklist, see the [Troubleshooting](#) Web page.

<b>Installation Checklist (for an iSCSI-attached integrated server)</b>	<b>Page</b>
— <b><u>Prerequisites</u></b>	<b><u>142</u></b>
— <u>Review iSCSI solution concepts</u>	<u>142</u>
— <u>Ensure that you have access to the required documentation</u>	<u>142</u>
— <u>Verify that you have access to the required IBM i products</u>	<u>143</u>
— <u>Load required IBM i products</u>	<u>143</u>
— <u>Load latest required fixes (each time servers are installed)</u>	<u>145</u>
— <b><u>Prepare for the hardware installation</u></b>	<b><u>146</u></b>
— <u>Obtain required hardware</u>	<u>146</u>
— <u>Obtain firmware updates and drivers for your integrated server hardware</u>	<u>148</u>
— <u>Obtain the integrated server operating system</u>	<u>149</u>
— <b><u>Plan the iSCSI network and integrated server installation</u></b>	<b><u>150</u></b>
— <u>Planning for the service processor connection</u>	<u>152</u>
— <u>Planning for the remote system configuration</u>	<u>157</u>
— <u>Planning for the network server host adapter (NWSH) object</u>	<u>168</u>
— <u>Planning for the integrated server installation</u>	<u>173</u>
— <b><u>Install the hardware</u></b>	<b><u>183</u></b>
— <u>Install each new IBM i iSCSI target</u>	<u>183</u>
— <u>Install the BladeCenter or System x hardware and iSCSI initiators</u>	<u>184</u>
— <u>Update and configure the BladeCenter or System x hardware</u>	<u>185</u>
— <u>Configure the iSCSI initiators</u>	<u>187</u>
— <u>Configure the integrated server start options</u>	<u>187</u>
— <u>Cable the network</u>	<u>187</u>
— <b><u>Prepare IBM i for the integrated server installation</u></b>	<b><u>189</u></b>
— <u>Create an NWSH for each new IBM i iSCSI target</u>	<u>189</u>
— <u>Start the NWSH for each IBM i iSCSI target that the server uses</u>	<u>192</u>
— <u>Create and initialize a service processor configuration</u>	<u>193</u>
— <u>Create a remote system configuration</u>	<u>195</u>
— <u>Verify that the remote system is accessible and powered off</u>	<u>196</u>
— <u>Create a QCNNSEC connection security configuration, if necessary</u>	<u>196</u>
— <u>Prepare for IBM i memory requirements</u>	<u>197</u>
— <u>Set the IBM i QRETSVRSEC system value for integrated servers</u>	<u>198</u>
— <u>Ensure that NetServer is configured</u>	<u>199</u>
— <u>WIN2003 only: Configure IBM i TCP/IP</u>	<u>200</u>
— <b><u>Install the integrated server</u></b>	<b><u>200</u></b>
— <u>Start the installation from IBM i</u>	<u>201</u>
— <u>Continue the operating system installation from the integrated server console</u>	<u>205</u>
— <u>Complete the integrated server installation</u>	<u>210</u>
— <b><u>After the integrated server installation</u></b>	<b><u>218</u></b>
— <u>Scale the iSCSI network</u>	<u>218</u>
— <u>Create additional virtual storage for applications and data</u>	<u>218</u>
— <u>Configure the integrated server to automatically start</u>	<u>218</u>
— <u>Windows only: Define additional virtual Ethernet LANs</u>	<u>221</u>
— <u>Windows only: Enroll IBM i users to the Windows server or domain</u>	<u>221</u>
— <u>Keep the IBM i Integrated Server Support software up to date</u>	<u>221</u>

## 4.1 Prerequisites

Several preliminary tasks need to be performed to prepare yourself and the IBM i environment before planning for and installing a specific iSCSI-attached server. These tasks can take a considerable amount of time to complete, so you should normally perform the steps in this **Prerequisites** section well before planning for and installing a specific iSCSI-attached server.

**Related information:**

- [Installation Checklist](#)

### 4.1.1 Review iSCSI solution concepts

The [BladeCenter](#) or [System x iSCSI Installation Overview](#) Flash animation provides an overview of the iSCSI-attached server installation process. It also provides a conceptual overview of the various hardware and software components and shows how they work together in the IBM i iSCSI solution.

See the [Concepts](#) chapter for additional iSCSI solution concepts.

**Related information:**

- [Installation Checklist](#)

### 4.1.2 Ensure that you have access to the required documentation

Many of the steps in this document link to other required documents and are written assuming that you have access to the Internet. However, in some environments you might not have access to the Internet. For example, some customer datacenters do not have a connection to the Internet.

If you will not have access to the Internet while performing all of the steps in this document, then you should gather the required documents ahead of time so that you have them on-hand when you need to reference them. The following list contains the key documents that you will need:

- **IBM i iSCSI Solution Guide** (this document)
- [IBM i iSCSI Solution Work Sheets](#)
- The appropriate **PCI adapter** installation topic for your Power server model in the [IBM Power Systems Hardware Information Center](#) for installing Ethernet NIC and iSCSI HBA adapters.

You should save these PDFs to your PC so that you can view them from your PC during the appropriate steps below.

In addition to the documents listed above, you may want to have access to the following Web pages:

- [IBM i PTFs](#)
- [IBM i Information Center](#)

**Note:** The above PDFs and Web pages might change over time, so if you have previously saved or printed them, please verify that you have the latest versions.

Finally, you should have on-hand the **BladeCenter or System x hardware setup documents**. These documents are normally included in hardcopy or softcopy form with your BladeCenter or System x model. The actual document titles and contents depend on your BladeCenter or System x hardware.

**Related information:**

- [Installation Checklist](#)

### 4.1.3 Verify that you have access to the required IBM i products

Several IBM i products are required when attaching BladeCenter or System x models with an iSCSI network. See [IBM i products and options](#). If necessary, obtain the electronic or physical installation media for the listed products.

**Related information:**

- [Installation Checklist](#)

### 4.1.4 Load required IBM i products

If this is the first iSCSI-attached server being installed in the IBM i logical partition, you should verify that any required products shown in the [IBM i products and options](#) section are installed.

If any of the required IBM i products are not installed, do these steps to install them.

1. Insert the IBM i media containing the licensed program or option in an available IBM i device.
2. Type GO LICPGM and press **Enter**.
3. Choose option 10 from the **Work with Licensed Programs** menu; then press **Enter**.
  - a. Determine which required licensed programs are already installed as the same release as the 57xx-SS1 \*BASE IBM i.

**Note:** The product IDs for each release are: **5770** for **i 7.2 and i 7.1**, **5761** for **i 6.1**, and **5722** for **i 5.4**.

- b. If you do not see the version number, press **F11**.
  - c. Press **F3** to return to the **Work with Licensed Programs** menu.
4. Choose option 11 from the **Work with Licensed Programs** menu; then press **Enter**.
  5. Page down the list of licensed programs and enter a 1 in the **Option** field next to each required licensed program.
  6. Press **Enter**.
  7. Enter the name of the installation device in which you inserted the IBM i install media.
  8. Press **Enter**. The system installs the selected licensed programs.

**Note:** In addition to installing the required products on the IBM i system, see [Install System i \(iSeries\) Navigator on a PC](#).

**Related information:**

- [Installation Checklist](#)

#### 4.1.4.1 Install System i (iSeries) Navigator on a PC

In configurations where the [Web GUI](#) is not available (for example, on i 5.4 systems), use the System i (iSeries) Navigator GUI to perform IBM i iSCSI configuration tasks, whenever possible. System i Navigator is part of IBM i (System i) Access for Windows.

**Attention:** Use of the GUI interfaces is optional. Almost all of the tasks that the GUI supports have CL command equivalents, so you can use CL commands if you prefer to do so. However, the CL command prompter has permanent restrictions that adversely affect prompting of some commands, so the GUI is considerably easier to use for some tasks. See the [CRTNWSCFG and CHGNWSCFG Prompting Problems When defining more than one remote interface](#) troubleshooting topic for more information.

To install System i Navigator, perform the steps in the [Installing System i Navigator](#) topic in the Information Center.

When installing IBM i Access, be sure to do either a **Full** install or do a **Custom** install and select the following **minimum** set of System i Navigator components:

- **Configuration and Service**
- **Network**
- **Integrated Server Administration**

You should also install the latest IBM i Access service pack.



## 4.1.5 Load latest required fixes (each time servers are installed)

IBM i PTFs are required when attaching BladeCenter or System x models with an iSCSI network.

**Attention:** Additional iSCSI-related fixes are released from time to time. If it has been a while since you originally installed the required fixes, you should perform this step again so that you have the latest fixes loaded.

After installing licensed programs, install the latest cumulative program temporary fix (PTF) package that is listed on the [IBM i PTFs](#) Web page. Note that there should be no users signed on to IBM i when you install PTFs. If your system uses logical partitions, load the PTFs on all of the logical partitions on which you are installing IBM i **Integrated Server Support** and set them for apply delay.

1. To install the latest cumulative PTF package, complete the following steps:
  - a) On the IBM i command line, type GO PTF and press **Enter**.
  - b) To install the program temporary fix package, type 8 and press **Enter**.
  - c) In the **Device** field, enter the name of your optical device.
  - d) Changed the **Automatic IPL** value to \*NO. Press **Enter** to install all PTFs.

For more information about PTFs see [Software fixes](#) in the **Basic system operations** topic collection of the Information Center.

2. After installing the latest cumulative PTF package, install the **IBM i integration with BladeCenter and System x** group PTF and any additional PTFs or that are listed on the [IBM i PTFs](#) Web page.
3. IPL the IBM i partition after the cumulative PTF package, group PTF and any individual PTFs are installed.

**Note:** If you already have integrated Windows or VMware ESX servers installed, you might need to synchronize the integration software that is used to manage those servers with the latest software that was loaded on IBM i above. See [Installing IBM i integration service packs](#).

### Related information:

- [Installation Checklist](#)

## 4.2 Prepare for the hardware installation

Before starting the hardware installation, you should perform the following steps to ensure that you have the necessary hardware and firmware updates on hand and plan the hardware configuration.

**Note:** Before performing the steps below, you should be familiar with key concepts for iSCSI-attached servers, such as how the various hardware, software and networking pieces relate to each other in the iSCSI environment. If necessary, refer to the [Review iSCSI solution concepts](#) section before continuing.

At this time, get a copy of the [IBM i iSCSI Solution Work Sheets](#) so that you can fill in the work sheets as you progress through the server planning and installation process. Record the following items in the **Integrated server deployment overview** work sheet:

Item	Item Description
OV1	Description of this deployment
OV2	Company or organization
OV3	Contact (name, email, phone)

**Related information:**

- [Installation Checklist](#)

### 4.2.1 Obtain required hardware

Obtain the hardware that is required for your integrated server environment.

1. [Obtain IBM i iSCSI target adapter](#)
2. [Obtain BladeCenter or System x server and associated hardware](#)

**Related information:**

- [Installation Checklist](#)
- [Clone Server Hardware Checklist](#)

#### 4.2.1.1 Obtain IBM i iSCSI target adapter

One or more IBM i iSCSI target adapters is required so that the integrated server iSCSI initiator adapters can access storage on IBM i. See:

- [IBM i iSCSI targets](#)
- [Power Server IBM i iSCSI target support](#)

**Note:** IBM i iSCSI target adapters can be used by one or more integrated servers. If you already have an iSCSI-attached integrated server, then you might not need to add another iSCSI target adapter when installing another integrated server. See [Attaching servers to IBM i using iSCSI](#).

**Record** your choices for the following items in the **Integrated server deployment overview** work sheet in the [IBM i iSCSI Solution Work Sheets](#):

Item	Item Description
OV4	IBM i version
OV5	IBM i iSCSI target type

**Related information:**

- [Installation Checklist](#)

## 4.2.1.2 Obtain BladeCenter or System x server and associated hardware

Obtain the required hardware for your type of server:

Server Type	Required Hardware	Supported Configurations
BladeCenter Blade	Blade server	See <a href="#">Blade server models</a> .
	iSCSI initiators	See <a href="#">Blade server models</a> and <a href="#">Blade iSCSI initiators</a> .
	BladeCenter chassis	See <a href="#">BladeCenter chassis models</a> .
	Management module (MM or AMM)	See <a href="#">BladeCenter chassis models</a> .
	Monitor, keyboard, and mouse	See <a href="#">Integrated server console</a> .
	Ethernet network adapter for external network	An Ethernet NIC (embedded or expansion card). <b>Tip:</b> The network adapter does not need to be dedicated to iSCSI management and might already be installed.
	Switches	See <a href="#">External switch considerations</a> and <a href="#">BladeCenter switch module considerations</a> . <b>Note:</b> A switch is not needed if using <a href="#">Direct connect</a> support.
	Ethernet cables	See <a href="#">Ethernet cables needed</a> below.
System x	System x server	See <a href="#">System x server models</a> .
	iSCSI initiator	See <a href="#">System x server models</a> and <a href="#">System x iSCSI initiators</a> .
	Service processor (IMM II, IMM, RSA II, or BMC)	See <a href="#">System x server models</a> .
	Monitor, keyboard, and mouse	See <a href="#">Integrated server console</a> .
	Ethernet network adapter for external network	An Ethernet NIC (embedded or adapter card). <b>Tip:</b> The network adapter does not need to be dedicated to iSCSI management and might already be installed.
	Switches	See <a href="#">External switch considerations</a> . <b>Note:</b> A switch is not needed if using <a href="#">Direct connect</a> support.
	Ethernet cables	See <a href="#">Ethernet cables needed</a> below.
<b>Ethernet cables needed:</b> <ul style="list-style-type: none"> <li>• <b>iSCSI network:</b> One cable from each iSCSI target adapter and any additional cables that you might need to connect the iSCSI initiator ports (all iSCSI network cables must be category 5e or better, or fiber optic).</li> <li>• <b>Service processor network:</b> One cable from a hosting IBM i network adapter port and one cable from each service processor Ethernet port.</li> <li>• <b>External network:</b> One cable from a hosting IBM i network adapter port (if external network is different than the service processor network) and one cable from the server's external network port.</li> </ul>		

### Additional items you will need:

1. Documentation for your server hardware and options – hardcopy, CD, or both.
2. An additional computer with a network interface capable of running a Web browser (used to update and configure server and service processor hardware.)
3. Writable media (flash memory, DVD, or compact discs).

Record your choices for the following items in the **Integrated server deployment overview** and **IBM i remote system configuration** work sheets in the [IBM i iSCSI Solution Work Sheets](#):

Item	Item Description	Additional Information
OV6	Integrated server OS version	None
OV7	Server model name	None
OV8	Server type and model number	None
OV9	iSCSI initiator option P/N	Determine the iSCSI initiator adapter types and put checks in the corresponding boxes of work sheet item <b>RS13</b> .

**Related information:**

- [Installation Checklist](#)
- [Clone Server Hardware Checklist](#)

### 4.2.2 Obtain firmware updates and drivers for your integrated server hardware

In later steps, you will need to install firmware updates and drivers for your integrated server hardware.

Download the firmware and drivers using the referenced sections for your type of server:

Server Type	Items to Download
BladeCenter Blade	<ol style="list-style-type: none"> <li>1. <a href="#">Downloading firmware updates for the BladeCenter chassis</a></li> <li>2. <a href="#">Downloading server updates with Bootable Media Creator</a></li> <li>3. <a href="#">Downloading Windows Ethernet NIC software initiator driver</a></li> </ol>
System x	<ol style="list-style-type: none"> <li>1. <a href="#">Downloading server updates with Bootable Media Creator</a></li> <li>2. <a href="#">Downloading Windows Ethernet NIC software initiator driver</a></li> <li>3. <a href="#">Downloading System x Windows Server 2012/2008 iSCSI HBA driver</a></li> </ol>

**Note:** The firmware updates and drivers that are downloaded above will be installed in later installation road map tasks (not at this point yet).

**Related information:**

- [Installation Checklist](#)
- [Clone Server Hardware Checklist](#)

### 4.2.3 Obtain the integrated server operating system

Verify that the operating system you plan to install is listed in the [Server OS](#) table and is supported with the hardware you plan to use. See:

- [Blade server models](#)
- [System x server models](#)

Then obtain the installation media for the operating system.

Additional considerations for specific operating systems:

<b>Server OS</b>	<b>Additional Considerations</b>
WIN2008	<p><b>Windows Server 2008 R2</b> using a <b>Broadcom 10 Gb NetXtreme II</b> software initiator:</p> <ul style="list-style-type: none"> <li>• Installation of this OS/initiator combination requires special installation media. See Microsoft Knowledge Base article <a href="#">You cannot provide versions of iSCSI storage drivers during installation of Windows Server 2008 R2 if the drivers differ from those on the installation media</a> for details.</li> </ul>
WIN2003	<p><b>Windows Server 2003</b> requires Service Pack 1 (SP1) or later integrated with the base Windows Server 2003 installation image. Some of the options that are available:</p> <ul style="list-style-type: none"> <li>• Obtain a Windows Server 2003 R2 CD, which has SP1 built-in.</li> <li>• Obtain a Windows Server 2003 CD with SP1 already integrated.</li> </ul> <p><b>Note:</b> This can be obtained through various channels such as Microsoft Developer Network (MSDN®).</p> <ul style="list-style-type: none"> <li>• Create an integrated install image. To do this, see <a href="#">Integrating a service pack with Windows Server 2003</a>.</li> </ul>
Embedded ESX versions	<p>The IBM USB Memory Key for VMware ESXi Embedded is an option that can be ordered with your IBM Blade or System x server.</p> <p>You can also order the option for VMware ESXi Embedded from the <a href="#">IBM solutions for VMware ESXi</a> Web page.</p>
All ESX versions	<p>Obtain the install media for the <b>guest operating systems</b> that you plan to run on the virtual machines that are hosted by the VMware ESX server. For more information on supported guest operating systems, see the <a href="#">VMware Documentation</a> Web page.</p>

**Related information:**

- [Installation Checklist](#)

## 4.3 Plan the iSCSI network and integrated server installation

**Note:** This step corresponds to slide 7 in the [BladeCenter](#) or [System x iSCSI Installation Overview](#) Flash animation.

**Note:** Before performing the steps below, you should already have available the IBM i and integrated server hardware and operating system you plan to install. If necessary, go back to the [Prepare for the hardware installation](#) section and complete those tasks before continuing.

**Important:** You must do thorough planning of your iSCSI environment before starting to install and configure the hardware and software. Configuration information in the hardware/firmware and in IBM i must be coordinated in order for the installation to succeed. The planning information in this step will help you produce some work sheets to document the key information that you need in later steps.

Fill out the [IBM i iSCSI Solution Work Sheets](#) to plan for the iSCSI network, hardware installation, and integrated server operating system installation. Do not fill out the work sheets until directed to do so in the following sections.

**Note:** You will use the items from the planning work sheets when performing tasks in later steps of the installation road map.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

### 4.3.1 Planning work sheets overview

The items in the planning work sheets are referred to throughout this document using item identifiers (IDs). For example, the **Name** entry in the **IBM i service processor configuration** work sheet is referred to using item ID **SP1**.

The following work sheet item ID naming convention is used throughout the work sheets and this guide:

Item IDs	Associated Work Sheets
<b>OVn</b>	Overview of integrated server deployment
<b>XSPn</b>	BladeCenter or System x service processor
<b>SPn</b>	IBM i service processor configuration
<b>RSn</b>	IBM i remote system configuration
<b>Inn</b>	iSCSI initiator
<b>NHn</b>	IBM i iSCSI target network server host adapter
<b>LDn</b>	IBM i line description for iSCSI software target NWSH
<b>IFn</b>	IBM i TCP/IP interface for iSCSI software target NWSH
<b>ISn</b>	Integrated server installation
<b>EMn</b>	Integrated VMware ESX server management

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

### 4.3.2 Configuration objects

IBM i objects configure aspects of the integrated server connection and hardware.

The following figure shows the hardware, connections, and key IBM i objects that are used to configure the connections for the integrated server. The item IDs for the fields in the [IBM i iSCSI Solution Work Sheets](#) are listed next to components in the image. Use this figure to help identify the fields as you do the following tasks.

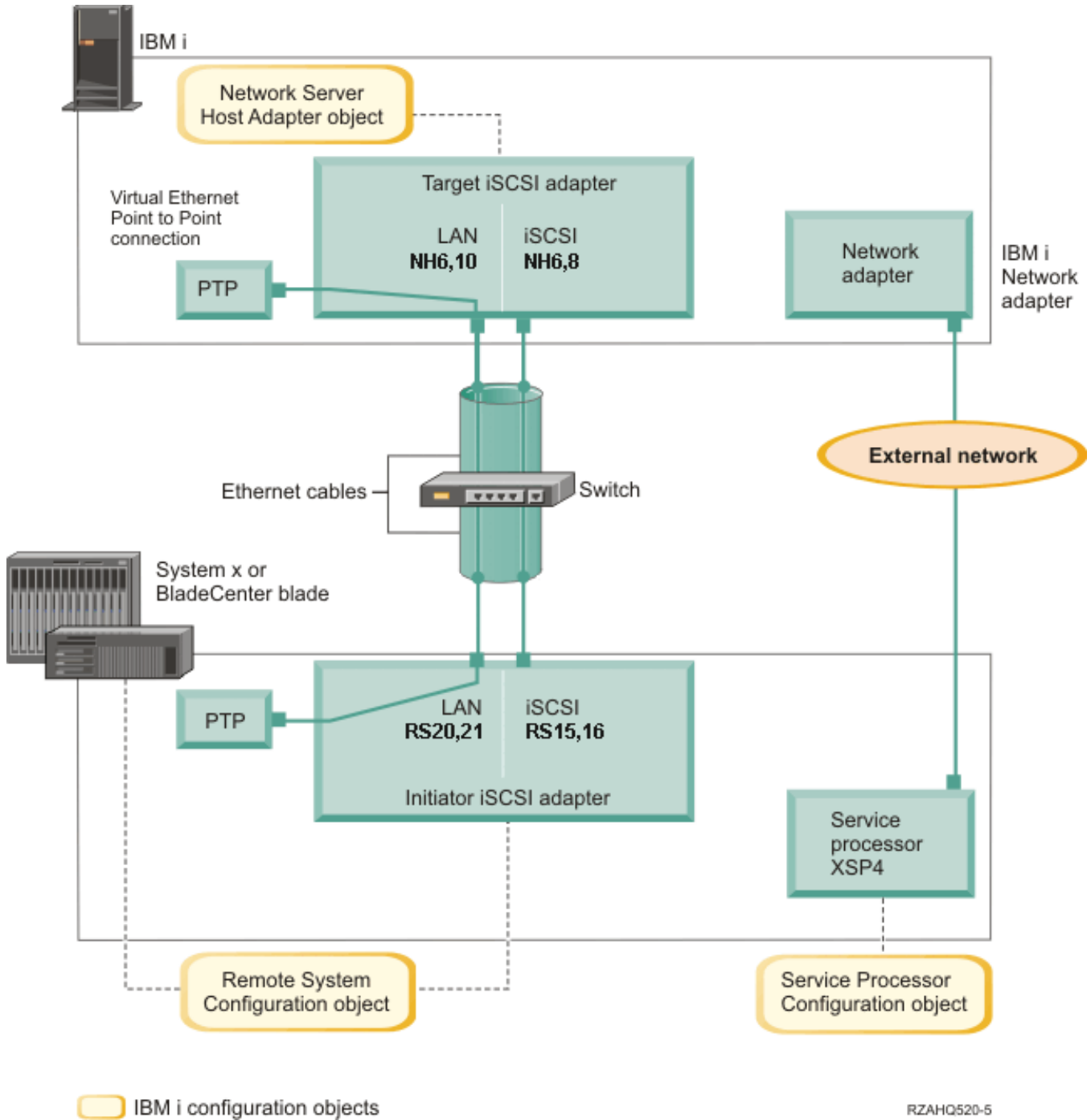


Figure 12 IBM i configuration objects for iSCSI-attached integrated server connections

You need to define values for your iSCSI network that include addresses for all of the connections shown in the above figure. If you are not sure what value to use, you can use the example addressing scheme shown in the following sections:

- [Selecting IP addresses for the System x or blade iSCSI initiator](#)
- [Selecting IP addresses for the IBM i iSCSI target](#)

**Note:** The addressing examples in the referenced sections assume that your iSCSI network uses an isolated Ethernet switch and you do not have another network using IP addresses that start with 192.168.99. If you plan to use your own addressing scheme, you can verify it with the addresses in the examples.

**Related information:**

- [Installation Checklist](#)
- [Clone Server Hardware Checklist](#)

### 4.3.3 Planning for the service processor connection

Have you already created an IBM i service processor configuration for the BladeCenter management module or the System x service processor?

Answer	Do the Following
Yes	You should reuse the <b>existing</b> IBM i service processor configuration.
	1. Record the existing service processor configuration name in work sheet item <b>SP1</b> .
	2. Put a check in the box labeled <b>Existing</b> in work sheet item <b>SP1</b> .
No	3. Skip to the <a href="#">Planning for the remote system configuration</a> task.
	You must create a <b>new</b> IBM i service processor configuration.
	1. Put a check in the box labeled <b>New</b> in work sheet item <b>SP1</b> .
	2. Continue with the tasks in the following sub-sections.
	<b>Service Processor Configuration Planning Tasks</b>
	<a href="#">Identifying a BladeCenter or System x service processor type</a>
	<a href="#">Selecting a service processor connection method</a>
<a href="#">Recording the system serial number and type/model</a>	
<a href="#">Selecting a name for the service processor configuration</a>	
<a href="#">Selecting a login ID and password for the service processor</a>	

**Related information:**

- [Installation Checklist](#)
- [Clone Server Hardware Checklist](#)



### 4.3.3.1 Identifying a BladeCenter or System x service processor type

Record the type of service processor that is installed in the integrated server hardware. Put a check in the box next to your service processor type in work sheet item **XSP1**.

#### Tips:

- For a **blade** server, select the type of BladeCenter management module that is installed in the BladeCenter chassis.
- For a **System x** server, if you are not sure what type of service processor your model has, see the **Service Processor** column of the [System x server models](#) table:

Service Processor Shown	Value to select for work sheet item XSP1
IMM II	IMM II (System x Integrated Management Module II)
IMM	IMM (System x Integrated Management Module)
RSA II Included <b>or</b> RSA II Required	RSA II with BMC (System x Remote Supervisor Adapter II)
BMC (RSA II Optional)	Check your System x model order information to determine if an RSA II SlimLine service processor is included as part of your system configuration and select either: <ul style="list-style-type: none"><li>• RSA II with BMC (System x Remote Supervisor Adapter II) <b>or</b></li><li>• BMC (System x Baseboard Management Controller, without an IMM II, IMM, or RSA II)</li></ul>

#### Related information:

- [Installation Checklist](#)
- [Clone Server Hardware Checklist](#)
- [Supported functions by service processor type](#)

### 4.3.3.2 Selecting a service processor connection method

The service processor is a part of a BladeCenter server or a System x product. It provides the interface for IBM i to power the server on and off.

For the BladeCenter or System x service processor interface, use an external network, such as a company's campus LAN or intranet, rather than using the iSCSI network. See [Considerations for connecting service processors to IBM i](#) for considerations that might affect how you configure your network for IBM i to service processor communications.

IBM i can use one of the following methods to connect to a server's service processor on its network. Decide the connection method to use for the service processor and do the associated planning tasks:

Connection Method	Planning Tasks
<p><b>IP address</b> (Recommended)</p>	<p>This connection method is recommended since it is supported by all types of service processors and does not require a domain name server (DNS) or a dynamic host configuration protocol (DHCP) server.</p> <ol style="list-style-type: none"> <li>Put a check in the box labeled <b>Internet address</b> in work sheet item <b>SP4</b>.</li> <li>Optional: Record the service processor host name in work sheet item <b>XSP2</b> (you can leave it blank).</li> </ol> <p><b>Tip:</b> If the service processor is connected to the same LAN that your other systems (PCs, servers, etc.) are connected to, then you can assign a host name to the service processor using your normal LAN host name assignment policies, the same as if you were adding another PC to your network.</p> <ol style="list-style-type: none"> <li>Put a check in the box labeled <b>Disabled</b> (for DHCP) in work sheet item <b>XSP3</b>.</li> <li>Record address values for work sheet items <b>XSP4</b>, <b>XSP5</b> and <b>XSP6</b>.</li> </ol> <p>You need to choose a TCP/IP address subnet that allows IBM i and the service processor to communicate readily.</p> <p><b>Tip:</b> If the service processor is connected to the same LAN that your other systems (PCs, servers, etc.) are connected to, then you would normally assign an IP address to the service processor using your normal LAN IP address assignment policies, the same as if you were adding another PC to your network.</p>
<p><b>Host name</b></p>	<p>You can use this connection method for all service processor types <u>except</u> a Baseboard Management Controller (BMC). The network that the service processor is connected to must include DNS and DHCP servers.</p> <ol style="list-style-type: none"> <li>Put a check in the box labeled <b>Host name</b> in work sheet item <b>SP3</b>.</li> <li>Record the service processor host name in work sheet item <b>XSP2</b>.</li> </ol> <p><b>Tip:</b> If the service processor is connected to the same LAN that your other systems (PCs, servers, etc.) are connected to, then you can assign a host name to the service processor using your normal LAN host name assignment policies, the same as if you were adding another PC to your network.</p> <p><b>Important:</b> Make sure that the service processor host name that you specify is registered in your network domain name server (DNS).</p> <ol style="list-style-type: none"> <li>Put a check in the box labeled <b>Enabled</b> (for DHCP) in work sheet item <b>XSP3</b>.</li> <li>Leave work sheet items <b>XSP4</b>, <b>XSP5</b> and <b>XSP6</b> blank.</li> </ol>

**Related information:**

- [Installation Checklist](#)
- [Clone Server Hardware Checklist](#)
- [Service processor connection](#)

### 4.3.3.3 Recording the system serial number and type/model

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

1. On the BladeCenter or System x chassis, find the label that contains the system serial number, type and model values. If you are installing a blade, find the values for the BladeCenter chassis. Do not use the label on the blade.
2. If you are installing a System x model with only a BMC service processor (no RSA II) installed, leave work sheet items **SP5** and **SP6** blank.  
Skip to [Selecting a name for the service processor configuration](#).
3. For all other configurations, do the following steps.
  - a. Record the serial number value in work sheet item **SP5**.
  - b. Record the type and model values in work sheet item **SP6**.

**Tip:** Do not include a space or dash ('-') in the type and model value.

For example, record 7379A2U for a System x model x3400 M3 with type 7379 and model A2U.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

### 4.3.3.4 Selecting a name for the service processor configuration

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

The service processor configuration name can be from 1 to 10 characters in length, consisting of characters a-z, A-Z, 0-9 and special characters '\$', '#' and '@'. The first character cannot be a number. You can define your own naming convention to help you associate the service processor configuration name to the physical hardware (BladeCenter or System x model) that contains the service processor.

Record values for the following work sheet items.

1. Fill in the name you choose in work sheet item **SP1**.
2. Fill in a description of the object (up to 50 characters) in item **SP2**.

**Notes:**

1. The service processor configuration name cannot match the associated IBM i remote system configuration name.
2. Using the NWSD name as part of the service processor configuration name works fine for simple configurations where there is a one-to-one relationship between NWSDs and service processors. However, in more complex configurations, the same service processor configuration might be used by multiple NWSDs. For example, multiple NWSDs could be defined to use the same service processor hardware (multiple blades in a BladeCenter) or the NWSD could be switched to use different "hot spare" server hardware, so that the service processor configuration is used with a different NWSD than it was originally created for. In these cases, it might be confusing to use the NWSD name as part of the service processor configuration name.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

### 4.3.3.5 Selecting a login ID and password for the service processor

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

It is strongly recommended that you define a unique login ID that is used only by the IBM i partition or system that controls your BladeCenter or System x through its service processor. Each BladeCenter or System x service processor can only have one controlling partition or system. Use a naming convention that ties the service processor login ID to the hosting IBM i logical partition (or the system name for a non-partitioned system). For example, if the hosting IBM i logical partition name is ROCH03, then the service processor login ID could be set to ROCH03.

You also need this information to synchronize the IBM i service processor configuration with the BladeCenter or System x service processor before installing the operating system on the server. IBM i uses the login ID and password to connect to the System x or blade model to do specific management tasks (for example, to start the server).

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

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

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

Fill out the planning work sheet items as follows:

1. Record the new **Login ID** and **Password** values for IBM i to use in work sheet items **XSP7** and **XSP8**.
2. If the service processor is a MM or AMM in a BladeCenter or an IMM II, IMM, or RSA II in a System x model, you can configure **additional login IDs** and passwords for your administrators to access the service processor from any web browser connected on the same network. If you want to configure additional login IDs, record the new **Login ID** and **Password** values for your administrators to use in work sheet items **XSP9** and **XSP10**. For most environments, you should create an additional login ID and password for use by your administrators.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

### 4.3.4 Planning for the remote system configuration

The remote system configuration defines the communications connections for iSCSI and virtual Ethernet traffic for the System x or blade hardware that will be connecting to IBM i.

Have you already created an IBM i remote system configuration for the BladeCenter blade or the System x server?

Answer	Do the Following
Yes	You should reuse the <b>existing</b> IBM i remote system configuration.
	1. Record the existing remote system configuration name in work sheet item <b>RS1</b> .
	2. Put a check in the box labeled <b>Existing</b> in work sheet item <b>RS1</b> .
No	3. Skip to the <a href="#">Planning for the network server host adapter (NWSH) object</a> task.
	You must create a <b>new</b> IBM i remote system configuration.
	1. Put a check in the box labeled <b>New</b> in work sheet item <b>RS1</b> .
	2. Continue with the tasks in the following sub-sections.
	<b>Remote System Configuration Planning Tasks</b>
	<a href="#">Recording the blade system serial number and type/model</a>
	<a href="#">Selecting a name for the remote system configuration</a>
	<a href="#">Selecting a boot parameter delivery method</a>
	<a href="#">Selecting CHAP settings</a>
	<a href="#">Selecting the MTU for the iSCSI network</a>
	<a href="#">Recording iSCSI initiator (local adapter) MAC addresses</a>
<a href="#">Selecting IP addresses for the System x or blade iSCSI initiator</a>	
<a href="#">Selecting the initiator iSCSI Qualified Name (IQN)</a>	
<a href="#">Selecting the target iSCSI Qualified Name (IQN)</a>	

**Related information:**

- [Installation Checklist](#)
- [Clone Server Hardware Checklist](#)

#### 4.3.4.1 Recording the blade system serial number and type/model

Do these steps if you are installing a blade system.

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

**Tip:** Do not include a space or dash ('-') in the type and model value. For example, record 7872AC1 for a HX5 blade with type 7872 and model AC1.

**Related information:**

- [Installation Checklist](#)
- [Clone Server Hardware Checklist](#)

### 4.3.4.2 Selecting a name for the remote system configuration

You need to assign a name to the IBM i remote system configuration that you will create to configure the attributes of the iSCSI-attached BladeCenter blade or System x model.

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

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

Record values for the following work sheet items.

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

#### Notes:

1. The remote system configuration name cannot match the associated IBM i service processor configuration name.
2. Avoid using the NWSD name as part of the remote system configuration name. In more complex configurations, the same remote system configuration might be used by multiple NWSDs. For example, multiple NWSDs could be defined to use the same remote system hardware (multiple production or test servers defined to use the same System x hardware at different points in time) or the NWSD could be switched to use different "hot spare" server hardware, so that the remote system configuration is used with a different NWSD than it was originally created for. In these cases, it might be confusing to use the NWSD name as part of the remote system configuration name.

#### Related information:

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

### 4.3.4.3 Selecting a boot parameter delivery method

An integrated server iSCSI initiator adapter must be configured after it is installed in the System x or blade hardware.

**Note:** Integrated servers that run ESXi Embedded boot from flash memory, so they do not boot over the iSCSI network. All other integrated server operating systems use the iSCSI network to boot, and the boot device is a port configured on the iSCSI initiator adapter installed in the System x or blade hardware. See [Booting over the iSCSI network](#) for more information.

Decide the addressing method to use for booting and fill out the planning work sheets as follows:

<a href="#">Server OS</a>	Addressing Method	Description	Work Sheet Item RS6	iSCSI Initiator Work Sheet Column	Work Sheet Item IN9
ESXi <u>Embedded</u>	Not applicable	Integrated servers that run ESXi <u>Embedded</u> boot from flash memory, so they do <u>not</u> boot over the iSCSI network.	Dynamically delivered to remote system via DHCP	<b>Dynamic</b>	<b>Disabled</b> for all ports
All other server operating systems	<b>Dynamic</b> (Recommended)	Use dynamic addressing for most environments. When a network server description (NWSD) is varied on, the initiator system is automatically configured with the parameters provided in the IBM i remote system configuration and NWSD.	Dynamically delivered to remote system via DHCP	<b>Dynamic</b>	<b>DHCP for Port 1.</b>  All other ports are <b>Disabled</b> for boot during the installation.
	<b>Manual</b>	<b>Attention:</b> You should <b>not</b> use manual addressing unless you have run into problems when using the dynamic method.	Manually configured on remote system	<b>Manual</b>	<b>Manual for Port 1.</b>  All other ports are <b>Disabled</b> for boot during the installation.

**Notes:**

1. Only one of the iSCSI initiator ports can be configured as the boot device during the server installation. All other ports must be disabled for boot during the installation.
2. After the server installation is completed, if the server operating system supports booting from multiple iSCSI initiator ports, then additional ports can be enabled for boot.

**Related information:**

- [Installation Checklist](#)
- [Booting over the iSCSI network](#)
- [Clone Server Hardware Checklist](#)
- [Integrated iSCSI DHCP server](#)

#### 4.3.4.4 Selecting CHAP settings

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

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

There are two types of CHAP authentication:

CHAP Type	Planning Tasks
<b>One-way CHAP</b>	The target (IBM i) authenticates the initiator (System x or blade).
<b>Bidirectional CHAP</b>	In addition to the one-way CHAP authentication described above, the initiator (System x or blade) also authenticates the target (IBM i).

Do **one** of the following:

- If you do **not** want to use CHAP, select **Disabled** for work sheet items **RS7** and **RS10**. Then skip to [Selecting the MTU for the iSCSI network](#).
- Otherwise, continue with the tasks in the following sub-sections.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

##### 4.3.4.4.1 Selecting parameters for target CHAP

Do the following steps to select parameters for target CHAP authentication.

1. Put a check next to **Enabled** in work sheet item **RS7**.
2. Record the CHAP name in work sheet item **RS8**. You can use the remote system configuration name from item **RS1** as the CHAP name.
3. Record the CHAP secret.

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

- If the iSCSI network is physically secure and there is no possibility that unauthorized parties can monitor the iSCSI network traffic, you can use a unique non-trivial CHAP secret that you assign. For example, use a combination of letters and numbers that is at least 8 characters long. If you choose this approach, then record the CHAP secret you choose in work sheet item **RS9**.
- If the iSCSI network is not physically secure or there is a possibility that unauthorized parties can monitor the iSCSI network traffic, use the remote system configuration option to generate a strong CHAP secret. If you choose this approach, then put a check in the box next to **Generate** in work sheet item **RS9** and leave the CHAP secret value blank for now.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)



#### 4.3.4.4.2 **Selecting parameters for initiator CHAP**

If you do not want to configure initiator CHAP or if your IBM i system is running **i 5.4**, select **Disabled** for work sheet item **RS10**. Then skip to [Selecting the MTU for the iSCSI network](#).

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

1. Put a check next to **Enabled** in work sheet item **RS10**.
2. Record the CHAP name in work sheet item **RS11**. You can use the remote system configuration name from item **RS1** as the CHAP name.
3. Record the CHAP secret.

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

- If the iSCSI network is physically secure and there is no possibility that unauthorized parties can monitor the iSCSI network traffic, you can use a unique non-trivial CHAP secret that you assign. For example, use a combination of letters and numbers that is at least 8 characters long. If you choose this approach, then record the CHAP secret you choose in work sheet item **RS12**.
- If the iSCSI network is not physically secure or there is a possibility that unauthorized parties can monitor the iSCSI network traffic, use the remote system configuration option to generate a strong CHAP secret. If you choose this approach, then put a check in the box next to **Generate** in work sheet item **RS12** and leave the CHAP secret value blank for now.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

#### 4.3.4.5 **Selecting the MTU for the iSCSI network**

The iSCSI network normally uses standard 1500 byte frames. It might be possible to configure the iSCSI initiator adapters to use jumbo 9000 byte frames on the iSCSI network.

**Attention:** Ensure that all components of the iSCSI network support larger frames before deciding to use them. See [MTU considerations for the iSCSI network](#) for more information. If you are not sure that your switch and iSCSI initiators perform well with larger frames, use the default settings for 1500 byte frames.

Do the following steps to record the MTU settings to use.

1. Put a check in the box next to your **MTU** choice for **Port 1** in work sheet item **IN16**.
2. If your server has more ports (for example, a blade with a dual port iSCSI initiator adapter), then also put a check in the box next to your **MTU** choice for any additional ports in work sheet item **IN16**.

**Note:** If you plan to use jumbo frame support, you also need to configure it on the switch, if not already enabled.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

### 4.3.4.6 Recording iSCSI initiator (local adapter) MAC addresses

Do these steps to record the iSCSI initiator local adapter (MAC) address for your remote system configuration. The MAC address consists of 12–digit hexadecimal values. These are unique addresses that are assigned for the adapter.

Depending on the server type and iSCSI initiator adapter type, look in the following locations for the iSCSI initiator MAC address:

Server Type	Adapter Type	Location of iSCSI Initiator MAC Address
Blade	LAN on Motherboard (SWI)	On a label that is attached to the blade. <b>Note:</b> LAN on Motherboard (LOM) is also called embedded Ethernet or integrated Ethernet.
	Ethernet NIC expansion card (SWI)	On a label that is attached to the expansion card. On a label that is attached to the box the expansion card came in.  For Ethernet NICs with two ports, the label shows two addresses.
	iSCSI HBA expansion card (HWI)	On a label that is attached to the expansion card. On a label that is attached to the box the expansion card came in.  Each port has an iSCSI address and a TOE address.  For iSCSI HBAs with two ports, the label shows four addresses.
System x	LAN on Motherboard port (SWI)	On a label that is attached to the system unit. <b>Note:</b> LAN on Motherboard (LOM) is also called embedded Ethernet or integrated Ethernet.
	Ethernet NIC adapter (SWI)	On a label that is attached to the tail stock of the adapter.  For Ethernet NICs with two ports, the label shows two addresses.
	iSCSI HBA (HWI)	On a label that is attached to the tail stock of the adapter.  Each port has an iSCSI address and a TOE address.  For iSCSI HBAs with two ports, the label shows four addresses.  <b>Important:</b> The System x iSCSI HBA parts 30R5201 (CCIN 1986) and 30R5501 (CCIN 1987) look identical to the Power server iSCSI HBA features 5713 (CCIN 573B), 5714 (CCIN 573C), 5783 (CCIN 573B), and 5784 (CCIN 573C), but they have different firmware, so they are <b>not</b> interchangeable. If you get them mixed up and use an iSCSI HBA in the wrong system, it does not work. If you are not sure which system type a particular iSCSI HBA is for, look for the CCIN values on the tail stock of the iSCSI HBA card.

**Note:** For more information about these addresses, see [iSCSI network](#).

Record the iSCSI initiator type and MAC addresses.

1. Determine the iSCSI initiator adapter type and put a check in the corresponding box in work sheet item **RS13**, if necessary.

2. Record the iSCSI initiator local adapter (MAC) address. Use the appropriate method for your iSCSI initiator adapter type:

Adapter Type	Planning Tasks
Software initiator (Ethernet NIC)	<p>Look for the word MAC on the label. Record the 12–digit hexadecimal address in work sheet items <b>RS14</b> and <b>RS19</b>.</p> <p>Note that the same adapter address is used for both the SCSI and LAN interfaces.</p>
Hardware initiator (iSCSI HBA)	<ol style="list-style-type: none"> <li>1. Look for the word '<b>iSCSI</b>' on the label. Record the 12–digit hexadecimal address in work sheet item <b>RS14</b>.</li> </ol> <p><b>Note:</b> The iSCSI connection is used for disk traffic.</p> <ol style="list-style-type: none"> <li>2. Look for the word '<b>TOE</b>' on the label. Record the 12–digit hexadecimal address in work sheet item <b>RS19</b>.</li> </ol> <p><b>Note:</b> TOE stands for TCP Offload Engine. Think of it as an I/O processor for the adapter. The TOE is used for virtual Ethernet LAN traffic.</p>

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

#### 4.3.4.7 Selecting IP addresses for the System x or blade iSCSI initiator

You need to select an IP address scheme for the SCSI and LAN interfaces of the System x or blade iSCSI initiators before you configure your server. You can use the sample information in the table below for up to 19 System x or blade servers connected to the same switch, or use your own scheme. The IP addressing scheme you choose must be consistent with the one used for the IBM i iSCSI targets. See [Selecting IP addresses for the IBM i iSCSI target](#).

Do these steps to record IP address information for the iSCSI initiator ports.

1. Record the **SCSI interface internet address** and **subnet mask** from the table below (or use your own values) in work sheet items **RS15** and **RS16**.
2. Record the **LAN interface internet address** and **subnet mask** from the table below (or use your own values) in work sheet items **RS20** and **RS21**.

**Sample IP addressing scheme for iSCSI initiator ports** on the iSCSI network:

Hosted System	Interface	Configuration parameter	Initiator Port 1	Initiator Port 2	Initiator Port 3	Initiator Port 4
Hosted System 1	SCSI interface	Internet address	192.168.99.11	192.168.99.12	192.168.99.13	192.168.99.14
		Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
		Gateway address <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>
	LAN interface (iSCSI HBA)	Internet address	192.168.99.15	192.168.99.16	192.168.99.17	192.168.99.18
		Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
		Gateway address <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>
Hosted System 2	SCSI interface	Internet address	192.168.99.21	192.168.99.22	192.168.99.23	192.168.99.24
		Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
		Gateway address <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>
	LAN interface (iSCSI HBA)	Internet address	192.168.99.25	192.168.99.26	192.168.99.27	192.168.99.28
		Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
		Gateway address <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>
...	...	...	...	...	...	
Hosted System 19	SCSI interface	Internet address	192.168.99.191	192.168.99.192	192.168.99.193	192.168.99.194
		Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
		Gateway address <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>
	LAN interface (iSCSI HBA)	Internet address	192.168.99.195	192.168.99.196	192.168.99.197	192.168.99.198
		Subnet mask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
		Gateway address <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>

#### Notes:

1. You do not need a gateway address because these System x and blade iSCSI initiators are on the same switch and subnet as the IBM i iSCSI targets. Routers are not supported in the iSCSI network.
2. If you want to plan for more than 19 hosted systems on the same switch, see [Expanding on the iSCSI network addressing scheme for integrated servers](#).
3. The last part of the **SCSI Interface Internet address** is a concatenation of a system number and a port number. For example, system 1, port 1 = 11. Add 4 to the SCSI Interface Internet address to get the corresponding **LAN interface IP address**.

If you use this convention, you can assign any numbers to systems, ports, and iSCSI initiators within the indicated ranges.

4. This table gives sample IP addresses for the physical iSCSI network. Do not use these IP addresses for any virtual Ethernet networks you might have. The physical network and the virtual Ethernet network must use IP addresses on different subnets. If you have a network for your Power Server Hardware Management Console (HMC), it should not be on the same subnet as the iSCSI or virtual Ethernet networks.
5. If you will be setting up multipath I/O (MPIO) on the iSCSI network or if you anticipate having more than 19 hosted systems or more than 19 iSCSI targets on the iSCSI network, see [Expanding on the iSCSI network addressing scheme for integrated servers](#) for some more considerations.

**Related information:**

- [Installation Checklist](#)
- [Clone Server Hardware Checklist](#)
- [Multipath I/O \(MPIO\)](#)

#### 4.3.4.7.1 *Expanding on the iSCSI network addressing scheme for integrated servers*

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

- When setting up multipath I/O (MPIO) on the iSCSI network, the iSCSI network typically has multiple physically disjoint segments, such as a BladeCenter with two switches dedicated to iSCSI traffic. In this multipath configuration, the initiators and targets on one switch should be on a different subnet than the initiators and targets on the other switch. Therefore, if you are using the suggested IP addressing scheme in the tables in [Selecting IP addresses for the System x or blade iSCSI initiator](#) and [Selecting IP addresses for the IBM i iSCSI target](#) and have multiple switches:
  - Use subnet 192.168.**99** for the initiators and targets on the **first** switch.
  - Use subnet 192.168.**98** for the initiators and targets on the **second** switch.
  - Use subnet 192.168.**97** for the initiators and targets on the **third** switch.
  - Use subnet 192.168.**96** for the initiators and targets on the **fourth** switch.
- With a subnet mask of 255.255.255.0 there are 254 IP addresses available. IP addresses with a last digit of 0 or 255 should not be used with this subnet mask.
- If you anticipate eventually having an iSCSI network with more than 19 IBM i iSCSI target adapter ports or more than 19 hosted systems, you may modify the IP address convention in the tables to maximize the use of all 254 available IP addresses.
- If you anticipate eventually needing more than 254 IP addresses, consider using a different subnet mask to begin with, to avoid the need to change this later.
  - For 510 IP addresses, use a subnet mask of 255.255.254.0
  - For 1022 IP addresses, use a subnet mask of 255.255.252.0
  - For 65534 IP addresses, use a subnet mask of 255.255.0.0
  - For the above subnet masks, you must use IP addresses that start with a number less than 192.
- In IP networking, different subnets may be interconnected using routers. IBM i does not currently support routers in the iSCSI network.

**Related information:**

- [Installation Checklist](#)
- [Clone Server Hardware Checklist](#)

### 4.3.4.8 Selecting the initiator iSCSI Qualified Name (IQN)

IBM i can automatically generate a unique initiator (System x or blade) iSCSI Qualified Name (IQN) for you, or you can provide a specific initiator IQN yourself.

Initiator IQN	Description
<b>Generated</b>	<p>The generated IQN format is: <b>iqn.1924-02.com.ibm:sssssss.p</b> where:</p> <ol style="list-style-type: none"><li><b>sssssss</b> is the System x (see item <b>SP5</b>) or blade (see item <b>RS4</b>) serial number, in lower case.</li><li><b>p</b> depends on the IBM i version:<ul style="list-style-type: none"><li>For <b>IBM i 7.2, 7.1</b> and <b>6.1</b>: <b>p</b> is always <b>0</b> (zero). Note that the same IQN value is used for all initiator ports for <b>i 7.2, 7.1</b> and <b>6.1</b>.</li><li>For <b>IBM i 5.4</b>: <b>p</b> is the System x or blade iSCSI adapter interface/port number (<b>0-3</b>, with <b>0</b>=first port).</li></ul></li></ol>
<b>Specific</b>	Choose an IQN value that is unique within the iSCSI network.

Record the following items in work sheet item **RS18**:

- Put a check in **Generate** or **Specific** to indicate your method for obtaining an initiator IQN value.
- Record the initiator IQN value.

**Note:** If you checked **Manually configured on remote system** (manual addressing) for the **Boot parameter delivery method** in work sheet item **RS6**, then you will later need to manually configure the initiator IQN value in the iSCSI initiator settings.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

### 4.3.4.9 Selecting the target iSCSI Qualified Name (IQN)

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

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

1. **sssssss** is the Power server serial number, in lower case letters.  
**Note:** You can display the Power server serial number by entering DSPSYSVAL QSRLNBR at the IBM i command line.
2. **i** is the Power server logical partition ID.
3. **nnnnnnnn** is the network server description (NWSD) name, in lower case letters.
4. **p** is the storage path number from the NWSD (1-4 or **m**, with **1**=first and only storage path for new installations and **m**=the multipath group for MPIO support).

Record the target IQN value in work sheet item **IN11**.

**Note:** If you have not decided on an NWSD name yet, wait until you fill in item **IS7** in [Selecting a name for the NWSD](#). Then finish filling in the target IQN value in work sheet item **IN11**.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

### 4.3.5 Planning for the network server host adapter (NWSH) object

The network server host adapter (NWSH) device description represents a port for an iSCSI target adapter that is installed inside the Power server or its associated expansion units and assigned to the IBM i partition. The NWSH defines the communications connections for SCSI and virtual Ethernet traffic to IBM i.

Have you already created an NWSH for the IBM i iSCSI target adapter?

Answer	Do the Following
Yes	You should reuse the <b>existing</b> IBM i NWSH device description.
	1. Record the existing NWSH name in work sheet item <b>NH1</b> .
	2. Put a check in the box labeled <b>Existing</b> in work sheet item <b>NH1</b> .
No	3. Skip to the <a href="#">Planning for the integrated server installation</a> task.
	You must create a <b>new</b> IBM i NWSH device description.
	1. Put a check in the box labeled <b>New</b> in work sheet item <b>NH1</b> .
	2. Continue with the tasks in the following sub-sections.
	<b>NWSH Planning Tasks</b>
	<a href="#">Selecting a name for the NWSH</a>
	<a href="#">Selecting a hardware resource name</a>
<a href="#">Selecting a connection type for the NWSH</a>	
<a href="#">Selecting IP addresses for the IBM i iSCSI target</a>	
<a href="#">Selecting line description values for a software target</a>	

**Related information:**

- [Installation Checklist](#)

#### 4.3.5.1 Selecting a name for the NWSH

You need to assign a name to the IBM i network server host adapter (NWSH) device description that you will create to configure the IBM i iSCSI target adapter.

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

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

Record values for the following work sheet items.

1. Fill in the name you choose in work sheet item **NH1**.
2. Also fill in a description of the object (up to 50 characters) in item **NH2**.

**Related information:**

- [Installation Checklist](#)



### 4.3.5.2 Selecting a hardware resource name

The iSCSI target adapter hardware resource name is not available until the iSCSI target adapter is installed in the Power server and assigned to the IBM i partition.

Determine the type of iSCSI target adapter hardware being used and record work sheet items **NH3** and **NH4**:

iSCSI Target Adapter Type	Do the Following
Software Target (Ethernet NIC)	For item <b>NH3</b> , put a check in the box labeled <b>Software Target</b> . <b>Note:</b> Software targets are supported on IBM i <b>7.2</b> , <b>7.1</b> and <b>6.1.1</b> .
Hardware Target (iSCSI HBA)	For item <b>NH3</b> , put a check in the box labeled <b>Hardware Target</b> .  For item <b>NH4</b> , fill in the hardware resource name. <ul style="list-style-type: none"> <li>• If the iSCSI target adapter has not been installed yet, leave the hardware resource name blank. You will record this value after you install the iSCSI target adapter.</li> <li>• Otherwise, record the hardware resource name now. For more information, see <a href="#">Determining the hardware resource name for an iSCSI target adapter</a>.</li> </ul> For item <b>NH5</b> , if you want the NWSH to automatically start at IPL, put a check in the box labeled <b>Yes</b> . Otherwise, put a check in the box labeled <b>No</b> .

**Related information:**

➤ [Installation Checklist](#)

### 4.3.5.3 Selecting a connection type for the NWSH

There are two ways that IBM i iSCSI targets can physically connect to a System x or a blade system.

1. If this Network server host adapter (NWSH) object will be connected to an **Ethernet switch** (or a BladeCenter switch module), put a check in the box by **Network** in work sheet item **NH7**.
2. If this Network server host adapter (NWSH) object will be connected directly to an iSCSI initiator port in a System x server or to a BladeCenter pass through module, put a check in the box next to **Direct** in work sheet item **NH7**.

**Note:** See the [Direct connect](#) capabilities matrix before choosing the **Direct** option to verify that it is supported with your configuration.

**Related information:**

➤ [Installation Checklist](#)

### 4.3.5.4 Selecting IP addresses for the IBM i iSCSI target

You need to select an IP address scheme for the SCSI and LAN interfaces of the IBM i iSCSI targets installed in the Power server. You can use the sample information in the table below for up to 19 IBM i iSCSI targets connected to the same switch, or use your own scheme. The IP addressing scheme you choose must be consistent with the one used for the System x or blade iSCSI initiators. See [Selecting IP addresses for the System x or blade iSCSI initiator](#).

Do these steps to record IP address information for the iSCSI target ports.

1. Record the **SCSI interface internet address** in work sheet item **NH8**.
2. Record the remaining values based on your iSCSI target adapter type:

iSCSI Target Adapter Type	Do the Following
<p><b>Software Target</b> (Ethernet NIC)</p>	<p>a. Do <b>not</b> fill in the <b>Subnet mask</b> in work sheet item <b>NH6</b> or the <b>LAN interface internet address</b> in work sheet item <b>NH10</b>.</p> <p>b. If an IBM i TCP/IP interface for the iSCSI target adapter port currently exists, put a check in the box labeled <b>Existing</b> in work sheet item <b>IF1</b>.</p> <p>Otherwise:</p> <ol style="list-style-type: none"> <li>1. Put a check in the box labeled <b>New</b> in work sheet item <b>IF1</b>.</li> <li>2. Record the <b>Subnet mask</b> in work sheet item <b>IF2</b>.</li> <li>3. Record a description of the interface (up to 50 characters) in item <b>IF3</b>.</li> </ol> <p><b>Tip:</b> Use a description that is similar to the NWSH description to make it easy to associate the TCP/IP interface with the corresponding NWSH.</p> <ol style="list-style-type: none"> <li>4. If you want the TCP/IP interface and the corresponding NWSH to automatically start whenever TCP/IP is started (for example, at IPL), put a check in the box labeled <b>Yes</b> in work sheet item <b>IF4</b>.</li> </ol> <p>Otherwise, put a check in the box labeled <b>No</b> in work sheet item <b>IF4</b>.</p> <p><b>Note:</b> Software targets are supported on IBM i <b>7.2</b>, <b>7.1</b> and <b>6.1.1</b>.</p>
<p><b>Hardware Target</b> (iSCSI HBA)</p>	<ol style="list-style-type: none"> <li>a. Record the <b>Subnet mask</b> in work sheet item <b>NH6</b>.</li> <li>b. Record the <b>LAN interface internet address</b> in work sheet item <b>NH10</b>.</li> </ol>

**Sample IP addressing scheme for iSCSI target ports** on the iSCSI network:

Interface	Configuration parameter	Target 1	Target 2	...	Target 19
Common	Subnet mask	255.255.255.0	255.255.255.0	...	255.255.255.0
<b>SCSI interface</b>	Internet address	192.168.99. <b>201</b>	192.168.99. <b>202</b>	...	192.168.99. <b>219</b>
	Gateway address <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>	...	None <sup>1</sup>
<b>LAN interface</b> (iSCSI HBA)	Internet address	192.168.99. <b>221</b>	192.168.99. <b>222</b>	...	192.168.99. <b>239</b>
	Gateway address <sup>1</sup>	None <sup>1</sup>	None <sup>1</sup>	...	None <sup>1</sup>

**Notes:**

1. You do not need a gateway address because these System x and blade iSCSI initiators are on the same switch and subnet as the IBM i iSCSI targets. Routers are not supported in the iSCSI network.
2. If you want to plan for more than 19 IBM i iSCSI targets on the same switch, see [Expanding on the iSCSI network addressing scheme for integrated servers](#).
3. The last part of the **SCSI Interface Internet address** is 200 + an iSCSI target number.

The **LAN Interface Internet address** is determined as follows:

- For a **software target** (Ethernet NIC): The LAN interface internet address is not used.
- For a **hardware target** (iSCSI HBA): Add 20 to the SCSI Interface Internet addresses to get the IP addresses for the LAN interfaces.

If you use this convention, you can assign numbers to systems, ports, and iSCSI targets within the indicated ranges any way you want.

4. This table gives sample IP addresses for the physical iSCSI network. Do not use these IP addresses for any virtual Ethernet networks you might have. The physical network and the virtual Ethernet network must use IP addresses on different subnets. If you have a network for your Power Server Hardware Management Console (HMC), it should not be on the same subnet as the iSCSI or virtual Ethernet networks.
5. If you will be setting up multipath I/O (MPIO) on the iSCSI network or if you anticipate having more than 19 hosted systems or more than 19 iSCSI targets on the iSCSI network, see [Expanding on the iSCSI network addressing scheme for integrated servers](#) for some more considerations.

**Related information:**

- [Installation Checklist](#)

### 4.3.5.5 Selecting line description values for a software target

You need to determine values to use for an IBM i line description (LIND) that is created to configure an IBM i iSCSI software target adapter (Ethernet NIC).

**Note:** This task does not apply to an iSCSI hardware target adapter (iSCSI HBA).

Fill out the work sheet items for the line description:

- If you have already created a LIND object for the iSCSI target adapter port, use the existing LIND object.

1. Put a check in the box labeled **Existing** in work sheet item **LD1**.
2. Record the existing LIND object name in work sheet item **LD1**.

- Otherwise, you need to create a LIND object:

1. Put a check in the box labeled **New** in work sheet item **LD1**.
2. Record a name for the line description in work sheet item **LD1**.

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

**Tip:** Use the same name as the associated network server host adapter (NWSH) to make it easy to associate the LIND with the corresponding NWSH.

3. Record a description of the object (up to 50 characters) in item **LD2**.

**Tip:** Use a description that is similar to the associated NWSH description to make it easy to associate the LIND with the corresponding NWSH.

4. Record the hardware resource name (**LD3**) as follows:

- If the iSCSI target adapter has not been installed yet, leave the hardware resource name blank. You will record this value after you install the iSCSI target adapter.
- Otherwise, record the hardware resource name now. For more information, see [Determining the hardware resource name for an iSCSI target adapter](#).

5. Record the maximum frame size (**LD4**) as follows:

- Put a check in the box labeled **Default (8996)**, unless there is a reason to use a different value.
- If you have a reason to use a different value, put a check in the box labeled **Value** and record the value to use.

**Related information:**

- [Installation Checklist](#)

### 4.3.6 Planning for the integrated server installation

Plan the configuration for the integrated server operating system installation.

**Note:** The server installation process uses values that were recorded in previous planning work sheets. Fill out those work sheets before planning the server installation.

Continue with the tasks in the following sub-sections.

Server Planning Tasks
<a href="#">Selecting the server operating system type</a>
<a href="#">Choosing the system drive capacity and storage pool</a>
<a href="#">Selecting a memory pool for iSCSI I/O</a>
<a href="#">Selecting a name for the NWSD</a>
<a href="#">Selecting a language version</a>
<a href="#">Selecting IBM i tape and optical devices to allow (i 7.2 only)</a>
<a href="#">Selecting IBM i tape and optical devices to restrict</a>
<a href="#">Selecting point-to-point virtual Ethernet IP addresses</a>
<a href="#">Selecting preferred storage unit to store virtual storage on (i 7.2 only)</a>
<a href="#">Selecting additional INSxxxSVR command parameters</a>
<a href="#">Planning for VMware ESX server management</a>

**Related information:**

- [Installation Checklist](#)

#### 4.3.6.1 Selecting the server operating system type

Select the operating system type that you plan to install on the server.

1. Review the list of operating systems that are supported on your server hardware. Refer to the server manufacturer type and model values that you recorded in work sheet item **RS5** (for a blade server) or **SP6** (for a System x server). Use one of the following support matrices to determine if the operating system you plan to install is supported on your server model:
  - [Blade server models](#)
  - [System x server models](#)
2. Put a check in the box next to the appropriate operating system type in work sheet item **IS1**.

**Note:** The Work sheet combines ESXi Embedded 4 and 5 into one choice and ESXi Installable 4 and 5 into another choice, since that is the way the IBM i GUI and install commands group them.

**Related information:**

- [Installation Checklist](#)

### 4.3.7 Choosing the system drive capacity and storage pool

Choose the capacity for the virtual storage that contains the integrated server operating system. Also choose which IBM i storage pool to allocate the virtual storage from.

**Embedded VMware ESX versions only:** Since embedded versions of ESX boot from flash memory and a system disk is not needed, leave work sheet items **IS2** and **IS3** blank and skip the remainder of this planning task. Note that for **i 7.1 or later**, IBM i does not allocate any virtual storage for the ESX system disk. However, for **i 6.1**, IBM i allocates a small (1 MB) placeholder virtual storage space for the ESX system disk. Do not unlink, change the link type, or put any data on this placeholder system disk.

The minimum system drive size is 2 GB for Microsoft Windows Server 2003 and 15 GB for all other supported operating system types. This minimum size assumes that only the integrated server operating system is stored on the system drive and that no applications or data are stored on the system drive. Allocate additional storage on the system drive to accommodate swap files, operating system fixes, and any applications or data that you plan to store on the system drive.

Record values for the following work sheet items.

1. Record your choice for the system drive capacity in work sheet item **IS2**.  
(Leave it blank for an embedded version of VMware ESX.)
2. Record the name or number of the associated IBM i storage pool (ASP) in work sheet item **IS3**.  
(Leave it blank for an embedded version of VMware ESX.)

#### Notes:

- You can add more IBM i virtual storage to the server (as additional drives) after the initial server installation.
- Store applications and data on drives other than the system drive.

#### Related information:

- [Installation Checklist](#)

### 4.3.7.1 Selecting a memory pool for iSCSI I/O

Select a memory pool that is dedicated to iSCSI I/O to prevent iSCSI operations from affecting other applications.

Review the IBM i memory requirements for an integrated server and plan for a shared data memory pool. See [Prepare for IBM i memory requirements](#).

Record values in work sheet item **IS6** as follows:

IBM i	Description
i 7.2 i 7.1 i 6.1	<p>If you plan to use the <b>Create Server <a href="#">Web GUI</a></b> task to install your server and you want to use the default iSCSI memory pool, put a check mark in the box labeled <b>GUI default memory pool</b>.</p> <p>Otherwise, put a check mark in the box labeled <b>Pool</b>. Also record the number (1-60) of the shared data memory pool that you plan to use for the integrated server.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"><li>• For most environments, you can use a shared data memory pool with a size of <b>512 MB</b> that is shared among all the iSCSI-attached servers on your system.</li><li>• The <b>Create Server <a href="#">Web GUI</a></b> task provides an option to create a default iSCSI memory pool with a size of 512 MB.</li></ul>
i 5.4	<p>A private memory pool for iSCSI I/O is enabled later on by creating a subsystem description named QGPL/<b>QFPHIS</b>, as described in <a href="#">Prepare for IBM i memory requirements</a>.</p>

**Related information:**

- [Installation Checklist](#)

### 4.3.7.2 Selecting a name for the NWSD

You need to assign a name to the IBM i network server description (NWSD) object. The NWSD is created to configure the IBM i hosting environment for the integrated server.

The NWSD name can be from 1 to 8 characters in length, consisting of characters a-z, A-Z, and 0-9. The first character cannot be a number.

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

Record values for the following work sheet items.

1. Record the name you choose in work sheet item **IS7**.
2. Also record a description of the object (up to 50 characters) in item **IS8**.

**Note:** If you are using manual addressing and need to finish filling in the target IQN value in work sheet item **IN11**, see [Selecting the target iSCSI Qualified Name \(IQN\)](#).

**Related information:**

- [Installation Checklist](#)

### 4.3.7.3 Selecting a language version

If your IBM i system has multiple national language versions installed, then you can choose which language version is used for the IBM i Integrated Server Support programs that run on the server.

For most environments, use the primary national language that is installed on IBM i. For information about supported language versions, see the install command documentation referenced in the **Related information** below.

Record values in work sheet item **IS14** as follows:

- To use the primary language of IBM i, put a check mark in the box labeled **Primary**. Primary is the default value.
- Otherwise, put a check mark in the box labeled **Other** and also record the IBM i secondary language identifier (for example, 2924 for English).

**Note:** If you choose a non-default value, then you cannot use the **Create Server Web GUI** task to install your server. You must use the appropriate IBM i CL command to install your server.

**Related information:**

- [Installation Checklist](#)
- i 7.2: [Install Integrated Server \(INSINTSVR\)](#)
- i 7.1: [Install Integrated Server \(INSINTSVR\)](#)
- i 7.1: [Install Windows Server \(INSWNTSVR\)](#)
- i 6.1: [Install Windows Server \(INSWNTSVR\)](#)
- i 6.1: [Install Linux Server \(INSLNXSVR\)](#)
- i 5.4: [Install Windows Server \(INSWNTSVR\)](#)
- i 5.4: [Install Linux Server \(INSLNXSVR\)](#)



#### 4.3.7.4 Selecting IBM i tape and optical devices to allow (i 7.2 only)

Since IBM i 7.2, you can choose to either allow or restrict which IBM i tape and optical devices the integrated server can access.

Server OS	Considerations
Windows	For most environments, allow access to all IBM i tape and optical devices for the initial integrated Windows server installation. If necessary, you can update the list of allowed devices after the server is installed.
ESX	VMware ESX servers cannot use IBM i tape and optical devices, so none of the tape and optical devices should be allowed.

Record values in work sheet item **IS15** as follows:

IBM i	Description
i 7.2	<p>To allow an integrated Windows server access to all tape and optical devices, put a check mark in the box labeled <b>Unrestricted</b>. You should also put a check mark in the box labeled <b>OS type</b> for work sheet item <b>IS16</b> (Restricted device resources).</p> <p>Otherwise, for an integrated Windows server, you can put a check mark in the box labeled <b>Other</b> and also record *ALLTAPE or *ALLOPT or the list of IBM i tape and optical devices to allow. You should also put a check mark in the box labeled <b>OS type</b> for work sheet item <b>IS16</b> (Restricted device resources).</p> <p>For an integrated ESX server, you must put a check mark in the box labeled <b>Unrestricted</b>. You should also put a check mark in the box labeled <b>OS type</b> for work sheet item <b>IS16</b> (Restricted device resources).</p>

**Related information:**

- [Installation Checklist](#)
- [i 7.2: Install Integrated Server \(INSINTSVR\)](#)

#### 4.3.7.5 Selecting IBM i tape and optical devices to restrict

You can choose to restrict which IBM i tape and optical devices the integrated server can access.

Server OS	Considerations
Windows	For most environments, allow access to all IBM i tape and optical devices for the initial integrated Windows server installation. If necessary, you can update the list of restricted devices after the server is installed.
ESX	VMware ESX servers cannot use IBM i tape and optical devices, so all tape and optical devices must be restricted.

Record values in work sheet item **IS16** as follows:

IBM i	Description
i 7.2	To allow an integrated Windows server access to all tape and optical devices, or if you are installing a VMware ESX server, put a check mark in the box labeled <b>OS type</b> . You should also put a check mark in the box labeled <b>Unrestricted</b> for <b>IS15</b> (Allowed device resources).

		Otherwise, for an integrated Windows server, you can put a check mark in the box labeled <b>Other</b> and also record *ALL or the list of IBM i tape and optical devices to restrict. You should also put a check mark in the box labeled <b>Unrestricted</b> for IS16 (Allowed device resources).
i 7.1 i 6.1		To allow an integrated Windows server access to all tape and optical devices, or if you are installing a VMware ESX server, put a check mark in the box labeled <b>OS type</b> .  Otherwise, for an integrated Windows server, you can put a check mark in the box labeled <b>Other</b> and also record *ALL or the list of IBM i tape and optical devices to restrict.
i 5.4	Windows	To allow an integrated Windows server access to all tape and optical devices, put a check mark in the box labeled <b>OS type</b> .  Otherwise, put a check mark in the box labeled <b>Other</b> and also record the list of IBM i tape and optical devices to restrict or *ALL.
	ESX	Put a check mark in the box labeled <b>Other</b> and also record *ALL or the list of IBM i tape and optical devices to restrict.

**Note:** If you do not choose **OS type**, then you cannot use the **Create Server Web GUI** task to install your server. You must use the appropriate IBM i CL command to install your server.

**Related information:**

- [Installation Checklist](#)
- i 7.2: [Install Integrated Server \(INSINTSVR\)](#)
- i 7.1: [Install Integrated Server \(INSINTSVR\)](#)
- i 7.1: [Install Windows Server \(INSWNTSVR\)](#)
- i 6.1: [Install Windows Server \(INSWNTSVR\)](#)
- i 6.1: [Install Linux Server \(INSLNXSVR\)](#)
- i 5.4: [Install Windows Server \(INSWNTSVR\)](#)
- i 5.4: [Install Linux Server \(INSLNXSVR\)](#)

### 4.3.7.6 Selecting point-to-point virtual Ethernet IP addresses

A point-to-point virtual Ethernet connection is created for the following configurations:

Server OS	IBM i	Point-to-point Virtual Ethernet Connection
Windows	All	<p>The integrated Windows server installation process automatically generates default IP addresses and an associated subnet for the point-to-point virtual Ethernet connection between IBM i and the integrated Windows server. The generated IP addresses are on a subnet that is not used for other IBM i communications.</p> <p>For most environments, use these generated IP address values. However, you can assign your own IP addresses for this point-to-point virtual Ethernet connection.</p>
ESX	All	<p>VMware ESX servers do <b>not</b> support virtual Ethernet connections.</p> <p>However, the install command allows you to specify *GEN or IP addresses for the virtual Ethernet point-to-point connection. This creates an Ethernet line description and an associated TCP/IP interface.</p> <ul style="list-style-type: none"> <li>This Ethernet line description will <b>not</b> go active when the server is varied on since the virtual Ethernet connection is not recognized by the VMware ESX server.</li> <li>The point-to-point virtual Ethernet port on an integrated VMware ESX server can <b>only</b> be used to automatically start the integrated VMware ESX server when IBM i TCP/IP starts.</li> <li>The point-to-point virtual Ethernet port does <b>not</b> provide a virtual Ethernet communication connection between the integrated VMware ESX server and any other systems.</li> </ul>
	i 7.2 i 7.1	When installing a VMware ESX server, the default value for the point-to-point virtual Ethernet connection does <b>not</b> generate an IP address and associated subnet.
	i 6.1 i 5.4	The integrated ESX server installation process automatically generates default IP addresses and an associated subnet for the point-to-point virtual Ethernet connection.

You can choose the IP addresses to use for the point-to-point virtual Ethernet connection between IBM i and the integrated server.

**Note:** The subnet mask that is used for the point-to-point virtual Ethernet connection is 255.255.255.0. Keep this subnet mask in mind if you assign your own IP addresses for this connection.

Record values for the following work sheet items.

- To use the generated IP addresses for an integrated server (or no IP addresses if you are installing an ESX server on i 7.1 or higher), put a check mark in the box labeled **OS type** in work sheet item **IS17**. OS type is the default value.

- Otherwise, put a check mark in the box labeled **Other** in work sheet item **IS17**. Also record your choices for the **IBM i** and integrated **Windows** server IP addresses to use for the point-to-point virtual Ethernet connection.

**Note:** If you choose a non-default value, then you cannot use the **Create Server Web GUI** task to install your server. You must use the appropriate IBM i CL command to install your server.

**Related information:**

- [Installation Checklist](#)
- [i 7.2: Install Integrated Server \(INSINTSVR\)](#)
- [i 7.1: Install Integrated Server \(INSINTSVR\)](#)
- [i 7.1: Install Windows Server \(INSWNTSVR\)](#)
- [i 6.1: Install Windows Server \(INSWNTSVR\)](#)
- [i 6.1: Install Linux Server \(INSLNXSVR\)](#)
- [i 5.4: Install Windows Server \(INSWNTSVR\)](#)
- [i 5.4: Install Linux Server \(INSLNXSVR\)](#)

#### 4.3.7.7 Selecting preferred storage unit to store virtual storage on (i 7.2 only)

Since IBM i 7.2, you can choose to store the virtual storage that contains the integrated server operation system on solid-state drive units if you prefer, or if no preference is specified, the virtual storage will be stored on any disk units in the storage pool.

Record values in work sheet item **IS18** as follows:

- To store the virtual storage on solid-state drive units if available, put a check mark in the box labeled **\*SSD**.
- Otherwise, put a check mark in the box labeled **\*ANY**.

**Related information:**

- [Installation Checklist](#)
- [i 7.2: Install Integrated Server \(INSINTSVR\)](#)

#### 4.3.7.8 Selecting additional INSxxxSVR command parameters

If you are installing your integrated server using the Install Windows Server (**INSWNTSVR**) or Install Linux Server (**INSLNXSVR**) command, then you can specify additional command parameters.

The install commands have many parameters that you can use to customize the integrated server installation process. For example, you can provide the Windows license key as a parameter on the INSWNTSVR command. Refer to the INSWNTSVR or INSLNXSVR command documentation for details on the additional parameters that are available.

Record values in work sheet item **IS19** as follows:

1. To use a non-default value for an install command parameter, record the parameter keyword name and the associated value in work sheet item **IS19**.

**Note:** If you choose a non-default value, then you cannot use the **Create Server Web GUI** task to install your server. You must use the appropriate IBM i CL command to install your server.

2. Repeat step 1 as needed to record any additional install command parameter keywords and values that you need.

**Related information:**

**Related information:**

- [Installation Checklist](#)
- [i 7.2: Install Integrated Server \(INSINTSVR\)](#)
- [i 7.1: Install Windows Server \(INSWNTSVR\)](#)
- [i 6.1: Install Windows Server \(INSWNTSVR\)](#)
- [i 6.1: Install Linux Server \(INSLNXSVR\)](#)
- [i 5.4: Install Windows Server \(INSWNTSVR\)](#)
- [i 5.4: Install Linux Server \(INSLNXSVR\)](#)

### 4.3.7.9 Planning for VMware ESX server management

**Note:** This planning task **only** applies to ESX servers.

Determine the ESX server management infrastructure to use and perform the instructions below:

Infrastructure	Instructions
<a href="#">Management server based infrastructure</a>	<p>This infrastructure is <b>required</b> for IBM i 7.2, i 7.1 and for ESXi Embedded or ESXi Installable servers on i 6.1. It is optional for ESX 4 servers on i 6.1.</p> <p>To complete the installation process for a VMware ESX server that use the <a href="#">Management server based infrastructure</a>, you must select an associated management server (integrated Windows server). Then you must configure connection information so that the Windows server can connect to the VMware ESX server or the associated platform manager.</p> <p>The supported operating system versions on the iSCSI attached integrated Windows server are as follows:</p> <ul style="list-style-type: none"> <li>• Windows Server 2012</li> <li>• Windows Server 2008 R2</li> <li>• Windows Server 2008</li> <li>• Windows Server 2003 R2</li> <li>• Windows Server 2003</li> </ul> <p>Record values for the following work sheet items.</p> <ol style="list-style-type: none"> <li>1. Put a check in the <b>Management server based infrastructure</b> box in item <b>EM1</b>.</li> <li>2. Record the NWSD name of the management server (integrated Windows server) in work sheet item <b>EM2</b>.</li> <li>3. Record the ESX server IP address or host name in work sheet item <b>EM4</b>.</li> <li>4. Optional: If an ESX platform manager is used, record the platform manager IP address or host name in work sheet item <b>EM5</b>.</li> </ol>
<a href="#">Service console based infrastructure</a>	<p>This infrastructure is <b>required</b> for IBM i 5.4 and for ESX 3.5 servers on i 6.1. It is optional for ESX 4 servers on i 6.1.</p> <p>Record values for the following work sheet items.</p> <ol style="list-style-type: none"> <li>1. Put a check in the <b>Service console based infrastructure</b> box in item <b>EM1</b>.</li> <li>2. Skip the remaining items in the <b>Integrated VMware ESX server management</b> work sheet, since they do not apply.</li> </ol>

**Related information:**

- [Installation Checklist](#)

## 4.4 Install the hardware

The steps in this section address:

- Installing the hardware that is required to run the server.
- Updating the BladeCenter or System x firmware.
- Configuring the BladeCenter or System x UEFI/BIOS, service processor, iSCSI initiator adapter, and server start option settings.
- Attaching all the cables that are needed.

**Important:** The IBM i iSCSI HBA and the PCI-X versions of the System x iSCSI HBA cards look identical, but they have different firmware and function, so they are **not** interchangeable. If you get them mixed up and use an iSCSI HBA in the wrong system, it will **not** work. If you are not sure which system type a particular iSCSI HBA is for, look for the following CCIN values on the tail stock of the iSCSI HBA card:

System x iSCSI initiators	Option Part Number	CCIN
QLogic QLA4050C	30R5201	1986
QLogic QLA4050	30R5501	1987

IBM i iSCSI targets	Feature Code	CCIN
Power System 1 Gigabit iSCSI TOE PCI-X Adapter	5713	573B
Power System 1 Gigabit iSCSI TOE PCI-X Adapter	5714	573C
System i iSCSI Host Bus Adapter	5783	573B
System i iSCSI Host Bus Adapter	5784	573C

**Note:** Before performing the steps below, you should already have the [IBM i iSCSI Solution Work Sheets](#) filled out.

### Related information:

- [Installation Checklist](#)

### 4.4.1 Install each new IBM i iSCSI target

**Note:** This step corresponds to slide 8 in the [BladeCenter](#) or [System x iSCSI Installation Overview](#) Flash animation.

If new IBM i iSCSI target adapters need to be installed, refer to the appropriate **PCI adapter** installation topic for your Power server model in the [IBM Power Systems Hardware Information Center](#).

If your Power server is partitioned, make sure that the newly installed iSCSI target adapters are assigned to the IBM i logical partition that will host the BladeCenter or System x models.

### Related information:

- [Installation Checklist](#)

## 4.4.2 Install the BladeCenter or System x hardware and iSCSI initiators

Install the BladeCenter or System x hardware using the documentation that came with the server. Make sure to install any iSCSI initiator adapters that are needed as well as an IBM USB Memory Key for ESXi Embedded, if needed.

**Note:** For an overview of PCI slot locations for your iSCSI initiators and the internal USB port location for the ESXi Embedded Memory Key, select your server from the [IBM x86 servers](#) Web page and refer to the **Product guide**. If your server is not listed on the IBM x86 servers Web page, then refer to your server documentation for guidance on USB port and PCI slot locations.

**Important notes** for specific configurations:

Configuration	Notes
System x models <b>336</b> and <b>236</b> with a QLogic <b>iSCSI HBA</b> and Windows Server <b>2003</b>	<p>When initially installing Microsoft Windows Server 2003 with Service Pack 1 on an <b>x336</b> or <b>x236</b> server, there is a known problem that restricts where an iSCSI HBA can be installed in the server:</p> <ul style="list-style-type: none"><li>For the <b>x336</b>, only <b>one</b> iSCSI HBA can be present when installing and it <b>must</b> be installed in <b>slot 1</b>. Also note that you need to remove the "full height" tail stock from the iSCSI HBA and install the "1/2 height" tailstock on the iSCSI HBA when installing it in slot 1 of an x336.</li><li>For the <b>x236</b>, only <b>one</b> iSCSI HBA can be present when installing and it <b>must</b> be installed in <b>slot 6</b>.</li></ul> <p><b>After</b> Windows Server 2003 is installed on the x336 or x236, you can optionally install a Microsoft Windows hot fix that lifts the above restrictions to allow the iSCSI HBA to be moved to a different slot than shown above and to allow additional iSCSI HBAs to be installed. See Microsoft Knowledge Base entry <a href="#">Pci.sys resource configuration conflicts cause an error in Windows Server 2003 SP1 or in an x64-based version of Windows Server 2003: "Stop 0x0000007B"</a> for information on how to obtain the hot fix from Microsoft.</p>

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)



## 4.4.2.1 Update and configure the BladeCenter or System x hardware

**Note:** This step corresponds to slides **8-10** in the [BladeCenter](#) or [System x iSCSI Installation Overview](#) Flash animation.

Update the firmware and configure the system using the referenced sections for your type of server:

Server Type	Tasks to Perform
BladeCenter Blade	To update and configure the <b>BladeCenter</b> chassis and <b>blade</b> server hardware: <ol style="list-style-type: none"><li>1. <a href="#">Updating and configuring the BladeCenter chassis</a></li><li>2. <a href="#">Updating the server using Bootable Media Creator (BoMC) media</a></li><li>3. <a href="#">Verifying blade information</a></li></ol>
System x	To update and configure the <b>System x</b> server hardware: <ol style="list-style-type: none"><li>1. <a href="#">Updating the server using Bootable Media Creator (BoMC) media</a></li><li>2. <a href="#">Configuring the System x service processor</a></li></ol>

### Notes:

- Do not power on the server until instructed to do so in the above tasks.
- Wait until the **Cable the network** step later on to attach the cables.

#### Related information:

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

### 4.4.2.1.1 Updating and configuring the BladeCenter chassis

Use these tasks to prepare your BladeCenter hardware for integration with IBM i.

At this time, the management module must have an Ethernet cable plugged into its Ethernet port. Refer to BladeCenter or management module documentation to complete these tasks. Plug the other end of this cable into the Ethernet connector of the computer containing the downloaded management module update package. In some cases, a switch or hub might also be necessary to connect.

Also ensure that the BladeCenter AC power cords are plugged into an appropriate power source to provide power for the management module.

Perform the following tasks to update and configure the BladeCenter chassis:

1. [Updating the BladeCenter management module firmware](#)
2. [Configuring the BladeCenter management module](#)
3. [Updating and configuring the BladeCenter I/O module](#)

#### Related information:

➤ [Installation Checklist](#)

### 4.4.2.1.2 Verifying blade information

Verify that the blade configuration matches the information in **IBM i remote system configuration** work sheet from the [IBM i iSCSI Solution Work Sheets](#).

Follow this procedure:

1. Sign on to the management module Web interface.  
See [Connecting to the service processor Web interface](#).
2. Select **Hardware VPD** under **Monitors** on the navigation pane on the left side of the screen.
3. In the **BladeCenter Hardware Vital Product Data** section, click on the link for the blade server in the **Blades** portion of the table that corresponding to the blade server bay or bays that are used by the blade server that is to be attached to IBM i.
4. Click on the **Inventory** tab for the blade and verify the information in the **Machine Type/Model** and **Machine Serial No.** columns in the table with the information in the work sheet (items **RS5** and **RS4**, respectively). Correct any discrepancies on the work sheet.
5. Click on the **Ports** tab for the blade and verify the iSCSI initiator information with the work sheet.

iSCSI Initiator Adapter	Initiator Port	MAC Address	Address Usage	Work Sheet Item
LAN on Motherboard (LOM) or an Ethernet NIC expansion card	1	1	iSCSI	<b>RS14</b>
			LAN	<b>RS19</b>
	2	2	iSCSI	<b>RS14</b>
			LAN	<b>RS19</b>
iSCSI HBA expansion card	1	1	iSCSI	<b>RS14</b>
		2	LAN	<b>RS19</b>
	2	3	iSCSI	<b>RS14</b>
		4	LAN	<b>RS19</b>

Correct any discrepancies on the work sheet.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

## 4.4.2.2 Configure the iSCSI initiators

**Note:** This step corresponds to slide 11 in the [BladeCenter](#) or [System x iSCSI Installation Overview](#) Flash animation.

Perform the indicated tasks below for your environment to configure the iSCSI Initiator adapter ports:

Server OS	Initiator Ports	Tasks
Embedded ESXi versions	All initiator ports	<a href="#">Configuring non-boot iSCSI initiator ports</a>
All other OS versions	Initiator port used for boot during the installation	<a href="#">Configuring a boot iSCSI initiator port</a> <a href="#">Configuring advanced iSCSI initiator port settings</a>
	All other initiator ports	<a href="#">Configuring non-boot iSCSI initiator ports</a>

Be sure to use the BladeCenter or System x iSCSI initiator configuration information from the [IBM i iSCSI Solution Work Sheets](#).

Note that different configuration steps are required for various iSCSI initiator and server configurations, so use the appropriate sub-sections for your configuration.

Do not power on the server until instructed to do so in the above tasks. Also, wait until the **Cable the network** step later on to attach the cables.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

## 4.4.2.3 Configure the integrated server start options

See [Setting the integrated server start options](#).

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

## 4.4.3 Cable the network

**Note:** This step corresponds to slide 12 in the [BladeCenter](#) or [System x iSCSI Installation Overview](#) Flash animation.

Once the System x or blade system has been configured, the network needs to be cabled to complete the configuration.

The first step is to locate the ports that need to be cabled into the network. Locate each point or port that you will connect from the following:

- The IBM i partition network interface; either a new adapter or an existing adapter being used for a TCP/IP connection.
- The System x or blade server service processor.

Depending on which server you are attaching, the location of the service processor will vary. Refer

to your System x or blade server documentation to complete this connection.

- For a System x server, the IMM II, IMM, RSA II, or BMC might be used as the service processor.
- For a blade server, the BladeCenter management module (MM or AMM) is used as a service processor.
- The iSCSI network connection is as follows:
  - In the IBM i partition and the System x server, the port to connect to is located on the tailstock of the iSCSI adapter or a system planar for a LAN on Motherboard (LOM) port.
  - In the blade server the port to connect is located on the I/O module plugged into a BladeCenter I/O bay. This might be an internally wired port on an integrated switch or a fan-out cable from a pass-through module. Refer to the I/O module documentation to complete this connection.

There are many different ways to cable the network – the iSCSI configuration could even be added to an existing Ethernet network. All the possibilities are not covered here. There are a couple of important considerations that must be observed when cabling the iSCSI configuration:

- Ensure each iSCSI target to be used in IBM i is reachable from at least one iSCSI initiator in the System x or blade system.
  - Ensure any iSCSI target in IBM i that is required for integrated server installation or boot is reachable from at least one boot iSCSI initiator port in the System x or blade system.
  - For maximum availability, ensure that alternate paths are present upon failure of an individual cable, iSCSI adapter, or switch in the iSCSI network. After you install the server, you can also use multipath I/O (MPIO) and enable boot on multiple adapters.
  - If you want to take advantage of spare iSCSI adapters for integrated servers, ensure that the spare iSCSI adapters in the IBM i system are reachable from iSCSI adapters in the System x or blade system. See [Using hot spare hardware](#).
- Ensure that the IBM i network interface card and the service processor connection reside in the same network.

For help understanding different external switch considerations see [Ethernet switches for the iSCSI solution](#).

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

## 4.5 Prepare IBM i for the integrated server installation

Before starting the operating system installation, you should perform the following steps to prepare IBM i for the install.

**Note:** Before performing the steps below, you should already have installed the hardware, updated the firmware, configured the BladeCenter blade or System x model and attached all the cables. If necessary, go back to the **Install the hardware** section and complete those tasks before continuing.

### Related information:

➤ [Installation Checklist](#)

### 4.5.1 Create an NWSH for each new IBM i iSCSI target

**Note:** This step corresponds to slide 14 in the [BladeCenter](#) or [System x iSCSI Installation Overview](#) Flash animation.

A network server host adapter (NWSH) object that represents the iSCSI target port must be created before IBM i and your integrated server can use the target.

**Note:** Use the following [IBM i iSCSI Solution Work Sheets](#) to help you do these tasks:

- **IBM i iSCSI target network server host adapter**
- **IBM i line description for iSCSI software target NWSH**
- **IBM i TCP/IP interface for iSCSI software target NWSH**

If the **IBM i iSCSI target network server host adapter** work sheet indicates that a new NWSH needs to be created, use the information from the work sheet to create it now. You can accept the default values for any items that are not listed in the work sheet.

Use the following steps to use the GUI to create an NWSH object for each iSCSI target port:

1. Determine the IBM i hardware resource name that was assigned to the iSCSI target adapter port. For more information, see [Determining the hardware resource name for an iSCSI target adapter](#).
2. Select **Integrated Server Administration** from the [Web GUI](#) (7.2/7.1/6.1) or [System i Navigator](#) (5.4).

**Attention:** [System i Navigator](#) does **not** support creating a **software target** (virtual) NWSH, so you must use the [Web GUI](#) or the equivalent CL commands to create a **software target** NWSH.

3. Select **New Network Server Host Adapter**.

<a href="#">Web GUI</a>	To launch the task, look on the main <b>Integrated Server Administration</b> page. Click <b>Continue</b> on the <b>Select Base Object</b> page.
<a href="#">System i Navigator</a>	To launch the task, expand the <b>iSCSI Connections</b> folder and then right-click the <b>Network Server Host Adapters</b> folder.

4. On the **General** tab:
  - a. Enter the NWSH device **Name** and **Description**.
  - b. Select the **Hardware resource** for your type of target adaptor:

Type of iSCSI Target Adaptor	Hardware Resource
Software target (Ethernet NIC)	Select <b>Virtual</b> .
Hardware target (iSCSI HBA)	Select the resource name that was determined in step 1.

- c. Optional: Select **Online at IPL** if your iSCSI target adapter is a hardware target (iSCSI HBA) and you want it to automatically start when IBM i starts.

**Note:** If your iSCSI target adapter is a software target (Ethernet NIC), the equivalent function is accomplished by setting the corresponding TCP/IP interface to automatically start when TCP/IP is started on IBM i.

- d. Optional: Select the **Object authority**. You can use the default value **Change**.

5. On the **Local (Target) Interface** tab:

- a. Select the cable connection type. If the hardware is physically connected to an Ethernet switch, you can use the default value Network.
- b. Specify the remaining values based on the iSCSI target adapter type.

Type of iSCSI Target Adaptor	Values
Software target (Ethernet NIC)	<p>Select an IBM i TCP/IP interface for the SCSI interface Internet address.</p> <p><b>Tip:</b> If you did not previously create an IBM i TCP/IP interface and corresponding line description for your iSCSI target adapter, click <b>New</b> to create them now:</p> <ol style="list-style-type: none"> <li>1. For <b>TCP/IP interface</b>: <ol style="list-style-type: none"> <li>a. Enter an <b>Internet address</b>, <b>Subnet mask</b> and <b>Description</b>.</li> <li>b. Select <b>Start this TCP/IP interface every time TCP/IP is started</b> if you want the new NWSH to start automatically.</li> </ol> </li> <li>2. For <b>Line description to use for the TCP/IP interface</b>: <ul style="list-style-type: none"> <li>• If the line description exists, select it from the list.</li> <li>• Otherwise, enter the remaining values to create a line description. <ol style="list-style-type: none"> <li>a. Enter a <b>Name</b> and <b>Description</b>.</li> <li>b. Select the <b>Hardware resource</b> for your iSCSI target adapter port that was determined in step 1.</li> <li>c. Set the <b>Maximum frame size</b>.</li> </ol> </li> </ul> </li> <li>3. Click <b>Create</b>.</li> </ol>
Hardware target (iSCSI HBA)	<ol style="list-style-type: none"> <li>1. Enter a <b>Subnet mask</b>.</li> <li>2. Enter a SCSI interface <b>Internet address</b>.</li> <li>3. Enter a LAN interface <b>Internet address</b>.</li> </ol>

6. Click **OK** to create the NWSH.

**Related information:**

- [Installation Checklist](#)
  - [Work with Device Descriptions \(WRKDEVD\)](#)  
(use WRKDEVD \*NWSH)
  - [Create Device Desc \(NWSH\) \(CRTDEVNWSH\)](#)
  - [Work with TCP/IP Network Sts \(NETSTAT\)](#)  
(use NETSTAT \*IFC)
- [Configure TCP/IP \(CFGTCP\)](#)
  - [Add TCP/IP Interface \(ADDTCPIFC\)](#)
  - [Work with Line Descriptions \(WRKLIND\)](#)
  - [Create Line Desc \(Ethernet\) \(CRTLINETH\)](#)  
(use parameters: MAXFRAME(8996)  
CMNRCYLMT(1 0))

### 4.5.1.1 Determining the hardware resource name for an iSCSI target adapter

You must determine the IBM i iSCSI target adapter hardware resource name. The resource name is used when creating a network server host adapter (NWSH), or when creating a line description (LIND) that is used with a virtual NWSH.

Determine the IBM i hardware resource name that was assigned to the iSCSI target adapter port. Find the iSCSI target adapter port resource with physical location values that match the location of the iSCSI target adapter.

1. From the IBM i command line, run the following command to display a list of the communications resources:

```
WRKHDWRSC *CMN
```

2. Use option **7=Display resource detail** on each iSCSI target adapter port resource until the correct one is found.

**Note:** The iSCSI target adapter port resource description that is shown is:

Type of iSCSI Target Adaptor	Description Shown
Software target (Ethernet NIC)	<b>Ethernet Port</b>
Hardware target (iSCSI HBA)	<b>Network Server Host Port</b> <b>Note:</b> Ignore resources with type <b>573F</b> , which are for software target (virtual) ports.

3. On the **Display Resource Detail** panel for the iSCSI target adapter port, examine the Location value to determine the frame ID, card position, and port values. If the location value corresponds to the iSCSI target adapter port for the new NWSH, record the **Resource name** value so that it is available when creating the NWSH or LIND.

For example, if you are using the [IBM i iSCSI Solution Work Sheets](#), then record the **Resource name** value in one of the following work sheet items:

Type of iSCSI Target Adaptor	Work Sheet Item ID
Software target (Ethernet NIC)	<b>LD3</b>
Hardware target (iSCSI HBA)	<b>NH4</b>

## 4.5.2 Start the NWSH for each IBM i iSCSI target that the server uses

Start any NWSHs that are used by the iSCSI-attached integrated server. Starting the NWSH makes the iSCSI target available during the operating system installation.

Make sure that you have cabled the IBM i iSCSI target adapter to the iSCSI network. See [Cable the network](#).

1. Select **Integrated Server Administration** from the [Web GUI](#) or [System i Navigator](#).
2. Select **Network Server Host Adapters**.
3. Select the **Start** action for the network server host adapter.

**Note:** If the NWSH is for a software target (Ethernet NIC), then the associated TCP/IP interface and line description (LIND) are started automatically.

If the NWSH does not start or returns a failed status, see the [Troubleshooting](#) Web page.

### Related information:

- [Installation Checklist](#)
- [Vary Configuration \(VRYCFG\)](#)
- [Work with Configuration Status \(WRKCFGSTS\)](#)  
(use WRKCFGSTS \*DEV \*NWSH)



### 4.5.3 Create and initialize a service processor configuration

**Note:** This step corresponds to slide 15 in the [BladeCenter](#) or [System x iSCSI Installation Overview](#) Flash animation.

This object represents the service processor for the integrated server hardware.

#### Notes:

1. **IBM i 6.1 or 5.4 only:** If IBM Director (5722-DR1) is installed on your IBM i system and you have not already enabled **Service Processor Manager**, then enable it now.  
See [Configuring IBM i to use Service Processor Manager on i 6.1 and i 5.4](#).
2. Use the following [IBM i iSCSI Solution Work Sheets](#) to help you do this task:
  - **IBM i service processor configuration**
3. If the **IBM i service processor configuration** work sheet indicates that a new service processor configuration needs to be created, use the information from the work sheet to create it now. You can accept the default values for any items that are not listed in the work sheet.
4. A service processor network server configuration (NWSCFG subtype SRVPRC) object must be created for the service processor or Management Module of each System x or BladeCenter that is used to run an iSCSI-attached integrated server.
5. A service processor configuration is not needed for each blade in an IBM BladeCenter chassis. Only one service processor configuration is needed for the BladeCenter chassis.

To create a service processor configuration, follow these steps:

1. Select **Integrated Server Administration** from the [Web GUI](#) or [System i Navigator](#).
2. Select **New Service Processor Configuration**.

<a href="#">Web GUI</a>	To launch the task, look on the main <b>Integrated Server Administration</b> page. Click <b>Continue</b> on the <b>Select Base Object</b> page.
<a href="#">System i Navigator</a>	To launch the task, expand the <b>iSCSI Connections</b> folder and then right-click the <b>Service Processors</b> folder.

3. Enter the **Name** and **Description**
4. Specify either a **Host name** or **Internet address** to identify the service processor on the network.
5. Optional: Specify the System x or BladeCenter **Serial number** and **Manufacturer type and model**. If you leave these values blank, they are automatically retrieved when the service processor configuration is initialized.
6. Optional: Select the **Object authority**. You can use the default value **Change**.
7. Click **OK** to create the service processor configuration.
8. Next, select the **Initialize** action for the service processor configuration that was created above.

9. Choose the **Validate service processor user ID and password and store in {NWSCFG NAME}** option.
10. Enter the **User** and **Password**.
11. Click **Initialize** to complete the task.

Once the service processor configuration is created and initialized, the following is verified:

- The connection to the remote system service processor is physically cabled and configured properly.
- The correct service processor user and password are stored in the service processor configuration.

**Related information:**

- [Installation Checklist](#)
- [Clone Server Hardware Checklist](#)
- [Work with NWS Configuration \(WRKNWSCFG\)](#)
- [Create NWS Configuration \(CRTNWSCFG\)](#)
- [Initialize NWS Configuration \(INZNWSCFG\)](#)

### 4.5.3.1 Configuring IBM i to use Service Processor Manager on i 6.1 and i 5.4

The **Service Processor Manager** function of IBM i **Integrated Server Support** is used for iSCSI-attached integrated server discovery and power control.

By default for i 6.1 and i 5.4, if **IBM Director** (5722-DR1) is installed, then an **IBM Director Server** running on your IBM i system is used for integrated server discovery and power control. However, IBM Director Server running on IBM i does not provide support for newer System x and BladeCenter blade servers. Therefore, the tasks described in this document require that IBM i uses Service Processor Manager for integrated server discovery and power control.

Enable Service Processor Manager on i 6.1 and i 5.4 as follows:

IBM Director Installed on IBM i?	Method to enable Service Processor Manager
No	<b>No action</b> is required. Service Processor Manager is used by default if IBM Director is not installed.
Yes	Create a <b>QITDSMGR</b> data area on IBM i using the following command:  CRTDTAARA DTAARA(QUSRSYS/QITDSMGR) TYPE(*DEC) LEN(4 0) VALUE(2)

## 4.5.4 Create a remote system configuration

**Note:** This step corresponds to slide 16 in the [BladeCenter](#) or [System x iSCSI Installation Overview](#) Flash animation.

This IBM i object contains information about the integrated server hardware and iSCSI initiators.

**Attention:** If you need to define more than one remote interface (more than one iSCSI initiator port on the BladeCenter blade or System x model), then use the GUI interface described in this section to create the remote system configuration. See the [CRTNWSCFG and CHGNWSCFG Prompting Problems When defining more than one remote interface](#) troubleshooting topic for more information.

### Notes:

1. Use the following [IBM i iSCSI Solution Work Sheets](#) to help you do this task:
  - **IBM i remote system configuration**
2. If the **IBM i remote system configuration** work sheet indicates that a new remote system configuration needs to be created, use the information from the work sheet to create it now. You can accept the default values for any items that are not listed in the work sheet.

To create a remote system configuration, follow these steps:

1. Select **Integrated Server Administration** from the [Web GUI](#) or [System i Navigator](#).
2. Select **New Remote System Configuration**.

<a href="#">Web GUI</a>	To launch the task, look on the main <b>Integrated Server Administration</b> page. Click <b>Continue</b> on the <b>Select Base Object</b> page.
<a href="#">System i Navigator</a>	To launch the task, expand the <b>iSCSI Connections</b> folder and then right-click the <b>Remote Systems</b> folder.

3. On the **General** tab:
  - a. Enter the **Name** and **Description**.
  - b. Select the **Service processor configuration**.
  - c. Specify the **Remote system identity**.
  - d. Optional: Select the **Object authority**. You can use the default value **Change**.
4. On the **Remote Interfaces** tab, enter information to define the SCSI and LAN interface attributes for the remote system.
5. Optional: Specify values on the **Boot Parameters** and **CHAP Authentication** tabs if wanted.
6. Click **OK** to create the remote system configuration.

### Related information:

- [Installation Checklist](#)
- [Clone Server Hardware Checklist](#)
- [Work with NWS Configuration \(WRKNWSCFG\)](#)
- [Create NWS Configuration \(CRTNWSCFG\)](#)

## 4.5.5 Verify that the remote system is accessible and powered off

Verify that IBM i can contact the service processor of the System x or blade hardware and that the hardware is powered off or offline before you begin installing an iSCSI-attached integrated server.

1. Select **Integrated Server Administration** from the [Web GUI](#) or [System i Navigator](#).
2. Select **Remote Systems**.
3. Select the **Status** action for the new remote system configuration.
4. The status of the remote system hardware is shown.

If the remote system is not in a **Powered off (Offline)** state, power it off now before continuing. If installing a blade, just the blade must be powered off, not the BladeCenter chassis

**Note:** If you get a “not found” error or get some other error, see the [Troubleshooting](#) Web page.

5. Click **Cancel** to close the status panel.

**Related information:**

➤ [Installation Checklist](#)

➤ [Work with NWS Configuration \(WRKNWSCFG\)](#)

## 4.5.6 Create a QCNNSEC connection security configuration, if necessary

Depending on the IBM i version and the integrated server installation method used, you might need to create a QCNNSEC connection security configuration, as shown below:

<a href="#">IBM i</a>	Installation Method	Methods to Create the Connection Security Configuration
i 7.2 i 7.1 i 6.1	Create Server <a href="#">Web GUI</a> task	The <b>Create Server</b> task automatically creates a default connection security configuration named <b>QCNNSEC</b> , so you do <b>not</b> need to create one now.
i 7.2 i 7.1	INSINTSVR command	The <b>INSINTSVR</b> command automatically creates a default connection security configuration named <b>QCNNSEC</b> , so you do <b>not</b> need to create one now.
i 7.1	INSWNTSVR command	A QCNNSEC connection security configuration must be created if one does not already exist. Run the following IBM i command to create it:  <b>CRTNWSCFG NWSCFG(QCNNSEC) TYPE(*CNNSEC)</b>
i 6.1 i 5.4	INSWNTSVR and INSLNXSVR commands	<b>Note:</b> In a later task, you must specify <b>QCNNSEC</b> for the connection security NWSCFG parameter when using the INSWNTSVR or INSLNXSVR command to install the integrated server.

**Related information:**

➤ [Installation Checklist](#)

## 4.5.7 Prepare for IBM i memory requirements

Configuring IBM i with enough memory allocated to iSCSI-attached servers is very important for performance.

It is particularly important to create a memory pool for iSCSI disk I/O. If you have already configured an iSCSI memory pool, you can skip this task.

Otherwise, create a shared data memory pool for all iSCSI-attached servers using one of the following methods:

IBM i	Memory Pool Type	Methods to Create the Memory Pool
i 7.2 i 7.1 i 6.1	Shared data memory pool	<p>The <b>Create Server <a href="#">Web GUI</a></b> task provides an option to create a default iSCSI memory pool with a size of 512 MB, so you can use that method in a later step when you install the integrated server.</p> <p>If you do <b>not</b> plan to use the <b>Create Server <a href="#">Web GUI</a></b> task to install the integrated server, or if you prefer a different memory pool size, then you should create a shared data memory pool now.</p> <p>Run the following IBM i command:</p> <pre>CHGSHRPOOL POOL(*SHRPOOLnn) ACTLVL(*DATA) TEXT(*ISCSI) SIZE(524288)</pre> <p>where <i>nn</i> is the number (1-60) of an unused shared data memory pool.</p> <p><b>Tip:</b> Use the <a href="#">Work with Shared Storage Pools (WRKSHRPOOL)</a> command to find an unused shared data memory pool.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Use the assigned memory pool (<i>*SHRPOOLnn</i>) when installing the integrated server later on.</li> <li>• The activity level of <i>*DATA</i> allocates the memory to a shared data memory pool that does not allow any thread to run in the same shared memory pool.</li> <li>• The <i>*ISCSI</i> value in the memory pool description allows the <b>Create Server <a href="#">Web GUI</a></b> task to use this memory pool as the default when installing new servers.</li> </ul>
i 5.4	Private memory pool	<p>The private memory pool is enabled by creating a subsystem description named QGPL/<b>QFPHIS</b> and allocating a private memory pool of at least 4096 kilobytes. The amount of memory you want to allocate will depend on a number of factors, including number of iSCSI network servers, expected sustained disk activity for all servers, etc.</p> <p>To allocate a private memory pool for all iSCSI network servers, run the following IBM i command:</p> <pre>CRTSBSD SBS(D(QGPL/QFPHIS) POOLS((1 10000 1))</pre> <p>where <i>10000</i> is the size of the memory pool, in kilobytes.</p> <p>The QFPHIS subsystem is automatically started, if necessary, when an</p>

IBM i	Memory Pool Type	Methods to Create the Memory Pool
		<p>iSCSI Network Server Description (NWSD) is varied on (or an iSCSI-attached server is installed, which does an implicit vary on). The subsystem will activate the private memory pool. iSCSI network server descriptions that are varied on will then utilize the first private memory pool configured with at least the minimum (4MB) size for virtual storage I/O operations.</p> <p>The private memory pool is used by the server as long as the subsystem remains active. If the QFPHIS subsystem is ended prematurely (while an iSCSI network server is active), the server will continue to function properly, but future virtual disk I/O operations will revert to the *BASE memory pool until the private memory pool is once again allocated.</p> <p><b>Note:</b> When ending the QFPHIS subsystem, IBM i can reallocate the memory pool, possibly assigning the same identifier to another subsystem! Any active iSCSI network servers that are varied on and using the memory pool at the time the subsystem is ended may adversely impact other applications either when the memory pool reverts to *BASE or when the memory pool identifier is reassigned to another subsystem! To prevent unexpected impacts – do not end the QFPHIS subsystem while iSCSI servers are active.</p>

**Related information:**

- [Installation Checklist](#)
- [IBM i memory requirements](#)
- [Change Shared Storage Pool \(CHGSHRPOOL\)](#)
- [Integrated BladeCenter and System x Performance](#) chapter of the [Performance Capabilities Reference](#)

### 4.5.8 Set the IBM i QRETSVRSEC system value for integrated servers

Configure the IBM i QRETSVRSEC system value to work with your integrated server.

**Note:** If you have already set the QRETSVRSEC system value to 1, you can skip this task.

**Important:** If the QRETSVRSEC system value is not set to 1, change the QRETSVRSEC system value to ensure that IBM i keeps passwords. This setting is required to allow IBM i to start and shut down integrated servers. It also prevents delays for enrolled users when they sign on to IBM i.

1. On the IBM i command line, enter the command:  
  
WRKSYSVAL SYSVAL(QRETSVRSEC)
2. To change the value, enter a **2** in the **Option** field and press **Enter**.
3. Change the value of **Retain server security data** to **1** and press **Enter**.

**Related information:**

- [Installation Checklist](#)

## 4.5.9 Ensure that NetServer is configured

IBM i NetServer is used for file-level backup from IBM i, updating the Integrated Server Support software, and ESX server management. Also, to install updates to the IBM i integrated server support software on the Windows operating system, you must be signed on with a Windows account that has local administrator authority. That Windows account must correspond to an IBM i user profile with the same password. Alternatively, you must have a guest NetServer user profile configured.

To set up NetServer and the required user accounts, do the following:

1. If NetServer is not set up on your system yet, set it up using [Getting started with NetServer](#).
2. Once NetServer is set up, use **one** of the following methods to enable access to NetServer:

Methods to Enable Access to NetServer
<p><b>Method 1: Create a Windows user with authorities to access NetServer</b></p> <p>The user signs onto Windows with an account that has a corresponding IBM i user profile with the same password. This Windows account must also be a member of <b>Windows Administrators</b> group.</p> <p><b>Note:</b> You must wait until <b>after</b> the Window server has been installed to implement this method.</p> <p><b>Tip:</b> You can enroll an IBM i user to Windows to implement this method. See <a href="#">Enrolling IBM i users to integrated Windows servers</a>.</p>
<p><b>Method 2: Create a guest user profile for NetServer</b></p> <p>Perform these steps to set up a <b>guest</b> user profile for NetServer:</p> <ol style="list-style-type: none"><li>1. On IBM i, run the following command to create a user profile with no special authorities and no password:  <code>CRTUSRPRF USRPRF(<i>username</i>) PASSWORD(*NONE) SPCAUT(*NONE)</code>  <b>Note:</b> See the <a href="#">Security</a> topic collection for information about user profiles.</li><li>2. Run the following command, where <i>username</i> is the name of the user profile that you created in step 1:  <code>CALL QZLSCHSG PARM(<i>username</i> X'00000000')</code></li><li>3. Stop NetServer. Run the following command:  <code>ENDTCPSVR SERVER(*NETSVR)</code></li><li>4. Restart NetServer. Run the following command:  <code>STRTCPSVR SERVER(*NETSVR)</code></li></ol>

### Related information:

- [Installation Checklist](#)

## 4.5.10 WIN2003 only: Configure IBM i TCP/IP

IBM i TCP/IP domain name and TCP/IP domain name server values are used by default when you install an integrated Windows Server 2003 server. Verify that they are configured on IBM i before installing the Windows Server 2003 operating system on your integrated server.

If you have already configured IBM i TCP/IP domain name and TCP/IP domain name server values, you can skip this task.

Perform these steps to configure the IBM i TCP/IP domain values:

1. On IBM i, run the CFGTCP command.

The **Configure TCP/IP** menu appears.

2. From the **Configure TCP/IP** menu, choose 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**.

### Related information:

- [Installation Checklist](#)



## 4.6 *Install the integrated server*

The steps in this section address installing the operating system on the integrated server and configuring it to operate in the IBM i hosting environment.

**Note:** Before performing the steps below, you should already have configured IBM i objects and settings that are needed for the server installation. If necessary, go back to the [Prepare IBM i for the integrated server installation](#) section and complete those tasks before continuing.

**Related information:**

- [Installation Checklist](#)

## 4.6.1 Start the installation from IBM i

Use the IBM i **Create Server [Web GUI](#)** task or an IBM i **CL command** to begin installing the integrated server.

### Notes:

- This step corresponds to slides **19-22** in the [BladeCenter](#) or [System x iSCSI Installation Overview](#) Flash animation.
- To install an integrated server, you need IBM i \*IOSYSCFG, \*ALLOBJ, and \*JOBCTL special authority.
- For Windows servers, you must have your Windows server license key available. In most cases, it is printed on the back of the installation CD jewel case.
- Use the following [IBM i iSCSI Solution Work Sheets](#) to help you do this task:
  - **Integrated server installation**

To start the integrated server installation, follow these steps:

1. Insert the installation media in the optical drive that is appropriate for the operating system that you plan to install.

Server OS	Where to insert Server OS Installation Media
WIN2012 or WIN2008	Place the Windows Server 2012 or Windows Server 2008 DVD in the BladeCenter media tray or the System x DVD drive. Alternatively, you might be able to mount the install media ISO image using the <b>Remote Control</b> function of the server service processor.
WIN2003	Place the Windows Server 2003 installation CD in the IBM i optical drive or mount the CD ISO image in an IBM i virtual optical drive.
<u>Non-embedded</u> ESXi5 ESXi4 ESX4 ESX3.5	For <u>non-embedded</u> ESX versions, place the ESX installation DVD in the BladeCenter media tray or System x DVD drive. Alternatively, you might be able to mount the install media ISO image using the <b>Remote Control</b> function of the server service processor.
<u>Embedded</u> ESXi5 ESXi4	For <u>embedded</u> ESX versions, installation media is not required because ESXi is preinstalled in flash memory on the server.

Additional considerations based on the integrated server hardware type:

Hardware Type	Additional Considerations
BladeCenter blade server	You must also assign the BladeCenter KVM and media tray to the blade.
System x server	You cannot insert the installation media at this time, since the server is not initially powered on. Wait until IBM i powers on the server at the end of this task. Then insert the installation media when the server is performing the power on self test (POST).  <b>Note:</b> If the media is not available by the time POST completes, a boot source is not found. If a boot source is not found, insert the installation media and then restart the server by pressing <b>CTRL-ALT-DEL</b> on the integrated server console.

2. Choose **one** of the following methods to start the installation:

<b>IBM i</b>	<b>Installation Method</b>	<b>Tasks</b>
i 7.2 i 7.1 i 6.1	<b>Create Server</b> <a href="#">Web GUI</a> task	<p><b>Note:</b> If you chose any non-default values for work sheet items <b>IS9</b> through <b>IS19</b>, then you cannot use the GUI. You must use the appropriate CL command to start the installation.</p> <p>Perform the following steps to start the integrated server installation:</p> <ol style="list-style-type: none"> <li>1. Select <b>Integrated Server Administration</b> from the <a href="#">Web GUI</a>.</li> <li>2. Select <b>Create Server</b>.</li> <li>3. Click <b>Continue</b> on the <b>Select Base Object</b> page to start the <b>Create Server</b> wizard.</li> <li>4. Use the <b>Integrated server installation</b> work sheet to help you enter values on the pages of the wizard. <p><b>Note:</b> On the <b>Memory Pool</b> page of the wizard: If you selected <b>GUI default memory pool</b> for work sheet item <b>IS6</b> and a default iSCSI memory pool does not exist on IBM i, then click <b>Create Default iSCSI Memory Pool</b> to create it now.</p> </li> <li>5. On the <b>Summary</b> page of the wizard, click <b>Finish</b> to start the IBM i portion of the installation process.</li> </ol>
i 7.2 i 7.1	<b>INSINTSVR</b> command (for WIN2012, WIN2008 and ESX)  or  <b>INSWNTSVR</b> command (for WIN2003)	<p>Perform the following steps to start the integrated server installation:</p> <ol style="list-style-type: none"> <li>1. At the IBM i command line, type the appropriate CL command, and then press <b>F4</b> to prompt the command. <p><b>Note:</b> Use the CL command that is shown for your IBM i version and integrated server operating system in the first two columns of this table.</p> </li> </ol>
i 6.1 i 5.4	<b>INSWNTSVR</b> command (for Windows)  or  <b>INSLNXSVR</b> command (for ESX)	<ol style="list-style-type: none"> <li>2. Use the <b>Integrated server installation</b> work sheet to help you enter values for the command parameters. Leave the default values for any parameters that are not listed in the work sheet. <p><b>Note:</b> Different terminology is used in the commands than is used in the work sheet for some of the attributes.</p> </li> <li>3. Press <b>Enter</b> to start the IBM i portion of the installation process.</li> </ol>

The IBM i installation process creates the network server description (NWSD) and any required virtual storage for the server.

3. When the IBM i portion of the installation process is completed, the NWSD is then started (varied on) to boot the integrated server and install the server operating system. Then the **Create Server Web GUI** task or the install command prompts you to go to the integrated server console to perform additional tasks.

See [Continue the operating system installation from the integrated server console](#).

**Related information:**

- [Installation Checklist](#)
- [Integrated Server Operating System \(Server OS\) Versions](#)
- i 7.2: [Install Integrated Server \(INSINTSVR\)](#)
- i 7.1: [Install Integrated Server \(INSINTSVR\)](#)
- i 7.1: [Install Windows Server \(INSWNTSVR\)](#)
- i 6.1: [Install Windows Server \(INSWNTSVR\)](#)
- i 6.1: [Install Linux Server \(INSLNXSVR\)](#)
- i 5.4: [Install Windows Server \(INSWNTSVR\)](#)
- i 5.4: [Install Linux Server \(INSLNXSVR\)](#)

## 4.6.2 Continue the operating system installation from the integrated server console

When the IBM i configuration is complete, the integrated server operating system installation starts. You must then go to the server console to complete the operating system installation process.

Perform the tasks for your integrated server operating system below:

Server OS	Tasks
WIN2012 WIN2008	<a href="#">Continuing the Windows Server 2012/2008 installation from the Windows console</a>
WIN2003	<a href="#">Continuing the Windows Server 2003 installation from the Windows console</a>
<u>Embedded</u> ESXi5 ESXi4	<a href="#">Continuing the VMware ESXi Embedded installation from the ESX console</a>
<u>Non-embedded</u> ESXi5	<a href="#">Continuing the VMware ESX 5 installation from the ESX console</a>
<u>Non-embedded</u> ESXi4 ESX4	<a href="#">Continuing the VMware ESX 4 installation from the ESX console</a>
ESX3.5	<a href="#">Continuing the VMware ESX 3.5 installation from the ESX console</a>

### Related information:

- [Installation Checklist](#)
- [Integrated Server Operating System \(Server OS\) Versions](#)

### 4.6.2.1 Continuing the Windows Server 2012/2008 installation from the Windows console

When the IBM i phase of the installation completes, the integrated server starts. The Windows Server 2012/2008 phase of the installation begins.

To complete installation of Windows Server 2012/2008, follow the prompts from the Windows operating system. Be prepared to:

- Select language, time zone, and keyboard settings.
- Enter a product key for activation.
- Select the type of the Windows Server operating system to install. For a list of the supported versions for your BladeCenter blade or System x model, see [Blade server models](#) and [System x server models](#).

**Tip:** Both full and core installations are supported.

- Accept Microsoft license terms.

Select installation type.

You might need to load a driver for your iSCSI initiator in the following cases:

- If you are installing an integrated server that uses an iSCSI software initiator (Ethernet NIC), you might need to load the latest Ethernet NIC driver.  
See [Downloading Windows Ethernet NIC software initiator driver](#) to download it if you have not already done so.
- If you are installing a System x server that uses a QLogic PCIe iSCSI initiator adapter (PN 39Y6146 or PN 42C1770), you need to load the iSCSI HBA driver.  
See [Downloading System x Windows Server 2012/2008 iSCSI HBA driver](#) to download it if you have not already done so.

To load the driver, complete the following steps:

1. Select **Custom (Advanced)** when you see this message: **Which type of installation do you want?**
  2. Select **Load driver**.
  3. At the **Load Driver** screen, insert the Ethernet NIC or iSCSI HBA driver media that you created and click **OK**.
  4. Click **Next** to continue with the installation.
- Specify to install the Windows Server 2012/2008 operating system on the larger of **Disk 0** or **Disk 1**.

The Windows operating system will automatically format and partition the unallocated space for the system disk.

**Note:** If no disks appear in the list of available disks, then load the appropriate iSCSI initiator device driver as described previously.

The Windows operating system proceeds with the installation and might restart as necessary in order to complete the installation.

Be prepared to change the **Administrator** user password. After you change the password, the operating system will prompt you to begin the initial configuration tasks.

#### 4.6.2.2 Continuing the Windows Server 2003 installation from the Windows console

When the IBM i phase of the installation completes, the integrated server starts. The Windows Server 2003 phase of the installation begins.

To complete installation of Windows Server 2003, perform these tasks:

1. In the **License Agreement** step (in Windows Server Setup window), click **I accept this agreement**. 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.
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 Windows time zone is correct and matches the **Time Zone** system value in IBM i. See [Setting the Time zone \(QTIMZON\) system value](#).
  - b. Select a setting for Daylight Saving Time.
    - If you are in an area that observes Daylight Savings Time, leave the **Automatically adjust clock for daylight savings changes** 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 **Restart Now**, or wait a short time 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.

#### 4.6.2.3 Continuing the VMware ESXi Embedded installation from the ESX console

The VMware ESXi Embedded operating system is normally pre-installed on the USB Memory Key and you can skip to the [Complete the integrated server installation](#) task.

However, if the VMware ESXi Embedded operating system does **not** exist on the USB Memory Key, you might see an error message similar to the following on the server console:

```
Disk error.  
Press any key to Restart.
```

If this occurs, you can use the VMware ESXi Embedded Recovery CD that comes with the USB Memory Key option package to install the ESXi Embedded operating system on the USB Memory Key:

1. Place the VMware ESXi Embedded Recovery CD in the CD/DVD drive of the server.
  - If the server is a blade in a BladeCenter, ensure the CD/DVD drive is assigned to the blade.
2. Restart the server. The server boots from the Recovery CD.
3. Follow the instructions displayed for installing the ESXi Embedded operation system.

When the installation is complete, press **Enter** and remove the CD from the drive. Then reboot the server.

#### 4.6.2.4 Continuing the VMware ESX 5 installation from the ESX console

When the IBM i phase of the installation completes, the integrated server starts. The VMware ESX phase of the installation begins.

To complete installation of VMware ESXi 5, perform these tasks:

1. Follow the steps listed in the *Installing ESXi Interactively* chapter in the *vSphere Installation and Setup Guide*. This guide is available on the [VMware vSphere Documentation](#) Web page for VMware vSphere 5.
2. You can use the default values for most options during the installation. You must specify the following options on these screens:

Option	Description
ESX Storage Device	You must install ESX on <b>IBM VDASD nwsd1</b> , where <i>nwsd</i> is the ESX NWSD name.  On <b>i 6.1</b> , you must not modify the partition on <b>IBM VDASD nwsd2</b> . Otherwise, your server will fail to boot after installation. This is the install drive which is intended only for integrated server functionality.
Bootloader	You must install GRUB on the Master Boot Record. This is the default option.

#### 4.6.2.5 Continuing the VMware ESX 4 installation from the ESX console

When the IBM i phase of the installation completes, the integrated server starts. The VMware ESX phase of the installation begins.

To complete installation of VMware ESXi 4 or ESX 4, perform these tasks:

1. Follow the steps listed in the *Installing VMware ESX* chapter in the *ESX and vCenter Server Installation Guide* for VMware vSphere 4. This guide is available on the [VMware ESX 4.0 and VMware vCenter Server 4.0](#) Web page.
2. You can use the default values for most options during the installation. You must specify the following options on these screens:

Option	Description
ESX Storage Device	You must install ESX on <b>IBM VDASD nwsd1</b> , where <i>nwsd</i> is the ESX NWSD name.  On <b>i 6.1</b> , you must not modify the partition on <b>IBM VDASD nwsd2</b> . Otherwise, your server will fail to boot after installation. This is the install drive which is intended only for integrated server functionality.
Bootloader	You must install GRUB on the Master Boot Record. This is the default option.



## 4.6.2.6 Continuing the VMware ESX 3.5 installation from the ESX console

When the IBM i phase of the installation completes, the integrated server starts. The VMware ESX phase of the installation begins.

To complete installation of VMware ESX, perform these tasks:

1. Follow the steps listed in the **Installing VMware ESX Server Software** chapter in the **Installation and Upgrade Guide** for VMware Infrastructure 3 available on the [VMware Infrastructure 3 Documentation](#) Web page.
2. You can use the default values for most options during the installation. You must specify the following options on these screens:

Option	Description
Partitioning Options	You must install ESX on <b>/dev/sda</b> which is listed as <b>SCSI Disk sda IBM VDASD nwsd1</b> , where <b>nwsd</b> is the ESX NWSD name.  You must not modify the partition on <b>/dev/sdb</b> . Otherwise, your server will fail to boot after installation. This is the install drive which is intended only for integrated server functionality.
Advanced Options	You must install GRUB on the Master Boot Record. This is the default option.

### 4.6.3 Complete the integrated server installation

Some tasks are necessary to complete the server installation and verify that the server is correctly configured for the IBM i environment.

Perform the tasks for your integrated server operating system below:

Server OS	Tasks
WIN2012,WIN2008	<a href="#">Completing the Windows Server 2012/2008 installation</a>
WIN2003	<a href="#">Completing the Windows Server 2003 installation</a>
ESXi5, ESXi4, ESX4 (Management server based infrastructure)	<a href="#">Completing the ESX installation – Management server based infrastructure</a>
ESX4, ESX3.5 (Service console based infrastructure)	<a href="#">Completing the ESX installation – Service console based infrastructure</a>

**Related information:**

- [Installation Checklist](#)
- [Integrated Server Operating System \(Server OS\) Versions](#)

#### 4.6.3.1 Completing the Windows Server 2012/2008 installation

Do **one** of the tasks below to complete the Windows Server 2012/2008 installation.

Installation Type	Task
Full installation	<a href="#">Completing the Windows Server 2012/2008 full installation</a>
Core installation	<a href="#">Completing the Windows Server 2012/2008 core installation</a>

After performing the appropriate task above, do the following additional tasks:

1. Disable the **NetBIOS over TCP/IP** protocol on the following Ethernet adapters:
  - All QLogic Ethernet adapters.
  - The point-to-point virtual Ethernet adapter and any additional virtual Ethernet adapters configured on the Windows server.

If this protocol is enabled on the previously mentioned adapters, intermittent delays and hangs of iSCSI-attached Windows servers might occur. For more information, see [Software Knowledge Base article 460560441](#).

2. Install the latest supported Microsoft service pack that is listed in the [Microsoft service packs](#) section.
3. Run **Windows Update** to install the latest Windows security hot fixes. From the Windows server console, run **Windows Update** or visit (<http://windowsupdate.microsoft.com>) and install the latest security hot fixes.

### 4.6.3.1.1 *Completing the Windows Server 2012/2008 full installation*

If you are performing a full installation, complete these steps from the Windows console to mount the installation drive and to run the **ibmsetup.exe** program.

1. Sign in to the Windows operating system as the **Administrator** user.
2. Go to the **Server Manager**.
3. Ensure that the install drive is available to the integrated server operating system.
  - a. Select **Storage > Disk Management**.
  - b. Locate **Disk 1**. If the partition has no drive letter, right-click this partition and select **Online**. The Windows operating system assigns a letter to the partition.

**Note:** The install drive is typically assigned drive letter **D:**, but not in all situations.

Note the letter that is assigned. This drive is the install drive.

4. Run the **ibmsetup.exe** program to finish configuring the integrated server.

The **ibmsetup.exe** program is located in the root directory of the install drive.

For example, if the install drive is D:, run the command `D:\ibmsetup.exe` at the Windows command line.

5. If your integrated server hardware requires additional drivers, install them now. See the Windows or System x or BladeCenter documentation.

### 4.6.3.1.2 *Completing the Windows Server 2012/2008 core installation*

If you are performing a core installation, complete these steps from the Windows console to mount the installation drive and to run the **ibmsetup.exe** program.

1. Sign in to the Windows operating system as the **Administrator** user.
2. Ensure that the install drive is available to the integrated server operating system. Run these commands:

```
C:\> diskpart
```

```
DISKPART> select disk 1
```

```
DISKPART> online disk
```

The Windows operating system assigns a letter to the partition.

**Note:** The installation drive is typically assigned drive letter **D:**, but not in all situations.

Note the letter that is assigned. This drive is the installation drive.

```
DISKPART> attribute disk clear readonly
```

```
DISKPART> exit
```

3. Run the **ibmsetup.exe** program to finish configuring the integrated server.

The **ibmsetup.exe** program is located in the root directory of the install drive.

Run these commands:

```
C:\> d:
```

```
D:\> ibmsetup
```

### 4.6.3.2 Completing the Windows Server 2003 installation

Perform a few final tasks after installing Windows Server 2003 on the integrated server to verify that it is correctly installed and ready.

1. Install updates to Microsoft Windows and run Windows Update.
  - a. Install the latest supported Microsoft service pack that is listed in the [Microsoft service packs](#) section.
  - b. Run **Windows Update** to install the latest Windows security hot fixes. From the Windows server console, run **Windows Update** or visit (<http://windowsupdate.microsoft.com>) and install the latest security hot fixes.
  - c. In addition to any other Microsoft hot fixes that are available for your server, install the Microsoft hot fix for the storport.sys driver. Follow the instructions on the Microsoft Knowledge Base Article 903081 [An updated Storport storage driver is available for Windows Server 2003](#) to download and install this Microsoft hot fix.
2. **System x models 336 or 236 with an iSCSI HBA only:** When initially installing Microsoft Windows Server 2003 with Service Pack 1 on an **x336** or **x236** server, there is a known problem that restricts where an iSCSI HBA can be installed in the server:
  - For the **x336**, only **one** iSCSI HBA can be present when installing and it **must** be installed in **slot 1**. Also note that you need to remove the "full height" tail stock from the iSCSI HBA and install the "1/2 height" tailstock on the iSCSI HBA when installing it in slot 1 of an x336.
  - For the **x236**, only **one** iSCSI HBA can be present when installing and it **must** be installed in **slot 6**.

**After** Windows is installed on the x336 or x236, you can optionally install a Microsoft Windows hot fix that lifts the above restrictions to allow the iSCSI HBA to be moved to a different slot than shown above and to allow additional iSCSI HBAs to be installed. See Microsoft Knowledge Base entry [Pci.sys resource configuration conflicts cause an error in Windows Server 2003 SP1 or in an x64-based version of Windows Server 2003: "Stop 0x0000007B"](#) for information on how to obtain the hot fix from Microsoft.

3. Disable the **NetBIOS over TCP/IP** protocol on the following Ethernet adapters:
  - All QLogic Ethernet adapters.
  - The point-to-point virtual Ethernet adapter and any additional virtual Ethernet adapters configured on the Windows server.

If this protocol is enabled on the previously mentioned adapters, intermittent delays and hangs of iSCSI-attached Windows servers might occur. For more information, see [Software Knowledge Base article 460560441](#).

4. If you want the server to have a name that is different than the NWSD name (for example, a name that is longer than 8 characters), you can change the computer name from the Windows console. See the Windows documentation for more information.

5. You can 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.)
6. If you want to set up time synchronization for your integrated server, do the following steps:
  - a. Configure IBM i for time synchronization. See [Configuring time synchronization for integrated Windows server](#).
  - 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**.
7. Verify that the Microsoft Windows operating system is reporting all of the installed memory. If your system has 4GB or more of memory installed but not all of it is being reported by Windows, see [When 4 GB or more of memory is installed, why does Windows report less memory than is actually installed?](#)

### 4.6.3.3 Completing the ESX installation – Management server based infrastructure

Complete the required configuration tasks for an integrated ESX server that uses the [Management server based infrastructure](#).

These configuration tasks are **not** optional. These tasks ensure that the ESX server can shut down properly when the Network Server Description (NWS) is varied off.

#### Notes:

1. When ESX server is shut down by varying off the NWS, it does not attempt to shut down any virtual machines that the ESX server is hosting. You must manually shut down the virtual machines before shutting down the ESX server to ensure a clean shutdown.
2. Use the following [IBM i iSCSI Solution Work Sheets](#) to help you do this task:
  - **Integrated VMware ESX server management**

To complete the VMware ESX or ESXi server installation, follow these steps:

1. Configure the QVMWINT user profile. See [Configuring the QVMWINT user for integrated VMware ESX server management](#).
2. Log into the management server (integrated Windows server) with a user profile that has administrator rights. Open a **Command Prompt** window and run the following program to install the IBM i Integrated Server Support programs for managing VMware ESX servers:

#### **ibmvmins.exe**

The `ibmvmins.exe` program is located in one of the following directories, depending on your IBM i version:

- i 7.1 or higher:** %SystemRoot%\as400wsv\ESX
- i 6.1:** %SystemRoot%\as400wsv\admin

If `ibmvmins.exe` is **not** present in the indicated directory, then install it using one of the methods shown in [Updating the integration software running on Microsoft Windows](#).

**Note:** The integrated server support for VMware ESX requires the following software on the integrated Windows server:

Software	Description
Microsoft .NET Framework 2.0	You may need to install this software on your Windows server. You can obtain Microsoft .NET Framework 2.0 from the Windows server installation media or from the <a href="#">Microsoft Download Center</a> Web page.
Microsoft Visual C++ Runtime Library	The <code>ibmvmins.exe</code> utility automatically installs the required Microsoft Visual C++ Redistributable package.

3. Configure a connection to manage the VMware ESX server. See [Adding connection information](#).

4. **ESXi Embedded only:** Since no iSCSI initiators are required for booting embedded versions of ESX, none were configured in earlier steps of the installation checklist. Configure one or more iSCSI initiators at this time using the procedures in section [Configuring multipath I/O for integrated servers](#).

**Note:** If you only have one iSCSI initiator, you can configure just one initiator port and skip the steps for setting up multiple iSCSI initiators and multipath I/O.

#### 4.6.3.4 Completing the ESX installation – Service console based infrastructure

Complete the required configuration tasks for an integrated ESX server that uses the [Service console based infrastructure](#).

These configuration tasks are **not** optional. These tasks ensure that the ESX server can shut down properly when the Network Server Description (NWSD) is varied off.

**Note:** When ESX server is shut down by varying off the NWSD, it does not attempt to shut down any virtual machines that the ESX server is hosting. You must manually shutdown the virtual machines before shutting down the ESX server to ensure a clean shutdown.

To complete the VMware ESX server installation, follow these steps:

1. At the VMware ESX Server console, press **ALT-F1** and sign on as **root**.
2. Identify the install drive device name. List the SCSI devices and search on "Console Device" and "Model" by running the following command:

```
esxcfg-scsidevs -l | grep -i -e "Console Device" -e "Model"
```

In the output for the above command, the **Console Device** is listed above **Vendor** and **Model** information for each SCSI device. The install drive is the SCSI device with Model: VDASD *MYNWSD2* where *MYNWSD* is the name of the NWSD for the ESX server. In the example output below, the Console Device for the install drive is /dev/sda.

```
Console Device: /dev/sr0
Vendor: TSSTcorp Model: CDWDVD TS-L463A Revis: IB02
Console Device: /dev/sdb
Vendor: IBM      Model: VDASD MYNWSD1   Revis: 0001
Console Device: /dev/sda
Vendor: IBM      Model: VDASD MYNWSD2   Revis: 0001
```

3. Create mount point directory /mnt/ibmlsv using the following command:

```
mkdir /mnt/ibmlsv
```

4. Mount the install drive using the mount command. Use the device name that was determined in step 2 appended with a "1" and the mount point directory created in step 3. For the example above, we would mount the install drive as follows:

```
mount /dev/sda1 /mnt/ibmlsv
```



5. Enter **one** of the following commands, depending on your IBM i version:

**i 6.1:** `/mnt/ibmlsv/install/ibmsetup.sh address`

**i 5.4:** `/mnt/ibmlsv/install/esxsetup.sh address`

where *address* is the IP address or hostname of your IBM i system.

6. **i 5.4 only:** Restrict all IBM i devices. From the IBM i command prompt, run the following command:

```
CHGNWSD NWSD(esxnwsd) RSTDDEVRSC(*ALL)
```

Where **esxnwsd** is the name of the ESX NWSD.

5. **i 5.4 only:** Enable shutdown. From the IBM i command prompt, run the following command:

```
CRTDTAARA DTAARA(QUSRSYS/esxnwsdIT) TYPE(*DEC) LEN(4 0) VALUE(3)
```

Where **esxnwsd** is the name of the ESX NWSD.

## 4.7 After the integrated server installation

After the integrated server is installed, perform the following tasks, if appropriate.

**Related information:**

- [Installation Checklist](#)

### 4.7.1 Scale the iSCSI network

See [Configuring multipath I/O for integrated servers](#) to enable MPIO for your integrated server.

**Note:** The installation process described in this document addresses iSCSI-attached servers that use 1 target (IBM i) iSCSI adapter and 1 initiator (System x or blade) iSCSI adapter. Multipath I/O (MPIO) support provides data path redundancy and additional bandwidth when multiple iSCSI adapters are used on the initiator and target sides of the iSCSI network.

**Related information:**

- [Installation Checklist](#)
- [Multipath I/O \(MPIO\)](#)
- [Scaling your iSCSI network](#) chapter of the [Implementing Integrated Windows Server through iSCSI to System i5](#) Redbook

### 4.7.2 Create additional virtual storage for applications and data

To create additional virtual storage for applications and data, see [Adding virtual storage to integrated servers](#) in the Information Center.

**Related information:**

- [Installation Checklist](#)

### 4.7.3 Configure the integrated server to automatically start

You can configure integrated servers to start when IBM i TCP/IP starts.

There are a couple of prerequisites that must be met before performing this task:

1. The integrated server must have a **point-to-point virtual Ethernet** port and an associated TCP/IP interface.
  - These items are automatically configured when an integrated Windows server is installed.
  - On IBM i **6.1** or **5.4**, these items are automatically configured when an integrated ESX server is installed.
  - However, on IBM i **7.1 or higher**, these items are **not** automatically configured for an integrated ESX server. If you are performing this task for an ESX server that does not have a point-to-point virtual Ethernet port, see [Configuring a point-to-point virtual Ethernet port for an integrated ESX server](#).

2. In order for the integrated server to automatically start, the **iSCSI target** adapters that the integrated server uses must also be configured to automatically start.
  - To automatically start a hardware target (iSCSI HBA), configure the **Online at IPL** attribute in the network server host adapter (NWSH) object for the iSCSI target adapters:
    1. Select **Integrated Server Administration** from the [Web GUI](#) or [System i Navigator](#).
    2. Select **Network Server Host Adapters**.
    3. Select the **Properties** action for the network server host adapter.
    4. Select the **Online at IPL** check box.
    5. Click **OK** on the NWSH properties panel to save the change.
  - To automatically start a software target (Ethernet NIC), configure the **Start interface when TCP/IP is started** attribute in the IBM i TCP/IP interface that is used by the NWSH objects for the iSCSI target adapters. Starting the TCP/IP interface also causes the associated line description and NWSH to start. See the procedure shown in the following task steps.

**Attention:** If multiple integrated servers use the same System x or BladeCenter blade server hardware, configure only **one** of them to automatically start. Only one integrated server can use the server hardware at a time. Configuring multiple TCP/IP interfaces to automatically start for integrated servers that share the same server hardware can cause unpredictable results.

To have an integrated server automatically vary on when you start TCP/IP, follow these steps:

1. Select **Network** from the [Web GUI](#) or [System i Navigator](#).
2. **Web GUI only:** Click **Show All Network Tasks**.
3. Select **Network > TCP/IP Configuration > IPv4 > Interfaces**.
4. Select the **Properties** action for the interface for the point-to-point virtual Ethernet LAN line description for the server.

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

5. On the **Advanced** tab, select the **Start interface when TCP/IP is started** check box and click **OK** to save the change.

The integrated server automatically varies on when you start TCP/IP. TCP/IP can be automatically started by the system at IPL by changing the system IPL attributes. Any TCP interfaces that have been enabled to automatically start are started along with TCP/IP at IPL.

**Related information:**

➤ [Installation Checklist](#)

➤ [Configure TCP/IP \(CFGTCP\)](#) (use CFGTCP, then option 1)

### 4.7.3.1 Configuring a point-to-point virtual Ethernet port for an integrated ESX server

Configure a point-to-point virtual Ethernet port for an integrated VMware ESX server so that it can be automatically started when IBM i TCP/IP starts.

**Restriction:** The point-to-point virtual Ethernet port on an integrated VMware ESX server can only be used to automatically start the integrated VMware ESX server when IBM i TCP/IP starts. The point-to-point virtual Ethernet port does **not** provide a virtual Ethernet communication connection between the integrated VMware ESX server and any other systems.

Do these steps to configure a point-to-point virtual Ethernet port for an integrated VMware ESX server:

1. Select **Integrated Server Administration** from the [Web GUI](#) (7.2/7.1/6.1) or [System i Navigator](#) (5.4).
2. Select **Servers**.
3. Select the **Properties** action for the integrated VMware ESX server.
4. On the server properties panel, click the **Virtual Ethernet** tab.
5. Click **Add...** to add a new virtual Ethernet port.
6. On the virtual Ethernet properties panel, specify the values for the point-to-point virtual Ethernet port:
  - a. Type the **Internet address** for the integrated server side of the point-to-point virtual Ethernet.  
**Note:** This IP address is not used by the integrated VMware ESX server.
  - b. Type the **IBM i internet address** for the IBM i TCP/IP interface.  
**Note:** This IP address is not used by IBM i for communications. Its only purpose is to provide a mechanism to automatically start the integrated VMware ESX server when IBM i TCP/IP starts.
  - c. Type the **Subnet mask** for the point-to-point virtual Ethernet network.
  - d. Leave the default values for the remaining items.
  - e. Click **OK** to add the new port to the **Virtual Ethernet** tab on the server properties panel.
7. On the server properties panel, click **OK** to save the changes. The NWSD is updated and a line description and IBM i TCP/IP interface for the new point-to-point virtual Ethernet port are created.

**Related information:**

- [Change Network Server Desc \(CHGNWSD\)](#)  
(see the VRTETHPTH and TCPPORTCFG keywords)
- [Create Line Desc \(Ethernet\) \(CRTLINETH\)](#)
- [Add TCP/IP Interface \(ADDTCPIFC\)](#)

#### 4.7.4 Windows only: Define additional virtual Ethernet LANs

To define additional virtual Ethernet LANs for your server, see [Managing virtual Ethernet networks](#).

**Related information:**

- [Installation Checklist](#)

#### 4.7.5 Windows only: Enroll IBM i users to the Windows server or domain

To enroll some of your IBM i users to the Windows server or domain, see, [Administering integrated Windows server users from IBM i](#) in the Information Center.

**Related information:**

- [Installation Checklist](#)

#### 4.7.6 Keep the IBM i Integrated Server Support software up to date

The IBM i Integrated Server Support software that runs on the iSCSI-attached server needs to be updated periodically to provide the latest fixes. Fixes are provided by IBM i service pack PTFs that are installed on the server.

Periodically check the [Service pack PTFs](#) Web page for the latest IBM i Integrated Server Support service pack PTFs that are available.

See [Installing IBM i integration service packs](#) for information on how to install the service packs (or refresh the IBM i Integrated Server Support software) on your integrated System x or blade server.

**Related information:**

- [Installation Checklist](#)

## 5 Server cloning road map and checklist

Use the checklist in this chapter to step through the process of cloning an existing integrated Windows server that is attached to IBM i using an iSCSI network (iSCSI).

### Notes:

1. The checklist in this chapter applies to IBM i **7.2, 7.1** and **6.1**.
2. Use the checklist in this chapter when creating a new integrated Windows server based on a previously installed integrated Windows server.  
  
Use the [Installation Checklist](#) on page [141](#) when installing a new integrated server from scratch.
3. You might want to **print** the checklist so that you can check off the tasks as you complete them.
4. If you run into problems while installing an iSCSI-attached server using this checklist, see the [Troubleshooting](#) Web page.

<b>Cloning Checklist (for an iSCSI-attached integrated Windows server)</b>		<b>Page</b>
—	<b><a href="#">Prepare for server cloning</a></b>	<b><a href="#">223</a></b>
—	<a href="#">Review IBM i integrated server cloning concepts</a>	<a href="#">223</a>
—	<a href="#">Identify the base server to clone</a>	<a href="#">223</a>
—	<a href="#">Run sysprep to prepare the base server for cloning</a>	<a href="#">223</a>
—	<a href="#">Obtain necessary software licenses</a>	<a href="#">226</a>
—	<a href="#">Install and configure new server hardware, if necessary</a>	<a href="#">227</a>
—	<b><a href="#">Run the IBM i integrated server cloning Wizard</a></b>	<b><a href="#">227</a></b>
—	<b><a href="#">Configure the clone server</a></b>	<b><a href="#">230</a></b>
—	<a href="#">Verify or change the clone server NWSD properties</a>	<a href="#">230</a>
—	<a href="#">Start the clone server from IBM i</a>	<a href="#">232</a>
—	<a href="#">Complete the Windows Mini-Setup Wizard</a>	<a href="#">232</a>
—	<a href="#">Set the clone server point-to-point virtual Ethernet IP address</a>	<a href="#">233</a>
—	<a href="#">Change clone server properties on Windows</a>	<a href="#">234</a>
—	<a href="#">Shut down and start the clone server from IBM i and regenerate path certificates</a>	<a href="#">238</a>
—	<a href="#">Verify that IBM i can manage the clone server</a>	<a href="#">240</a>
—	<a href="#">After the integrated server has been cloned</a>	<a href="#">240</a>

Also, if new hardware will be used for the clone server, see the [Clone Server Hardware Checklist](#).

## 5.1 Prepare for server cloning

Perform a few preliminary tasks as described in the following sections before cloning an integrated server.

### 5.1.1 Review IBM i integrated server cloning concepts

Review the **Integrated server cloning** section before cloning integrated Windows servers that are hosted by IBM i.

**Related information:**

➤ [Cloning Checklist](#)

### 5.1.2 Identify the base server to clone

Identify the [Base NWSD \(Base Server\)](#) that will be cloned and make sure that it meets the [Base NWSD Requirements](#) described in section [Review IBM i integrated server cloning concepts](#).

**Record** the name of the base NWSD, since it is needed when running the cloning Wizard in a later step of the cloning process.

**Related information:**

➤ [Cloning Checklist](#)

### 5.1.3 Run sysprep to prepare the base server for cloning

You must run a tool called **sysprep** to reset key attributes of the base server, such as the system security ID (SID), so that it can be cloned. See [Microsoft System Preparation Tool \(Sysprep\)](#) for more information.

If you have previously run sysprep on the base server, then skip this task. Otherwise, continue.

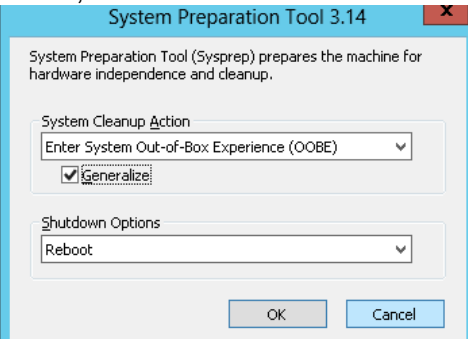
**Important:**

- Failure to use sysprep prior to cloning a Windows server might result in a server that does not start, does not function properly, or does not meet Microsoft licensing requirements.
- Sysprep has restrictions on server roles, server components that are installed (for example, Active Directory), encrypted files and other items. For details, see the [Microsoft Sysprep Technical Reference](#) TechNet articles. Ensure that the base server meets these restrictions before using sysprep. Running sysprep on a server that does not meet these requirements might result in a server that does not start or does not function properly.
- **Back up** the virtual storage for the base server before running sysprep. Then if the need arises, you can restore the base server back to the original (pre-sysprep) state. See [Backing up virtual storage for integrated servers](#) in the Information Center.

- There are limits to how many times sysprep can be run on a server, so only run sysprep after all software installation and configuration tasks are completed on the base server and it is ready for deployment to clone servers. Normally, sysprep only needs to be run once on the base server, regardless of how many times the base server is cloned. You should not run sysprep each time you clone the base server.

To run sysprep on the server, do the following:

1. Start the base server:
  - a) Select **Integrated Server Administration** from the [Web GUI](#).
  - b) Select **Servers**.
  - c) Select the **Start** action for the server.
2. From the Windows console, perform the appropriate tasks below for your operating system:

Server OS	Tasks
WIN2012 or WIN2008	<ol style="list-style-type: none"> <li>1. Open a command prompt and change to the sysprep directory on the C drive:               <pre>&gt; cd c:\windows\system32\sysprep</pre> <p>Run sysprep with the following options to prepare the server for cloning:</p> <pre>&gt; sysprep /generalize /oobe</pre> <p><b>Note:</b> You can also double click the <b>sysprep.exe</b> and set the option in the GUI like below, then click <b>OK</b>.</p>  </li> </ol>
WIN2003	<ol style="list-style-type: none"> <li>1. To install the sysprep tool on the base server, open a command prompt and:           <ol style="list-style-type: none"> <li>a. Make a directory on the C: drive to hold the sysprep tool:               <pre>&gt; md c:\sysprep</pre> </li> <li>b. Open <b>\Support\Tools\Deploy.cab</b> on the Windows Server 2003 installation CD and extract <b>sysprep.exe</b> and <b>setupcl.exe</b> to <b>c:\sysprep</b>.</li> </ol> </li> <li>2. Change to the sysprep directory on the C drive:           <pre>&gt; cd c:\sysprep</pre> </li> <li>3. Run sysprep with the following options to prepare the server for cloning:           <pre>&gt; sysprep -reseal -mini</pre> </li> </ol>



3. Shut down the base server:
  - a) Select **Integrated Server Administration** from the [Web GUI](#).
  - b) Select **Servers**.
  - c) Select the **Shut Down** action for the server.
  - d) Click **Shut Down** on the confirmation page.

**Related information:**

- [Cloning Checklist](#)

## 5.1.4 Obtain necessary software licenses

Determine if you have the necessary software licenses for the clone server. If not, obtain any software licenses before continuing with the cloning process. See [Software Licenses](#) in section [Review IBM i integrated server cloning concepts](#) for more information.

**Related information:**

- [Cloning Checklist](#)

## 5.1.5 Install and configure new server hardware, if necessary

**Note:** If the BladeCenter blade or System x server hardware that the clone server will use was previously installed and configured and an IBM i remote system configuration object has already been configured for that server hardware, then you can skip this step. Otherwise, continue with the tasks listed below for the new server hardware.

When using new server hardware for a clone server, some tasks must be performed in order to set up the server hardware for use with IBM i integrated servers.

Perform the tasks listed below and follow the additional instructions that are provided.

<b>Clone Server Hardware Checklist</b>		<u>Page</u>
—	<a href="#">Obtain required hardware</a>	<u>146</u>
	<b>Note:</b> Make sure that the server meets the <a href="#">Compatible Server Hardware</a> requirements.	
—	<a href="#">Obtain firmware updates and drivers for your integrated server hardware</a>	<u>148</u>
—	<a href="#">Plan the iSCSI network and integrated server installation</a>	<u>150</u>
	<b>Note:</b> Fill out just the following work sheets from the <a href="#">IBM i iSCSI Solution Work Sheets</a> :	
	<ul style="list-style-type: none"><li>• BladeCenter or System x service processor *</li><li>• IBM i service processor configuration *</li><li>• IBM i remote system configuration</li></ul>	
	* You can skip the two service processor work sheets for a blade in a BladeCenter that already has a previously created IBM i service processor configuration.	
—	<a href="#">Install the BladeCenter or System x hardware and iSCSI initiators</a>	<u>184</u>
—	<a href="#">Update and configure the BladeCenter or System x hardware</a>	<u>185</u>
—	<a href="#">Configure the iSCSI initiator</a>	<u>187</u>
—	<a href="#">Configure the integrated server start options</a>	<u>187</u>
—	<a href="#">Cable the network</a>	<u>187</u>
—	<a href="#">Create and initialize a service processor configuration</a>	<u>193</u>
	<b>Note:</b> You can skip this task for a blade in a BladeCenter that already has an IBM i service processor configuration created and initialized.	
—	<a href="#">Create a remote system configuration</a>	<u>195</u>
—	<a href="#">Verify that the remote system is accessible from IBM i</a>	<u>228</u>

### Related information:

- [Cloning Checklist](#)

### 5.1.5.1 Verify that the remote system is accessible from IBM i

Display the status of the remote system from IBM i to verify that the new remote system configuration and the corresponding service processor configuration are set up properly. This ensures that IBM i can power the server on and off.

1. Select **Integrated Server Administration** from the [Web GUI](#).
2. Select **Remote Systems**.
3. Select the **Status** action for the new remote system configuration.
4. The status of the remote system hardware is shown.

**Note:** The new server hardware does not need to be powered off at this point in the cloning process. However, later in the cloning process the new server hardware must be powered off before starting the clone server.

**Note:** If you get a “not found” error or get some other error, see the [Troubleshooting](#) Web page.

5. Click **Cancel** to close the status panel.

**Related information:**

➤ [Cloning Checklist](#)

➤ [Work with NWS Configuration \(WRKNWSCFG\)](#)

## 5.2 Run the IBM i integrated server cloning Wizard

The cloning Wizard duplicates the base server's IBM i configuration and storage to create a clone server.

To clone an existing integrated Windows server, use the **base NWSD** option on the IBM i **Create Server Web GUI** task. Make sure that the [Base NWSD \(Base Server\)](#) that will be cloned meets the [Base NWSD Requirements](#) described in section [Review IBM i integrated server cloning concepts](#).

### Notes:

- To clone a server, you need IBM i \*IOSYSCFG, \*ALLOBJ, and \*JOBCTL special authority.
- Cloning large amounts of virtual storage might cause some performance degradation for other applications on the IBM i system. If this is a concern, consider running the cloning Wizard during off-peak hours.

Perform the following steps to run the cloning Wizard:

1. Select **Integrated Server Administration** from the [Web GUI](#).
2. Select the **Create Server** task. The **Select Base Object** page is shown.
3. Select the **Base on an existing object** option and specify the base object (NWSD) name that was determined in section [Identify the base server to clone](#).  
**Note:** You can use **Browse** to select the base NWSD.
4. Click **Continue** on the **Select Base Object** page.  
The **Create Server based on Basenwsd** Wizard (the cloning Wizard) is started.
5. Enter or select values on the pages of the cloning Wizard:

Wizard Page	Values
<b>Name</b>	Specify the NWSD name and description for the clone server.
<b>Storage</b>	Select the base server virtual storage to copy to the clone server. <b>Notes:</b> <ol style="list-style-type: none"><li>1. Normally, all of the base server virtual storage should be copied to the clone server.</li><li>2. Verify that there is sufficient storage available on IBM i to clone the server.</li></ol>
<b>Server Hardware</b>	Select the remote system configuration that identifies the server hardware that the clone server will use.

6. On the **Summary** page of the wizard, click **Finish** to start the IBM i portion of the cloning process.
7. When the IBM i portion of the cloning process is completed, the **Create Server Web GUI** task prompts you to see documentation for additional tasks. Then continue with section [Configure the clone server](#).

### Related information:

- [Cloning Checklist](#)

## 5.3 Configure the clone server

Running the cloning Wizard duplicates the base server's IBM i configuration objects and virtual storage to create a clone server. However, additional configuration tasks for the clone server are required. See the following sections for details.

### Related information:

➤ [Cloning Checklist](#)

### 5.3.1 Verify or change the clone server NWSD properties

The clone server NWSD is created with the same properties as the base server NWSD with one exception:

- The **point-to-point virtual Ethernet (PTP VE)** connection for the clone server is required to use a different subnet than the base server. Therefore, the cloning process generates a new pair of IP addresses for the Windows and IBM i sides of the clone server PTP VE connection. Also, an IBM i TCP/IP interface is created for the IBM i side of the PTP VE connection.

You might want to verify that the generated PTP VE connection IP addresses are appropriate for your environment and change them if they are not appropriate. You might also want to change other NWSD properties at this time as well.

Verify or change NWSD properties for the clone server as follows:

1. Select **Integrated Server Administration** from the [Web GUI](#).
2. Select the **Servers** task to display the **Servers** list.
3. Locate the clone server in the list.

**Note:** At this point in the cloning process, the **Servers** list shows the same **Server** name (Windows computer name) for both the base server and the clone server. Therefore, you must view the **NWSD Name** column in the **Servers** list in order to determine which server in the list is the clone server and which server is the base server. Make sure to locate the server that shows the clone server NWSD name.

If the **NWSD Name** column in the **Servers** list is not currently shown:

- a. Launch the **Columns...** action from the **--- Select Action ---** control at the top of the list.
  - b. Add the **NWSD Name** column to the **Current columns** list and click **OK**.
4. Launch the **Properties** action for the clone server.
  5. Verify or change the clone server NWSD properties as shown below:  
(Continued on next page)

Property	Tasks
PTP VE connection IP addresses	<ol style="list-style-type: none"> <li>1. Click on the <b>Virtual Ethernet</b> tab.</li> <li>2. Select the <b>Point to point</b> port and click <b>Properties</b> (below the table).</li> <li>3. On the <b>Point to Point Properties</b> dialog, review the generated IP addresses for the Windows and IBM i sides of the PTP VE connection.  If the generated IP addresses are acceptable, click <b>Cancel</b> to return to the <b>Virtual Ethernet</b> tab.  Otherwise, do the following to change the PTP VE IP addresses: <ol style="list-style-type: none"> <li>a. Specify new IP addresses for both the Windows and IBM i sides of the PTP VE connection.  <b>Note:</b> Ensure that both IP addresses are on the same subnet and that the subnet is unique in your IBM i environment.</li> <li>b. Click <b>OK</b> to return to the <b>Virtual Ethernet</b> tab.</li> </ol> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• At this point, the new IP addresses are not saved in the NWSD yet. They will be saved later when you click <b>OK</b> to exit the server properties page.</li> <li>• When the NWSD properties are saved, the TCP/IP interface for the IBM i side of the connection is automatically updated with the new IP address.</li> </ul> </li> <li>4. <b>Record the Windows side IP address and subnet mask for the PTP VE connection.</b>  <b>Note:</b> When you get to section <a href="#">Set the clone server point-to-point virtual Ethernet IP address</a> later on, you need to configure this IP address and subnet mask on the Windows server.</li> </ol>
iSCSI target adapters for storage	<p>To use different iSCSI target adapters to access storage, click the <b>Storage Paths</b> tab and change the network server host adapter (NWSH) that is used for the storage paths.</p> <p>Also verify that the NWSH has available file server storage resources for the clone server to use (see <a href="#">Checking NWSH resource usage</a>).</p>
iSCSI target adapters for virtual Ethernet ports	<p>To use different iSCSI target adapters for virtual Ethernet ports, click the <b>Virtual Ethernet</b> tab and change the NWSH that is used for the virtual Ethernet ports.</p> <p>Also verify that the NWSH has available virtual Ethernet line resources for the clone server to use (see <a href="#">Checking NWSH resource usage</a>).</p>
Other NWSD properties	<p>Some other properties that you might also want to update at this time include:</p> <ul style="list-style-type: none"> <li>• Message queues: Use the <b>Messages</b> tab.</li> <li>• Restricted devices: Click <b>Advanced...</b> from the <b>System</b> tab.</li> </ul>

6. Click **OK** to save any changes that were made and exit the server properties page.

**Related information:**  
➤ [Cloning Checklist](#)

### 5.3.1.1 Checking NWSH resource usage

Check the network server host adapter (NWSH) resource usage as follows:

1. Select **Integrated Server Administration** from the [Web GUI](#).
2. Select the **Network Server Host Adapters** task to display the **Network Server Host Adapters** list.
3. Locate the NWSH of interest in the list and launch the **Properties** action for the NWSH.
4. Click the **Resource Usage** tab. Verify that resources are available for the clone server to use.
5. Click **Cancel** to close the NWSH property sheet.

**Related information:**

- [Cloning Checklist](#)

### 5.3.2 Start the clone server from IBM i

Start the clone server from IBM i as follows:

1. Select **Integrated Server Administration** from the [Web GUI](#).
2. Select the **Servers** task to display the **Servers** list.
3. Locate the clone server in the list.  
Make sure to locate the server that shows the clone server NWSD name.
4. Launch the **Start** action for the clone server.
5. Click **Close** on the **Task Progress** panel.

**Note:** The **Servers** list shows **Starting...** for the clone server status at this point in the cloning process, since the clone server point-to-point virtual Ethernet has not been configured yet on Windows.

**Related information:**

- [Cloning Checklist](#)

### 5.3.3 Complete the Windows Mini-Setup Wizard

Since the sysprep tool was run on the base server to prepare it for cloning, Windows runs a Mini-Setup Wizard the first time that the clone server starts.

**Notes:**

- Some system attributes, such as the system security ID (SID), are automatically regenerated the first time that the clone server starts.
- The server may restart itself one or more times before displaying the Windows Mini-Setup Wizard.

Once the Windows Mini-Setup Wizard is shown on the Windows console, do the following:

1. Answer any questions the wizard asks you to set up Windows.  
For example, the wizard might prompt you for a Windows product key and ask you to accept license



terms.

2. If the wizard tells you to restart Windows, do so.

**Related information:**

➤ [Cloning Checklist](#)

### 5.3.4 Set the clone server point-to-point virtual Ethernet IP address

The clone server point-to-point virtual Ethernet IP address on Windows must match the Windows side PTP VE IP address value in the clone server NWSD. Otherwise, the IBM i system cannot manage the clone server.

From the Windows server console, do the task below for your operating system:

<b>Server OS</b>	<b>Tasks</b>
WIN2012	<ol style="list-style-type: none"><li>1. Click <b>Control Panel &gt; Network and Internet &gt; Network and Sharing Center</b>.</li><li>2. Locate the <b>IBM Virtual Ethernet Point-to-Point</b> connection and launch the <b>Properties</b> dialog for that connection.</li><li>3. On the <b>IBM Virtual Ethernet Point-to-Point Properties</b> dialog, select <b>Internet Protocol Version 4 (TCP/IPv4)</b> and click <b>Properties</b>.</li><li>4. For the <b>IP address</b> and <b>Subnet mask</b> values on the <b>Internet Protocol Version 4 (TCP/IPv4) Properties</b> dialog, type the <b>Windows side IP address and subnet mask for the PTP VE connection</b> that you recorded when you completed the task in section <a href="#">Verify or change the clone server NWSD properties</a>.</li><li>5. Click <b>OK</b> on the <b>Internet Protocol Version 4 (TCP/IPv4) Properties</b> dialog to save the change.</li></ol> <p>Click <b>Close</b> on the <b>IBM Virtual Ethernet Point-to-Point Properties</b> dialog.</p>
WIN2008	<ol style="list-style-type: none"><li>1. Launch <b>Server Manager</b> and click the <b>View Network Connections</b> link.</li><li>2. Locate the <b>IBM Virtual Ethernet Point-to-Point</b> connection and launch the <b>Properties</b> dialog for that connection.</li><li>3. On the <b>IBM Virtual Ethernet Point-to-Point Properties</b> dialog, select <b>Internet Protocol Version 4 (TCP/IPv4)</b> and click <b>Properties</b>.</li><li>4. For the <b>IP address</b> and <b>Subnet mask</b> values on the <b>Internet Protocol Version 4 (TCP/IPv4) Properties</b> dialog, type the <b>Windows side IP address and subnet mask for the PTP VE connection</b> that you recorded when you completed the task in section <a href="#">Verify or change the clone server NWSD properties</a>.</li><li>5. Click <b>OK</b> on the <b>Internet Protocol Version 4 (TCP/IPv4) Properties</b> dialog to save the change.</li><li>6. Click <b>Close</b> on the <b>IBM Virtual Ethernet Point-to-Point Properties</b> dialog.</li></ol>

Server OS	Tasks
WIN2003	<ol style="list-style-type: none"> <li>1. Click <b>Start &gt; Control Panel &gt; Network Connections</b>.</li> <li>2. Locate the <b>IBM Virtual Ethernet Point-to-Point</b> connection and launch the <b>Properties</b> dialog for that connection.</li> <li>3. On the <b>IBM Virtual Ethernet Point-to-Point Properties</b> dialog, select <b>Internet Protocol (TCP/IP)</b> and click <b>Properties</b>.</li> <li>4. For the <b>IP address</b> and <b>Subnet mask</b> values on the <b>Internet Protocol (TCP/IP) Properties</b> dialog, type the <b>Windows side IP address and subnet mask for the PTP VE connection</b> that you recorded when you completed the task in section <a href="#">Verify or change the clone server NWSD properties</a>.</li> <li>5. Click <b>OK</b> on the <b>Internet Protocol (TCP/IP) Properties</b> dialog to save the change.</li> <li>6. Click <b>Close</b> on the <b>IBM Virtual Ethernet Point-to-Point Properties</b> dialog.</li> </ol>

**Note:** The above changes might require a server restart before the changes take effect. Normally, you can wait until you get to section [Shut down and start the clone server from IBM i and regenerate path certificates](#) before restarting the server.

**Related information:**

- [Cloning Checklist](#)

### 5.3.5 Change clone server properties on Windows

The virtual storage for the clone server is an exact copy of the virtual storage from the base server, so when the clone server is first started it has the same properties as the base server, including things like IP addresses, computer name, license keys, etc. However, some of these properties can or must be changed in order for the clone server to function properly in the network and meet applicable software licensing requirements.

Here are the key properties of the clone server to change:

#### 1. Windows Server license:

**Note:** If you provided a Windows product key during the Windows Mini-Setup Wizard, then you can skip the remainder of this item.

Ensure that licensing requirements for Windows Server are met. For example, specify a different Windows product key, unless a volume license is used.

**Note:** The Windows **sysprep** support described in section [Run sysprep to prepare the base server for cloning](#) resets the base server to a pre-activated state. Therefore, on the clone server, simply activate Windows to supply an appropriate Windows product key.

#### 2. Other software licenses:

Ensure licensing requirements for other software installed on the clone server are met. For example, install different license keys for installed software products. Refer to your software product documentation for instructions on how to install new license keys.

### 3. Clone server network identity:

Change the Windows server properties that identify the clone server on the network. See:

- **Change the clone server computer name (host name)**
- **Change any clone server static IP addresses**

### 4. Other server properties:

If there are other properties of the clone server that need to be changed for your environment, go ahead and change them at this time.

**Note:** Some of the above changes might require a server restart before the changes take effect. Normally, you can wait until you get to section [Shut down and start the clone server from IBM i and regenerate path certificates](#) before restarting the server.

#### **Related information:**

- [Cloning Checklist](#)

### 5.3.5.1 Change the clone server computer name (host name)

The clone server must have a unique computer name on the network. Even if a unique computer name has already been generated by Windows, you might want to change it to a name that meets your organization's naming conventions.

**Note:** You can skip this task if you specified a new computer name using the Windows Mini-Setup Wizard when the clone server was started the first time.

From the Windows server console, do the following:

1. Launch the **System Properties** dialog for your version of Windows:

<b>Server OS</b>	<b>Tasks</b>
WIN2012	Click <b>Start &gt; Control Panel &gt; System and Security &gt; System &gt; Change setting</b>
WIN2008	Launch <b>Server Manager</b> and click <b>Change System Properties</b> .
WIN2003	Click <b>Start &gt; Control Panel &gt; System</b> .

2. Click **Change...** on the **Computer Name** tab.
3. Specify a different computer name and click **OK**.
4. Click **Close** on the **System Properties** dialog.

**Note:** The above change might require a server restart. Normally, you can wait until you get to section [Shut down and start the clone server from IBM i and regenerate path certificates](#) before restarting the server.

**Related information:**

- [Cloning Checklist](#)

### 5.3.5.2 Change any clone server static IP addresses

The clone server must have a unique IP address on the network.

**Note:** If the clone server does **not** use a **static IP address** (for example, the clone server obtains an IP address automatically using DHCP), then you can skip the remainder of this task.

From the Windows server console, do the task below for your operating system:

Server OS	Tasks
WIN2012	<ol style="list-style-type: none"> <li>1. Click <b>Control Panel &gt; Network and Internet &gt; Network and Sharing Center</b>.</li> <li>2. Locate a system LAN connection that uses a static IP address and launch the <b>Properties</b> dialog for that connection.  <b>Note:</b> Do <u>not</u> modify the <b>IBM Virtual Ethernet Point-to-Point</b> connection.  <b>Note:</b> Do <u>not</u> modify any connections that are used as iSCSI initiators (those connections are automatically configured by IBM i).</li> <li>3. On the connection <b>Properties</b> dialog, select one of the following, whichever is appropriate for your network:  <b>Internet Protocol Version 6 (TCP/IPv6)</b>  <b>Internet Protocol Version 4 (TCP/IPv4)</b>  then click <b>Properties</b>.</li> <li>4. On the <b>TCP/IP Properties</b> dialog, type the new static IP address and click <b>OK</b> to save the change.</li> <li>5. Click <b>Close</b> on the connection <b>Properties</b> dialog.</li> </ol>
WIN2008	<ol style="list-style-type: none"> <li>1. Launch <b>Server Manager</b> and click the <b>View Network Connections</b> link.</li> <li>2. Locate a system LAN connection that uses a static IP address and launch the <b>Properties</b> dialog for that connection.  <b>Note:</b> Do <u>not</u> modify the <b>IBM Virtual Ethernet Point-to-Point</b> connection.  <b>Note:</b> Do <u>not</u> modify any connections that are used as iSCSI initiators (those connections are automatically configured by IBM i).</li> <li>3. On the connection <b>Properties</b> dialog, select one of the following, whichever is appropriate for your network:  <b>Internet Protocol Version 6 (TCP/IPv6)</b>  <b>Internet Protocol Version 4 (TCP/IPv4)</b>  then click <b>Properties</b>.</li> <li>4. On the <b>TCP/IP Properties</b> dialog, type the new static IP address and click <b>OK</b> to save the change.</li> <li>5. Click <b>Close</b> on the connection <b>Properties</b> dialog.</li> </ol>

Server OS	Tasks
WIN2003	<ol style="list-style-type: none"> <li>1. Click <b>Start &gt; Control Panel &gt; Network Connections</b>.</li> <li>2. Locate a system LAN connection that uses a static IP address and launch the <b>Properties</b> dialog for that connection.  <b>Note:</b> Do <u>not</u> modify the <b>IBM Virtual Ethernet Point-to-Point</b> connection.  <b>Note:</b> Do <u>not</u> modify any connections that are used as iSCSI initiators (those connections are automatically configured by IBM i).</li> <li>3. On the connection <b>Properties</b> dialog, select <b>Internet Protocol (TCP/IP)</b> and click <b>Properties</b>.</li> <li>4. On the <b>TCP/IP Properties</b> dialog, type the new static IP address and click <b>OK</b> to save the change.</li> <li>5. Click <b>Close</b> on the connection <b>Properties</b> dialog.</li> </ol>

**Note:** If the clone server has multiple system LAN connections with static IP addresses, then repeat the above steps for each of them.

**Note:** The above changes might require a server restart. Normally, you can wait until you get to section [Shut down and start the clone server from IBM i and regenerate path certificates](#) before restarting the server.

**Related information:**

➤ [Cloning Checklist](#)

### 5.3.6 Shut down and start the clone server from IBM i and regenerate path certificates

Once the changes described in the prior sections are completed, the clone server must be shut down from IBM i and then started from IBM i using the regenerate path certificates option so that all of the changes take effect.

Shut down and start the clone server from IBM i using the regenerate path certificates option as follows:

1. Select **Integrated Server Administration** from the [Web GUI](#).
2. Select the **Servers** task to display the **Servers** list.
3. Locate the clone server in the list.  
Make sure to locate the server that shows the clone server **NWSD name**.

**Note:** At this point in the cloning process, the **Server** name that is shown for the clone server might still be the base server name or a name that Windows generated for the server.

4. Shut down the clone server:
  - a. Launch the **Shut Down...** action for the clone server.
  - b. Click **Shut Down** on the **Confirm Shut Down** panel.
  - c. On the **Task Progress** panel, wait for the task to complete, then click **Close**.

5. Start the clone server using the **regenerate path certificates** option:
  - a. Launch the **Start with options...** action for the clone server.
  - b. Select the **Regenerate path certificates** option, then click **Start** to start the server.
  - c. Click **Close** on the **Task Progress** panel.

**Related information:**

➤ [Cloning Checklist](#)

### 5.3.7 Verify that IBM i can manage the clone server

Once the clone server has been restarted so that all of the changes described in the prior sections take effect, verify that IBM i can manage the server as follows:

1. Select **Integrated Server Administration** from the [Web GUI](#).
2. Select the **Servers** task to display the **Servers** list.
3. Locate the clone server in the list and verify that:
  - a. The name shown in the **Server** column matches the Windows computer name (host name) that was specified in section [Complete the Windows Mini-Setup Wizard](#) or section [Change the clone server computer name \(host name\)](#).
  - b. The value shown in the **Status** column is **Started**.

#### Notes:

- After restarting the clone server, it may take a few minutes for the status to show **Started** and the new computer name to appear.
- Click **Refresh** above the **Servers** list to update the entries in the list.
- If the clone server status continues to show **Starting** for an extended period of time, then the point-to-point virtual Ethernet LAN is not working properly. If this is the case, re-verify that the IBM Virtual Ethernet Point-to-Point TCP/IP configuration on Windows matches the configuration in the clone server NWSD. See sections [Verify or change the clone server NWSD properties](#) and [Set the clone server point-to-point virtual Ethernet IP address](#).

#### Related information:

- [Cloning Checklist](#)

### 5.3.8 After the integrated server has been cloned

Once the clone server is up and running normally, you might want to do additional customization beyond the basic cloning process.

See section [After the integrated server installation](#) for some customization ideas.

#### Related information:

- [Cloning Checklist](#)



## 6 BladeCenter and System x configuration

This chapter contains configuration tasks for BladeCenter blade and System x servers.

### Chapter Table of Contents

6.1	Downloading and updating firmware and drivers .....	243
6.1.1	Using Bootable Media Creator (BoMC) .....	243
6.1.1.1	Downloading server updates with Bootable Media Creator (BoMC) .....	243
6.1.1.1.1	Updating Bootable Media Creator to latest version .....	244
6.1.1.2	Updating the server using Bootable Media Creator (BoMC) media .....	245
6.1.2	Firmware updates for the BladeCenter chassis .....	246
6.1.2.1	Downloading firmware updates for the BladeCenter chassis .....	246
6.1.2.2	Updating the BladeCenter management module firmware .....	247
6.1.2.3	Updating and configuring the BladeCenter I/O module .....	248
6.1.3	Windows drivers for iSCSI initiators .....	249
6.1.3.1	Downloading Windows Ethernet NIC software initiator driver .....	249
6.1.3.2	Downloading System x Windows Server 2012/2008 iSCSI HBA driver .....	250
6.2	Configuring the BladeCenter or System x service processor .....	250
6.2.1	Configuring the BladeCenter management module .....	250
6.2.2	Configuring the System x service processor .....	252
6.2.2.1	Configuring the System x IMM II .....	252
6.2.2.1.1	Configuring the IMM II IP address and DHCP settings .....	254
6.2.2.2	Configuring the System x IMM .....	255
6.2.2.2.1	Configuring the IMM IP address and DHCP settings .....	257
6.2.2.3	Configuring the System x RSA II .....	258
6.2.2.3.1	Configuring the RSA II IP address and DHCP settings .....	260
6.2.2.4	Configuring the System x BMC .....	261
6.2.3	Connecting to the service processor Web interface .....	263
6.2.3.1	Determining an IP address for the service processor Web interface .....	264
6.3	iSCSI Initiator Hardware Configuration .....	265
6.3.1	iSCSI initiator configuration methods .....	265
6.3.2	"iSCSI Mode" for booting UEFI-based servers .....	266
6.3.3	Starting the iSCSI initiator configuration utility .....	266
6.3.3.1	Starting the QLogic Fast!UTIL utility .....	267
6.3.3.2	Starting the UEFI Setup utility .....	268
6.3.3.3	Starting the iSCSI Configuration Manger utility (SWI-BladeBoot) .....	268
6.3.3.3.1	Installing the iSCSI Configuration Manager application (SWI-BladeBoot) .....	269
6.3.4	Configuring a boot iSCSI initiator port .....	270
6.3.4.1	Configuring a boot iSCSI initiator port (HWI-QLogic) .....	270
6.3.4.1.1	Configuring a boot iSCSI initiator for dynamic addressing (HWI-QLogic) .....	271
6.3.4.1.2	Configuring a boot iSCSI initiator for manual addressing (HWI-QLogic) .....	272
6.3.4.2	Configuring a boot iSCSI initiator port (SWI-UEFI) .....	275
6.3.4.2.1	Configuring a boot iSCSI initiator for dynamic addressing (SWI-UEFI) .....	275
6.3.4.2.2	Configuring a boot iSCSI initiator for manual addressing (SWI-UEFI) .....	278
6.3.4.3	Configuring a boot iSCSI initiator port (SWI-BladeBoot) .....	280
6.3.4.3.1	Configuring a boot iSCSI initiator for dynamic addressing (SWI-BladeBoot) .....	280
6.3.4.3.2	Configuring a boot iSCSI initiator for manual addressing (SWI-BladeBoot) .....	282
6.3.5	Configuring advanced iSCSI initiator port settings .....	285
6.3.5.1	Configuring advanced iSCSI initiator port settings (HWI-QLogic) .....	285
6.3.6	Configuring non-boot iSCSI initiator ports .....	286
6.3.6.1	Configuring non-boot iSCSI initiator ports (HWI-QLogic) .....	286
6.3.6.2	Configuring non-boot iSCSI initiator ports (SWI-UEFI) .....	287
6.3.7	Configuring boot iSCSI initiator with manual addressing for MPIO target .....	288

6.3.7.1	Configuring boot iSCSI initiator with manual addr. for MPIO target (HWI-QLogic) ..	289
6.3.7.2	Configuring boot iSCSI initiator with manual addr. for MPIO target (SWI-UEFI) .....	290
6.3.8	Configuring additional boot iSCSI initiators for Windows MPIO .....	291
6.3.8.1	Configuring additional boot iSCSI initiators for Windows MPIO (HWI-QLogic).....	291
6.3.8.1.1	Configuring additional boot iSCSI initiators with dynamic addr. (HWI-QLogic) ....	292
6.3.8.1.2	Configuring additional boot iSCSI initiators with manual addr. (HWI-QLogic).....	293
6.3.8.2	Configuring additional boot iSCSI initiators for Windows MPIO (SWI-UEFI) .....	296
6.3.8.2.1	Configuring additional boot iSCSI initiators with dynamic addr. (SWI-UEFI).....	296
6.3.8.2.2	Configuring additional boot iSCSI initiators with manual addr. (SWI-UEFI) .....	298
6.3.9	Restoring factory defaults for an iSCSI initiator.....	301
6.3.9.1	Restoring factory defaults for an iSCSI initiator (HWI-QLogic) .....	301
6.3.10	Resetting cached iSCSI initiator configuration information .....	302
6.3.10.1	Resetting cached iSCSI initiator configuration information (HWI-QLogic) .....	302
6.3.11	Verifying the iSCSI connection using ping.....	303
6.3.11.1	Verifying the iSCSI connection using ping (HWI-QLogic) .....	303
6.3.12	Configuring target CHAP .....	304
6.3.12.1	Configuring target CHAP (HWI-QLogic).....	304
6.3.12.2	Configuring target CHAP (SWI-UEFI) .....	305
6.3.13	Configuring initiator CHAP .....	306
6.3.13.1	Configuring initiator CHAP (HWI-QLogic) .....	306
6.3.13.2	Configuring initiator CHAP (SWI-UEFI).....	306
6.3.14	Changing the iSCSI initiator CHAP secret.....	308
6.3.14.1	Changing the iSCSI initiator CHAP secret (HWI-QLogic) .....	308
6.3.14.2	Changing the iSCSI initiator CHAP secret (SWI-UEFI).....	309
6.3.15	Changing the iSCSI initiator MTU.....	310
6.3.15.1	Changing the iSCSI initiator MTU (HWI-QLogic) .....	310
6.3.15.2	Changing the iSCSI initiator MTU (SWI-UEFI).....	311
6.3.16	Disabling iSCSI header and data digests .....	312
6.3.16.1	Disabling iSCSI header and data digests (HWI-QLogic).....	312
6.3.17	Ending the iSCSI initiator configuration utility .....	313
6.3.17.1	Ending the QLogic Fast!UTIL utility.....	313
6.3.17.2	Ending the UEFI Setup utility .....	313
6.3.17.3	Ending the iSCSI Configuration Manger utility (SWI-BladeBoot) .....	313
6.4	Setting the integrated server start options.....	314
6.4.1	Setting the integrated server start options (UEFI) .....	314
6.4.2	Setting the integrated server start options (BIOS).....	317

## 6.1 Downloading and updating firmware and drivers

BladeCenter blade and System x servers require the following firmware updates.

Item	Download and Update Methods
Server firmware (UEFI or BIOS)	The IBM ToolsCenter <b>Bootable Media Creator (BoMC)</b> is used to update IBM System x and BladeCenter blade server firmware. See <a href="#">Using Bootable Media Creator (BoMC)</a> .
iSCSI initiator firmware	
Many other firmware types	
BladeCenter management module	See <a href="#">Firmware updates for the BladeCenter chassis</a> .
BladeCenter I/O module	
Windows iSCSI initiator drivers	See <a href="#">Windows drivers for iSCSI initiators</a> .

### 6.1.1 Using Bootable Media Creator (BoMC)

The IBM ToolsCenter **Bootable Media Creator (BoMC)** is used to update IBM System x and BladeCenter blade server firmware. BoMC creates a bootable image on supported media that bundles multiple IBM System x and BladeCenter tools and updates from UpdateXpress System Packs. BoMC can run on a Windows or Linux PC.

#### 6.1.1.1 Downloading server updates with Bootable Media Creator (BoMC)

Firmware updates and drivers are required for the BladeCenter blade or System x server hardware that is integrated with IBM i.

**Important:** You must use **BoMC** to create a bootable image on supported media (such as CD, DVD, ISO image, USB flash drive, or set of PXE files) that bundles multiple IBM System x and BladeCenter tools and updates from UpdateXpress System Packs. BoMC can run on a Windows or Linux PC. If you have not yet downloaded BoMC to your PC, download it from the [IBM Bootable Media Creator \(BoMC\) Web page](#). See **Chapter 2** of the BoMC [Installation and User's Guide](#) for instructions.

**Note:** If you need detailed explanations of the Bootable Media Creator Wizard pages, see **Chapter 3** of the BoMC [Installation and User's Guide](#).

Download the firmware updates and drivers using BoMC as described below.

1. Launch the **Bootable Media Creator** program from your PC and accept the license agreement.

**Note:** Bootable Media Creator is a self-extracting application that does not need to be installed. Just run the Bootable Media Creator program that you downloaded to your PC.

2. (Optional) If it has been a long time since you downloaded BoMC, see [Updating Bootable Media Creator to latest version](#).
3. On the **Welcome** page, type a description for the media being created, then click **Next**.
4. On the **Media Purpose** page, select the **Updates** checkbox and any other options that you want, then click **Next**.

**Note:** Do **not** select the **Deployment** checkbox. Installation of Windows using **ServerGuide** is **not**

supported in the IBM i iSCSI environment.

5. On the **Acquire Location** page, select **Check the IBM web site** and **UpdateXpress System Packs (UXSP's)**, then click **Next**.
6. On the **HTTP Proxy** page, select the appropriate options for your environment, then click **Next**.
7. On the **Targeted Systems** page, select your BladeCenter blade or System x server models, then click **Next**.

**Tips:**

- To add support for new systems or get updates released after the current version of the Bootable Media Creator, use **Update List** to update the support list from the IBM web site.
  - You can select multiple server models and BoMC will include updates for all of the selected models on the same media.
8. On the **Target Directory** page, specify the location on your PC to download the files to, then click **Next**.
  9. On the **Media Format** page, specify the type of media that you will create, then click **Next**.

**Tip:** Create physical media or just an ISO image of the media. For some environments, you can mount an ISO image using the server's service processor and boot the server using the ISO image without actually creating physical media. If you do not create physical media and you later decide that you need it, you can use your favorite CD burning utility to put the ISO image on physical media.

10. On the **Unattended Mode Configuration** page, select **Do not use unattended mode**, then click **Next**.
11. On the **Confirm Choices** page, review your choices.  
If necessary, use **Previous** to go back and make changes to your choices.  
Once everything looks good, click **Next** on the **Confirm Choices** page.
12. On the **Creation Progress** page, answer any messages that are presented. Once the bootable media has been created, click **Next**.
13. On the **Finish** page, click **Finish**. The Bootable Media Creator tool closes.

#### **6.1.1.1 Updating Bootable Media Creator to latest version**

If it has been a long time since you downloaded BoMC, you might want to consider updating it to the latest version. To do this:

1. Launch the **Bootable Media Creator** program from your PC and accept the license agreement.
2. Select the **Check for the latest version of this tool** check box on the **Welcome** page and click **Next**.
3. Select the appropriate options on the **HTTP Proxy** page and click **Next**.

4. If a newer version of the tool is available, click **Download Now**.
5. Once the download is complete, close the Bootable Media Creator tool.

**Note:** The new version of BoMC is downloaded to the same directory as the previous version of BoMC, but has a different program name.

- From now on, be sure to launch BoMC using the new program name.
- If you have any shortcuts to the BoMC program, you should update them as well.
- You might also consider deleting the old version of BoMC to avoid confusion.

### 6.1.1.2 Updating the server using Bootable Media Creator (BoMC) media

Use the bootable media for your BladeCenter blade or System x server model that was created using BoMC to update your server hardware. Do this as follows:

1. Insert the bootable media in the BladeCenter blade or System x server.
  - For a blade server, use the BladeCenter media tray and assign the media tray to the blade.
  - If you have an ISO image of the media, either you must burn the ISO image to a CD or DVD, or you must mount the ISO image to the server using the virtual media function in the service processor (MM, AMM, IMM II, IMM, or RSA II), or other equivalent function.

2. Power on the BladeCenter blade or System x server.

**Tip:** If the device from which you want to boot is not first or second in the boot order, press **F12** to select that device.

3. The IBM ToolsCenter **Customized Media** utility starts automatically when you boot from the bootable media.

4. Perform these steps to install updates:

- a. On the **Welcome** page, click on **Updates**.
- b. On the **Updates** page, click on the **click here to start update** link. The **UpdateXpress System Pack Installer** is displayed.
- c. Accept the UpdateXpress System Pack Installer license terms to continue.
- d. On the **Update Recommendation** page, select all of the updates, then click **Next**.
- e. After the updates are complete, click **Next**, then on the next page click.
- f. To exit out of the **Customized Media** utility, click **Exit** on **Updates** page, then OK.

5. Power off the BladeCenter blade or System x server.

6. Remove the bootable media from the BladeCenter blade or System x server (or unmount the ISO image).

## 6.1.2 Firmware updates for the BladeCenter chassis

### 6.1.2.1 Downloading firmware updates for the BladeCenter chassis

Firmware updates are required for the BladeCenter chassis that contains a blade server that is integrated with IBM i.

**Tip:** The BladeCenter firmware must be updated the first time you install a blade that is integrated with IBM i. Normally, you do not need to update the BladeCenter firmware each time you install additional blades in the BladeCenter chassis.

Download the firmware updates for the BladeCenter using the following steps:

1. Select the link for your BladeCenter model below:

- [BladeCenter S](#)
- [BladeCenter E](#)
- [BladeCenter H](#)

The **Downloads** page for the selected model is displayed.

2. Select the **View BladeCenter Chassis downloads** link to show the **Fix Central** page.

3. For the **Operating System**, select **Operating system independent / None** and then select the **Continue** link to display the **Select fixes** page.

4. Search the available downloads list for the following BladeCenter firmware updates:

Firmware Type	Considerations
Management Module	Choose <u>one</u> of the following, whichever is appropriate for your BladeCenter: <ul style="list-style-type: none"><li>• IBM BladeCenter Advanced Management Module Firmware Update</li><li>• IBM BladeCenter Management Module Firmware Update</li></ul>
I/O module	Choose the firmware package that is appropriate for the type of BladeCenter I/O module that is used for the iSCSI network.

**Tip:** Use the links near the top of the page to jump to the **Management Module** and **Switches** sections of the list.

5. Select the checkbox next to each firmware update package identified above.

**Tip:** Also click the **Readme** file link for each update package and either bookmark it or print it so that you can refer back to it when performing the firmware update in a later task. Then return to the **Select fixes** page.

6. Click the **Continue** link at the bottom of the page and follow the instructions on the resulting Web pages to download the selected update packages to your PC.

**Related information:**

- [Installation Checklist](#)

## 6.1.2.2 Updating the BladeCenter management module firmware

Refer to the management module firmware download **Readme** file that you bookmarked or printed earlier during the [Downloading firmware updates for the BladeCenter chassis](#) task. Use the **Readme** instructions along with the steps below to perform the firmware update. The **Readme** contains any changes necessary to the general instructions listed below. Follow the directions in the **Readme** wherever differences occur.

Perform the following steps on the computer containing the update package (not on the BladeCenter).

1. Unpack the .zip file you downloaded earlier to extract the firmware update files.
2. Use your Web browser to connect to the management module Web interface.  
See [Connecting to the service processor Web interface](#).
3. Click **Firmware Update** on the navigation pane on the left, under **MM Control**.
4. On the **Update MM Firmware** window, select **Browse** and navigate to the files containing the firmware update. The files will have an extension of .PKT; and there might be multiple files with this extension.
5. Highlight one of these files and click **Open**. The **Readme** instructions may specify a particular order to select these files. If so, follow the **Readme** instructions. The full path of the selected file is displayed in the **Browse** field.
6. To start the update process, click **Update**. A progress indicator opens as the file is transferred to temporary storage on the Management Module. A confirmation window is displayed when the file transfer is complete.
7. Verify that the file shown on the **Confirm Firmware Update** window is the one you want to update. If not, click **Cancel**.
8. To complete the update process, click **Continue**. A progress indicator opens as the firmware on the Management Module is flashed. A confirmation window is displayed when the update has successfully completed.
9. The **Readme** instructions might direct you to restart the MM after completing the .PKT file update. If so, click **Restart MM** on the navigation pane on the left side of the window. Click **OK** to confirm the restart. The Web browser window will then close. A new Web browser window will have to be started and signed onto to continue.
10. Repeat the update procedure for any other .PKT files (steps 1 through 8).

### Related information:

- [Installation Checklist](#)

### 6.1.2.3 Updating and configuring the BladeCenter I/O module

Configure the BladeCenter I/O module to work in the integrated server environment.

The I/O module firmware update was downloaded previously. See [Downloading firmware updates for the BladeCenter chassis](#).

Refer to the **Readme** instructions obtained earlier during the I/O module firmware download. Use the **Readme** instructions along with the following steps to perform the firmware update. The **Readme** instructions might contain updates to the following instructions. Follow the directions in the **Readme** instructions wherever differences occur.

Perform the following steps on the computer containing the update package (not on the BladeCenter).

1. Use your Web browser to connect to the management module Web interface.  
See [Connecting to the service processor Web interface](#).
2. Select **Admin/Power/Restart** under **I/O Module Tasks** on the navigation pane on the left side of the screen.
3. Under the **I/O Module Advanced Setup** heading, use the **Select a module** menu to select the I/O module that is used for the iSCSI network (for example, I/O module 3 for the first port on an iSCSI HBA expansion card or I/O module 4 for the second port on the card).

**Note:** Make sure the menu for External ports has **Enabled** selected.

4. Click **Save** on the extreme lower right of the screen to save the values to the I/O module.
5. Update the I/O module firmware at this time.
  - The procedure varies depending on the manufacturer of the I/O module.
  - Refer to the **Readme** instructions for the update along with the I/O module documentation to complete this task.

**Related information:**

- [Installation Checklist](#)



## 6.1.3 Windows drivers for iSCSI initiators

### 6.1.3.1 Downloading Windows Ethernet NIC software initiator driver

If you are using an iSCSI software initiator (Ethernet NIC) on your integrated server, you might need to get an updated Ethernet NIC driver.

Download the Ethernet NIC driver as follows:

1. Go to **Fix Central**: <http://www.ibm.com/support/fixcentral/>
2. Select the appropriate **Product Group** and **Product** for your server model.
3. Depending on your Windows version, select one of the following for the **Operating system**:
  - **Windows Server 2012**
  - **Windows Server 2008 x64**
  - **Windows Server 2003**
4. Click **Continue** to show the **Select fixes** page.
5. Click the **Network** link to go to the list of Ethernet NIC firmware and driver downloads.
6. Select the checkbox next to the latest driver that is available on the download page for the Ethernet NICs that the server will use as iSCSI software initiators.  
  
**Tip:** Also click the **Readme** file link for each driver package and either bookmark it or print it so that you can refer back to it when performing the driver update in a later task.
7. Click the **Continue** link at the bottom of the **Select fixes** page and follow the instructions on the resulting Web pages to download the selected driver packages to your PC.
8. Extract the driver files into a local directory on your PC and copy them to a blank CD, DVD, or USB key. Choose media corresponding to a device that is available on your integrated server.

**Related information:**

- [Installation Checklist](#)

### 6.1.3.2 Downloading System x Windows Server 2012/2008 iSCSI HBA driver

If you are using either of the following QLogic iSCSI HBAs on your System x server and plan to install Windows Server 2012 or Windows Server 2008, you need to get the QLogic iSCSI HBA driver:

System x iSCSI initiators	Option Part Number
QLogic iSCSI Single Port PCIe HBA	39Y6146
QLogic iSCSI Dual Port PCIe HBA	42C1770

Download the QLogic iSCSI driver as follows:

1. Go to the QLogic [BladeCenter and System x Software Updates for Integration with IBM i](#) Web page.
2. Download the **IBM iSCSI STORport driver for Windows 2008** driver.

**Tip:** Also click the **Read Me** file link for the driver package and either bookmark it or print it so that you can refer back to it when performing the driver update in a later task.

3. Extract the driver files into a local directory on your PC and copy them to a blank CD, DVD, or USB key. Choose media corresponding to a device that is available on your integrated server.

**Related information:**

- [Installation Checklist](#)
- [System x iSCSI initiators](#)
- [iSCSI supported limits](#)

## 6.2 Configuring the BladeCenter or System x service processor

Configuration tasks for the various types of BladeCenter and System x service processors are described in the following sections.

### 6.2.1 Configuring the BladeCenter management module

You need the **BladeCenter or System x service processor** work sheet from the [IBM i iSCSI Solution Work Sheets](#) to complete this task.

**Note:** If this is the first time you are configuring the management module:

- The management module must have an Ethernet cable plugged into its Ethernet port. Plug the other end of this cable into the Ethernet connector of the computer that will be used to configure the service processor. In some cases, a switch or hub might also be necessary to connect.
- Also ensure that the BladeCenter power cords are plugged into an appropriate power source to provide power for the management module.

Configure a Management Module (MM) or Advanced Management Module (AMM) as follows:

1. Use your Web browser to connect to the management module Web interface.  
See [Connecting to the service processor Web interface](#).
2. Select **Login Profiles** under **MM Control** in the navigation pane on the left side of the window.
  - a. On the next window is a list of Login IDs, find the entry for the default login ID value of USERID and click that entry.

- b. A **Login Profile** window is displayed. Change the **Login ID** (work sheet item **XSP7**), and enter values for the **New password** (work sheet item **XSP8**) and **Confirm password** fields based on the information entered in the work sheets.  
Also, make sure the **Role** is set to **Supervisor**. Click **Save** to complete this step.
3. Select **Network Interfaces** under **MM Control** in the navigation pane on the left side of the screen. Use the values in the work sheets to complete the following steps:
  - a. Select **Enabled** from the **Interface** list.
  - b. Enter a name for this MM in the **Hostname** (work sheet item **XSP2**) field.
  - c. From the **IPv4 DHCP** list, select and set one of the following (work sheet item **XSP3**):
    - i. **Disabled - Use static IP configuration.**
    - ii. **Enabled - Obtain IP config from DHCP server.**  
This option requires an operating DHCP server in the service processor network.  
You must also configure a host name if you use this option.
  - d. Enter a value for the following fields under the **Static IP Configuration** heading if the **Disabled – Use static IP configuration** value was selected for the **DHCP** field:
    - o **IP address** – type in the IP address (work sheet item **XSP4**).
    - o **Subnet mask** – type in the subnet mask (work sheet item **XSP5**).
    - o **Gateway address** – type in the gateway address (work sheet item **XSP6**).
  - e. Click **Save** to complete configuring the network interfaces.
4. **AMM only:** Select **Network Protocols** under **MM control** in the navigation pane on the left side of the screen.
  - a. Page down to the **TCP Command Mode Protocol** section.
  - b. Change the **Command mode** value to the number of desired concurrent connections.  
  
**Tip:** Set it to **3** or more concurrent connections.
5. Select **Restart MM** on the navigation pane on the left side of the screen to restart the Management Module.
6. Click **OK** to confirm that you want to restart the Management Module. A window is displayed advising that the browser window will be closed. Click **OK**.

**Related information:**

- [Installation Checklist](#)

## 6.2.2 Configuring the System x service processor

You need the **BladeCenter or System x service processor** work sheet from the [IBM i iSCSI Solution Work Sheets](#) to complete this task. Refer to work sheet item **XSP1** to determine which type of service processor is installed.

**Note:** If this is the first time you are configuring the service processor:

- The service processor must have an Ethernet cable plugged into its Ethernet port. Plug the other end of this cable into the Ethernet connector of the computer that will be used to configure the service processor. In some cases, a switch or hub might also be necessary to connect.
- Also ensure that the System x server power cords are plugged into an appropriate power source to provide power for the service processor.

Use one of these tasks to configure the service processor:

Service Processor Type	Task
Integrated Management Module II (IMM II)	<a href="#">Configuring the System x IMM II</a>
Integrated Management Module (IMM)	<a href="#">Configuring the System x IMM</a>
Remote Supervisor Adaptor II (RSA II)	<a href="#">Configuring the System x RSA II</a>
Baseboard Management Controller (BMC)	<a href="#">Configuring the System x BMC</a>

### Related information:

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

### 6.2.2.1 Configuring the System x IMM II

You need the **BladeCenter or System x service processor** work sheet from the [IBM i iSCSI Solution Work Sheets](#) to complete this task. Refer to work sheet item **XSP1** to determine which type of service processor is installed.

Configure an Integrated Management Module II (IMM II) as follows:

1. Use your Web browser to connect to the service processor Web interface.  
See [Connecting to the service processor Web interface](#).

**Note:** If this is the first time you are configuring the IMM II, see [Configuring the IMM II IP address and DHCP settings](#).

2. Select **Users** under **IMM Management** near the top of the page to show the **User Accounts** page.
3. Click the **Create User** button above the table.
4. Follow the Create New User Wizard as follows:
  - a) On the **User Credentials** page, set the **User name** (work sheet item **XSP7**) and enter values for the **Password** (work sheet item **XSP8**) and **Confirm password** fields based on the information entered in the work sheets, then click **Next**.
  - b) On the **Authority Level** page, select **Supervisor**, then click **Next**.

- c) On the **Configure SNMPv3** page, click **Finish**.
5. Log out and log back in using the new user name and password.
6. Select **Users** under **IMM Management** near the top of the page to show the **User Accounts** page.
7. Select user name **USERID** in the list of user names, then click the **Delete** button above the table. At the next panel, confirm this action to delete this default **USERID** profile.
8. Select **Network** under **IMM Management** near the top of the page to show the **Network Protocol Properties** page.
9. Use the values in the work sheets to complete the following steps:
  - a) On the **Ethernet** tab, enter a name for this IMM in the **Host name** field (work sheet item **XSP2**).
  - b) On the **IPv4** sub-tab, select **Enable IPv4**.
  - c) Under **Configure IP address settings**, select one of the following (work sheet item **XSP3**):
    1. If XSP3 = Enabled, then select **Obtain IP address from DHCP server**.  
This option requires an operating DHCP server in the service processor network.  
You must also configure a host name if you use this option.
    2. If XSP3 = Disabled, then select **Use static IP address**.
  - d) If **Use static IP address** was selected above, enter a value for the following fields under the **Static IP Address Settings** heading:
 

Item	Value
Static address	Type in the IP address from work sheet item <b>XSP4</b> .
Subnet mask	Type in the subnet mask from work sheet item <b>XSP5</b> .
Default gateway	Type in the gateway address from work sheet item <b>XSP6</b> .
  - e) Click the **Apply** button near the top of the page to save the changes.
10. Select **IMM Properties** under **IMM Management** near the top of the page to show the **Integrated Management Module (IMM) Properties** page.
11. On the **Date and Time** tab, set the current date and time and use the **GMT Offset** list to select the appropriate time zone. Also, select the check box to automatically adjust for daylight saving time, if necessary. Click the **Apply** button near the top of the page to save the changes.
12. When all the updates and configuration steps are complete, select **Restart IMM** under **IMM Management** near the top of the page to restart the Integrated Management Module.
13. Click **OK** to confirm that you want to restart the Integrated Management Module.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

### 6.2.2.1.1 *Configuring the IMM II IP address and DHCP settings*

If you are using a new integrated server with an Integrated Management Module II (IMM II) service processor, you might need to configure networking settings before you can sign into it with the Web interface.

Do the following steps to configure the network settings.

1. Power on the System x server. Refer to the system documentation to complete this step.
2. When the **IBM System x Server Firmware** image appears on the display, press **F1** to go to setup.
3. Highlight **System Settings** using the up or down arrow keys and press **Enter** to select.
4. Highlight **Integrated Management Module** using the up or down arrow keys and press **Enter** to select.
5. Highlight **Network Configuration** using the up or down arrow keys and press **Enter** to select.
6. Highlight **Network Interface Port** using the up or down arrow keys and select **Dedicated**.
7. Highlight **Hostname** using the up or down arrow keys and select **Hostname**. Enter the value from work sheet item **XSP2**.
8. Highlight **DHCP Control** using the up or down arrow keys and select **Static IP**.
9. Highlight **Static IP Address** using the up or down arrow keys, press **Enter**. Type in the IP address from work sheet item **XSP4**.
10. Highlight **Subnet Mask** using the up or down arrow keys, press **Enter**. Type in the subnet mask from work sheet item **XSP5**.
11. Highlight **Gateway** using the up or down arrow keys, press **Enter**. Type in the gateway address from work sheet item **XSP6**.
12. Highlight **Save Network Settings** using the up or down arrow keys and press **Enter** to select and perform the action. A screen displays confirming the action.
13. Press **Esc** until the **Main Menu** is shown. Then select **Save Settings** and then **Exit Setup**.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

## 6.2.2.2 Configuring the System x IMM

You need the **BladeCenter or System x service processor** work sheet from the [IBM i iSCSI Solution Work Sheets](#) to complete this task. Refer to work sheet item **XSP1** to determine which type of service processor is installed.

Configure an Integrated Management Module (IMM) as follows:

1. Use your Web browser to connect to the service processor Web interface.  
See [Connecting to the service processor Web interface](#).

**Note:** If this is the first time you are configuring the IMM, see [Configuring the IMM IP address and DHCP settings](#).

2. Select **Login Profiles** under **IMM Control** in the navigation pane on the left side of the screen.
3. Select **Add User** from the list of login IDs pane. The **Login Profile** window is displayed.
4. Do the following steps.
  - a) Set the **Login ID** (work sheet item **XSP7**) and enter values for the **Password** (work sheet item **XSP8**) and **Confirm password** fields based on the information entered in the work sheets.
  - b) Ensure the **Authority Level** is set to **Supervisor**.
  - c) Click **Save**.
5. Log off and log back on using the new Login ID and Password.
6. Select **Login Profiles** from the navigation pane on the left side of the screen.
7. Select user ID **USERID** in the list of login IDs. At the next panel select **Clear Login Profile** and confirm this action to delete this default profile.
8. Select **Network Interfaces** under **IMM Control** in the navigation pane on the left side of the screen.
9. Use the values in the work sheets to complete the following steps:

- a) Select **Enabled** from the **Interface** list.
- b) From the **DHCP** list, select and set one of the following (work sheet item **XSP3**):
  1. **Disabled - Use static IP configuration.**
  2. **Enabled - Obtain IP config from DHCP server.**  
This option requires an operating DHCP server in the service processor network.  
You must also configure a host name if you use this option.

- c) Enter a name for this IMM in the **Hostname** field (work sheet item **XSP2**).

- d) Enter a value for the following fields under the **Static IP Configuration** heading if the **Disabled – Use static IP configuration** value was selected for the **DHCP** field:

Item	Value
IP address	Type in the IP address from work sheet item <b>XSP4</b> .
Subnet mask	Type in the subnet mask from work sheet item <b>XSP5</b> .
Gateway address	Type in the gateway address from work sheet item <b>XSP6</b> .

- e) Click **Save** to complete configuring the network interfaces.
10. Select **System Settings** under **IMM Control** in the navigation pane on the left side of the window.
  11. Click **Set IMM Date and Time** under the heading **IMM Date and Time**.
  12. On the next window, set the current date and time (using a 24-hour clock) and use the **GMT offset** list to select the appropriate time zone. Also, select the box to automatically adjust for daylight saving time, if necessary. Click **Save** to complete.
  13. When all the updates and configuration steps are complete, select **Restart IMM** under **IMM Control** in the navigation pane to restart the Integrated Management Module.
  14. Click **OK** to confirm that you want to restart the Integrated Management Module. A window is displayed advising that the browser window will be closed. Click **OK** to continue.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)



### 6.2.2.2.1 *Configuring the IMM IP address and DHCP settings*

If you are using an integrated server with an Integrated Management Module (IMM) service processor, you might need to configure networking settings before you can sign into it with the Web interface.

Do the following steps to configure the network settings.

1. Power on the System x server. Refer to the system documentation to complete this step.
2. When the **IBM System x Server Firmware** image appears on the display, press **F1** to go to setup.
3. Highlight **System Settings** using the up or down arrow keys and press **Enter** to select.
4. Highlight **Integrated Management Module** using the up or down arrow keys and press **Enter** to select.
5. Highlight **Network Configuration** using the up or down arrow keys and press **Enter** to select.
6. Highlight **Network Interface Port** using the up or down arrow keys and select **Dedicated**.
7. Highlight **Hostname** using the up or down arrow keys and select **Hostname**. Enter the value from work sheet item **XSP2**.
8. Highlight **DHCP Control** using the up or down arrow keys and select **Static IP**.
9. Highlight **Static IP Address** using the up or down arrow keys, press **Enter**. Type in the IP address from work sheet item **XSP4**.
10. Highlight **Subnet Mask** using the up or down arrow keys, press **Enter**. Type in the subnet mask from work sheet item **XSP5**.
11. Highlight **Gateway** using the up or down arrow keys, press **Enter**. Type in the gateway address from work sheet item **XSP6**.
12. Highlight **Save Network Settings** using the up or down arrow keys and press **Enter** to select and perform the action. A screen displays confirming the action.
13. Press **Esc** until the **Main Menu** is shown. Then select **Save Settings** and then **Exit Setup**.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

### 6.2.2.3 Configuring the System x RSA II

You need the **BladeCenter or System x service processor** work sheet from the [IBM i iSCSI Solution Work Sheets](#) to complete this task. Refer to work sheet item **XSP1** to determine which type of service processor is installed.

Configure a Remote Supervisor Adaptor II (RSA II) as follows:

1. Use your Web browser to connect to the service processor Web interface.  
See [Connecting to the service processor Web interface](#).

**Note:** If this is the first time you are configuring the RSA II, see [Configuring the RSA II IP address and DHCP settings](#).

2. Select **Login Profiles** from under **ASM Control** in the navigation pane on the left side of the screen.
3. From the list of login IDs pane, select one of the unused entries in the table. The **Login Profile** window is displayed.
4. Do the following steps.
  - a) Change the **Login ID** (work sheet item **XSP7**) and enter values for the **Password** (work sheet item **XSP8**) and **Confirm password** fields based on the information entered in the work sheets.
  - b) Ensure the **Authority Level** is set to **Supervisor**.
  - c) Click **Save**.
5. Log off and log back on using the new Login ID and Password.
6. Select **Login Profiles** from under **ASM Control** in the navigation pane on the left side of the screen.
7. From the list of login IDs pane select user ID USERID. At the next pane select **Clear Login Profile** to delete this default profile.
8. On the navigation pane on the left side of the window, select **Network Interfaces** under **ASM Control** to start the configuration.
9. Use the values in the work sheets to complete the following steps:
  - a) Select **Enabled** from the **Interface** list.
  - b) From the **DHCP** list, select and set one of the following (work sheet item **XSP3**):
    1. **Disabled - Use static IP configuration.**
    2. **Enabled - Obtain IP config from DHCP server.**  
This option requires an operating DHCP server in the service processor network.  
You must also configure a host name if you use this option.
  - c) Enter a name for this RSA II in the **Hostname** field (work sheet item **XSP2**).

- d) Enter a value for the following fields under the **Static IP Configuration** heading if the **Disabled – Use static IP configuration** value was selected for the **DHCP** field:

Item	Value
IP address	Type in the IP address from work sheet item <b>XSP4</b> .
Subnet mask	Type in the subnet mask from work sheet item <b>XSP5</b> .
Gateway address	Type in the gateway address from work sheet item <b>XSP6</b> .

- e) Click **Save** to complete configuring the network interfaces.

10. Select **System Settings** in the navigation pane on the left side of the window.

11. On the same window, under the heading **ASM Date and Time**, click **Set ASM Date and Time**.

12. On the next window, set the current date and time (using a 24-hour clock) and use the **GMT offset** list to select the appropriate time zone. Also, select the box to automatically adjust for daylight saving time, if necessary. Click **Save** to complete.

13. When all the updates and configuration steps are complete, select **Restart ASM** on the navigation pane to restart the RSA II.

14. Click **OK** to confirm that you want to restart the RSA II. A window is displayed advising that the browser window will be closed. Click **OK** to continue.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

### 6.2.2.3.1 *Configuring the RSA II IP address and DHCP settings*

If you are using a new integrated server with a Remote Supervisor Adaptor II (RSA II) service processor, you might need to configure networking settings before you can sign into it with the Web interface.

Do the following steps to configure the RSA II.

1. Power on the System x server. Refer to the system documentation to complete this step.
2. Press **F1** when prompted to start **Setup**.
3. Highlight **Advanced Setup** using the up or down arrow keys and press **Enter** to select.
4. Highlight **RSA II Settings** using the up or down arrow keys and press **Enter** to select.
5. Highlight **DHCP Control** using the up or down arrow keys and select **Use static IP**.
6. Highlight **Static IP Address** using the up or down arrow keys.  
Type in the IP address from work sheet item **XSP4**.
7. Highlight **Subnet Mask** using the up or down arrow keys.  
Type in the subnet mask from work sheet item **XSP5**.
8. Highlight **Gateway** using the up or down arrow keys.  
Type in the gateway address from work sheet item **XSP6**.
9. Highlight **Save Values and Reboot RSA II** using the up or down arrow keys and press **Enter** to select and perform the action. A screen displays confirming the action.
10. Press **Esc** until the main menu is shown. Then select **Save Settings** and then **Exit Setup**.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

## 6.2.2.4 Configuring the System x BMC

You need the **BladeCenter or System x service processor** work sheet from the [IBM i iSCSI Solution Work Sheets](#) to complete this task. Refer to work sheet item **XSP1** to determine which type of service processor is installed.

**Note:** These steps are required only for System x products that contain a Baseboard Management Controller (BMC) service processor and do **not** also have a Remote Supervisor Adapter II (RSA II) service processor installed.

Configure a Baseboard Management Controller (BMC) as follows:

1. Power on the System x server. Refer to the system documentation to complete this step.
2. Press **F1** when prompted to start **Setup**.
3. Highlight **Advanced Setup** using the up or down arrow keys and press **Enter** to select.
4. Look for a **RSA II Settings** link and do one of the following:

<b>RSA II Settings</b>	<b>Next Step</b>
Link shown	RSA II hardware is installed and the BMC does <b>not</b> need to be configured. In this case, skip to the last step of this section.
Link not shown	RSA II hardware is not installed and you must continue with the next step of this procedure to configure the BMC.

5. Highlight **Baseboard Management Controller (BMC) Settings** using the up or down arrow keys and press **Enter**.
6. Highlight **BMC Network Configuration** using the up or down arrow keys and press **Enter** to select.
7. Highlight **Static IP Address** using the up or down arrow keys and use the backspace key to position the cursor for entry of the IP address from work sheet item **XSP4**.
8. Highlight **Subnet Mask** using the up or down arrow keys and use the backspace key to position the cursor for entry of the subnet mask from work sheet item **XSP5**.
9. Highlight **Gateway** using the up or down arrow keys and use the backspace key to position the cursor for entry of the gateway address from work sheet item **XSP6**.
10. Highlight **Save Network Settings in BMC** using the up or down arrow keys and press **Enter** to select and perform the action. This displays the **BMC Settings saved!** screen.
11. Press **Enter** to return to the **Baseboard Management Controller (BMC) Settings** menu.
12. Highlight **User Account Settings** using the up or down arrow keys and press **Enter**.
13. Highlight **UserID 2** using the up or down arrow keys and press **Enter**.
14. On the **UserID 2 Account Settings** screen, highlight **UserID 2** using the up or down arrow keys and use the left or right arrow keys to change the value to **Enabled**.

15. Highlight **Username** using the up or down arrow keys. Using the backspace key to position the cursor, fill in the field using the information from work sheet item **XSP7**.
16. Highlight **Password** using the up or down arrow keys. Using the backspace key to position the cursor, fill in the field using the information from work sheet item **XSP8**.
17. Highlight **Confirm Password** using the up or down arrow keys. Using the backspace key to position the cursor, fill in the same password as above.
18. Highlight **Privileged Limit** using the up or down arrow keys and use the left or right arrow keys to change the value to **Administrator**.
19. Highlight **Save User Account Settings to BMC** using the up or down arrow keys and press **Enter**.
20. The **BMC User Account Settings Saved!** screen is displayed. Press **Enter** to return to the **User Account Settings** menu.
21. Press **Esc** to return to the **Baseboard Management Controller (BMC) Settings** menu.
22. Press **Esc** to return to the **Advanced Setup** menu.
23. Press **Esc** to return to the main setup menu.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

### 6.2.3 Connecting to the service processor Web interface

You can connect to BladeCenter Management Module (MM), BladeCenter Advanced Management Module (AMM), System x Integrated Management Module II (IMM II), System x Integrated Management Module (IMM), and System x Remote Supervisor Adapter II (RSA II) service processors using a Web browser.

Use the following procedure to connect to the service processor Web interface:

1. Use one of the following methods to start the service processor Web interface:

Method	Description
Web Browser	Type the IP address or host name of the service processor in the Web browser address field.  <b>Note:</b> If you do not know the IP address or host name of the service processor, or if the service processor <b>Welcome</b> page does <b>not</b> appear, see <a href="#">Determining an IP address for the service processor Web interface</a> .
IBM i <a href="#">Web GUI</a>	If you already have an iSCSI-attached server configured on IBM i for the server hardware, then you can use the IBM i 7.2, 7.1 or 6.1 <a href="#">Web GUI</a> to connect to the associated service processor Web interface using one of the following tasks: <ul style="list-style-type: none"><li>• <a href="#">Launching the Web console for an integrated server</a></li><li>• <a href="#">Launching the Web console for a remote system</a></li><li>• <a href="#">Launching the Web console for a service processor</a></li></ul>

Any of the above methods displays the service processor **Welcome** page, or a sign on page.

2. Type the user ID and password on the **Welcome** page and click **Log In**.

**Note:** The service processor has a default user name of **USERID** and default password of **PASSWORD** (where 0 is a zero, not the letter O), so if you have not set up a user ID yet, use these values.

3. Select a timeout value on the next screen and click **Continue** to go to the service processor **System Status** page.

### 6.2.3.1 Determining an IP address for the service processor Web interface

Use the tasks below in the following situations:

- If you are connecting to the service processor Web interface for the first time.
- If you do not know the IP address or host name of the service processor.
- If the service processor **Welcome** page does **not** appear when you try to connect to the service processor Web interface.

**Note:** If the service processor does **not** already have a static IP address or host name, the service processor factory defaults are set as follows:

- **Try DHCP server. If it fails, use static IP config.**
- If the DHCP attempt fails, it uses a default static IP address of **192.168.70.125**.

Therefore, try the following methods to determine an IP address to use to connect to the service processor Web interface:

Method	Description
Try default IP address <b>192.168.70.125</b>	Try using the default static IP address of <b>192.168.70.125</b> .  <b>Note:</b> 192.168.70.125 is a non-routable address. You cannot connect a browser through a router to the service processor using this address. You might be able to connect a browser to the service processor with the default IP address through most (but not all) brands of switches, and most Ethernet hubs.
Try the IP address assigned by DHCP	If the service processor network has a DHCP server, try determining the IP address that was assigned by the DHCP server and use that IP address.
Reset service processor to factory defaults, then use default IP address <b>192.168.70.125</b>	If the above methods fail, do the following: <ol style="list-style-type: none"> <li>1. Connect your PC to the service processor using a network that does <b>not</b> contain a DHCP server.</li> <li>2. Set the IP address of your PC to something such as 192.168.70.101, which must be in the same subnet as the service processor default IP address of 192.168.70.125. Also set the subnet mask to 255.255.255.0.</li> <li>3. Reset the service processor IP address to factory defaults, using the <b>IP reset</b> button on the service processor. Refer to service processor documentation to complete this task.</li> <li>4. Connect to the Web interface using the default static IP address of <b>192.168.70.125</b>.</li> </ol>



## 6.3 iSCSI Initiator Hardware Configuration

This section describes various iSCSI initiator configuration tasks that are required for BladeCenter blade and System x servers that are attached to IBM i via an iSCSI network.

The installation road map refers to various iSCSI initiator configuration tasks in this section.

### 6.3.1 iSCSI initiator configuration methods

There are several methods to configure iSCSI initiators, depending on the iSCSI initiator hardware and server firmware that is used:

Configuration Method	Description
SWI-UEFI	<p>This method addresses servers that have <b>UEFI</b> server firmware and use an Ethernet NIC software initiator (<b>SWI</b>) as the iSCSI initiator hardware.</p> <p><b>UEFI Setup</b> is the utility that is used to configure the iSCSI initiators in this environment.</p> <p><b>Note:</b> SWI-UEFI is not used for iSCSI-attached servers on IBM i 5.4.</p>
SWI-BladeBoot	<p>This method addresses BladeCenter blade servers that have <b>BIOS</b> server firmware, support <b>BladeBoot™</b> technology, and use an Ethernet NIC software initiator (<b>SWI</b>) as the iSCSI initiator hardware.</p> <p><b>iSCSI Configuration Manager</b> is the primary utility that is used to configure the iSCSI initiators in this environment.</p> <p><b>Note:</b> SWI-BladeBoot is not used for iSCSI-attached servers on IBM i 5.4.</p> <p>For more information, refer to the <a href="#">BladeBoot SAN Guide</a>.</p>
HWI-QLogic	<p>This method addresses servers that use a <b>QLogic</b> iSCSI host bus adapter (iSCSI HBA) hardware initiator (<b>HWI</b>) as the iSCSI initiator hardware.</p> <p><b>Fast!UTIL</b> is the primary utility that is used to configure the iSCSI initiator in this environment.</p>

iSCSI initiator configuration methods that are used for various server and iSCSI initiator configurations:

Configuration Method	Server Firmware	Server Type	iSCSI Initiator Part Numbers
SWI-UEFI	UEFI	Blade	LOM <sup>1</sup> , 44W4479, 44W4475, 46W6164, 46W6168, 49Y4235, 90Y3566, 44W4465
		System x	LOM <sup>1</sup> , 49Y4220, 42C1780
SWI-BladeBoot	BIOS	Blade	LOM <sup>1</sup> , 44W4479
HWI-QLogic	UEFI or BIOS	Blade	32R1923
		System x	39Y6146, 42C1770, 30R5201, 30R5501

<sup>1</sup> LAN on Motherboard (LOM). Note that LOM is also called embedded Ethernet or integrated Ethernet.

When you are directed to perform a specific task:

1. Locate the configuration method above that corresponds to the type of iSCSI initiator hardware used in your integrated server and the configuration method that is used for that iSCSI initiator hardware.
2. Go to the appropriate section that corresponds to your configuration to perform the specific task.

**Related information:**

- [Blade iSCSI initiators](#)
- [System x iSCSI initiators](#)

### 6.3.2 “iSCSI Mode” for booting UEFI-based servers

There are two methods (iSCSI modes) that can be used to configure a UEFI-based server to boot from iSCSI-attached storage. You must use the method indicated in the table below based on the criteria that is listed:

iSCSI Mode	Criteria
UEFI	Use the <b>UEFI</b> method for servers that do <b>not</b> meet the <b>Legacy</b> criteria listed in the next table row.
Legacy	<p>Use the <b>Legacy</b> method for servers that meet <b>any</b> of the following criteria:</p> <ol style="list-style-type: none"> <li>1. The <b>HWI-QLogic Configuration Method</b> is used for the BladeCenter blade or System x server boot port.</li> <li>2. <b>VMware ESXi Installable 4.1</b> will be installed on the BladeCenter blade or System x server.</li> <li>3. A <b>System x server</b> that has an <b>IMM</b> or any previous generation service processor (for example, an x3500 M3). See the service processor type for your server model in <a href="#">System x server models</a>.</li> </ol> <p><b>Note:</b> This item does <b>not</b> apply to servers with an <b>IMM II</b> or later generation service processor.</p>

**Related information:**

- [Configuring a boot iSCSI initiator for dynamic addressing \(SWI-UEFI\)](#)
- [Configuring a boot iSCSI initiator for manual addressing \(SWI-UEFI\)](#)
- [Setting the integrated server start options \(UEFI\)](#)

### 6.3.3 Starting the iSCSI initiator configuration utility

Perform the task corresponding to your configuration method:

Configuration Method	Task
HWI-QLogic	<a href="#">Starting the QLogic Fast!UTIL utility</a>
SWI-UEFI	<a href="#">Starting the UEFI Setup utility</a>
SWI-BladeBoot	<a href="#">Starting the iSCSI Configuration Manger utility (SWI-BladeBoot)</a>

### 6.3.3.1 Starting the QLogic Fast!UTIL utility

Perform this task to start the QLogic Fast!UTIL utility for a BladeCenter blade or System x server that uses **QLogic iSCSI HBAs**. You can use the configuration utility to make changes to the iSCSI initiator settings.

The steps below are performed from the BladeCenter blade or System x display and keyboard or using the service processor remote console support.

Do these steps to start the Fast!UTIL utility on the server:

1. If you are configuring a blade server, select the appropriate blade server for the BladeCenter KVM and media tray. Refer to the BladeCenter hardware documentation to complete this step.
2. Turn the server power on. Refer to the BladeCenter or System x hardware documentation to complete this step. This will start the power on system test (POST) on the server.
3. Wait for the QLogic BIOS prompt on the server display. This will appear sometime after the eServer™ logo has been displayed.

**Important:** If you have more than one adapter version installed in a System x server, the prompt will appear for each version. The screen will display QLA405x then QLA406x. You must respond to the prompt for the adapter version that you want to configure.

The prompt will read something like this: **Press CTRL-Q for Fast!UTIL**. Respond to this prompt by pressing Ctrl + Q. This will start the configuration utility.

4. Successful initiation of the utility is confirmed by a message that reads **CTRL-Q Detected, Initialization in progress, Please wait...**

**Note:** It may take several minutes before the next screen is displayed.

**Tip:** A red status bar may appear at the bottom of the screen. This bar provides information about status or errors.

5. If more than one iSCSI HBA port is available for use, either because the iSCSI HBA has multiple ports (as in a blade server) or there are multiple iSCSI HBAs plugged into the server (as can be done with System x), the **Select Host Adapter** menu will appear. Highlight the iSCSI HBA port you are configuring as identified by its MAC address using the up or down arrow keys and press **Enter**. It might take several seconds for the next window to appear.
6. The next **Configuration Settings** window will have two panes:
  - The **Selected Adapter** pane is at the top. This pane shows the iSCSI HBA port currently selected for configuration.
  - On the lower pane is the **Fast!UTIL Options** pane.
7. Continue with the specific iSCSI initiator configuration task that you are performing.

### 6.3.3.2 Starting the UEFI Setup utility

Perform this task to enter the **UEFI Setup** utility for a BladeCenter or System x server that supports **UEFI** and uses **Ethernet NICs** as the iSCSI initiators. Use the UEFI Setup utility to make changes to the iSCSI initiator settings.

The steps below are performed from the BladeCenter blade or System x display and keyboard or using the service processor remote console support.

Do these steps to start the UEFI Setup utility on the server:

1. If you are configuring a blade server, select the appropriate blade server for the BladeCenter KVM and media tray. Refer to the BladeCenter hardware documentation to complete this step.
2. Power on the server. Refer to the server documentation to complete this step.
3. Press **F1** when prompted, shortly after the IBM logo appears on the display, to enter the UEFI Setup utility.  
**Tip:** You can press F1 as soon as the IBM logo appears, prior to seeing the prompt for pressing F1, which goes away quickly.
4. After pressing F1, the **System Configuration and Boot Management** menu is displayed.
5. Continue with the specific iSCSI initiator configuration task that you are performing.

### 6.3.3.3 Starting the iSCSI Configuration Manger utility (SWI-BladeBoot)

Blades that use BladeBoot require the use of the **iSCSI Configuration Manger** utility running on a separate management PC to setup the Ethernet NIC that is used to boot a blade server using iSCSI.

**Note:** If you have not already installed the **iSCSI Configuration Manger** utility on a management PC, see [Installing the iSCSI Configuration Manager application \(SWI-BladeBoot\)](#) before performing this procedure.

Do these steps to start the iSCSI Configuration Manager utility on the management PC:

1. Launch the iSCSI Configuration Manager wizard using one of the following methods:
  - a) For a **Windows** management PC, use the desktop shortcut to the application or type on the command line or double click on the **wizard.bat** file in the directory where the iSCSI Configuration Manager utility was extracted to.
  - b) For a **Linux** management PC, type on the command line or double click on the **wizard.sh** file in the directory where the iSCSI Configuration Manager utility was extracted to.  
**Note:** a “.” might be needed on the command line to execute the file, like **./wizard.sh**.
2. Once the utility is active, a window appears asking which type of configuration to perform. The choices are **Quick configuration** and **Advanced configuration**.
3. Select the **Advanced configuration** method, and then click **Next**.

### 6.3.3.3.1 *Installing the iSCSI Configuration Manager application (SWI-BladeBoot)*

The **iSCSI Configuration Manager** is a stand-alone application that is installed on a Windows or Linux management PC that is connected to the IP Network of the BladeCenter Management Module. See the [iSCSI Configuration Manager](#) documentation for a list of supported platforms and minimum system requirements.

To install the iSCSI Configuration Manager on the management PC:

1. Download the .zip file for the iSCSI Configuration Manager utility from the [iSCSI Configuration Manager](#) Web site.
  - a) For a **Windows** management PC, download the MSI file to the PC.
  - b) For a **Linux** management PC, download the .zip file and extract it to the PC.
2. Install the iSCSI Configuration Manager utility.
  - The steps necessary to install the utility vary depending on what operating system is running on your management PC. Refer to the iSCSI Configuration Manager documentation to complete this step.
  - On a Windows PC, the installation process adds a desktop shortcut to start the utility.

## 6.3.4 Configuring a boot iSCSI initiator port

Perform the task corresponding to your configuration method:

Configuration Method	Task
HWI-QLogic	<a href="#">Configuring a boot iSCSI initiator port (HWI-QLogic)</a>
SWI-UEFI	<a href="#">Configuring a boot iSCSI initiator port (SWI-UEFI)</a>
SWI-BladeBoot	<a href="#">Configuring a boot iSCSI initiator port (SWI-BladeBoot)</a>

**Note:** This section does not apply to VMware ESXi Embedded servers, since the operating system does not boot from iSCSI-attached storage.

### 6.3.4.1 Configuring a boot iSCSI initiator port (HWI-QLogic)

Perform this task to configure the iSCSI initiator boot settings for a BladeCenter blade or System x server that uses **QLogic iSCSI HBAs**.

**Note:** This section does not apply to VMware ESXi Embedded servers, since the operating system does not boot from iSCSI-attached storage.

**Note:** The following tasks reference items from the [IBM i iSCSI Solution Work Sheets](#). These work sheets should be filled out and available for reference while completing the tasks:

- **iSCSI initiator** work sheet. Item names from this work sheet start with “**IN**”.
- **IBM i remote system configuration** work sheet. Item names from this work sheet start with “**RS**”.

**Attention:** If you are using a **QLogic** iSCSI hardware initiator that might have been previously used, do these two procedures before continuing:

- [Restoring factory defaults for an iSCSI initiator \(HWI-QLogic\)](#).
- [Resetting cached iSCSI initiator configuration information \(HWI-QLogic\)](#).

Select one of the two procedures listed below, based on the boot parameter delivery method selected in work sheet item **RS6**:

- [Configuring a boot iSCSI initiator for dynamic addressing \(HWI-QLogic\) – Recommended](#). Configure the iSCSI initiator to allow IBM i to dynamically provide IP addresses and IQNs using an [Integrated iSCSI DHCP server](#).
- [Configuring a boot iSCSI initiator for manual addressing \(HWI-QLogic\)](#). Configure the iSCSI initiator to use manual addressing. You will need to configure an IP address for the iSCSI initiator.

### 6.3.4.1.1 *Configuring a boot iSCSI initiator for dynamic addressing (HWL-QLogic)*

Configure the iSCSI initiator to allow IBM i to dynamically provide IP addresses and IQNs using an [Integrated iSCSI DHCP server](#).

**Note:** This section does not apply to VMware ESXi Embedded servers, since the operating system does not boot from iSCSI-attached storage.

**Note:** This procedure starts from the **Fast!UTIL Options** menu in the configuration utility. If you need to restore this menu, see [Starting the QLogic Fast!UTIL utility](#), then return to this procedure.

1. On the **Fast!UTIL Options** menu, highlight **Configuration Settings** using the up or down arrow keys and press **Enter**.
2. Highlight **Host Adapter settings** using the up or down arrow keys and press **Enter**.
3. Specify CHAP settings.

**Note:** Use the **Disabled** bullet below for i 5.4 systems (initiator CHAP is not supported on i 5.4).

- If **Enabled** is selected for work sheet item **RS10**, highlight the **Initiator Chap Name** field, type the name from work sheet item **RS11** and press **Enter**. Then highlight the **Initiator Chap Secret** field, type the name from work sheet item **RS12** and press **Enter**.
  - If **Disabled** is selected for work sheet item **RS10**, clear the **Initiator Chap Name** and **Initiator Chap Secret** fields. Highlight each field using the up or down arrow keys, press **Enter**, type in a single space and press **Enter** to clear each field.
4. Highlight **Initiator IP address by DHCP** using the up or down arrow keys and press **Enter** until the value shows **No**.
  5. Press **Esc** to return to the **Configuration Settings** menu.
  6. Highlight **ISCSI Boot Settings** using the up or down arrow keys and press **Enter**.
  7. The **iSCSI Boot Settings** menu is displayed.
  8. Highlight **Adapter Boot Mode** using the up or down arrow keys and press **Enter**.
  9. Highlight **DHCP using vendor ID** (or **DHCP** if only **DHCP** is shown on the panel) using the up or down arrow keys and press **Enter**.
  10. Highlight **Primary Boot Device Settings** using the up or down arrow keys and press **Enter**.
  11. Highlight **Security Settings** using the up or down arrow keys and press **Enter** to select. The next menu displayed is the **Primary Boot Security Settings** menu.
  12. Highlight **Chap** using the up or down arrow keys and press **Enter** to change the value to **Enabled** or **Disabled**, depending on whether or not CHAP is used. Refer to work sheet item **RS7** for this information.  
Skip to step **16** if CHAP has been disabled.

13. Highlight **Chap Name** using the up or down arrow keys and press **Enter**. This will bring up the **Enter Chap Name** pane. Type the target CHAP name from work sheet item **RS8** and press **Enter**.
14. Highlight **Chap Secret** using the up or down arrow keys and press **Enter**. This will bring up the **Enter New Secret** pane. Type the target CHAP secret from work sheet item **RS9** and press **Enter**. The **Confirm New Secret** pane is then displayed. Retype the same secret and press **Enter**.
15. Highlight **Bidirectional Chap** using the up or down arrow keys.  
**Note:** Use the **Disabled** bullet below for **i 5.4** systems.
  - If **Enabled** is selected for work sheet item **RS10**, press **Enter** to change the value to **Enabled**.
  - If **Disabled** is selected for work sheet item **RS10**, press **Enter** to change the value to **Disabled**.
16. Press **Esc** to return to the **Primary Boot Device Settings** menu.
17. Press **Esc** to return to the **iSCSI Boot Settings** menu.
18. Press **Esc**. The **Configuration setting modified** pane is displayed.
19. Highlight **Save changes** using the up or down arrow keys and press **Enter**. It might take several minutes to complete the save process. When complete, the **Fast!UTIL Options** menu is displayed.

If you are done making changes to the iSCSI initiator configuration, exit the Fast!UTIL utility and restart the system. See [Ending the QLogic Fast!UTIL utility](#) for details.

**Related information:**

➤ [Booting over the iSCSI network](#)

➤ [Integrated iSCSI DHCP server](#)

### 6.3.4.1.2 **Configuring a boot iSCSI initiator for manual addressing (HWI-QLogic)**

Configure the iSCSI initiator to use manual addressing. You will need to configure an IP address for the iSCSI initiator.

**Tip:** This manual addressing method should only be used if the dynamic addressing method does not work. See [Configuring a boot iSCSI initiator for dynamic addressing \(HWI-QLogic\)](#).

**Note:** This section does not apply to VMware ESXi Embedded servers, since the operating system does not boot from iSCSI-attached storage.

**Note:** This procedure starts from the **Fast!UTIL Options** menu in the configuration utility. If you need to restore this menu see [Starting the QLogic Fast!UTIL utility](#), then return to this procedure.

1. On the **Fast!UTIL Options** menu, highlight **Configuration Settings** using the up or down arrow keys and press **Enter**.
2. Highlight **Host Adapter settings** using the up or down arrow keys and press **Enter**.
3. Highlight **LUNs per Target** using the up or down arrow keys and press **Enter**. Use the arrow keys to select the value **64** and press **Enter**. This option is not available in System x adapter version 406x.



4. Highlight **Initiator IP Address via DHCP** using the up or down arrow keys and press **Enter** until the value shows **No**.

**Important:** In adapter version 406x select only the **IPv4** options for the following steps.

5. Highlight **Initiator IP address** using the up or down arrow keys and press **Enter**. Type the initiator (integrated server) SCSI internet address from work sheet item **RS15** and press **Enter**.
6. Highlight **Subnet mask** using the up or down arrow keys and press **Enter** to select. Type the iSCSI Initiator subnet mask from work sheet item **RS16** and press **Enter**.
7. Highlight **Gateway IP Address** using the up or down arrow keys and press **Enter** to select. Clear any value currently in the field or set it to blanks, then press **Enter**.
8. Highlight **Initiator iSCSI Name** using the up or down arrow keys and press **Enter** to select. Type the name from work sheet item **RS18** and press **Enter**.
9. Do one of the following:  
**Note:** Use the **Disabled** bullet below for **i 5.4** systems (initiator CHAP is not supported on i 5.4).
  - If **Enabled** is selected for work sheet item **RS10**, highlight the **Initiator Chap Name** field, type the name from item **RS11** and press **Enter**. Then highlight the **Initiator Chap Secret** field, type the name from item **RS12** and press **Enter**.
  - If **Disabled** is selected for work sheet item **RS10**, clear the **Initiator Chap Name** and **Initiator Chap Secret** fields. Highlight each field using the up or down arrow keys, press **Enter**, type in a single space and press **Enter** to clear each field.
10. Press **Esc** to return to the **Configuration Settings** menu.
11. Highlight **iSCSI Boot Settings** using the up or down arrow keys and press **Enter** to display the **iSCSI Boot Settings** menu.
12. Highlight **Adapter Boot Mode** using the up or down arrow keys and press **Enter**.
13. Highlight **Manual** using the up or down arrow keys and press **Enter**.
14. Highlight **Primary Boot Device Settings** using the up or down arrow keys and press **Enter**.
15. Highlight **Target IP** using the up or down arrow keys and press **Enter** to select. Type the target (IBM i) SCSI internet address from work sheet item **NH8** and press **Enter**.
16. Highlight **iSCSI Name** using the up or down arrow keys and press **Enter**. IBM i will generate the IQN for the target side and it must be matched here. Type the iSCSI name from work sheet item **IN11** and press **Enter**.
17. Highlight **Security Settings** using the up or down arrow keys and press **Enter** to display the **Primary Boot Security Settings** menu.
18. Highlight **Chap** using the up or down arrow keys and press **Enter** to change the value to **Enabled** or **Disabled**, based on whether or not CHAP is used. Refer to work sheet item **RS7** for this information.  
Skip to step **22** if CHAP has been disabled.

19. Highlight **Chap Name** using the up or down arrow keys and press **Enter** to select. This will bring up the **Enter Chap Name** pane. Type the target CHAP name from work sheet item **RS8** and press **Enter**.
20. Highlight **Chap Secret** using the up or down arrow keys and press **Enter** to select. This will bring up the **Enter New Secret** pane. Type the target chap secret from work sheet item **RS9** and press **Enter** and confirm by retyping the same chap secret on the next pane and press **Enter**.
21. Highlight **Bidirectional Chap** using the up or down arrow keys.
  - If **Enabled** is selected for work sheet item **RS10**, press **Enter** to change the value to **Enabled**.
  - If **Disabled** is selected for work sheet item **RS10**, press **Enter** to change the value to **Disabled**.  
**Note: Disabled** is required for **i 5.4** systems.
22. Press **Esc** to return to the **Primary Boot Device Settings** menu.
23. Press **Esc** to return to the **iSCSI Boot Settings** menu.
24. Press **Esc**. The **Configuration setting modified** pane is displayed.
25. Highlight **Save changes** using the up or down arrow keys and press **Enter**. It might take several minutes to complete the save process. When complete, the **Fast!UTIL Options** menu is displayed.

If you are done making changes to the iSCSI initiator configuration, exit the Fast!UTIL utility and restart the system. See [Ending the QLogic Fast!UTIL utility](#) for details.

**Related information:**

- [Booting over the iSCSI network](#)

### 6.3.4.2 Configuring a boot iSCSI initiator port (SWI-UEFI)

Perform this task to configure the iSCSI initiator boot settings for a BladeCenter blade or System x server that supports **UEFI** and uses **Ethernet NICs** as the iSCSI initiators.

**Note:** This section does not apply to VMware ESXi Embedded servers, since the operating system does not boot from iSCSI-attached storage.

**Note:** The following tasks reference items from the [IBM i iSCSI Solution Work Sheets](#). These work sheets should be filled out and available for reference while completing the tasks:

- **iSCSI initiator** work sheet. Item names from this work sheet start with “**IN**”.
- **IBM i remote system configuration** work sheet. Item names from this work sheet start with “**RS**”.

Select one of the two procedures listed below, based on the boot parameter delivery method selected in work sheet item **RS6**:

- [Configuring a boot iSCSI initiator for dynamic addressing \(SWI-UEFI\) – Recommended.](#)  
Configure the iSCSI initiator to allow IBM i to dynamically provide IP addresses and IQNs using an [Integrated iSCSI DHCP server](#).
- [Configuring a boot iSCSI initiator for manual addressing \(SWI-UEFI\).](#)  
Configure the iSCSI initiator to use manual addressing. You will need to configure an IP address for the iSCSI initiator.

#### 6.3.4.2.1 *Configuring a boot iSCSI initiator for dynamic addressing (SWI-UEFI)*

Configure the iSCSI initiator to allow IBM i to dynamically provide IP addresses and IQNs using an [Integrated iSCSI DHCP server](#).

**Note:** This section does not apply to VMware ESXi Embedded servers, since the operating system does not boot from iSCSI-attached storage.

**Note:** This procedure starts from the **System Configuration and Boot Management** menu in the UEFI **Setup** utility. If you need to restore this menu, see [Starting the UEFI Setup utility](#), then return to this procedure.

1. Highlight **System Settings** using the up or down arrow keys and press **Enter**
2. Highlight **Network** using the up or down arrow keys and press **Enter**.
3. Highlight **iSCSI Configuration** using the up or down arrow keys and press **Enter**.
4. Highlight **iSCSI Initiator Name** using the up or down arrow keys and press **Enter** to select. Type the name from work sheet item **RS18** and press **Enter**.
5. Highlight **Add an Attempt** using the up or down arrow keys and press **Enter** to select.
6. Highlight the MAC address for the initiator you are configuring using the up and down arrow keys and press **Enter** to select.

7. Highlight **iSCSI Attempt Name** using the up or down arrow keys and press **Enter** to select. Type in a name to identify the attempt and press **Enter**.
8. Highlight **iSCSI Mode** using the up or down arrow keys and press **Enter** to select. Highlight **Enabled** and press **Enter** to select.
9. Highlight **Internet Protocol** using the up or down arrow keys and press **Enter** to select. Highlight **IP4** and press **Enter** to select.
10. Highlight **Enable DHCP** using the up or down arrow keys and press **Space** to indicate DHCP is used.
11. Highlight **Get target info via DHCP** using the up or down arrow keys and press **Space** to indicate the target information is retrieved via DHCP.
12. Highlight **Authentication Type** using the up or down arrow keys and press **Enter** to select. Highlight the correct authentication method (**CHAP** or **None**).  
If **None** was selected, skip to step **13**. Otherwise follow these steps:
  - a. Highlight **CHAP Type** using the up or down arrow keys and press **Enter** to select the appropriate CHAP type. Refer to work sheet items **RS7** and **RS10** for this information.  
**Note:** Select **One way** CHAP to use only target CHAP and select **Mutual** CHAP to use both target and initiator CHAP.
  - b. Highlight **CHAP Name** using the up or down arrow keys and press **Enter**. Type the target CHAP name from work sheet item **RS8** and press **Enter**.
  - c. Highlight **CHAP Secret** using the up or down arrow keys and press **Enter**. Type the target CHAP secret from work sheet item **RS9** and press **Enter**.  
For **One way** CHAP, skip to step **13**.
  - d. Highlight **Reverse CHAP Name** using the up or down arrow keys and press **Enter**. Type the initiator CHAP name from work sheet item **RS11** and press **Enter**.
  - e. Highlight **Reverse CHAP Secret** using the up or down arrow keys and press **Enter**. Type the initiator CHAP secret from work sheet item **RS12** and press **Enter**.
13. Highlight **Save Changes** using the up or down arrow keys and press **Enter**.
14. Highlight **Back to Previous Page** and press **Enter** to select.
15. Press **Esc** to return to the **Network** menu.
16. Highlight **Network Boot Configuration** using the up or down arrow keys and press **Enter**.
17. Highlight the MAC address for the initiator you are attempting to configure using the up and down arrow keys and press **Enter** to select.
18. Highlight **PXE Mode** using the up or down arrow keys and press **Enter**. Then highlight the option below for the iSCSI mode and press **Enter** to select:

iSCSI Mode	Option	Comments
UEFI	Disabled	<b>Tip:</b> To improve boot time, disable PXE mode for <b>all</b> ports, including ports that are <b>not</b> used for iSCSI traffic.
Legacy	Legacy Support	

19. Highlight the attempt under **iSCSI Mode Configuration** using the up or down arrow keys and press **Enter**. Then highlight the option below for the iSCSI mode and press **Enter** to select:

iSCSI Mode	Option
UEFI	UEFI Support
Legacy	Legacy Support

Repeat this step for any other attempts that are defined for this MAC address.

20. Highlight **Save Changes** using the up or down arrow keys and press **Enter**.
21. Repeat the prior 4 steps for any other MAC addresses that have attempts defined.
22. Press **Esc** to return to the **Network Boot Configuration** menu.
23. Press **Esc** to return to the **Network** menu.
24. Press **Esc** to return to the **System Settings** menu.
25. Press **Esc** to return to the **System Configuration and Boot Management** menu.
26. Highlight **Save Settings** using the up or down arrow keys and press **Enter**.

**Next**, perform the steps in section [Setting the integrated server start options \(UEFI\)](#) to ensure that the server will start correctly.

If you are done making changes to the iSCSI initiator configuration, exit the iSCSI initiator configuration utility and restart the system. See [Ending the UEFI Setup utility](#) for details.

**Related information:**

- [Booting over the iSCSI network](#)
- ["iSCSI Mode" for booting UEFI-based servers](#)
- [Integrated iSCSI DHCP server](#)

### 6.3.4.2.2 *Configuring a boot iSCSI initiator for manual addressing (SWI-UEFI)*

Configure the Ethernet NIC to use manual addressing. You will need to configure an IP address for the Ethernet NIC.

**Tip:** This manual addressing method should only be used if the dynamic addressing method does not work. See [Configuring a boot iSCSI initiator for dynamic addressing \(SWI-UEFI\)](#).

**Note:** This section does not apply to VMware ESXi Embedded servers, since the operating system does not boot from iSCSI-attached storage.

**Note:** This procedure starts from the **System Configuration and Boot Management** menu in the UEFI **Setup** utility. If you need to restore this menu, see [Starting the UEFI Setup utility](#), then return to this procedure.

1. Highlight **System Settings** using the up or down arrow keys and press **Enter**
2. Highlight **Network** using the up or down arrow keys and press **Enter**.
3. Highlight **iSCSI Configuration** using the up or down arrow keys and press **Enter**.
4. Highlight **iSCSI Initiator Name** using the up or down arrow keys and press **Enter** to select. Type the name from work sheet item **RS18** and press **Enter**.
5. Highlight **Add an Attempt** using the up or down arrow keys and press **Enter** to select.
6. Highlight the MAC address for the initiator you are attempting to configure using the up and down arrow keys and press **Enter** to select.
7. Highlight **iSCSI Attempt Name** using the up or down arrow keys and press **Enter** to select. Type in a name to identify the attempt and press **Enter**.
8. Highlight **iSCSI Mode** using the up or down arrow keys and press **Enter** to select. Highlight **Enabled** and press **Enter** to select.
9. Highlight **Internet Protocol** using the up or down arrow keys and press **Enter** to select. Highlight **IP4** and press **Enter** to select.
10. Highlight **Initiator IP address** using the up or down arrow keys and press **Enter**. Type the initiator (integrated server) SCSI internet address from work sheet item **RS15** and press **Enter**.
11. Highlight **Initiator Subnet mask** using the up or down arrow keys and press **Enter** to select. Type the iSCSI Initiator subnet mask from work sheet item **RS16** and press **Enter**.
12. Highlight **Gateway IP Address** using the up or down arrow keys and press **Enter** to select. If it is set to something other than 0.0.0.0, reset it to **0.0.0.0**, then press **Enter**.
13. Highlight **Target Name** using the up or down arrow keys and press **Enter**. IBM i will generate the IQN for the target side and it must be matched here. Type the iSCSI name from work sheet item **IN11** and press **Enter**.
14. Highlight **Target IP Address** using the up or down arrow keys and press **Enter** to select. Type the target (IBM i) SCSI internet address from work sheet item **NH8** and press **Enter**.

15. Highlight **Authentication Type** using the up or down arrow keys and press **Enter** to select. Highlight the correct authentication method (**CHAP** or **None**).  
If **None** was selected, skip to step **16**. Otherwise follow these steps:
  - a. Highlight **CHAP Type** using the up or down arrow keys and press **Enter** to select the appropriate CHAP type. Refer to work sheet items **RS7** and **RS10** for this information.
  - b. Highlight **CHAP Name** using the up or down arrow keys and press **Enter**. Type the target CHAP name from work sheet item **RS8** and press **Enter**.
  - c. Highlight **CHAP Secret** using the up or down arrow keys and press **Enter**. Type the target CHAP secret from work sheet item **RS9** and press **Enter**.  
For **One way** CHAP, skip to step **16**.
  - d. Highlight **Reverse CHAP Name** using the up or down arrow keys and press **Enter**. Type the initiator CHAP name from work sheet item **RS11** and press **Enter**.
  - e. Highlight **Reverse CHAP Secret** using the up or down arrow keys and press **Enter**. Type the initiator CHAP secret from work sheet item **RS12** and press **Enter**.
16. Highlight **Save Changes** using the up or down arrow keys and press **Enter**.

17. Highlight **Back to Previous Page** and press **Enter** to select.

18. Press **Esc** to return to the **Network** menu.

19. Highlight **Network Boot Configuration** using the up or down arrow keys and press **Enter**.

20. Highlight the MAC address for the initiator you are attempting to configure using the up and down arrow keys and press **Enter** to select.

21. Highlight **PXE Mode** using the up or down arrow keys and press **Enter**. Then highlight the option below for the iSCSI mode and press **Enter** to select:

iSCSI Mode	Option	Comments
UEFI	Disabled	<b>Tip:</b> To improve boot time, disable PXE mode for <b>all</b> ports, including ports that are <b>not</b> used for iSCSI traffic.
Legacy	Legacy Support	

22. Highlight the attempt under **iSCSI Mode Configuration** using the up or down arrow keys and press **Enter**. Then highlight the option below for the iSCSI mode and press **Enter** to select:

iSCSI Mode	Option
UEFI	UEFI Support
Legacy	Legacy Support

Repeat this step for any other attempts that are defined for this MAC address.

23. Highlight **Save Changes** using the up or down arrow keys and press **Enter**.

24. Repeat the prior 4 steps for any other MAC addresses that have attempts defined.

25. Press **Esc** to return to the **Network Boot Configuration** menu.

26. Press **Esc** to return to the **Network** menu.

27. Press **Esc** to return to the **System Settings** menu.

28. Press **Esc** to return to the **System Configuration and Boot Management** menu.

29. Highlight **Save Settings** using the up or down arrow keys and press **Enter**.

**Next**, perform the steps in section [Setting the integrated server start options \(UEFI\)](#) to ensure that the server will start correctly.

If you are done making changes to the iSCSI initiator configuration, exit the UEFI Setup utility and restart the system. See [Ending the UEFI Setup utility](#) for details.

**Related information:**

➤ [Booting over the iSCSI network](#)

➤ ["iSCSI Mode" for booting UEFI-based servers](#)

### 6.3.4.3 Configuring a boot iSCSI initiator port (SWI-BladeBoot)

Perform this task to configure the iSCSI initiator boot settings for a System x or blade server that uses **Ethernet NICs**.

**Note:** The following tasks reference items from the [IBM i iSCSI Solution Work Sheets](#). These work sheets should be filled out and available for reference while completing the tasks:

- **iSCSI initiator** work sheet. Item names from this work sheet start with **"IN"**.
- **IBM i remote system configuration** work sheet. Item names from this work sheet start with **"RS"**.

Select one of the two procedures listed below, based on the boot parameter delivery method selected in work sheet item **RS6**:

- [Configuring a boot iSCSI initiator for dynamic addressing \(SWI-BladeBoot\) – Recommended](#). Configure the iSCSI initiator to allow IBM i to dynamically provide IP addresses and IQNs using an [Integrated iSCSI DHCP server](#).
- [Configuring a boot iSCSI initiator for manual addressing \(SWI-BladeBoot\)](#). Configure the iSCSI initiator to use manual addressing. You will need to configure an IP address for the iSCSI initiator.

#### 6.3.4.3.1 *Configuring a boot iSCSI initiator for dynamic addressing (SWI-BladeBoot)*

Configure the iSCSI initiator to allow IBM i to dynamically provide IP addresses and IQNs using an [Integrated iSCSI DHCP server](#).

**Note:** This procedure starts from the first page after selecting **Advanced configuration** from the main page for the **iSCSI Configuration Manager** utility. If you need to start the utility see, [Starting the iSCSI Configuration Manger utility \(SWI-BladeBoot\)](#), then return to this procedure.

1. On the **Welcome** page:

- a) Select or type in a new configuration file to save the data for later use.



- b) Click **Next** to move to the next page.
2. On the **BladeCenter Initiator Retrieval – Login** page:
  - a) Select **Enter Initiator Data Manually** and fill in the connection information (the IP Address and User Login information) for BladeCenter's Management Module if it hasn't been filled in before.
  - b) Click **Next** to move to the next page.
3. On the **Target Properties** page:
  - a) If a previous target has been setup and saved, select a **Known Targets** by double clicking on it or select it, then click **Add/Update**. Otherwise fill in a new name in the **Description** box.

**Note:** A target configuration is not needed unless CHAP has been enabled.
  - b) Refer to the work sheet items **RS7** and **RS10** for this information. Click **Next** to skip if CHAP has been disabled. If work sheet item **RS10** is enabled, then select **Mutual** under the **Security Context** selection. Otherwise if work sheet item **RS7** is enabled with work sheet item **RS10** is disabled, select **Oneway** under the **Security Context** selection.

**Note:** The Target CHAP information is filled in the **Initiator Properties** page and the Initiator CHAP is supplied on the **Target Properties** page if **Mutual CHAP** is selected.
  - c) If **Mutual CHAP** is selected, refer to work sheet item **RS11** for the initiator CHAP Name/ID to fill in for the **CHAP ID** field and work sheet item **RS12** for the initiator CHAP password/secret to fill in for the **CHAP Password**, and **Confirm Password** fields
  - d) Leave all the other fields as default and click **Add/Update** to save Target configuration.
  - e) Click **Next** to move to the next page.
4. On the **Initiator Properties** page:
  - a) Select a **Known Initiator** by double clicking on it or select it, then click **Add/Update**. Otherwise fill in a new name in the **Description** box.
  - b) In the **Dynamic Mode** area, select **All via DHCP except Security** if CHAP has been enabled. Otherwise select **All Parameters via DHCP**.

**Note:** If **All via DHCP except Security** has been selected, refer to work sheet item **RS8** for the target CHAP Name/ID to fill in for the **CHAP ID** field and work sheet item **RS9** for the target CHAP password/secret to fill in for the **CHAP Password**, and **Confirm Password** fields.
  - c) Leave all the other fields as default and click **Add/Update** to save the Initiator configuration.
  - d) Click **Next** to move to the next page.
5. On the **Blade Properties** page:
  - a) Select configuration from the **Known Blades** section by double clicking on it or select it, then click **Add/Update**. Otherwise fill in a new name in the **Description** box.
  - b) Fill in the slot number of the blade in the **Slot #** field if it is empty or if it needs to be updated.

- c) Click **Scan Blade** to have the data filled in for the **Attempts**.
  - d) Click on the **Enabled** box under **Attempt 1** to enable the attempt.
  - e) Pull down the menu for the **Port Index** selection window and select the correct port to use. Either 0 or 1 should be selected if the internal Broadcom adapter on the blade is to be used (0 goes through Ethernet switch 1 and 1 goes through Ethernet switch 2).
  - f) Pull down the **Initiator selection** box and select which Initiator configuration should be associated with this **Attempt**. In this case, select the configuration identified under step **4-a** above.
  - g) Leave all the other fields as default and click **Add/Update** to save the configuration.
  - h) Click **Next** to move to the next page.
6. On the **Initiator/Target Mapping** page:
- a) Select configuration from the **Known Targets** section by double clicking on it or select it, then click **Update**.
  - b) If CHAP was enabled, then select the **Target configuration** from the pull down menu under the **Target 1** section.
  - c) Click on **Update** to save the mapping.
  - d) Click **Next** to move to the next page.
7. On the **Blade(s) Available to Flash** page:
- a) Select the checkboxes next to the specific configurations from the **Blade Properties** page to be flashed onto the blades themselves. Or select the checkbox to flash all configurations.
  - b) Click **Flash NVS on Blade** to flash the selected configurations from the previous step. The updating of the servers might take a minute or two to update. If the flash was successful or not will be identified on a pop-up window once the flash is done. Click **Okay** to get back to the main utility.
  - c) Click **Finished** to exit the utility. The utility asks if the new/modified configuration should be saved to a file before exiting. Save the configuration so that it can be retrieved later if needed.

**Next**, perform the steps in section [Setting the integrated server start options \(BIOS\)](#) to finish the setup and enable the iSCSI initiator port for boot.

**Related information:**

➤ [Booting over the iSCSI network](#)

➤ [Integrated iSCSI DHCP server](#)

### **6.3.4.3.2 Configuring a boot iSCSI initiator for manual addressing (SWI-BladeBoot)**

Configure the Ethernet NIC to use manual addressing. You will need to configure an IP address for the Ethernet NIC.

**Tip:** This manual addressing method should only be used if the dynamic addressing method does not work. See [Configuring a boot iSCSI initiator for dynamic addressing \(SWI-BladeBoot\)](#).

This procedure starts from the first page after selecting **Advanced configuration** from the main page for the **iSCSI Configuration Manager** utility. If you need to start the utility see, [Starting the iSCSI Configuration Manger utility \(SWI-BladeBoot\)](#), then return to this procedure.

1. On the **Welcome** page:
  - a) Select or type in a new configuration file to save the data for later use.
  - b) Click **Next** to move to the next page.
2. On the **BladeCenter Initiator Retrieval – Login** page:
  - a) Select **Enter Initiator Data Manually** and fill in the connection information (the IP Address and User Login information) for BladeCenter’s Management Module if it hasn’t been filled in before.
  - b) Click **Next** to move to the next page.
3. On the **Target Properties** page:
  - a) If a previous Target has been setup and saved, select a **Known Targets** by double clicking on it or select it, then click **Add/Update**. Otherwise fill in a new name in the **Description** box.
  - b) Fill in the **IP** using work sheet item **NH8**.
  - c) Fill in the **Target IQN** using work sheet item **IN11**.
  - d) Select the appropriate CHAP authentication method. Refer to the work sheet items **RS7** and **RS10** for this information. If work sheet item **RS10** is enabled, then select **Mutual** under the **Security Context** selection. Otherwise if work sheet item **RS7** is enabled and work sheet item **RS10** is disabled, select **Oneway** under the **Security Context** selection.  
  
**Note:** The Target CHAP is filled in the **Initiator Properties** page and the Initiator CHAP is supplied on the **Target Properties** page if Mutual CHAP is selected.
  - e) If Mutual CHAP has been selected, refer to work sheet item **RS11** for the initiator CHAP Name/ID to fill in for the **CHAP ID** field and work sheet item **RS12** for the initiator CHAP password/secret to fill in for the **CHAP Password**, and **Confirm Password** fields
  - f) Leave all the other fields as default and click **Add/Update** to save the Target configuration.
  - g) Click **Next** to move to the next page.
4. On the **Initiator Properties** page:
  - a) Select a **Known Initiator** by double clicking on it or select it, then click **Add/Update**. Otherwise fill in a new name in the **Description** box.
  - b) Fill in the **IP Address** box using work sheet item **RS15**.
  - c) Fill in the **Initiator IQN** box using work sheet item **RS18**.
  - d) Fill in the **Subnet** box using work sheet item **RS16**.

- e) Clear any value currently in the **Gateway Address** box or set it to blanks.
  - f) Click on **All in VPD** for the **Dynamic Mode** selection.
  - g) Leave all the other fields as default and click **Add/Update** to save the initiator configuration.
  - h) Click **Next** to move to the next page.
5. On the **Blade Properties** page:
- a) Select configuration from the **Known Blades** section by double clicking on it or select it, then click **Add/Update**. Otherwise fill in a new name in the **Description** box.
  - b) Fill in the slot number of the blade in the **Slot #** field if it is empty or update if needed.
  - c) Click **Scan Blade** to have the data filled in for the **Attempts**.
  - d) Click on the **Enabled** box under **Attempt 1** to enable the attempt.
  - e) Pull down the menu for **Port Index** selection window, and select the correct port to use. Either 0 or 1 should be selected if the internal Broadcom adapter on the blade is to be used (0 goes through Ethernet Switch 1 and 1 goes through Ethernet Switch 2).
  - f) Pull down the **Initiator selection** box and select which Initiator configuration should be associated with this **Attempt**. In this case, select the configuration identified under step **4-a**.
  - g) Leave all the other fields as default and click **Add/Update** to save the configuration.
  - h) Click **Next** to move to the next page.
6. On the **Initiator/Target Mapping** page:
- a) Select configuration from the **Known Targets** section by double clicking on it or select it, then click **Update**.
  - b) Select the Target configuration from the pull down menu under the **Target 1** section.
  - c) Leave the **Retry Count** and **Timeout** fields as their default values.
  - d) Click on **Update** to save the mapping.
  - e) Click **Next** to move to the next page.
7. On the **Blade(s) Available to Flash** page:
- a) Select the checkboxes next to the specific configurations from the **Blade Properties** page to be flashed onto the blades themselves. Or select the checkbox to flash all configurations.
  - b) Click **Flash NVS on Blade** to flash the selected configurations from the previous step. The updating of the servers might take a minute or two to update. If the flash was successful or not will be identified on a pop-up window once the flash is done. Click **Okay** to get back to the main utility.

- c) Click **Finished** to exit out the utility. The utility asks if the new/modified configuration should be saved to a file before exiting. Save the configuration so that it can be retrieved later if needed.

**Next**, perform the steps in section [Setting the integrated server start options \(BIOS\)](#) to finish the setup and enable the iSCSI initiator port for boot.

**Related information:**

- [Booting over the iSCSI network](#)

### 6.3.5 Configuring advanced iSCSI initiator port settings

Perform the task corresponding to your configuration method:

Configuration Method	Task
HWI-QLogic	<a href="#">Configuring advanced iSCSI initiator port settings (HWI-QLogic)</a>
SWI-UEFI	See <a href="#">Changing the iSCSI initiator MTU (SWI-UEFI)</a> to change the MTU settings for an Ethernet NIC.
SWI-BladeBoot	This task is not applicable for blades that use <b>BladeBoot</b> technology to boot using the iSCSI protocol over <b>Ethernet NICs</b> .

#### 6.3.5.1 Configuring advanced iSCSI initiator port settings (HWI-QLogic)

Perform this task to configure iSCSI initiator Maximum Transmission Unit (MTU) and acknowledgement (ACK) settings for a BladeCenter blade or System x server that uses **QLogic iSCSI HBAs**.

**Note:** The following tasks reference items from the [IBM i iSCSI Solution Work Sheets](#). These work sheets should be filled out and available for reference while completing the tasks:

- **iSCSI initiator** work sheet. Item names from this work sheet start with “**IN**”.

**Note:** This procedure starts from the **Fast!UTIL Options** menu in the configuration utility. If you need to restore this menu, see [Starting the QLogic Fast!UTIL utility](#), then return to this procedure.

1. On the **Fast!UTIL Options** menu, highlight **Configuration Settings** using the up or down arrow keys and press **Enter**.
2. Highlight **Advanced Adapter Settings** using the up or down arrow keys and press **Enter**.
3. Highlight **Delayed ACK** using the up or down arrow keys and press **Enter** until the value shows **Disabled**.
4. Highlight **MTU** (maximum transmission unit) using the up or down arrow keys and press **Enter** until the value shows the desired frame size setting from work sheet item **IN16** (either 1500 or 9000). Ensure the network the iSCSI HBA is attached to supports the value selected here.
5. Press **Esc**. The **Configuration setting modified** pane is displayed.
6. Highlight **Save changes** using the up or down arrow keys and press **Enter**. It might take several minutes to complete the save process. When complete, the **Fast!UTIL Options** menu is displayed.

If you are done making changes to the iSCSI initiator configuration, exit the Fast!UTIL utility and restart the system. See [Ending the QLogic Fast!UTIL utility](#) for details.

## 6.3.6 Configuring non-boot iSCSI initiator ports

Perform the task corresponding to your configuration method:

Configuration Method	Task
HWI-QLogic	<a href="#">Configuring non-boot iSCSI initiator ports (HWI-QLogic)</a>
SWI-UEFI	<a href="#">Configuring non-boot iSCSI initiator ports (SWI-UEFI)</a>
SWI-BladeBoot	This task is not applicable for blades that use <b>BladeBoot</b> technology to boot using the iSCSI protocol over <b>Ethernet NICs</b> .

### 6.3.6.1 Configuring non-boot iSCSI initiator ports (HWI-QLogic)

Perform this task to disable iSCSI initiator ports other than the boot device for a BladeCenter blade or System x server that uses **QLogic iSCSI HBAs**.

**Note:** For VMware ESXi Embedded servers, disable boot for all iSCSI initiator ports, since the operating system does not boot from iSCSI-attached storage.

**Note:** The following tasks reference items from the [IBM i iSCSI Solution Work Sheets](#). These work sheets should be filled out and available for reference while completing the tasks:

- **iSCSI initiator** work sheet. Item names from this work sheet start with “**IN**”.

**Note:** This procedure starts from the **Fast!UTIL Options** menu in the configuration utility. If you need to restore this menu, see [Starting the QLogic Fast!UTIL utility](#), then return to this procedure.

1. On the **Fast!UTIL Options** menu, highlight **Select Host Adapter** using the up or down arrow keys and press **Enter**.
2. From the **Select Host Adapter** menu, find any unused adapter ports and check to see if the **Adapter Boot Mode** is already set to **Disable**. If so, there is no need to continue. Otherwise, highlight the unused adapter port using the up or down arrow keys and press **Enter** to select. It may take several seconds for the next screen to appear.
3. On the **Fast!UTIL Options** menu, highlight **Configuration Settings** using the up or down arrow keys and press **Enter** to select.
4. On the **Configuration Settings** menu, highlight **iSCSI Boot Settings** using the up and down arrow keys and press **Enter** to select.
5. Highlight **Adapter Boot Mode** using the up or down arrow keys and press **Enter** to select.
6. Highlight **Disable** using the up or down arrow keys and press **Enter** to select.
7. Press **Esc** to return to the **Configuration Settings** menu.
8. Highlight **Advanced Adapter Settings** using the up or down arrow keys and press **Enter**.
9. Highlight **MTU** (maximum transmission unit) using the up or down arrow keys and press **Enter** until the value shows the desired frame size setting from work sheet item **IN16** (either 1500 or 9000). Ensure the network the iSCSI HBA is attached to supports the value selected here.

10. Press **Esc**. The **Configuration setting modified** pane is displayed.
11. Highlight **Save changes** using the up or down arrow keys and press **Enter**. It might take several minutes to complete the save process. When complete, the **Fast!UTIL Options** menu is displayed.

If you are done making changes to the iSCSI initiator configuration, exit the Fast!UTIL utility and restart the system. See [Ending the QLogic Fast!UTIL utility](#) for details.

### 6.3.6.2 Configuring non-boot iSCSI initiator ports (SWI-UEFI)

Perform this task to remove an attempt to boot for specific Ethernet NICs on a BladeCenter blade or System x server that supports **UEFI** and uses **Ethernet NICs** as the iSCSI initiators.

**Note:** For VMware ESXi Embedded servers, disable boot for all iSCSI initiator ports, since the operating system does not boot from iSCSI-attached storage.

**Note:** This procedure starts from the **System Configuration and Boot Management** menu in the **UEFI Setup** utility. If you need to restore this menu, see [Starting the UEFI Setup utility](#), then return to this procedure.

1. Highlight **System Settings** using the up or down arrow keys and press **Enter**.
2. Highlight **Network** using the up or down arrow keys and press **Enter**.
3. Highlight **iSCSI Configuration** using the up or down arrow keys and press **Enter**.
4. Highlight **Delete Attempts** using the up or down arrow keys and press **Enter**.
5. Select the attempt(s) you wish to delete by pressing the **Space** bar.

**Note:** The MAC address used for a given attempt is displayed on the right side of the screen for reference.

6. Highlight **Commit Changes and Exit** using the up or down arrow keys and press **Enter**.
7. Press **Esc** to return to the **Network** menu.
8. Press **Esc** to return to the **System Settings** menu.
9. Press **Esc** to return to the **System Configuration and Boot Management** menu.
10. Highlight **Save Settings** using the up or down arrow keys and press **Enter**.

If you are done making changes to the iSCSI initiator configuration, exit the iSCSI initiator configuration utility and restart the system. See [Ending the UEFI Setup utility](#) for details.

### 6.3.7 Configuring boot iSCSI initiator with manual addressing for MPIO target

Use this section for both **Windows** and **ESX** servers when the server system drive storage space is linked to the multipath group that is defined in the IBM i network server description (NWSA). With this configuration, you must change the initiator configuration settings to specify the iSCSI qualified name (IQN) for the **multipath group** IBM i target instead of the IQN for a specific IBM i target.

**Note:** This section does not apply to VMware ESXi Embedded servers, since the operating system does not boot from iSCSI-attached storage.

Perform the task corresponding to your configuration method:

<b>Configuration Method</b>	<b>Task</b>
HWI-QLogic	<a href="#">Configuring boot iSCSI initiator with manual addr. for MPIO target (HWI-QLogic)</a>
SWI-UEFI	<a href="#">Configuring boot iSCSI initiator with manual addr. for MPIO target (SWI-UEFI)</a>
SWI-BladeBoot	This task is not applicable for blades that use <b>BladeBoot</b> technology to boot using the iSCSI protocol over <b>Ethernet NICs</b> .



### 6.3.7.1 Configuring boot iSCSI initiator with manual addr. for MPIO target (HWI-QLogic)

Use this section for a server that boots using a hardware initiator with manual addressing and the server system drive storage space is linked to the multipath group that is defined in the IBM i network server description (NWS). With this configuration, you must change the initiator configuration settings to specify the iSCSI qualified name (IQN) for the multipath group IBM i target instead of the IQN for a specific IBM i target.

**Note:** This section does not apply to VMware ESXi Embedded servers, since the operating system does not boot from iSCSI-attached storage.

**Note:** This procedure starts from the **Fast!UTIL Options** menu in the configuration utility. If you need to restore this menu see [Starting the QLogic Fast!UTIL utility](#), then return to this procedure.

1. On the **Fast!UTIL Options** menu, highlight **Configuration Settings** using the up or down arrow keys and press **Enter**.
2. Highlight **iSCSI Boot Settings** using the up or down arrow keys and press **Enter** to display the **iSCSI Boot Settings** menu.
3. Highlight **Primary Boot Device Settings** using the up or down arrow keys and press **Enter**.
4. Highlight **iSCSI Name** using the up or down arrow keys and press **Enter**.
5. Type the target name value for the multipath group. See work sheet item **IN11** for the complete target IQN format. Be sure to specify the multipath group IQN, which ends with “**tm**” instead of “**tp**” (where **p** is 1-4). Then press **Enter**.
6. Press **Esc** to return to the **iSCSI Boot Settings** menu.
7. Press **Esc**. The **Configuration setting modified** pane is displayed.
8. Highlight **Save changes** using the up or down arrow keys and press **Enter**. It might take several minutes to complete the save process. When complete, the **Fast!UTIL Options** menu is displayed.

If you are done making changes to the iSCSI initiator configuration, exit the Fast!UTIL utility and restart the system. See [Ending the QLogic Fast!UTIL utility](#) for details.

### 6.3.7.2 Configuring boot iSCSI initiator with manual addr. for MPIO target (SWI-UEFI)

Use this section for a UEFI-based server that boots using a software initiator with manual addressing and the server system drive storage space is linked to the multipath group that is defined in the IBM i network server description (NWSD). With this configuration, you must change the UEFI settings to specify the iSCSI qualified name (IQN) for the multipath group IBM i target instead of the IQN for a specific IBM i target.

**Note:** This section does not apply to VMware ESXi Embedded servers, since the operating system does not boot from iSCSI-attached storage.

**Note:** This procedure starts from the **System Configuration and Boot Management** menu in the UEFI **Setup** utility. If you need to restore this menu, see [Starting the UEFI Setup utility](#), then return to this procedure.

1. Highlight **System Settings** using the up or down arrow keys and press **Enter**
2. Highlight **Network** using the up or down arrow keys and press **Enter**.
3. Highlight **iSCSI Configuration** using the up or down arrow keys and press **Enter**.
4. Highlight the existing attempt name and press **Enter** to select.
5. Highlight **Target Name** using the up or down arrow keys and press **Enter**.
6. Type the target name value for the multipath group. See work sheet item **IN11** for the complete target IQN format. Be sure to specify the multipath group IQN, which ends with “**tm**” instead of “**tp**” (where **p** is 1-4). Then press **Enter**.
7. Highlight **Save Changes** using the up or down arrow keys and press **Enter**.
8. Highlight **Back to Previous Page** and press **Enter** to select.
9. Press **Esc** to return to the **Network** menu.
10. Press **Esc** to return to the **System Settings** menu.
11. Press **Esc** to return to the **System Configuration and Boot Management** menu.
12. Highlight **Save Settings** using the up or down arrow keys and press **Enter**.

If you are done making changes to the iSCSI initiator configuration, exit the UEFI Setup utility and restart the system. See [Ending the UEFI Setup utility](#) for details.

### 6.3.8 Configuring additional boot iSCSI initiators for Windows MPIO

For **Windows** servers, more than one iSCSI initiator port can be enabled for booting in some multi-path I/O (MPIO) configurations.

**Note:** VMware **ESX** servers are only supported with one iSCSI initiator port enabled for booting.

Perform the task corresponding to your configuration method:

Configuration Method	Task
HWI-QLogic	<a href="#">Configuring additional boot iSCSI initiators for Windows MPIO (HWI-QLogic)</a>
SWI-UEFI	<a href="#">Configuring additional boot iSCSI initiators for Windows MPIO (SWI-UEFI)</a>
SWI-BladeBoot	This task is not applicable for blades that use <b>BladeBoot</b> technology to boot using the iSCSI protocol over <b>Ethernet NICs</b> .

#### 6.3.8.1 Configuring additional boot iSCSI initiators for Windows MPIO (HWI-QLogic)

Perform this task to configure additional boot iSCSI initiators for a Windows server running on a BladeCenter blade or System x server that uses **QLogic iSCSI HBAs**.

**Note:** For **Windows** servers, more than one iSCSI initiator port can be enabled for booting. VMware **ESX** servers are only supported with one iSCSI initiator port enabled for booting.

**Note:** The minimum IBM i group PTF levels required when configuring more than one port on a QLogic iSCSI HBA for booting are:

IBM i	Minimum IBM i Group PTF Level
i 7.1	<a href="#">SF99369</a> Level 5
i 6.1	<a href="#">SF99357</a> Level 19
i 5.4	No PTF is available for 5.4, so only <b>one</b> port on a QLogic iSCSI HBA is supported for booting. The second port on the iSCSI HBA can only be used for non-boot MPIO.

After loading the appropriate group PTF, see [Updating the integration software running on Microsoft Windows](#) to install the corresponding integrated server service pack on the Window server.

**Note:** The following tasks reference items from the [IBM i iSCSI Solution Work Sheets](#). These work sheets should be filled out and available for reference while completing the tasks:

- **iSCSI initiator** work sheet. Item names from this work sheet start with “**IN**”.
- **IBM i remote system configuration** work sheet. Item names from this work sheet start with “**RS**”.

Select one of the two procedures listed below, based on the boot parameter delivery method selected in work sheet item **RS6**:

- [Configuring additional boot iSCSI initiators with dynamic addr. \(HWI-QLogic\)](#) – **Recommended**. Configure the iSCSI initiators to allow IBM i to dynamically provide IP addresses and IQNs using an [Integrated iSCSI DHCP server](#).

- [Configuring additional boot iSCSI initiators with manual addr. \(HWI-QLogic\)](#).  
Configure the iSCSI initiators to use manual addressing. You will need to configure an IP address for the iSCSI initiator.

### 6.3.8.1.1 **Configuring additional boot iSCSI initiators with dynamic addr. (HWI-QLogic)**

Configure the iSCSI initiators to allow IBM i to dynamically provide IP addresses and IQNs using an [Integrated iSCSI DHCP server](#).

**Note:** For **Windows** servers, more than one iSCSI initiator port can be enabled for booting. VMware **ESX** servers are only supported with one iSCSI initiator port enabled for booting.

**Note:** This procedure starts from the **Fast!UTIL Options** menu in the configuration utility. If you need to restore this menu, see [Starting the QLogic Fast!UTIL utility](#), then return to this procedure.

1. On the **Fast!UTIL Options** menu, highlight **Configuration Settings** using the up or down arrow keys and press **Enter**.
2. Highlight **Host Adapter settings** using the up or down arrow keys and press **Enter**.
3. Specify CHAP settings.

**Note:** Use the **Disabled** bullet below for **i 5.4** systems (initiator CHAP is not supported on i 5.4).

- If **Enabled** is selected for work sheet item **RS10**, highlight the **Initiator Chap Name** field, type the name from work sheet item **RS11** and press **Enter**. Then highlight the **Initiator Chap Secret** field, type the name from work sheet item **RS12** and press **Enter**.
  - If **Disabled** is selected for work sheet item **RS10**, clear the **Initiator Chap Name** and **Initiator Chap Secret** fields. Highlight each field using the up or down arrow keys, press **Enter**, type in a single space and press **Enter** to clear each field.
4. Highlight **Initiator IP address by DHCP** using the up or down arrow keys and press **Enter** until the value shows **No**.
  5. Press **Esc** to return to the **Configuration Settings** menu.
  6. Highlight **ISCSI Boot Settings** using the up or down arrow keys and press **Enter**.
  7. The **iSCSI Boot Settings** menu is displayed.
  8. Highlight **Adapter Boot Mode** using the up or down arrow keys and press **Enter**.
  9. Highlight **DHCP using vendor ID** (or **DHCP** if only **DHCP** is shown on the panel) using the up or down arrow keys and press **Enter**.
  10. Highlight **Primary Boot Device Settings** using the up or down arrow keys and press **Enter**.
  11. Highlight **Security Settings** using the up or down arrow keys and press **Enter** to select. The next menu displayed is the **Primary Boot Security Settings** menu.

12. Highlight **Chap** using the up or down arrow keys and press **Enter** to change the value to **Enabled** or **Disabled**, depending on whether or not CHAP is used. Refer to work sheet item **RS7** for this information.  
Skip to step **16** if CHAP has been disabled.
13. Highlight **Chap Name** using the up or down arrow keys and press **Enter**. This will bring up the **Enter Chap Name** pane. Type the target CHAP name from work sheet item **RS8** and press **Enter**.
14. Highlight **Chap Secret** using the up or down arrow keys and press **Enter**. This will bring up the **Enter New Secret** pane. Type the target CHAP secret from work sheet item **RS9** and press **Enter**. The **Confirm New Secret** pane is then displayed. Retype the same secret and press **Enter**.
15. Highlight **Bidirectional Chap** using the up or down arrow keys.  
**Note:** Use the **Disabled** bullet below for **i 5.4** systems.
  - If **Enabled** is selected for work sheet item **RS10**, press **Enter** to change the value to **Enabled**.
  - If **Disabled** is selected for work sheet item **RS10**, press **Enter** to change the value to **Disabled**.
16. Press **Esc** to return to the **Primary Boot Device Settings** menu.
17. Press **Esc** to return to the **iSCSI Boot Settings** menu.
18. Press **Esc**. The **Configuration setting modified** pane is displayed.
19. Highlight **Save changes** using the up or down arrow keys and press **Enter**. It might take several minutes to complete the save process. When complete, the **Fast!UTIL Options** menu is displayed.
20. **Repeat** all of the above steps for each additional iSCSI initiator that must be configured for booting.

If you are done making changes to the iSCSI initiator configuration, exit the Fast!UTIL utility and restart the system. See [Ending the QLogic Fast!UTIL utility](#) for details.

**Related information:**

- [Booting over the iSCSI network](#)
- [Integrated iSCSI DHCP server](#)

### **6.3.8.1.2 Configuring additional boot iSCSI initiators with manual addr. (HW/QLogic)**

Configure the iSCSI HBA to use manual addressing. You will need to configure an IP address for the iSCSI initiator.

**Note:** For **Windows** servers, more than one iSCSI initiator port can be enabled for booting. VMware **ESX** servers are only supported with one iSCSI initiator port enabled for booting.

**Note:** This procedure starts from the **Fast!UTIL Options** menu in the configuration utility. If you need to restore this menu see [Starting the QLogic Fast!UTIL utility](#), then return to this procedure.

1. On the **Fast!UTIL Options** menu, highlight **Configuration Settings** using the up or down arrow keys and press **Enter**.
2. Highlight **Host Adapter settings** using the up or down arrow keys and press **Enter**.

3. Highlight **LUNs per Target** using the up or down arrow keys and press **Enter**. Use the arrow keys to select the value **64** and press **Enter**. This option is not available in System x adapter version 406x.
4. Highlight **Initiator IP Address via DHCP** using the up or down arrow keys and press **Enter** until the value shows **No**.

**Important:** In adapter version 406x select only the **IPv4** options for the following steps.

5. Highlight **Initiator IP address** using the up or down arrow keys and press **Enter**. Type the initiator (integrated server) SCSI internet address from work sheet item **RS15** and press **Enter**.
6. Highlight **Subnet mask** using the up or down arrow keys and press **Enter** to select. Type the iSCSI Initiator subnet mask from work sheet item **RS16** and press **Enter**.
7. Highlight **Gateway IP Address** using the up or down arrow keys and press **Enter** to select. Clear any value currently in the field or set it to blanks, then press **Enter**.
8. Highlight **Initiator iSCSI Name** using the up or down arrow keys and press **Enter** to select. Type the name from work sheet item **RS18** and press **Enter**.
9. Do one of the following:
  - Note:** Use the **Disabled** bullet below for **i 5.4** systems (initiator CHAP is not supported on i 5.4).
  - If **Enabled** is selected for work sheet item **RS10**, highlight the **Initiator Chap Name** field, type the name from item **RS11** and press **Enter**. Then highlight the **Initiator Chap Secret** field, type the name from item **RS12** and press **Enter**.
  - If **Disabled** is selected for work sheet item **RS10**, clear the **Initiator Chap Name** and **Initiator Chap Secret** fields. Highlight each field using the up or down arrow keys, press **Enter**, type in a single space and press **Enter** to clear each field.
10. Press **Esc** to return to the **Configuration Settings** menu.
11. Highlight **iSCSI Boot Settings** using the up or down arrow keys and press **Enter** to display the **iSCSI Boot Settings** menu.
12. Highlight **Adapter Boot Mode** using the up or down arrow keys and press **Enter**.
13. Highlight **Manual** using the up or down arrow keys and press **Enter**.
14. Highlight **Primary Boot Device Settings** using the up or down arrow keys and press **Enter**.
15. Highlight **Target IP** using the up or down arrow keys and press **Enter** to select. Type the target (IBM i) SCSI internet address from work sheet item **NH8** and press **Enter**.
16. Highlight **iSCSI Name** using the up or down arrow keys and press **Enter**. IBM i will generate the IQN for the target side and it must be matched here. Type the iSCSI name from work sheet item **IN11**.

**Note:** If the server system drive storage space is linked to the **multipath group** that is defined in the IBM i network server description (NWSD), then you must specify the IQN for the multipath group IBM i target, which ends with “**tm**”, instead of the IQN for a specific IBM i target, which ends with “**tp**” (where **p** is 1-4).

Next, press **Enter**.

17. Highlight **Security Settings** using the up or down arrow keys and press **Enter** to display the **Primary Boot Security Settings** menu.
18. Highlight **Chap** using the up or down arrow keys and press **Enter** to change the value to **Enabled** or **Disabled**, based on whether or not CHAP is used. Refer to work sheet item **RS7** for this information.  
Skip to step **22** if CHAP has been disabled.
19. Highlight **Chap Name** using the up or down arrow keys and press **Enter** to select. This will bring up the **Enter Chap Name** pane. Type the target CHAP name from work sheet item **RS8** and press **Enter**.
20. Highlight **Chap Secret** using the up or down arrow keys and press **Enter** to select. This will bring up the **Enter New Secret** pane. Type the target chap secret from work sheet item **RS9** and press **Enter** and confirm by retyping the same chap secret on the next pane and press **Enter**.
21. Highlight **Bidirectional Chap** using the up or down arrow keys.
  - If **Enabled** is selected for work sheet item **RS10**, press **Enter** to change the value to **Enabled**.
  - If **Disabled** is selected for work sheet item **RS10**, press **Enter** to change the value to **Disabled**.  
**Note: Disabled** is required for **i 5.4** systems.
22. Press **Esc** to return to the **Primary Boot Device Settings** menu.
23. Press **Esc** to return to the **iSCSI Boot Settings** menu.
24. Press **Esc**. The **Configuration setting modified** pane is displayed.
25. Highlight **Save changes** using the up or down arrow keys and press **Enter**. It might take several minutes to complete the save process. When complete, the **Fast!UTIL Options** menu is displayed.
26. **Repeat** all of the above steps for each additional iSCSI initiator that must be configured for booting.

If you are done making changes to the iSCSI initiator configuration, exit the Fast!UTIL utility and restart the system. See [Ending the QLogic Fast!UTIL utility](#) for details.

**Related information:**

- [Booting over the iSCSI network](#)

### 6.3.8.2 Configuring additional boot iSCSI initiators for Windows MPIO (SWI-UEFI)

Perform this task to configure additional boot iSCSI initiators for a BladeCenter blade or System x server that supports **UEFI** and uses **Ethernet NICs** as the iSCSI initiators.

**Note:** For **Windows** servers, more than one iSCSI initiator port can be enabled for booting. VMware **ESX** servers are only supported with one iSCSI initiator port enabled for booting.

**Note:** The following tasks reference items from the [IBM i iSCSI Solution Work Sheets](#). These work sheets should be filled out and available for reference while completing the tasks:

- **iSCSI initiator** work sheet. Item names from this work sheet start with “**IN**”.
- **IBM i remote system configuration** work sheet. Item names from this work sheet start with “**RS**”.

Select one of the two procedures listed below, based on the boot parameter delivery method selected in work sheet item **RS6**:

- [Configuring additional boot iSCSI initiators with dynamic addr. \(SWI-UEFI\)](#) – **Recommended**. Configure the iSCSI initiator to allow IBM i to dynamically provide IP addresses and IQNs using an [Integrated iSCSI DHCP server](#).
- [Configuring additional boot iSCSI initiators with manual addr. \(SWI-UEFI\)](#). Configure the iSCSI initiator to use manual addressing. You will need to configure an IP address for the iSCSI initiator.

#### 6.3.8.2.1 *Configuring additional boot iSCSI initiators with dynamic addr. (SWI-UEFI)*

Configure the iSCSI initiator to allow IBM i to dynamically provide IP addresses and IQNs using an [Integrated iSCSI DHCP server](#).

**Note:** For **Windows** servers, more than one iSCSI initiator port can be enabled for booting. VMware **ESX** servers are only supported with one iSCSI initiator port enabled for booting.

**Note:** This procedure starts from the **System Configuration and Boot Management** menu in the UEFI **Setup** utility. If you need to restore this menu, see [Starting the UEFI Setup utility](#), then return to this procedure.

1. Highlight **System Settings** using the up or down arrow keys and press **Enter**
2. Highlight **Network** using the up or down arrow keys and press **Enter**.
3. Highlight **iSCSI Configuration** using the up or down arrow keys and press **Enter**.
4. Highlight **iSCSI Initiator Name** using the up or down arrow keys and press **Enter** to select. Type the name from work sheet item **RS18** and press **Enter**.
5. Highlight **Add an Attempt** using the up or down arrow keys and press **Enter** to select.



6. Highlight the MAC address for the initiator you are configuring using the up and down arrow keys and press **Enter** to select.
7. Highlight **iSCSI Attempt Name** using the up or down arrow keys and press **Enter** to select. Type in a name to identify the attempt and press **Enter**.
8. Highlight **iSCSI Mode** using the up or down arrow keys and press **Enter** to select. Highlight **Enabled** and press **Enter** to select.
9. Highlight **Internet Protocol** using the up or down arrow keys and press **Enter** to select. Highlight **IP4** and press **Enter** to select.
10. Highlight **Enable DHCP** using the up or down arrow keys and press **Space** to indicate DHCP is used.
11. Highlight **Get target info via DHCP** using the up or down arrow keys and press **Space** to indicate the target information is retrieved via DHCP.
12. Highlight **Authentication Type** using the up or down arrow keys and press **Enter** to select. Highlight the correct authentication method (**CHAP** or **None**).  
If **None** was selected, skip to step **13**. Otherwise follow these steps:
  - a. Highlight **CHAP Type** using the up or down arrow keys and press **Enter** to select the appropriate CHAP type. Refer to work sheet items **RS7** and **RS10** for this information.  
**Note:** Select **One way** CHAP to use only target CHAP and select **Mutual** CHAP to use both target and initiator CHAP.
  - b. Highlight **CHAP Name** using the up or down arrow keys and press **Enter**. Type the target CHAP name from work sheet item **RS8** and press **Enter**.
  - c. Highlight **CHAP Secret** using the up or down arrow keys and press **Enter**. Type the target CHAP secret from work sheet item **RS9** and press **Enter**.  
For **One way** CHAP, skip to step **13**.
  - d. Highlight **Reverse CHAP Name** using the up or down arrow keys and press **Enter**. Type the initiator CHAP name from work sheet item **RS11** and press **Enter**.
  - e. Highlight **Reverse CHAP Secret** using the up or down arrow keys and press **Enter**. Type the initiator CHAP secret from work sheet item **RS12** and press **Enter**.
13. Highlight **Save Changes** using the up or down arrow keys and press **Enter**.
14. Highlight **Back to Previous Page** and press **Enter** to select.
15. Press **Esc** to return to the **Network** menu.
16. Highlight **Network Boot Configuration** using the up or down arrow keys and press **Enter**.
17. Highlight the MAC address for the initiator you are attempting to configure using the up and down arrow keys and press **Enter** to select.

- Highlight **PXE Mode** using the up or down arrow keys and press **Enter**. Then highlight the option below for the iSCSI mode and press **Enter** to select:

iSCSI Mode	Option	Comments
UEFI	<b>Disabled</b>	<b>Tip:</b> To improve boot time, disable PXE mode for <b>all</b> ports, including ports that are <b>not</b> used for iSCSI traffic.
Legacy	<b>Legacy Support</b>	

- Highlight the attempt under **iSCSI Mode Configuration** using the up or down arrow keys and press **Enter**. Then highlight the option below for the iSCSI mode and press **Enter** to select:

iSCSI Mode	Option
UEFI	<b>UEFI Support</b>
Legacy	<b>Legacy Support</b>

Repeat this step for any other attempts that are defined for this MAC address.

- Highlight **Save Changes** using the up or down arrow keys and press **Enter**.
- Repeat the prior 4 steps for any other MAC addresses that have attempts defined.
- Press **Esc** to return to the **Network Boot Configuration** menu.
- Press **Esc** to return to the **Network** menu.
- Press **Esc** to return to the **System Settings** menu.
- Press **Esc** to return to the **System Configuration and Boot Management** menu.
- Highlight **Save Settings** using the up or down arrow keys and press **Enter**.
- Repeat** all of the above steps for each additional iSCSI initiator that must be configured for booting.

If you are done making changes to the iSCSI initiator configuration, exit the iSCSI initiator configuration utility and restart the system. See [Ending the UEFI Setup utility](#) for details.

**Related information:**

- [Booting over the iSCSI network](#)
- [Integrated iSCSI DHCP server](#)
- ["iSCSI Mode" for booting UEFI-based servers](#)

### 6.3.8.2.2 **Configuring additional boot iSCSI initiators with manual addr. (SWI-UEFI)**

Configure the Ethernet NIC to use manual addressing. You will need to configure an IP address for the Ethernet NIC.

**Note:** For **Windows** servers, more than one iSCSI initiator port can be enabled for booting. VMware **ESX** servers are only supported with one iSCSI initiator port enabled for booting.

**Note:** This procedure starts from the **System Configuration and Boot Management** menu in the UEFI **Setup** utility. If you need to restore this menu, see [Starting the UEFI Setup utility](#), then return to this procedure.

- Highlight **System Settings** using the up or down arrow keys and press **Enter**

2. Highlight **Network** using the up or down arrow keys and press **Enter**.
3. Highlight **iSCSI Configuration** using the up or down arrow keys and press **Enter**.
4. Highlight **iSCSI Initiator Name** using the up or down arrow keys and press **Enter** to select. Type the name from work sheet item **RS18** and press **Enter**.
5. Highlight **Add an Attempt** using the up or down arrow keys and press **Enter** to select.
6. Highlight the MAC address for the initiator you are attempting to configure using the up and down arrow keys and press **Enter** to select.
7. Highlight **iSCSI Attempt Name** using the up or down arrow keys and press **Enter** to select. Type in a name to identify the attempt and press **Enter**.
8. Highlight **iSCSI Mode** using the up or down arrow keys and press **Enter** to select. Highlight **Enabled** and press **Enter** to select.
9. Highlight **Internet Protocol** using the up or down arrow keys and press **Enter** to select. Highlight **IP4** and press **Enter** to select.
10. Highlight **Initiator IP address** using the up or down arrow keys and press **Enter**. Type the initiator (integrated server) SCSI internet address from work sheet item **RS15** and press **Enter**.
11. Highlight **Initiator Subnet mask** using the up or down arrow keys and press **Enter** to select. Type the iSCSI Initiator subnet mask from work sheet item **RS16** and press **Enter**.
12. Highlight **Gateway IP Address** using the up or down arrow keys and press **Enter** to select. If it is set to something other than 0.0.0.0, reset it to **0.0.0.0**, then press **Enter**.
13. Highlight **Target Name** using the up or down arrow keys and press **Enter**. IBM i will generate the IQN for the target side and it must be matched here. Type the iSCSI name from work sheet item **IN11**.

**Note:** If the server system drive storage space is linked to the **multipath group** that is defined in the IBM i network server description (NWS), then you must specify the IQN for the multipath group IBM i target, which ends with “**tm**”, instead of the IQN for a specific IBM i target, which ends with “**tp**” (where **p** is 1-4).

Next, press **Enter**.

14. Highlight **Target IP Address** using the up or down arrow keys and press **Enter** to select. Type the target (IBM i) SCSI internet address from work sheet item **NH8** and press **Enter**.
15. Highlight **Authentication Type** using the up or down arrow keys and press **Enter** to select. Highlight the correct authentication method (**CHAP** or **None**). If **None** was selected, skip to step **16**. Otherwise follow these steps:
  - a. Highlight **CHAP Type** using the up or down arrow keys and press **Enter** to select the appropriate CHAP type. Refer to work sheet items **RS7** and **RS10** for this information.
  - b. Highlight **CHAP Name** using the up or down arrow keys and press **Enter**. Type the target CHAP name from work sheet item **RS8** and press **Enter**.

- c. Highlight **CHAP Secret** using the up or down arrow keys and press **Enter**. Type the target CHAP secret from work sheet item **RS9** and press **Enter**.  
For **One Way** CHAP skip to sub-step **16**.
- d. Highlight **Reverse CHAP Name** using the up or down arrow keys and press **Enter**. Type the initiator CHAP name from work sheet item **RS11** and press **Enter**.
- e. Highlight **Reverse CHAP Secret** using the up or down arrow keys and press **Enter**. Type the initiator CHAP secret from work sheet item **RS12** and press **Enter**.

16. Highlight **Save Changes** using the up or down arrow keys and press **Enter**.

17. Highlight **Back to Previous Page** and press **Enter** to select.

18. Press **Esc** to return to the **Network** menu.

19. Highlight **Network Boot Configuration** using the up or down arrow keys and press **Enter**.

20. Highlight the MAC address for the initiator you are attempting to configure using the up and down arrow keys and press **Enter** to select.

21. Highlight **PXE Mode** using the up or down arrow keys and press **Enter**. Then highlight the option below for the iSCSI mode and press **Enter** to select:

iSCSI Mode	Option	Comments
UEFI	Disabled	<b>Tip:</b> To improve boot time, disable PXE mode for <b>all</b> ports, including ports that are <b>not</b> used for iSCSI traffic.
Legacy	Legacy Support	

22. Highlight the attempt under **iSCSI Mode Configuration** using the up or down arrow keys and press **Enter**. Then highlight the option below for the iSCSI mode and press **Enter** to select:

iSCSI Mode	Option
UEFI	UEFI Support
Legacy	Legacy Support

Repeat this step for any other attempts that are defined for this MAC address.

23. Highlight **Save Changes** using the up or down arrow keys and press **Enter**.

24. Repeat the prior 4 steps for any other MAC addresses that have attempts defined.

25. Press **Esc** to return to the **Network Boot Configuration** menu.

26. Press **Esc** to return to the **Network** menu.

27. Press **Esc** to return to the **System Settings** menu.

28. Press **Esc** to return to the **System Configuration and Boot Management** menu.

29. Highlight **Save Settings** using the up or down arrow keys and press **Enter**.

30. **Repeat** all of the above steps for each additional iSCSI initiator that must be configured for booting.

If you are done making changes to the iSCSI initiator configuration, exit the UEFI Setup utility and restart the system. See [Ending the UEFI Setup utility](#) for details.

**Related information:**

➤ [Booting over the iSCSI network](#)

➤ [“iSCSI Mode” for booting UEFI-based servers](#)

### 6.3.9 Restoring factory defaults for an iSCSI initiator

Perform the task corresponding to your configuration method:

<b>Configuration Method</b>	<b>Task</b>
HWI-QLogic	<a href="#">Restoring factory defaults for an iSCSI initiator (HWI-QLogic)</a>
SWI-UEFI	This task is not applicable for <b>UEFI</b> -based servers that use an <b>Ethernet NIC</b> as the iSCSI initiator.
SWI-BladeBoot	This task is not applicable for blades that use <b>BladeBoot</b> technology to boot using the iSCSI protocol over <b>Ethernet NICs</b> .

#### 6.3.9.1 Restoring factory defaults for an iSCSI initiator (HWI-QLogic)

Perform this task to restore default settings for an iSCSI initiator in a BladeCenter blade or System x server that uses **QLogic iSCSI HBAs**.

**Note:** This procedure starts from the **Fast!UTIL Options** menu in the configuration utility. If you need to restore this menu, see [Starting the QLogic Fast!UTIL utility](#), then return to this procedure.

If your iSCSI initiator is not working properly or you are installing it in a new system, you can reset it to use the factory default settings.

1. On the **Fast!UTIL Options** menu, highlight **Configuration Settings** using the up or down arrow keys and press **Enter**.
2. Highlight **Restore Adapter Defaults** using the up or down arrow keys and press **Enter**.
3. On the **Restore Adapter Defaults** menu, highlight **Restore Adapter Defaults** using the up or down arrow keys and press **Enter** to restore the default settings. It might take several minutes to complete.
4. Once the operation is complete, the text in the **Restore Adapter Defaults** pane will change to **Adapter Defaults Restored**. Press any key to return to the **Configuration Settings** menu.
5. Press **Esc** to return to the **Fast!UTIL Options** menu.

If you are done making changes to the iSCSI initiator configuration, exit the Fast!UTIL utility and restart the system. See [Ending the QLogic Fast!UTIL utility](#) for details.

## 6.3.10 Resetting cached iSCSI initiator configuration information

Perform the task corresponding to your configuration method:

Configuration Method	Task
HWI-QLogic	<a href="#">Resetting cached iSCSI initiator configuration information (HWI-QLogic)</a>
SWI-UEFI	This task is not applicable for <b>UEFI</b> -based servers that use an <b>Ethernet NIC</b> as the iSCSI initiator.
SWI-BladeBoot	This task is not applicable for blades that use <b>BladeBoot</b> technology to boot using the iSCSI protocol over <b>Ethernet NICs</b> .

### 6.3.10.1 Resetting cached iSCSI initiator configuration information (HWI-QLogic)

Perform this task to reset iSCSI initiator configuration information that is stored in a BladeCenter blade or System x server **QLogic iSCSI HBA**.

**Important:** performing this procedure will likely erase iSCSI boot information, making it necessary to reconfigure the boot iSCSI initiator settings.

**Note:** This procedure starts from the **Fast!UTIL Options** menu in the configuration utility. If you need to restore this menu, see [Starting the QLogic Fast!UTIL utility](#), then return to this procedure.

Do these steps to reset iSCSI initiator configuration information.

1. On the **Fast!UTIL Options** menu, highlight **Configuration Settings** using the up or down arrow keys and press **Enter**.
2. Highlight **Clear persistent targets** using the up or down arrow keys and press **Enter**.
3. On the next screen, highlight **Clear Persistent Targets** using the up or down arrow keys and press **Enter**. The text in the **Clear Persistent Targets** pane will change to **Clearing Persistent Targets** while the clear is in progress. It might take several minutes to complete.
4. Once the clear is complete, the text in the **Clear Persistent Targets** pane will change to **Persistent Targets Cleared**. Press any key to return to the **Configuration Settings** menu.
5. Press **Esc** to return to the **Fast!UTIL Options** menu.

If you are done making changes to the iSCSI initiator configuration, exit the Fast!UTIL utility and restart the system. See [Ending the QLogic Fast!UTIL utility](#) for details.

### 6.3.11 Verifying the iSCSI connection using ping

Perform the task corresponding to your configuration method:

Configuration Method	Task
HWI-QLogic	<a href="#">Verifying the iSCSI connection using ping (HWI-QLogic)</a>
SWI-UEFI	This task is not applicable for <b>UEFI</b> -based servers that use an <b>Ethernet NIC</b> as the iSCSI initiator.
SWI-BladeBoot	This task is not applicable for blades that use <b>BladeBoot</b> technology to boot using the iSCSI protocol over <b>Ethernet NICs</b> .

#### 6.3.11.1 Verifying the iSCSI connection using ping (HWI-QLogic)

Perform this task to verify that an iSCSI initiator on the BladeCenter blade or System x server can communicate with an iSCSI target on the IBM i system over the iSCSI network. This task applies to a BladeCenter blade or System x server that uses **QLogic iSCSI HBAs**.

**Note:** This procedure starts from the **Fast!UTIL Options** menu in the configuration utility. If you need to restore this menu, see [Starting the QLogic Fast!UTIL utility](#), then return to this procedure.

Before you can use the ping utility, the iSCSI initiator must have an IP address. If you have already configured and know the IP address of the iSCSI initiator, continue with the rest of the procedure. To set the IP address, choose one of the two following options:

- If you are configuring the iSCSI initiator with dynamic addressing, see [Configuring a boot iSCSI initiator for dynamic addressing](#).
- If you are configuring the iSCSI initiator with manual addressing, see [Configuring a boot iSCSI initiator for manual addressing](#).

**Note:** If you have configured the iSCSI initiator to use dynamic addressing (DHCP), the network server description (NWSD) for the server must be started. This enables the integrated iSCSI DHCP server on IBM i to provide the IP address to the iSCSI initiator.

Use the following steps to access the ping utility to verify the physical connection of the BladeCenter blade or System x server to the IBM i system.

1. On the **Fast!UTIL Options** menu, highlight **Ping Utility** and press **Enter**.
2. Highlight the values for **Target IP** and press **Enter** to select. A red **Enter IP Address** pane is displayed.
3. Type the IP address of the iSCSI target adapter on the IBM i system into the **Enter IP Address** pane and press **Enter**. The **Enter IP Address** pane disappears and the address just entered is displayed in the **Target IP** field on the **Ping Utility** pane.
4. Highlight **Ping Target** and press **Enter** to perform the ping. A small pane will open with the results of the ping:
  - **Ping successful:** verifies the path from the BladeCenter blade or System x server iSCSI initiator to the IBM i iSCSI target.

- **Ping unsuccessful:** means the path from the BladeCenter blade or System x server iSCSI initiator to the IBM i iSCSI target cannot be verified. This may occur when the Ping Target is an iSCSI initiator LAN IP address in a different subnet, but on the same switched network as the BladeCenter blade or System x server iSCSI initiator used to send the ping.

5. Press **Enter** to close the ping utility pane.
6. Press **Esc** to return to the **Fast!UTIL Options** menu.

If you are done, exit the Fast!UTIL utility. See [Ending the QLogic Fast!UTIL utility](#) for details.

**Related information:**

- [Integrated iSCSI DHCP server](#)

## 6.3.12 Configuring target CHAP

Perform the task corresponding to your configuration method:

Configuration Method	Task
HWI-QLogic	<a href="#">Configuring target CHAP (HWI-QLogic)</a>
SWI-UEFI	<a href="#">Configuring target CHAP (SWI-UEFI)</a>
SWI-BladeBoot	<a href="#">Configuring a boot iSCSI initiator port (SWI-BladeBoot)</a>

### 6.3.12.1 Configuring target CHAP (HWI-QLogic)

Perform this task to configure the iSCSI initiator to authenticate the iSCSI target for a BladeCenter blade or System x server that uses **QLogic iSCSI HBAs**.

**Note:** This procedure starts from the **Fast!UTIL Options** menu in the configuration utility. If you need to restore this menu, see [Starting the QLogic Fast!UTIL utility](#), then return to this procedure.

1. Select the iSCSI initiator port that is configured to boot the integrated server operating system.
2. Enter the target CHAP name and secret from the remote system configuration properties into the CHAP name and secret fields of the target security configuration panel.

**Note:** Do not enter this information into the initiator configuration panel.

**Note:** For integrated servers running Windows, any non-boot iSCSI HBAs in the hosted system are automatically configured from the IBM i configuration.

If you are done making changes to the iSCSI initiator configuration, exit the Fast!UTIL utility and restart the system. See [Ending the QLogic Fast!UTIL utility](#) for details.



### 6.3.12.2 Configuring target CHAP (SWI-UEFI)

Perform this task to configure the iSCSI initiator to authenticate the iSCSI target for a BladeCenter blade or System x server that supports **UEFI** and uses **Ethernet NICs** as the iSCSI initiators.

**Note:** This procedure starts from the **System Configuration and Boot Management** menu in the UEFI **Setup** utility. If you need to restore this menu, see [Starting the UEFI Setup utility](#), then return to this procedure.

1. Highlight **System Settings** using the up or down arrow keys and press **Enter**.
2. Highlight **Network** using the up or down arrow keys and press **Enter**.
3. Highlight **iSCSI Configuration** using the up or down arrow keys and press **Enter**.
4. Highlight the attempt you wish to add the target CHAP credentials to using the up or down arrow keys and press **Enter**.
5. Highlight **CHAP Type** using the up or down arrow keys and press **Enter**.
6. Highlight **One Way** using the up or down arrow keys and press **Enter**.
7. Enter the target CHAP name and secret from the remote system configuration properties into the **CHAP Name** and **CHAP Secret** fields.
8. Highlight **Save Changes** using the up or down arrow keys and press **Enter**.
9. Press **Esc** to return to the **iSCSI Configuration** menu.
10. Press **Esc** to return to the **Network** menu.
11. Press **Esc** to return to the **System Settings** menu.
12. Press **Esc** to return to the **System Configuration and Boot Management** menu.
13. Highlight **Save Settings** using the up or down arrow keys and press **Enter**.

**Note:** For integrated servers running Windows, any non-boot iSCSI HBAs in the hosted system are automatically configured from the IBM i configuration.

If you are done making changes to the iSCSI initiator configuration, exit the iSCSI initiator configuration utility and restart the system. See [Ending the UEFI Setup utility](#) for details.

### 6.3.13 Configuring initiator CHAP

Perform the task corresponding to your configuration method:

Configuration Method	Task
HWI-QLogic	<a href="#">Configuring initiator CHAP (HWI-QLogic)</a>
SWI-UEFI	<a href="#">Configuring initiator CHAP (SWI-UEFI)</a>
SWI-BladeBoot	<a href="#">Configuring a boot iSCSI initiator port (SWI-BladeBoot)</a>

#### 6.3.13.1 Configuring initiator CHAP (HWI-QLogic)

Perform this task to configure the iSCSI target to authenticate the iSCSI initiator for a BladeCenter blade or System x server that uses **QLogic iSCSI HBAs**.

**Note:** This procedure starts from the **Fast!UTIL Options** menu in the configuration utility. If you need to restore this menu, see [Starting the QLogic Fast!UTIL utility](#), then return to this procedure.

1. Select the iSCSI initiator port that is configured to boot the integrated server operating system.
2. Enter the initiator CHAP name and secret from the remote system configuration properties into the CHAP name and secret fields of the CTRL-Q initiator security configuration panel. Do not enter this information into the CTRL-Q target configuration panel.

If you are done making changes to the iSCSI initiator configuration, exit the Fast!UTIL utility and restart the system. See [Ending the QLogic Fast!UTIL utility](#) for details.

#### 6.3.13.2 Configuring initiator CHAP (SWI-UEFI)

Perform this task to configure the iSCSI target to authenticate the iSCSI initiator for a BladeCenter blade or System x server that supports **UEFI** and uses **Ethernet NICs** as the iSCSI initiators.

**Note:** This procedure starts from the **System Configuration and Boot Management** menu in the **UEFI Setup** utility. If you need to restore this menu, see [Starting the UEFI Setup utility](#), then return to this procedure.

1. Highlight **System Settings** using the up or down arrow keys and press **Enter**.
2. Highlight **Network** using the up or down arrow keys and press **Enter**.
3. Highlight **iSCSI Configuration** using the up or down arrow keys and press **Enter**.
4. Highlight the attempt you wish to add the initiator CHAP credentials to using the up or down arrow keys and press **Enter**.
5. Highlight **CHAP Type** using the up or down arrow keys and press **Enter**.
6. Highlight **Mutual** using the up or down arrow keys and press **Enter**.
7. Enter the target CHAP name and secret from the remote system configuration properties into the **CHAP Name** and **CHAP Secret** fields.

8. Enter the initiator CHAP name and secret from the remote system configuration properties into the **Reverse CHAP Name** and **Reverse CHAP Secret** fields.
9. Highlight **Save Changes** using the up or down arrow keys and press **Enter**.
10. Press **Esc** to return to the **iSCSI Configuration** menu.
11. Press **Esc** to return to the **Network** menu.
12. Press **Esc** to return to the **System Settings** menu.
13. Press **Esc** to return to the **System Configuration and Boot Management** menu.
14. Highlight **Save Settings** using the up or down arrow keys and press **Enter**.

If you are done making changes to the iSCSI initiator configuration, exit the iSCSI initiator configuration utility and restart the system. See [Ending the UEFI Setup utility](#) for details.

### 6.3.14 Changing the iSCSI initiator CHAP secret

Perform the task corresponding to your configuration method:

Configuration Method	Task
HWI-QLogic	<a href="#">Changing the iSCSI initiator CHAP secret (HWI-QLogic)</a>
SWI-UEFI	<a href="#">Changing the iSCSI initiator CHAP secret (SWI-UEFI)</a>
SWI-BladeBoot	<a href="#">Configuring a boot iSCSI initiator port (SWI-BladeBoot)</a>

#### 6.3.14.1 Changing the iSCSI initiator CHAP secret (HWI-QLogic)

Perform this task to change the CHAP secret that is stored in the iSCSI initiator settings for a BladeCenter blade or System x server that uses **QLogic iSCSI HBAs**.

The generation of a CHAP secret can be deferred to when the IBM i remote system configuration object is created. This can be done when using either dynamic or manual addressing. This section provides a procedure for updating the CHAP secret once the initial configuration has already been done.

**Note:** The following tasks reference items from the [IBM i iSCSI Solution Work Sheets](#). These work sheets should be filled out and available for reference while completing the tasks:

- **iSCSI initiator** work sheet. Item names from this work sheet start with “**IN**”.
- **IBM i remote system configuration** work sheet. Item names from this work sheet start with “**RS**”.

**Note:** If you have previously set the challenge handshake authentication protocol (CHAP) secret and plan to change it you must know the original CHAP secret. If you do not know the original CHAP secret, you will need to restore the factory defaults and reconfigure the iSCSI initiator. Refer to **Restoring factory defaults for an iSCSI initiator**, then refer to [Configuring a boot iSCSI initiator port \(HWI-QLogic\)](#) in this case.

**Note:** This procedure starts from the **Fast!UTIL Options** menu in the configuration utility. If you need to restore this menu, see [Starting the QLogic Fast!UTIL utility](#), then return to this procedure.

1. On the **Fast!UTIL Options** menu, highlight **Configuration Settings** using the up or down arrow keys and press **Enter**.
2. **Highlight Host Adapter** settings using the up or down arrow keys and press **Enter**.
3. If **Enabled** is selected for work sheet item **RS10**, highlight the Initiator Chap Name field, type the name from work sheet item **RS11** and press **Enter**. Then highlight the **Initiator Chap Secret** field, type the name from work sheet item **RS12** and press **Enter**.  
**Note:** Ignore this step for **i 5.4** systems.
4. Press **Esc** to return to the **Configuration Settings** menu.
5. Highlight **iSCSI Boot Settings** using the up or down arrow keys and press **Enter** to display the **iSCSI Boot Settings** menu.
6. Highlight **Primary Boot Device Settings** using the up or down arrow keys and press **Enter**.

7. Highlight **Security Settings** using the up or down arrow keys and press **Enter** to select. The next menu displayed is the **Primary Boot Security Settings** menu
8. Highlight **Chap** using the up or down arrow keys and press **Enter** to change the value to **Enabled**, if necessary.
9. Highlight **Chap Name** using the up or down arrow keys and press **Enter** to select. This will bring up the **Enter Chap Name** pane. Type the target CHAP name if this hasn't been previously done, using work sheet item **RS8** and press **Enter**.
10. Highlight **Chap Secret** using the up or down arrow keys and press **Enter**. If CHAP was previously configured, the **Enter Old Secret** pane is displayed. Type the original CHAP secret and press **Enter**. At this point, in either case the **Enter New Secret** pane is displayed. Type the target chap secret from work sheet item **RS9** and press **Enter**. The **Confirm New Secret** pane is then displayed. Retype the same secret and press **Enter**.

**Remember:** The Chap secret is case sensitive.

11. Highlight **Bidirectional Chap** using the up or down arrow keys.

**Note:** Use the **Disabled** bullet below for **i 5.4** systems.

- If **Enabled** is selected for work sheet item **RS10**, press **Enter** to change the value to **Enabled**.
- If **Disabled** is selected for work sheet item **RS10**, press **Enter** to change the value to **Disabled**.

12. Press **Esc** to return to the **Primary Boot Device Settings** menu.

13. Press **Esc** to return to the **iSCSI Boot Settings** menu.

14. Press **Esc**. The **Configuration setting modified** pane is displayed.

15. Highlight **Save changes** using the up or down arrow keys and press **Enter**. It might take several minutes to complete the save process. When complete, the **Fast!UTIL Options** menu is displayed.

If you are done making changes to the iSCSI initiator configuration, exit the Fast!UTIL utility and restart the system. See [Ending the QLogic Fast!UTIL utility](#) for details.

### 6.3.14.2 Changing the iSCSI initiator CHAP secret (SWI-UEFI)

Perform this task to change the CHAP secret that is stored in the iSCSI initiator settings for a BladeCenter blade or System x server that supports **UEFI** and uses **Ethernet NICs** as the iSCSI initiators. The procedure for changing the CHAP secret is the same as initially configuring it. See [Configuring initiator CHAP \(SWI-UEFI\)](#) for details.

**Note:** The generation of a CHAP secret can be deferred to when the IBM i remote system configuration object is created. This can be done when using either dynamic or manual addressing. This section provides a procedure for updating the CHAP secret once the initial configuration has already been done.

## 6.3.15 Changing the iSCSI initiator MTU

**Attention:** Before configuring jumbo (9000 byte) frames, verify that all components of your iSCSI network support jumbo frames. If you try to install an integrated server using jumbo frames and the installation fails, it could be a sign that your network hardware does not support jumbo frames.

Perform the task corresponding to your configuration method:

Configuration Method	Task
HWI-QLogic	<a href="#">Changing the iSCSI initiator MTU (HWI-QLogic)</a>
SWI-UEFI	<a href="#">Changing the iSCSI initiator MTU (SWI-UEFI)</a>
SWI-BladeBoot	This task is not applicable for blades that use <b>BladeBoot</b> technology to boot using the iSCSI protocol over <b>Ethernet NICs</b> .

### 6.3.15.1 Changing the iSCSI initiator MTU (HWI-QLogic)

Perform this task to change the iSCSI initiator maximum transmission unit (MTU) settings for a BladeCenter blade or System x server that uses **QLogic iSCSI HBAs**.

**Note:** The following tasks reference items from the [IBM i iSCSI Solution Work Sheets](#). These work sheets should be filled out and available for reference while completing the tasks:

- **iSCSI initiator** work sheet. Item names from this work sheet start with “**IN**”.

**Note:** This procedure starts from the **Fast!UTIL Options** menu in the configuration utility. If you need to restore this menu, see [Starting the QLogic Fast!UTIL utility](#), then return to this procedure.

1. On the **Fast!UTIL Options** menu, highlight Configuration Settings using the up or down arrow keys and press **Enter**.
2. Highlight **Advanced Adapter Settings** using the up or down arrow keys and press **Enter**.
3. Highlight **MTU** using the up or down arrow keys and press **Enter** until the value shows the desired frame size setting from work sheet item **IN16**.
4. Press **Esc**. The **Configuration setting modified** pane is displayed.
5. Highlight **Save changes** using the up or down arrow keys and press **Enter**. It might take several minutes to complete the save process. When complete, the **Fast!UTIL Options** menu is displayed.

If you are done making changes to the iSCSI initiator configuration, exit the Fast!UTIL utility and restart the system. See [Ending the QLogic Fast!UTIL utility](#) for details.

### 6.3.15.2 Changing the iSCSI initiator MTU (SWI-UEFI)

Perform this task to configure iSCSI initiator Maximum Transmission Unit (MTU) settings for a BladeCenter blade or System x server that supports **UEFI** and uses **Ethernet NICs** as the iSCSI initiators.

**Note:** Not all adapters support jumbo frames. Refer to the adapter documentation for information regarding support for jumbo frames.

**Note:** This procedure starts from the Microsoft Windows **Network Connections** panel.

1. **Right-click** the **Network Adapter** you wish to configure the MTU settings on.
2. Select **Properties**.
3. Click **Configure**.
4. Select the **Advanced** tab.
5. Modify the **Jumbo MTU** setting to the desired value. By default this parameter is 1500 bytes. When modifying this value use 500-byte increments up to 9000 bytes.

### 6.3.16 Disabling iSCSI header and data digests

Perform the task corresponding to your configuration method:

Configuration Method	Task
HWI-QLogic	<a href="#">Disabling iSCSI header and data digests (HWI-QLogic)</a>
SWI-UEFI	This task is not applicable when using software initiators. iSCSI header and data digests are turned off by default when using software initiators.
SWI-BladeBoot	

#### 6.3.16.1 Disabling iSCSI header and data digests (HWI-QLogic)

Perform this task to turn off iSCSI header and data digests when using a **QLogic iSCSI HBA hardware initiator** to connect to an **Ethernet NIC software target** on IBM i.

**Note:** Software targets are only supported on IBM i 6.1 and later. Disabling digests improves IBM i performance when using a software target. However, iSCSI digests do not impact IBM i performance when using a hardware target, so it is not necessary to turn off iSCSI digests when using a hardware target.

**Note:** This procedure starts from the **Fast!UTIL Options** menu in the configuration utility for the **first** initiator port. If you need to restore this menu, see [Starting the QLogic Fast!UTIL utility](#), then return to this procedure.

1. On the **Fast!UTIL Options** menu, highlight **Configuration Settings** using the up or down arrow keys and press **Enter**.
2. On the **Configuration Settings** menu, highlight **Advanced Adapter Settings** using the up or down arrow keys and press **Enter**.
3. Select **Primary Boot Data Digest** and press **Enter** until the setting is **Disabled**.
4. Select **Primary Boot Header Digest** and press **Enter** until the setting is **Disabled**.
5. Press **Esc**. The **Configuration setting modified** pane is displayed.
6. Highlight **Save changes** using the up or down arrow keys and press **Enter**. It might take several minutes to complete the save process. When complete, the **Fast!UTIL Options** menu is displayed.
7. If there are multiple hardware initiator ports, repeat the above procedure for each hardware initiator port. Use the **Select Host Adapter** option on the **Fast!UTIL Options** menu to switch between hardware initiator ports.

If you are done making changes to the iSCSI initiator configuration, exit the Fast!UTIL utility and restart the system. See [Ending the QLogic Fast!UTIL utility](#) for details.



### 6.3.17 Ending the iSCSI initiator configuration utility

Perform the task corresponding to your configuration method:

Configuration Method	Task
HWI-QLogic	<a href="#">Ending the QLogic Fast!UTIL utility</a>
SWI-UEFI	<a href="#">Ending the UEFI Setup utility</a>
SWI-BladeBoot	<a href="#">Ending the iSCSI Configuration Manger utility (SWI-BladeBoot)</a>

#### 6.3.17.1 Ending the QLogic Fast!UTIL utility

Perform this task to exit the QLogic Fast!UTIL utility.

**Note:** This procedure starts from the **Fast!UTIL Options** menu. If you need to restore this menu, see [Starting the QLogic Fast!UTIL utility](#), then return to this procedure.

1. Press **Esc** on the **Fast!UTIL Options** menu.
2. Highlight **Reboot System** using the up or down arrow keys and press **Enter**.

The BladeCenter blade or System x server restarts. Turn off the server. Refer to the BladeCenter or System x hardware documentation to complete this step.

#### 6.3.17.2 Ending the UEFI Setup utility

Perform this task to exit the **UEFI Setup** utility.

**Note:** This procedure starts from the **System Configuration and Boot Management** menu. If you need to restore this menu, see [Starting the UEFI Setup utility](#), then return to this procedure.

1. Highlight **Exit Setup** using the up or down arrow keys and press **Enter**.
2. A dialog asking for confirmation to exit the **Setup Utility** is presented. Type **y** to exit **Setup**.

The BladeCenter blade or System x server continues with the boot process. Turn off the system. Refer to the BladeCenter or System x hardware documentation to complete this step.

#### 6.3.17.3 Ending the iSCSI Configuration Manger utility (SWI-BladeBoot)

After doing the **Flash NVS on Blade(s)** on the last **Advanced configuration** page, just click **Finished**. The utility will ask if you want to save the configuration given before exiting. It is recommended to save the configuration for later use.

## 6.4 Setting the integrated server start options

Configure the server start options, depending on the type of firmware your server uses:

Server Firmware	Task
UEFI	<a href="#">Setting the integrated server start options (UEFI)</a>
BIOS	<a href="#">Setting the integrated server start options (BIOS)</a>

### Related information:

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

### 6.4.1 Setting the integrated server start options (UEFI)

Perform this task to configure the start options in the **UEFI Setup** utility for a BladeCenter blade or System x server that uses **UEFI** firmware.

**Note:** This procedure starts from the **System Configuration and Boot Management** menu in the **UEFI Setup** utility. If you need to restore this menu, see [Starting the UEFI Setup utility](#), then return to this procedure.

1. Highlight **System Settings** using the up or down arrow keys and press **Enter**.
  - a) Highlight **Devices and I/O Ports** using the up or down arrow keys and press **Enter**.
    1. Highlight **Enable / Disable onboard device(s)** using the up or down arrow keys and press **Enter**.
    2. Select **SAS controller** using the up or down arrow keys and select the option to disable it. **Note:** If a SAS controller is not shown, you can skip this step.
    3. Press **Esc** two times to return to the **System Settings** menu.

#### b) HWI-QLogic only:

Highlight **Network** using the up or down arrow keys and press **Enter**.

1. Highlight **PXE Configuration** using the up or down arrow keys and press **Enter**.

Select the first port using the up or down arrow keys and press **Enter**.  
Select **Enable PXE** using the up or down arrow keys and press **Enter**.  
Select **Disabled** using the up or down arrow keys and press **Enter**.  
Select **Save Changes** using the up or down arrow keys and press **Enter**.  
Press **Esc** to return to the **PXE Configuration** menu.

**Disable** any other ports by repeating the above process for each port.

2. Press **Esc** two times to return to the **System Settings** menu.

- c) Press **Esc** to return to the **System Configuration and Boot Management** menu.

2. Highlight **Date and Time** using the up or down arrow keys and press **Enter**.
  - a) Set the system date and time.
  - b) Press **Esc** to return to the **System Configuration and Boot Management** menu.

3. Highlight **Boot Manager** using the up or down arrow keys and press **Enter**.

- a) Highlight **Add Boot Option** using the up or down arrow keys and press **Enter**.

1. Highlight **Generic Boot Option** using the up or down arrow keys and press **Enter**.

- a. Perform one of the following tasks, depending on the iSCSI mode used for booting:

iSCSI Mode	Task
UEFI	If <b>iSCSI</b> is listed, highlight it using the up or down arrow keys and press <b>Enter</b> .
Legacy	If <b>Legacy Only</b> is listed, highlight it using the up or down arrow keys and press <b>Enter</b> .

- b. If **CD/DVD Rom** is listed, highlight it using the up or down arrow keys and press **Enter**.

- c. If **Floppy Disk** is listed, highlight it using the up or down arrow keys and press **Enter**.

- d. Perform one of the following tasks, depending on the server operating system (OS):

Server OS	Task
ESXi Embedded	If <b>Embedded Hypervisor</b> is listed, highlight it using the up or down arrow keys and press <b>Enter</b> .
All Other OS's	If <b>Hard Disk 0</b> is listed, highlight it using the up or down arrow keys and press <b>Enter</b> .

- e. Press **Esc** to return to the **Add Boot Option** menu.

2. Press **Esc** to return to the **Boot Manager** menu.

- b) **HWI-QLogic only:**

Highlight <b>Delete Boot Option</b> using the up or down arrow keys and press <b>Enter</b> .
1. Select <b>PXE Network</b> using the up or down arrow keys and press the <b>Space Bar</b> key to delete it.
2. Highlight <b>Commit Changes</b> using the up or down arrow key and press <b>Enter</b> .
3. Press <b>Esc</b> to return to the <b>Boot Manager</b> menu.

c) Highlight **Change Boot Order** using the up or down arrow keys and press **Enter**.

1. The list of available boot options is highlighted, press **Enter**.
2. Order the boot options as listed below, depending on the [iSCSI Mode](#) and your server operating system (OS).

<a href="#">iSCSI Mode</a>	Boot Order	ESXi Embedded	All Other OS's
UEFI	First device	iSCSI	iSCSI
	Second device	CD/DVD Rom	CD/DVD Rom
	Third device	Floppy Disk	Floppy Disk
	Fourth device	Embedded Hypervisor	Hard Disk 0
Legacy	First device	Legacy Only	Legacy Only
	Second device	CD/DVD Rom	CD/DVD Rom
	Third device	Floppy Disk	Floppy Disk
	Fourth device	Embedded Hypervisor	Hard Disk 0

**Note:** To order the list, select the boot option using the up or down arrow keys and press the **+** or **-** key to move the boot option up or down in the list and press **Enter**.

3. Highlight **Commit Changes** using the up or down arrow key and press **Enter**.
4. Press **Esc** to return to the **Boot Manager** menu.

d) Highlight **Boot Modes** using the up or down arrow keys and press **Enter**.

**Note:** You might need to page down to see the **Boot Modes** item.

1. Highlight **System Boot Mode** using the up or down arrow keys and press **Enter**.
2. Highlight one of the following **System Boot Mode** values, depending on the [iSCSI Mode](#):

<a href="#">iSCSI Mode</a>	Value to Highlight
UEFI	UEFI Only
Legacy	Legacy Only

Then press **Enter**.

3. Press **Esc** to return to the **Boot Manager** menu.

e) Press **Esc** to return to the **System Configuration and Boot Management** menu.

4. Highlight **Save Settings** using the up or down arrow keys and press **Enter**.

If you are done making changes to the UEFI configuration, exit the UEFI Setup utility and restart the system. See [Ending the UEFI Setup utility](#) for details.

**Related information:**

- [Installation Checklist](#)
- [Clone Server Hardware Checklist](#)
- ["iSCSI Mode" for booting UEFI-based servers](#)

## 6.4.2 Setting the integrated server start options (BIOS)

Perform this task to configure the start options in the **BIOS Setup** utility for a BladeCenter blade or System x server that uses **BIOS** firmware.

1. Power on the integrated server. Refer to the server documentation to complete this step.
2. Press **F1** when prompted, shortly after the IBM logo appears on the display, to enter the **BIOS Configuration/Setup Utility**.
3. Highlight **Load Default Settings** using the up or down arrow keys and press the **Enter** key twice.
4. Highlight **Date and Time** using the up or down arrow keys and press **Enter**.
  - a) Set the system date and time.
  - b) Press **Esc** to return to the **Configuration/Setup Utility** menu.
5. If a **Devices and I/O Ports** option is available, highlight it and press **Enter**.
  - a) Highlight **Planar SAS** (or **Planar SATA** or **Planar SCSI**, depending on your server model) using the up or down arrow keys. Using the right or left arrow keys, select **Disabled**.
  - b) Press **Esc** to return to the **Configuration/Setup Utility** menu.
6. Highlight **Start Options** using the up or down arrow keys and press **Enter**.
  - a) Highlight **Startup Sequence Options** using the up or down arrow keys and press **Enter**.
    1. Under the **Primary Startup Sequence**, using the right or left arrow keys, select the following devices, depending on your iSCSI initiator configuration method:

Startup Sequence	Configuration Method	
	HWI-QLogic	SWI-BladeBoot
First Startup Device:	CD ROM (or DVD)	CD ROM (or DVD)
Second Startup Device:	Diskette Drive 0	Diskette Drive 0
Third Startup Device:	Hard Disk 0	iSCSI

2. Press the **Esc** key to exit out of the **Startup Sequence Options**.
- b) Do **one** of the following, depending on your iSCSI initiator configuration method:

Configuration Method	Tasks
HWI-QLogic	<ol style="list-style-type: none"> <li>1. Highlight <b>Planar Ethernet PXE/DHCP</b> using the up or down arrow keys. Using the right or left arrow keys, select <b>Disabled</b>.</li> <li>2. Highlight <b>PCI Device Boot Priority</b> using the up or down arrow keys. Using the right or left arrow keys, select the slot where the iSCSI adapter is installed.</li> </ol>
SWI-BladeBoot	<ol style="list-style-type: none"> <li>1. Highlight <b>Planar Ethernet PXE/DHCP</b>. Select the correct Planar Ethernet device by pressing the right or left arrow keys.</li> <li>2. Highlight <b>iSCSI Initiator</b> using the up or down arrow keys. Using the right or left arrow keys select <b>Enabled</b>.</li> </ol>

- c) Highlight **Boot Fail Count** using the up or down arrow keys. Using the right or left arrow keys, select **Disabled**.
  - d) Highlight **Virus Detection** using the up and down arrow keys. Using the right or left arrow keys, select **Disabled**.
  - e) Press the **Esc** key to exit out of the **Startup Options**.
7. Highlight **Save Settings** using the up or down arrow keys and press **Enter** twice.
8. Press the **Esc** key, then confirm to exit the **Configuration/Setup Utility**.

**Related information:**

➤ [Installation Checklist](#)

➤ [Clone Server Hardware Checklist](#)

## 7 Additional topics

This chapter contains various topics related to the IBM i iSCSI solution.

### 7.1 Installing IBM i integration service packs

Once the integrated server support service pack PTF is installed on IBM i, it must then be installed or synchronized on each integrated server as follows:

Server OS	IBM i	Service Pack Installation Methods	
Windows	All	<a href="#">Updating the integration software running on Microsoft Windows</a>	
ESX	i 7.2	<a href="#">Updating the integration software running on Microsoft Windows</a>	
	i 7.1	<a href="#">Updating the integration software running on Microsoft Windows</a>	
	i 6.1	<a href="#">Management server based infrastructure</a>	<a href="#">Updating the integration software running on Microsoft Windows</a>
		<a href="#">Service console based infrastructure</a>	<a href="#">Updating the integration software: ESX service console</a>
i 5.4	<a href="#">Updating the integration software: ESX service console</a>		

**Related information:**

- [Software updates](#)
- [IBM i PTFs](#)
- [Service pack PTFs](#)

#### 7.1.1 Determining the integration software level

Do these steps from the IBM i GUI to display the service level for the integrated server support software on the integrated server:

1. Select **Integrated Server Administration** from the [Web GUI](#) or [System i Navigator](#).
2. Select **Servers**.
3. Select **Properties** from the context menu of the integrated Windows server you want to synchronize.
4. Click the **Software** tab. The software levels are displayed there.

**Tip:** If you want to use a CL command, see:

- [Work with NWS Status \(WRKNWSSTS\)](#)

**Related information:**

- [Software updates](#)
- [Installing IBM i integration service packs](#)
- [IBM i PTFs](#)
- [Service pack PTFs](#)

## 7.1.2 Updating the integration software running on Microsoft Windows

Once an integrated Windows server service pack PTF is installed on IBM i, you must then install it on each integrated Windows server using one of the methods in the following sections.

**Attention:** 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 end applications, you risk data loss because the integrated server might require a restart after completing the installation.

**Note:** Updating the integration software requires that IBM i NetServer is set up. The user who performs the update must also have sufficient authority to copy the updates to the integrated Windows server. See [Installing and configuring IBM i NetServer](#) in the Information Center.

### 7.1.2.1 Updating the integration software: Windows server console

Do these steps on the integrated Windows server console to update the integrated server support software on the integrated Windows server:

1. i 7.2 or 7.1: Click **Start > All Programs > IBM i > IBM i Integrated Server Support**  
i 6.1 or 5.4: Click **Start > All Programs > IBM iSeries > IBM iSeries Integrated Server Support**
2. Expand **Integrated Server Support**
3. Expand the network server description name.
4. Select **Software Level**. The Integrated Server Support software level on IBM i and on the integrated Windows server is shown.
5. Click **Synchronize** to bring the Integrated Server Support software on Windows to the same level as on IBM i.

If the installation is performed successfully, a confirmation message appears. When the synchronization process is complete, the server automatically reboots to apply the updates, if necessary.

**Note:** If you log on to the integrated Windows server console as an administrator and there is a software level mismatch, you are automatically prompted to synchronize the software.

**Tip:** If you want to use a character based command, see [Updating the integration software: lvsync](#).

#### Related information:

- [Software updates](#)
- [Installing IBM i integration service packs](#)
- [IBM i PTFs](#)
- [Service pack PTFs](#)



### 7.1.2.1.1 Updating the integration software: lvlsync

You can use the `lvlsync` command to update the integration software that is installed on the Windows server.

Entering the command `lvlsync` at an integrated Windows server console command prompt will cause the integrated server to synchronize.

When the synchronization process is complete, the server automatically reboots to apply the updates, if necessary.

**Note:** If you run `lvlsync` from within a program, the following `lvlsync` error codes are provided:

Error Code	Error Description
0	No errors
1	Must be an administrator to run lvlsync
2	Release level on integrated Windows server higher than on IBM i
3	Service pack level on integrated server higher than on IBM i
4	Cannot install release from IBM i - language files not on IBM i
5	Syntax not valid
6	Cannot access service pack information on IBM i
7	Cannot map network drive
8	Cannot access service pack information in registry
9	Cannot open qvnacfg.txt file
10	No service pack installed on IBM i
11	NWSD not found
13	NWSD not active
20	No service pack available on IBM i
21	Cannot start InstallShield application
31	Unexpected error while starting lvlsync
44	Unexpected error during lvlsync

#### Related information:

- [Software updates](#)
- [Installing IBM i integration service packs](#)
- [IBM i PTFs](#)
- [Service pack PTFs](#)

### 7.1.2.2 Updating the integration software: IBM i GUI

Do these steps from the IBM i GUI to update the integrated server support software on the integrated Windows server:

1. Select **Integrated Server Administration** from the [Web GUI](#) or [System i Navigator](#)
2. Select **Servers**.
3. Select **Synchronize Software** from the context menu of the integrated Windows server you want to synchronize.
4. Click **Synchronize** to confirm the action. A progress page is shown.

When the synchronization process is complete, the server automatically reboots to apply the updates, if necessary.

**Related information:**

- [Software updates](#)
- [Installing IBM i integration service packs](#)
- [IBM i PTFs](#)
- [Service pack PTFs](#)

### 7.1.2.3 Updating the integration software: remote command

A key use of the `lvlsync` 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 an IBM i CL program to periodically synchronize your integrated Windows servers.

Here is a simple procedure to synchronize an integrated server by remotely submitting the `lvlsync` command from the IBM i character-based interface:

1. At the IBM i character-based interface, type `SBMNWSCMD` and press **F4**.
2. Enter `lvlsync` in the **Command** field.
3. Enter the NWSD name of your integrated server in the **Server** field.
4. Press **Enter** several times to submit the `lvlsync` command to the Window server.

When the synchronization process is complete, the server automatically reboots to apply the updates, if necessary.

**Related information:**

- [Software updates](#)
- [Installing IBM i integration service packs](#)
- [Updating the integration software: lvlsync](#)
- [IBM i PTFs](#)
- [Service pack PTFs](#)

### 7.1.3 Updating the integration software: ESX service console

Once an integrated ESX server service pack PTF is installed on IBM i, you must then install it on each integrated ESX server that use the [Service console based infrastructure](#).

**Note:** For integrated ESX servers that use the [Management server based infrastructure](#), see [Updating the integration software running on Microsoft Windows](#).

**Attention:** 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 end applications, you risk data loss because the integrated server might require a restart after completing the installation.

**Note:** Updating the integration software requires that IBM i NetServer is set up. The user who performs the update must also have sufficient authority to copy the updates to the integrated server. See [Installing and configuring IBM i NetServer](#) in the Information Center.

Do these steps on the VMware ESX server console to update the integrated server support software:

1. Press **ALT-F1** and log on as the **root** user.
2. At the command prompt, type the appropriate command below and press **Enter**.  
i6.1: `ibmlsvupdt userid [address]`  
i5.4: `ixsupdt userid [address]`  
where:
  - *userid* is an IBM i user profile
  - *address* is an optional IP address or host name of the hosting IBM i partition.  
**Note:** Specifying an address allows you to change the IP address or host name that is used for the hosting IBM i partition.
3. The command prompts for the specified IBM i user's password.  
Type in the password and press **Enter** to start the synchronization process.

When the synchronization process is complete, the server automatically reboots to apply the updates, if necessary.

**Related information:**

- [Software updates](#)
- [Installing IBM i integration service packs](#)
- [IBM i PTFs](#)
- [Service pack PTFs](#)

## 7.2 Configuring multipath I/O for integrated servers

Multipath I/O (MPIO) enables multiple storage connections for an integrated server. You need to configure both IBM i and the integrated server operating system.

Enable MPIO for your integrated server as follows:

1. Configure a **multipath group** and additional target and initiator iSCSI adapters on **IBM i**.

See [Configuring IBM i for multipath I/O](#).

2. If the original iSCSI initiator was configured to boot using **manual addressing**, then you must reconfigure it to specify the iSCSI qualified name (IQN) for the **multipath group** IBM i target, which ends with “**tm**”, instead of the IQN for a specific IBM i target, which ends with “**tp**” (where **p** is 1-4).

See [Configuring boot iSCSI initiator with manual addressing for MPIO target](#).

3. Configure MPIO depending on your iSCSI initiator types and integrated server operating system:

<b>Initiator Type</b>	<b>Server OS</b>	<b>Tasks</b>
SWI or HWI	WIN2012	<a href="#">Configuring Windows Server 2012 for multipath I/O</a>
SWI or HWI	WIN2008	<a href="#">Configuring Windows Server 2008 for multipath I/O</a>
HWI	WIN2003	<a href="#">Configuring Windows Server 2003 for multipath I/O</a>
SWI	ESXi5 ESXi4	<a href="#">Configuring ESXi 5 or ESXi 4 for multipath I/O with iSCSI software initiators</a>
HWI	ESXi4 ESX4	<a href="#">Configuring ESXi 4 or ESX 4 for multipath I/O with iSCSI HBAs</a>
HWI	ESX3.5	<a href="#">Configuring ESX 3.5 for multipath I/O with iSCSI HBAs</a>

### Related information:

- [Multipath I/O \(MPIO\)](#)

## 7.2.1 Configuring IBM i for multipath I/O

To configure your integrated Windows or VMware ESX server to use multipath I/O, set up a multipath group in the network server description and set up multiple initiator interfaces in the remote system configuration.

Complete the following steps after the initial installation, and any time that you add additional iSCSI ports to the topology.

1. Select **Integrated Server Administration** from the [Web GUI](#) (7.2/7.1/6.1) or [System i Navigator](#) (5.4).
2. Shut down the integrated server:
  - a. Select **Servers**.
  - b. Select the **Shut Down** action for the server.
  - c. Click **Shut Down** on the confirmation page.
3. Select the **Properties** action for the server.
4. Click the **Storage Paths** tab.
5. At least two storage paths are required to enable multipath I/O. If there is only one storage path currently shown in the table, do these steps to add an additional storage path:
  - a. Click **Add** on the **Storage Paths** tab.
  - b. On the next panel, select the network server host adapter (NWSH) to use for the storage path.
  - c. Click **OK**.
6. Below the storage paths table, click **Properties** for the multipath group.
7. Select the defined storage paths to be members of the multipath group.
8. Click **OK** to update the multipath group information on the server properties panel.
9. Select the multipath group as the default path for virtual storage.
10. Click **OK** on the server properties panel to save the changes to the NWSD.
11. Verify that the disks for the server are linked to the default path or the multipath group. If you need to change the links for a disk, do the following steps.
  - a. Unlink the disk from the integrated server:
    1. Select **All Virtual Storage**.
    2. Select the **Remove link...** action for the storage space.

3. Click **Remove** on the confirmation page.
- b. Link the disk to the server.
  1. Select the **Add link...** action for the storage space.
  2. Select the server.
  3. Specify either the multipath group or the default path.
  4. Click **OK**.
12. Ensure that all information for the iSCSI initiator ports exists in the remote system configuration for the integrated server. You need to know the MAC address and IP address for each initiator port. To add information for additional iSCSI initiator ports to the remote system configuration, follow these steps.
  - a. Select **Remote Systems**.
  - b. Select the **Properties** action for the remote system configuration.
  - c. Click the **Remote Interfaces** tab.
  - d. Click **Add** and type the MAC address and IP address. The MAC address is shown on a label on the iSCSI initiator adapter, and is also displayed when the iSCSI initiator configuration utility runs on the integrated server. For IP address guidelines, see [Selecting IP addresses for the System x or blade iSCSI initiator](#).
  - e. Click **OK** to save and exit.

**Related information:**

- [Multipath I/O \(MPIO\)](#)
- [Distributing iSCSI network traffic between multiple iSCSI targets](#)
- [Work with NWS Configuration \(WRKNWSCFG\)](#)
- [Change NWS Configuration \(CHGNWSCFG\)](#)
- [Work with Network Servers \(WRKNWSD\)](#)
- [Change Network Server Desc \(CHGNWSD\)](#)  
(see the STGPTH, MLTPHGRP, and DFTSTGPTH keywords)

## 7.2.2 Configuring Windows Server 2012 for multipath I/O

An integrated Windows server can use redundant iSCSI data paths to access virtual storage hosted by IBM i.

The integrated Windows server can have a maximum configuration of:

- 4 iSCSI initiators and
- 4 iSCSI targets

The Microsoft **Software Initiator** service must be configured before Windows Server 2012 can use multipath I/O. Use the Microsoft iSCSI Software Initiator version that is included with Windows Server 2012.

Do these steps to configure the Microsoft iSCSI Software Initiator service on Windows Server 2012:

1. Install Windows component MPIO.
  - a. Select **Server Manager > Manage > Add Roles and Features**.
  - b. Click **Next** and finish each step until **Features** tab become enabled.
  - c. Select and choose **Multipath I/O (MPIO)** from the list.
  - d. Click **Next** and then click **Install** to install the MPIO feature.

Alternatively, run the following command:

```
C:\>ocsetup MultipathIo /norestart
```

2. Discover and claim multipath devices.
  - a. Select **Server Manager > Tools > MPIO**.
  - b. Click the **Discover Multi-Paths** tab.
  - c. Check the box next to **Add support for iSCSI devices**.
  - d. Click **Add** and then click **Yes** on the **Reboot Required** panel.

Alternatively, run the following command:

```
C:\>mpclaim -r -i -a ""
```

Once the **Software Initiator** service is configured, you can enable more than one iSCSI adapter port for booting. To do this, use the appropriate [Configuring additional boot iSCSI initiators for Windows MPIO](#) sub-section. Use the same boot mode for all ports.

**Note:** The IBM i Integrated Server Support automatically configures multipath I/O sessions on the integrated Windows server if the server contains more than one iSCSI initiator or if the server uses more than one IBM i iSCSI target. There can be multiple I/O sessions from a single iSCSI initiator to multiple iSCSI targets.

### Related information:

➤ [Multipath I/O \(MPIO\)](#)

➤ [Configuring IBM i for multipath I/O](#)

## 7.2.3 Configuring Windows Server 2008 for multipath I/O

An integrated Windows server can use redundant iSCSI data paths to access virtual storage hosted by IBM i.

The integrated Windows server can have a maximum configuration of:

- 4 iSCSI initiators and
- 4 iSCSI targets

The Microsoft **Software Initiator** service must be configured before Windows Server 2008 can use multipath I/O. Use the Microsoft iSCSI Software Initiator version that is included with Windows Server 2008.

Do these steps to configure the Microsoft iSCSI Software Initiator service on Windows Server 2008:

1. Install Windows component MPIO.
  - a. From the **Start** menu, select **Administrative Tools > Server Manager**.
  - b. Scroll down to the **Features Summary** section.
  - c. Select **Add Features**, and choose **Multipath I/O (MPIO)** from the list.
  - d. Click **Next** and then click **Install** to install the MPIO feature.

Alternatively, run the following command:

```
C:\>ocsetup MultipathIo /norestart
```

2. Discover and claim multipath devices.
  - a. From the **Start** menu, select **All Programs > Administrative Tools > MPIO**.
  - b. Click the **Discover Multi-Paths** tab.
  - c. Check the box next to **Add support for iSCSI devices**.
  - d. Click **Add** and then click **Yes** on the **Reboot Required** panel.

Alternatively, run the following command:

```
C:\>mpclaim -r -i -a ""
```

Once the **Software Initiator** service is configured, you can enable more than one iSCSI adapter port for booting. To do this, use the appropriate [Configuring additional boot iSCSI initiators for Windows MPIO](#) sub-section. Use the same boot mode for all ports.

**Note:** The IBM i Integrated Server Support automatically configures multipath I/O sessions on the integrated Windows server if the server contains more than one iSCSI initiator or if the server uses more than one IBM i iSCSI target. There can be multiple I/O sessions from a single iSCSI initiator to multiple iSCSI targets.

**Related information:**

➤ [Multipath I/O \(MPIO\)](#)

➤ [Configuring IBM i for multipath I/O](#)



## 7.2.4 Configuring Windows Server 2003 for multipath I/O

An integrated Windows server can use redundant iSCSI data paths to access virtual storage hosted by IBM i.

The integrated Windows server can have a maximum configuration of:

- 4 iSCSI initiators and
- 4 iSCSI targets

Install the Microsoft iSCSI Software Initiator service, if necessary, to enable multipath I/O.

The Microsoft **Software Initiator** service must be installed before Windows Server 2003 can use multipath I/O. Use Microsoft iSCSI Software Initiator version **2.08** or later. If your Windows Server 2003 server does not have iSCSI Software Initiator version **2.08** or later, continue with this task.

Do these steps to install the Microsoft iSCSI Software Initiator service on Windows Server 2003:

1. Download and install the Microsoft iSCSI Software Initiator.
  - a. Go to the [Microsoft Download Center](#) Web page.
  - b. Search for iSCSI initiator.
  - c. Install **Virtual Port Driver, Initiator Service**, and **Microsoft MPIO Multipathing Support for iSCSI**.

**Important:** Do not manually configure the installed Microsoft components. The IBM i Virtual Ethernet Manager Service is aware of the target storage configured in IBM i and provides the optimal multipath configuration.

2. Restart the Windows operating system.

Once the **Software Initiator** service is installed, you can enable more than one iSCSI adapter port for booting. To do this, use the appropriate [Configuring additional boot iSCSI initiators for Windows MPIO](#) sub-section. Use the same boot mode for all ports.

**Related information:**

➤ [Multipath I/O \(MPIO\)](#)

➤ [Configuring IBM i for multipath I/O](#)

## 7.2.5 Configuring ESXi 5 or ESXi 4 for multipath I/O with iSCSI software initiators

IBM i integrated servers running supported VMware ESXi versions (see ESXi5 and ESXi4 in [Server OS](#) for specific versions) are supported with multipath I/O using iSCSI software initiators (Ethernet NICs).

The integrated ESX server can have a maximum configuration of:

- 4 iSCSI initiators and
- 4 iSCSI targets

**Note:** Before configuring iSCSI software initiator, you should have the following items available:

- The ESXi server network adapter port MAC address, Internet Address, Subnet Mask, and iSCSI qualified name (IQN) for each iSCSI software initiator port you have configured in your IBM i **remote system configuration**.
- The Internet address information for each IBM i iSCSI target (**NWSH**) that your server will use.

Configure ESXi to use software initiator as follows:

1. From a client workstation, start the **vSphere Client** interface.
  - a. You can connect to a vCenter server or directly to the ESXi server. Log into the vSphere Client with a user with Administrator permissions such as root. If connecting to a vCenter server, select the ESX server.
  - b. Click on the **Configuration** tab.
2. Determine the network adapter devices (vmnic<x>) that will be used for iSCSI connectivity:
  - a. Under **Hardware**, select **Network Adapters** in order to view the available network adapters.
  - b. In the **Network Adapters** panel, record each network adapter device (vmnic<x>) that corresponds to a MAC address from the IBM i remote system configuration.
3. Create an iSCSI initiator port (vmk<y>) for each network adapter device (vmnic<x>) identified in **step 2**:
  - a. Under **Hardware**, select **Networking**.
  - b. Select **Add Networking** to bring up the **Add Network Wizard**.
  - c. In the **Connection Type** panel, select **VMkernel** and click **Next**.
  - d. In the **VMkernel - Network Access** panel, select the option for your vSphere Client version:

vSphere Client Version	Option
5.x	Create a vSphere standard switch
4.x	Create a virtual switch

From the list of virtual switches you should see a list of network adapter devices (vmnic<x>). Select one network adapter device (vmnic<x>) from **step 2-b** above and click **Next**.

- e. In the **VMkernel - Connection Settings** panel, give the port an appropriate **Network Label** such as *iSCSI initiator port y* then click **Next**.
- f. In the **VMkernel - IP Connection Settings** panel specify the **IP Address** and **Subnet mask** from the IBM i remote system configuration associated with the MAC address of the network device you chose in **step d** above. Do **not** edit the **VMkernel Default Gateway**. Click **Next**.
- g. Review your port configuration in the summary panel. Confirm that the IP address information is correct, then click **Finish**.

**Repeat steps 3-a through 3-g** for each iSCSI software initiator port that is configured in your IBM i remote system configuration.

4. Enable the iSCSI Software Adapter and discover iSCSI targets:

- a. Under **Hardware**, select **Storage Adapters**.
- b. Select the iSCSI initiator adapter in the **Storage** list, under **iSCSI Software Adapter**.
- c. In the **Details** pane, select **Properties...** to display the **iSCSI Initiator Properties** dialog.
- d. In the **General** tab, click **Configure...** to display the **General Properties** dialog.
- e. In the **General Properties** dialog, select **Enabled** in the status pane. In the **iSCSI Properties** pane, change the **iSCSI Name** to match the IQN provided in your IBM i remote system configuration. Click **OK** to save the changes.

**Note:** If the **iSCSI Name** field is disabled, click **OK**, then click **Configure...** from **step d**, enter the IQN for the initiator, then click **OK**.

**Note:** Once the **iSCSI Software Adapter** is enabled, it is assigned a device name (vmhba<z>).

- f. Select the **Dynamic Discovery** tab on the **iSCSI Initiator Properties** panel.
- g. Click **Add...** to bring up the **Add Send Target Server** dialog. Enter the IP address of an NWSH that is associated with your server. Click **OK** to save your changes.

**Repeat this step** until the IP address for each NWSH associated with your server has been added.

- h. Click **Close** to dismiss the **iSCSI Initiator Properties** dialog.

**Note:** Perform the following steps only if you have created more than one iSCSI initiator port (vmk<y>) from **step 3**.

5. Activate **Multipath I/O** for the iSCSI Software Adapter (vmhba<z>):

- a. Identify the iSCSI initiator ports (vmk<y>) that were created in **step 3**.
  - i. Under **Hardware**, select **Networking**.
  - ii. Note each iSCSI initiator port (vmk<y>) created in **step 3**. The **Network Label** you choose in **step 3-e** might help.

- b. Identify the iSCSI initiator device (vmhba<z>).
  - i. Under **Hardware**, select **Storage Adapters**.
  - ii. Note the iSCSI initiator device (vmhba<z>) under the **iSCSI Software Adapter** section.
- c. Bind each iSCSI initiator port (vmk<y>) to the iSCSI initiator device (vmhba<z>) using the tasks below for your ESX version:

Server OS	Tasks
ESXi5	<ol style="list-style-type: none"> <li>1) Under <b>Hardware</b>, select <b>Storage Adapters</b>.</li> <li>2) Select the iSCSI initiator device (vmhba&lt;z&gt;) in the <b>Storage</b> list, under the <b>iSCSI Software Adapter</b> section.</li> <li>3) In the <b>Details</b> pane, select <b>Properties...</b> to display the <b>iSCSI Initiator Properties</b> dialog.</li> <li>4) In the <b>Network Configuration</b> tab, click <b>Add...</b> to display the <b>Bind with VMkernel Network Adapter</b> dialog.</li> <li>5) Select the VMkernel adapter (iSCSI initiator port vmk&lt;y&gt;) to bind with the iSCSI adapter (vmhba&lt;z&gt;) and then click <b>OK</b>.</li> <li>6) Repeat the prior two steps until all of the iSCSI initiator ports (vmk&lt;y&gt;) that were created earlier are bound to the iSCSI initiator device (vmhba&lt;z&gt;).</li> <li>7) Verify that each iSCSI initiator port (vmk&lt;y&gt;) was bound to the iSCSI initiator device (vmhba&lt;z&gt;) on the <b>iSCSI Initiator Properties</b> dialog.</li> <li>8) Click <b>Close</b> to dismiss the <b>iSCSI Initiator Properties</b> dialog.</li> </ol>
ESXi4	<p>For ESXi4, vSphere CLI commands are needed in the following steps, so you must download the <a href="#">vSphere Command Line Interface</a> and install it on a client workstation. Be sure to download the CLI version that matches your ESXi version.</p> <p><b>Note:</b> The vSphere CLI commands prompt for username and password, which must have <b>Administrator</b> permissions (such as root) on the ESXi server.</p> <ol style="list-style-type: none"> <li>1) Once the vSphere CLI is installed, open a Windows command prompt and change directories with the following command:           <pre>cd C:\Program Files\VMware\VMware vSphere CLI\bin</pre> </li> <li>2) Bind each iSCSI initiator port (vmk&lt;y&gt;) to the iSCSI initiator device (vmhba&lt;z&gt;) with the following command:           <pre>esxcli --server=&lt;ESXi IP address&gt; swiscsi nic add -n vmk&lt;y&gt; -d vmhba&lt;z&gt;</pre> </li> <li>3) Verify that each iSCSI initiator port (vmk&lt;y&gt;) was added to the iSCSI initiator device (vmhba&lt;z&gt;) with the following command:           <pre>esxcli --server=&lt;ESXi IP address&gt; swiscsi nic list -d vmhba&lt;z&gt;</pre> </li> </ol> <p>If you make a mistake or want to reconfigure, you can disconnect any iSCSI initiator ports (vmk&lt;y&gt;) bound to the iSCSI initiator device (vmhba&lt;y&gt;) with the</p>

Server OS	Tasks
	following command:  <pre>esxcli --server=&lt;ESXi IP address&gt; swiscsi nic remove -n vmk&lt;y&gt; -d vmhba&lt;z&gt;</pre>

**Related information:**

➤ [Multipath I/O \(MPIO\)](#)

➤ [Configuring IBM i for multipath I/O](#)

## 7.2.6 Configuring ESXi 4 or ESX 4 for multipath I/O with iSCSI HBAs

IBM i integrated servers running supported VMware ESXi or ESX versions (see ESXi4 and ESX4 in [Server OS](#) for specific versions) are supported with multipath I/O using iSCSI hardware initiators (iSCSI HBAs).

The integrated ESX server can have a maximum configuration of:

- 4 iSCSI initiators and
- 4 iSCSI targets

Each iSCSI initiator port can only connect to a single iSCSI target port. In order to achieve a maximum multipath configuration, each iSCSI initiator port needs to be configured to communicate with a unique iSCSI target port. Cable your iSCSI network to isolate initiator and target pairs by using separate switches, by using separate VLANs, or by directly cabling the initiator port to the target port. When isolating initiator and target pairs this way, you can simplify the multipath configuration by using **dynamic addressing**.

You use several utilities to configure a multiple iSCSI initiator or target configuration for an integrated ESX server. You perform some tasks from IBM i, some tasks from the System x or blade server console, and some tasks from the VMware vSphere Client.

Complete the following steps to configure multipath I/O after the initial installation, and any time that you add additional iSCSI ports to the topology.

1. Record all information for the iSCSI initiators that exist in the remote system configuration for the integrated server:
  - a. Select **Integrated Server Administration** from the [Web GUI \(7.2/7.1/6.1\)](#) or [System i Navigator \(5.4\)](#).
  - b. Select **Remote systems**.
  - c. Select the **Properties** action for a remote system configuration.
  - d. Click the **Remote Interfaces** tab.
  - e. Record the MAC address, IP address, subnet mask, and iSCSI qualified name for each iSCSI initiator port. These values are needed for a later step.
  - f. Click **Cancel** to close the properties panel.
2. Start the integrated server:
  - a) Select **Integrated Server Administration** from the [Web GUI \(7.2/7.1/6.1\)](#) or [System i Navigator \(5.4\)](#).
  - b) Select **Servers**.
  - c) Select the **Start** action for the server.
3. From a client workstation, start the **vSphere Client** interface. You can connect to the vCenter Server or directly to the ESX server. If connecting to the vCenter Server, select the ESX server that

you want to work with.

- a. Click the **Configuration** tab.
- b. Click **Storage Adapters**.
- c. A list of iSCSI initiator ports appears under **QLA4050X** or **QLE406X iSCSI Host Bus Adapter**. One of the initiator ports is configured during the boot process. You need to configure other initiator ports to match the information in the remote system configuration. Do the following steps for each port that appears under **QLA4050X** or **QLE406X iSCSI Host Bus Adapter**:
  - i. Select the initiator port and click **Properties**, which is located below and to the right of **QLA4050X** or **QLE406X iSCSI Host Bus Adapter**.
  - ii. On the **General** tab, note the MAC address and find the same MAC address in the remote system configuration.
  - iii. Click **Configure**.
  - iv. Enter the initiator iSCSI qualified name (IQN) from the remote system configuration, if not already configured.
  - v. Enter the initiator IP address and subnet mask information from the remote system object, if not already configured. Even though a gateway is not supported, the VMware interface requires one to be configured. Make the gateway address the same as the IP address. This signifies that there is no gateway.
  - vi. Click **OK** if you changed anything. Otherwise, click **Cancel**.
  - vii. Select the **Dynamic Discovery** tab. Then do the following:
    1. Click **Add** and enter the IP address of an NWSH that is part of the multipath group in IBM i.
    2. Repeat the previous step until the IP address of every NWSH in the multipath group has been added.
  - viii. Click **OK**.
- d. Under **Recent Tasks** near the bottom of the window, check the status associated with previous steps. When the status is **Completed**, click **Rescan**, which is located in the upper right corner **Storage Adapters** view. In the **Rescan** dialogue, click **OK**. When the rescan completes, more LUN information is shown in the **Storage Adapters** view.

**Related information:**

➤ [Multipath I/O \(MPIO\)](#)

➤ [Configuring IBM i for multipath I/O](#)

## 7.2.7 Configuring ESX 3.5 for multipath I/O with iSCSI HBAs

IBM i integrated servers running VMware ESX 3.5 are supported with multipath I/O using iSCSI hardware initiators (iSCSI HBAs).

The integrated ESX server can have a maximum configuration of:

- 2 iSCSI initiators and
- 4 iSCSI targets

Each iSCSI initiator port can only connect to a single iSCSI target port. In order to achieve a maximum multipath configuration, each iSCSI initiator port needs to be configured to communicate with a unique iSCSI target port. Cable your iSCSI network to isolate initiator and target pairs by using separate switches, by using separate VLANs, or by directly cabling the initiator port to the target port. When isolating initiator and target pairs this way, you can simplify the multipath configuration by using **dynamic addressing**.

To configure a multiple iSCSI initiator or target configuration for an integrated server running ESX 3.5, you need to do some configuration tasks on IBM i and other configuration tasks from the VMware Virtual Infrastructure Client.

Complete the following steps to configure multipath I/O after the initial installation, and any time that you add additional iSCSI ports to the topology.

1. Record all information for the iSCSI initiators that exist in the remote system configuration for the integrated server:
  - a. Select **Integrated Server Administration** from the [Web GUI](#) or [System i Navigator](#).
  - b. Select **Remote systems**.
  - c. Select the **Properties** action for a remote system configuration.
  - d. Click the **Remote Interfaces** tab.
  - e. Record the MAC address, IP address, subnet mask, and iSCSI qualified name for each iSCSI initiator port. These values are needed for a later step.
  - f. Click **Cancel** and close the properties panel.
2. Start the integrated server:
  - a) Select **Integrated Server Administration** from the [Web GUI](#) or [System i Navigator](#).
  - b) Select **Servers**.
  - c) Select the **Start** action for the server.
3. From a client workstation, start the **Virtual Infrastructure Client** interface. You can connect to the Virtual Center Server or directly to the ESX server. If connecting to the Virtual Center Server, select the ESX server that you want to work with.
  - a. Click the **Configuration** tab.



- b. Click **Storage Adapters**.
- c. A list of iSCSI initiator ports appears under **QLA4022**. One of the initiator ports is configured during the boot process. You need to configure other initiator ports to match the information in the remote system configuration. Do the following steps for each port that appears under **QLA4022**:
  - i. Select the initiator port and click **Properties**, which is located below and to the right of **QLA4022**.
  - ii. On the **General** tab, note the MAC address and find the same MAC address in the remote system configuration.
  - iii. Click **Configure**.
  - iv. Enter the initiator iSCSI qualified name (IQN) from the remote system configuration, if not already configured.
  - v. Enter the initiator IP address and subnet mask information from the remote system object, if not already configured. Even though a gateway is not supported, the VMware interface requires one to be configured. Make the gateway address the same as the IP address. This signifies that there is no gateway.
  - vi. If changes were made, click **OK**. Otherwise, click **Cancel**.
  - vii. Select the **Dynamic Discovery** tab. Then do the following:
    1. Click **Add** and enter the IP address of an NWSH that is part of the multipath group in IBM i.
    2. Repeat the previous step until the IP address of every NWSH in the multipath group has been added.
  - viii. Click **OK**.
- d. Under **Recent Tasks** near the bottom of the window, check the status associated with previous steps. When the status is **Completed**, click **Rescan**, which is located in the upper right corner **Storage Adapters** view. In the **Rescan** dialogue, click **OK**. When the rescan completes, you should see more LUN information in the **Storage Adapters** view.

**Related information:**

➤ [Multipath I/O \(MPIO\)](#)

➤ [Configuring IBM i for multipath I/O](#)

## 7.3 Using hot spare hardware

If there is a problem with your integrated server or iSCSI target adapter hardware, use the following tasks to change your IBM i configuration objects to point to new hardware.

Failing Hardware Type	Hot Spare Tasks
System x or Blade	<a href="#">Using hot spare integrated server hardware</a>
iSCSI hardware target	<a href="#">Using hot spare iSCSI hardware target adapters</a>
iSCSI software target	<a href="#">Using hot spare iSCSI software target adapters</a>

### Related information:

- [Hot spare support for integrated servers](#)

### 7.3.1 Using hot spare integrated server hardware

If there is a problem with your System x or blade hardware, you can change your IBM i configuration objects to point to new hardware.

Use these tasks to switch to hot spare integrated server hardware.

1. Select **Integrated Server Administration** from the [Web GUI](#) (7.2/7.1/6.1) or [System i Navigator](#) (5.4).
2. Select **Servers**.
3. If the server for which you want to swap hardware is not already shut down:
  - a. Select the **Shut Down** action for the server.
  - b. Click **Shut Down** on the confirmation panel.
4. Change the server configuration to point to the hot spare server hardware.
  - a. Select the **Properties** action for the server.
  - b. Select the **System** tab and select the new **Remote system configuration** name.
  - c. Click **OK**.
5. Select the **Start** action for the server.

**Attention:** If you have multiple Network Server Description (NWS) objects configured to use the same integrated server hardware, there is a potential compatibility problem when different operating systems are used. This incompatibility might affect the functionality of the server. As of this writing, the following issue exists when using hot spare between Windows servers and VMware ESX servers:

<b>Hot Spare Issue Between Windows and ESX</b>
<p>In the following hot spare scenario, multipath I/O (MPIO) needs to be manually configured again for a VMware ESX server:</p> <ol style="list-style-type: none"><li>1. A VMware ESX server is configured with MPIO on the server hardware.</li><li>2. The ESX server is stopped and then a Windows server that uses the same server hardware is started.  The Windows integration support automatically configures the iSCSI MPIO sessions for the Windows server.</li><li>3. The Windows server is stopped and then the ESX server that uses the same server hardware is started again.</li></ol> <p>In this scenario, the MPIO setup that was done for the Windows server is not compatible with the ESX server. Therefore, the ESX server initiator MPIO setup must be manually configured again in order for the ESX server to use MPIO.</p>

**Related information:**

- [Hot spare support for integrated servers](#)
  - [Vary Configuration \(VRYCFG\)](#)
  - [Work with Configuration Status \(WRKCFGSTS\)](#)
  - [Change Network Server Desc \(CHGNWSD\)](#)
- (use WRKCFGSTS \*NWS)

### 7.3.2 Using hot spare iSCSI hardware target adapters

If there is a problem with your IBM i iSCSI hardware target adapter (iSCSI HBA), you can change your IBM i configuration objects to point to another iSCSI hardware target adapter.

To hot spare iSCSI hardware target (iSCSI HBA) adapter hardware, do the following steps:

1. Shut down the integrated servers that use the iSCSI target network server host adapter (NWSH).
  - a. Select **Integrated Server Administration** from the [Web GUI](#) or [System i Navigator](#).
  - b. Select **Servers**.
  - c. Select the **Shut Down** action for the server.
  - d. Click **Shut Down** on the confirmation page.
2. Stop the NWSH for which you want to swap hardware:
  - a. Select **Network Server Host Adapters**.
  - b. Select the **Stop** action for the NWSH.
  - c. Click **Stop** on the confirmation panel.
  - d. If active servers are currently using the NWSH, a warning message is shown. Click **Continue**.
3. Change the NWSH to point to the hot spare iSCSI target adapter:
  - a. Select the **Properties** action for the NWSH.
  - b. Select the **General** tab and select a new value for the **Hardware resource** prompt. If you are unsure of the new hardware resource name, see [Determining the hardware resource name for an iSCSI target adapter](#).
  - c. Click **OK**.
4. Start the NWSH.
  - a. Select the **Start** action for the NWSH.
5. Start the integrated servers that use the NWSH:
  - a) Select **Servers**.
  - b) Select the **Start** action for the servers.

**Related information:**

- [Hot spare support for integrated servers](#)
- [Work with Configuration Status \(WRKCFGSTS\)](#)  
(use WRKCFGSTS \*DEV \*NWSH)
- [Vary Configuration \(VRYCFG\)](#)
- [Change Device Desc \(NWSH\) \(CHGDEVNWSH\)](#)

### 7.3.3 Using hot spare iSCSI software target adapters

If there is a problem with your IBM i iSCSI software target adapter (Ethernet NIC), you can change your IBM i configuration objects to point to another iSCSI software target adapter.

**Note:** This procedure allows integrated servers that use redundant iSCSI target storage connections (multipath I/O) to remain active during the hot spare process. If an integrated server uses multipath I/O, you can skip the first and last steps in this task.

To hot spare iSCSI software target (Ethernet NIC) adapter hardware, do the following steps:

1. **If** any integrated servers that use the iSCSI target network server host adapter (NWSH) do **not** have redundant iSCSI target storage connections (multipath I/O), shut down those integrated servers.
  - a. Select **Integrated Server Administration** from the [Web GUI](#).
  - b. Select **Servers**.
  - c. Select the **Shut Down** action for the server.
  - d. Click **Shut Down** on the confirmation page.
2. Do **one** of the following actions, depending on whether any integrated servers that use the NWSH are still active (they use multipath I/O):

Servers Active?	Tasks
No	If all servers that use the NWSH are shut down, then stop the NWSH. <ol style="list-style-type: none"><li>a. Select <b>Network Server Host Adapters</b>.</li><li>b. Select the <b>Stop</b> action for the NWSH.</li><li>c. Click <b>Stop</b> on the confirmation panel.</li></ol>

Servers Active?	Tasks
Yes	<p>Otherwise, when any integrated servers that use the NWSH are still active:</p> <ol style="list-style-type: none"> <li>a. Run the following command from the IBM i command line: <pre>CRTDTAARA DTAARA(QUSRSYS/QHNATCP) TYPE(*DEC) LEN(4 0) VALUE(1)</pre> <p><b>Note:</b> This data area allows any TCP/IP interface that is associated with an NWSH to be stopped without stopping the NWSH. Once the TCP/IP interface is stopped, the data area is automatically deleted.</p> </li> <li>b. Stop the TCP/IP interface that is associated with the NWSH: <ol style="list-style-type: none"> <li>1. Select <b>Network</b> from the <a href="#">Web GUI</a>.</li> <li>2. Click <b>Show All Network Tasks</b>.</li> <li>3. Select <b>Network &gt; TCP/IP Configuration &gt; IPv4 &gt; Interfaces</b>.</li> <li>4. Locate the TCP/IP interface that is associated with the NWSH.</li> <li>5. Select the <b>Stop</b> action for the TCP/IP interface.</li> </ol> </li> </ol>

3. Stop the line description (LIND) that is associated with the NWSH:

- a. Select **Network** from the [Web GUI](#).
- b. Select **Lines**.
- c. Select the **Stop** action for the LIND.

4. Run the following command from the IBM i command line to change the LIND to point to the hot spare iSCSI software target (Ethernet NIC):

```
CHGLINETH LIND(nwshlind) RSRNAME(cmnxx)
```

Where *nwshlind* is the LIND name and *cmnxx* is the new resource name. If you are unsure of the new hardware resource name, see [Determining the hardware resource name for an iSCSI target adapter](#).

5. Start the TCP/IP interface that is associated with the NWSH.

- a. Select **Network** from the [Web GUI](#).
- b. Click **Show All Network Tasks**.
- c. Select **Network > TCP/IP Configuration > IPv4 > Interfaces**.
- d. Locate the TCP/IP interface that is associated with the NWSH.
- e. Select the **Start** action for the TCP/IP interface.

Starting the TCP/IP interface also does the following actions:

- Starts the LIND that is associated with the TCP/IP interface.
  - Starts the NWSH if it was stopped in step 2.
  - Makes the iSCSI target available to any integrated servers that are using the NWSH.
6. **If** you shut down any integrated servers that use the NWSH earlier, start those integrated servers:
- a) Select **Integrated Server Administration**.
  - b) Select **Servers**.
  - c) Select the **Start** action for the servers.

**Related information:**

- [Hot spare support for integrated servers](#)
- [End TCP/IP Interface \(ENDTCPIFC\)](#)
- [Work with Configuration Status \(WRKCFGSTS\)](#)  
(use WRKCFGSTS \*LIN)
- [Vary Configuration \(VRYCFG\)](#)
- [Work with Line Descriptions \(WRKLIND\)](#)
- [Change Line Desc \(Ethernet\) \(CHGLINETH\)](#)
- [Start TCP/IP Interface \(STRTCPIFC\)](#)

## 7.4 Implementing IBM i clustering for integrated servers

The high availability clustering solution for IBM i allows you to mirror integrated server data and configuration information from one IBM i cluster node to another. To implement IBM i clustering for integrated servers, do the following:

1. Follow the instructions in the [Implementing high availability](#) topic in the Information Center to set up a high availability environment that includes iSCSI-attached integrated servers.
2. See the following sections for recommendations related to mirroring integrated server objects:
  - [Mirroring virtual storage \(NWSSTG\)](#)
  - [Mirroring the network server description \(NWSD\)](#)
  - [Mirroring network server configurations \(NWSCFGs\)](#)
  - [Mirroring the NWSH for an iSCSI target](#)
3. If your IBM i clustering environment uses geographic mirroring, see:
  - [Recommended settings for geographic mirroring in an iSCSI environment](#)
4. If your IBM i clustering environment includes VMware ESX servers, see:
  - [Switching an iSCSI-attached VMware ESX server from one node to another](#)

### Related information:

- [IBM i clustering for integrated servers](#)
- [Implementing high availability](#)



## 7.4.1 Mirroring virtual storage (NWSSTG)

In order for your IBM i virtual storage (network server storage space, or NWSSTG) to be mirrored, the NWSSTG must be located in an iASP that is mirrored between the nodes in the cluster. Mirroring NWSSTG between nodes in the cluster requires that you use one of the cross-site mirroring technologies (such as geographic mirroring), even if your cluster nodes are in the same data center. For **i 7.1**, you should also apply group PTF [SF99369](#) level 4 or later.

**First**, create the NWSSTG for your server in the desired iASP on the production node.

Considerations for creating the NWSSTG for your server:

- For certain server types it is best **not** to mirror all storage spaces between nodes in the cluster:

Server OS	Considerations
<b>ESX4</b> <b>ESX3.5</b>	<p>For non-ESXi versions of ESX, the <b>system</b> storage space should be in the <b>System ASP</b> to prevent corruption. This means that the ESX system storage space is <b>not</b> mirrored to the backup node.</p> <p>However, the storage spaces for the ESX virtual machines should be created in an iASP that is mirrored between the production node and the backup node.</p> <p><b>Note:</b> If the ESX server system storage space is not mirrored to the backup node, then the NWSD should <b>not</b> be added to the cluster administrative domain. Instead, install a second ESX server on the backup node and then link the mirrored ESX virtual machine storage spaces to the second ESX server on the backup node.</p>
<b>Windows and all ESXi versions</b>	<p>The storage spaces for Windows servers, ESXi versions of ESX, and the ESX virtual machines should be created in an iASP that is mirrored between the production node and the backup node.</p>

- You must specify the iASP name or number to identify where to create the NWSSTG on the production node. To determine these values:
  - iASP name:** Use **WRKDEVD \*ASP**, which shows only iASP names available.
  - iASP number:** Use **DSPASPSTS <iasp\_name>**, specifying the iASP name determined above.
- You can select the ASP location for the NWSSTG on the production node, either:
  - When installing the server using the **Web GUI** or install command (for the system and install drives only).
  - When creating the NWSSTG using the [Web GUI](#), [System i Navigator](#) GUI, or **CRTNWSSTG** command (use the **CRTNWSSTG** command *ASP device (ASPDEV)* or *Auxiliary storage pool ID (ASP)* keywords).
- If the NWSSTG have already been created, but are in the wrong ASP, you can move them to the correct ASP. See [Moving virtual storage between ASPs](#).
- After the storage spaces are created in the iASP on the production node:
  - They will show up under **WRKNWSSTG** on the production node.
  - However, they will not show up under **WRKNWSSTG** on the backup node until the configuration files are added to the list of monitored resources in the cluster administrative domain and sent to the backup node.

**Next**, once the NWSSTG for your server is created in the correct iASP on the production node, add the **NWSSTG** to the list of monitored resources in the cluster administrative domain. On the production node, use one of the following commands:

- **WRKCLU**: Use option 8 (Work with administrative domains), then option 7 (Monitored resources), then option 1 (Add).
- **ADDCADMRE**: Use a type of **\*NWSSTG**.

**Note**: All of the storage spaces used by the NWSD must be added to the list of monitored resources for the cluster administrative domain **before** the NWSD can be added to the cluster administrative domain.

**Related information:**

- [IBM i clustering for integrated servers](#)
- [Implementing high availability](#)
- [IBM i configuration objects for integrated servers](#)
- [Create NWS Storage Space \(CRTNWSSTG\)](#)
- [Work with NWS Storage Spaces \(WRKNWSSTG\)](#)
- [Work with Device Descriptions \(WRKDEVD\)](#)
- [Display ASP Status \(DSPASPSTS\)](#)
- [Work with Cluster \(WRKCLU\)](#)
- [Add Admin Domain MRE \(ADDCADMRE\)](#)

### 7.4.1.1 Moving virtual storage between ASPs

Use one of the following methods to move a storage space (NWSSTG) from one ASP to another ASP:

Method	Procedure
SAV/RST	<p><b>Note:</b> With this method, the new storage space has the same name as the original storage space, so the original storage space name is preserved.</p> <p>Procedure:</p> <ol style="list-style-type: none"> <li>1. Save the original storage space, using the <b>SAV</b> command.</li> <li>2. Unlink the original storage space from the NWSD, using the <b>RMVNWSSTGL</b> command, if necessary.</li> <li>3. Delete the original storage space, using the <b>DLTNWSSTG</b> command.</li> <li>4. Create a small (for example, 1 MB) temporary storage space in the desired ASP, specifying the <b>original</b> storage space name, using the <b>CRTNWSSTG</b> command.</li> <li>5. Restore the original storage space over the temporary storage space, using the <b>RST</b> command.</li> </ol> <p><b>Note:</b> The restored storage space is placed in the desired iASP.</p> <ol style="list-style-type: none"> <li>6. Link the storage space to the NWSD, using the <b>ADDNWSSTGL</b> command, if necessary.</li> </ol>
Copy	<p><b>Note:</b> With this method, the new storage space has a different name than the original storage space, so the original storage space name is <b>not</b> preserved.</p> <p>Procedure:</p> <ol style="list-style-type: none"> <li>1. Copy the original storage space to a new storage space in the desired iASP, using the <b>FROMNWSSTG</b> keyword on the <b>CRTNWSSTG</b> command.</li> <li>2. Unlink the original storage space from the NWSD, using the <b>RMVNWSSTGL</b> command, if necessary.</li> <li>3. Delete the original storage space using the <b>DLTNWSSTG</b> command.</li> <li>4. Link the new storage space to the NWSD, using the <b>ADDNWSSTGL</b> command, if necessary.</li> </ol>

**Related information:**

- [IBM i clustering for integrated servers](#)
- [Implementing high availability](#)
- [IBM i configuration objects for integrated servers](#)
- [Create NWS Storage Space \(CRTNWSSTG\)](#)
- [Work with NWS Storage Spaces \(WRKNWSSTG\)](#)
- [Remove Server Storage Link \(RMVNWSSTGL\)](#)
- [Add Server Storage Link \(ADDNWSSTGL\)](#)
- [Delete NWS Storage Space \(DLTNWSSTG\)](#)
- [Save Object \(SAV\)](#)
- [Restore Object \(RST\)](#)

## 7.4.2 Mirroring the network server description (NWSD)

The network server description (NWSD) for an iSCSI-attached server must be mirrored between nodes of the IBM i cluster.

**Note:** All of the storage spaces used by the NWSD must be added to the list of monitored resources for the cluster administrative domain **before** the NWSD can be added to the cluster administrative domain. See [Mirroring virtual storage](#).

### Mirroring the NWSD:

Add the **NWSD** to the list of monitored resources in the cluster administrative domain. On the production node, use one of the following commands:

- **WRKCLU:** Use option 8 (Work with administrative domains), then option 7 (Monitored resources), then option 1 (Add).
- **ADDCADMRE:** Use a type of **\*NWSD**.

The NWSD attributes to mirror depend on the setup of the IBM i clustering environment.

- If the same network server configuration (NWSCFG) objects and network server host adapter (NWSH) configurations are used on the production and backup nodes, then all of the NWSD attributes can be mirrored.
- If not, then you need to select specific NWSD attributes to be mirrored. Refer to the [Add Admin Domain MRE \(ADDCADMRE\)](#) command documentation for a list of NWSD attributes that can be mirrored.

### Mirroring the virtual Ethernets for an NWSD:

If the NWSD has associated **virtual Ethernets**, then add the line description (LIND) for each virtual to the list of monitored resources in the cluster administrative domain. On the production node, use one of the following commands:

- **WRKCLU:** Use option 8 (Work with administrative domains), then option 7 (Monitored resources), then option 1 (Add).
- **ADDCADMRE:** Use a type of **\*ETHLIN**.

#### Related information:

- [IBM i clustering for integrated servers](#)
- [Implementing high availability](#)
- [IBM i configuration objects for integrated servers](#)
- [Work with Cluster \(WRKCLU\)](#)
- [Add Admin Domain MRE \(ADDCADMRE\)](#)

### 7.4.3 Mirroring network server configurations (NWSCFGs)

The following network server configuration (NWSCFG) objects are used by a network server description (NWSD):

- Remote system configuration (NWSCFG subtype \*RMTSYS).
- Service processor configuration (NWSCFG subtype \*SRVPRC).
- Connection security configuration (NWSCFG subtype \*CNNSEC).

The NWSCFG objects to mirror depend on the setup of the IBM i clustering environment:

1. If the distance between nodes is short and the same System x or blade server hardware is used on the backup node, then mirror all of the NWSCFG objects.

Add the NWSCFG objects to the list of monitored resources in the cluster administrative domain. On the production node, use one of the following commands:

- **WRKCLU:** Use option 8 (Work with administrative domains), then option 7 (Monitored resources), then option 1 (Add).
  - **ADDCADMRE:** Use a type of \*NWSCFG.
2. If different System x or blade server hardware is used on the backup node, then do **not** mirror the NWSCFG objects. Instead, create independent NWSCFG objects on the backup node. Note that the clustering configuration is simplified if you use the same NWSCFG object names on the backup node as are used on the production node.

**Note:** If the NWSCFG objects on the backup node have different names than the ones on the production node, then the network server description (NWSD) on each node needs to reference different NWSCFG objects. In this case, you will need to mirror a **subset** of the NWSD attributes. See [Mirroring the network server description \(NWSD\)](#).

**Related information:**

- [IBM i clustering for integrated servers](#)
- [Implementing high availability](#)
- [IBM i configuration objects for integrated servers](#)
- [Work with Cluster \(WRKCLU\)](#)
- [Add Admin Domain MRE \(ADDCADMRE\)](#)

## 7.4.4 Mirroring the NWSH for an iSCSI target

The network server host adapter (NWSH) configuration for the iSCSI targets that the NWSD uses must be mirrored between nodes of the IBM i cluster.

See the considerations below for the type of iSCSI target NWSH that is used in your environment:

NWSH Type	Considerations
<b>Virtual NWSH (Software Target)</b>	<p>For the virtual NWSH information to be mirrored over properly, do the following:</p> <p><b>First</b>, add the NWSH device description to the list of monitored resources in the cluster administrative domain. On the production node, use one of the following commands:</p> <ul style="list-style-type: none"> <li>• <b>WRKCLU:</b> Use option 8 (Work with administrative domains), then option 7 (Monitored resources), then option 1 (Add).</li> <li>• <b>ADDCADMRE:</b> Use a type of <b>*NWSHDEV</b>.</li> </ul> <p><b>Second</b>, set up a matching line description (LIND) and interface on the backup node. The line description used for the virtual NWSH on the production node can be mirrored over with cluster administrative domain, but this requires some other work:</p> <ol style="list-style-type: none"> <li>1. The LIND hardware resource name used for the virtual NWSH must exist and match on both systems, and must be for the same type of hardware.</li> <li>2. You must manually create the controller description for the line description on the backup system. Use the <b>CRTCTLNET</b> command to create it. Use the same controller name that was used on the production node. To look up the controller name, display the line description (<b>DSPLIND</b> or <b>WRKLIND</b> command) on the production node.</li> <li>3. Add the line description to the list of monitored resources in the cluster administrative domain. On the production node, use one of the following commands: <ul style="list-style-type: none"> <li>• <b>WRKCLU:</b> Use option 8 (Work with administrative domains), then option 7 (Monitored resources), then option 1 (Add).</li> <li>• <b>ADDCADMRE:</b> Use a type of <b>*ETHLIN</b>.</li> </ul> </li> </ol>
<b>Physical NWSH (Hardware Target)</b>	<p>For the physical NWSH information to be mirrored over properly, do the following:</p> <p><b>First</b>, the NWSH hardware resource name used must exist and match on both systems.</p> <p><b>Second</b>, add the NWSH device description to the list of monitored resources in the cluster administrative domain. On the production node, use one of the following commands:</p> <ul style="list-style-type: none"> <li>• <b>WRKCLU:</b> Use option 8 (Work with administrative domains), then option 7 (Monitored resources), then option 1 (Add).</li> <li>• <b>ADDCADMRE:</b> Use a type of <b>*NWSHDEV</b>.</li> </ul>

### Related information:

- [IBM i clustering for integrated servers](#)
  - [Implementing high availability](#)
  - [IBM i configuration objects for integrated servers](#)
  - [Work with Cluster \(WRKCLU\)](#)
- [Add Admin Domain MRE \(ADDCADMRE\)](#)
  - [Create Ctl Desc \(Network\) \(CRTCTLNET\)](#)
  - [Work with Line Descriptions \(WRKLIND\)](#)
  - [Display Line Description \(DSPLIND\)](#)

## 7.4.5 Recommended settings for geographic mirroring in an iSCSI environment

Geographic mirroring of data in an independent auxiliary storage pool (iASP) from one node to another is part of the high availability clustering solution for IBM i. With geographic mirroring, the data mirroring is done in the machine code layer below the IBM i operating system. If your high availability environment uses geographic mirroring, then see the considerations and recommended settings below.

Geographic mirroring provides two modes for delivering the iASP data between nodes:

Delivery Mode	Considerations
<b>Synchronous</b>	<ol style="list-style-type: none"> <li>1. Provided on all supported IBM i versions.</li> <li>2. This is the only delivery mode available on i 6.1.</li> <li>3. In i 7.1 or higher, iSCSI kernel code uses an extended timeout to handle geographic mirroring events, which helps avoid timeouts.</li> </ol>
<b>Asynchronous (recommended)</b>	<ol style="list-style-type: none"> <li>1. Provided only on i 7.1 or higher.</li> <li>2. Avoids timeouts.</li> <li>3. Provides better performance characteristics than synchronous delivery.</li> </ol>

Use the following settings when your IBM i clustering configuration uses geographic mirroring for virtual storage data that resides in an iASP:

Configuration	Recommended Settings
IBM i 6.1 (or i 7.1 or higher when using <b>synchronous</b> delivery)	Set the <b>suspend timeout</b> to <b>1 minute</b> (60 seconds), using the following command:  <pre>CHGASPSSN SSN(<i>yoursession</i>) OPTION(*CHGATTR) SSPTIMO(60)</pre> <b>i 6.1 only:</b> Also apply the latest iSCSI group PTF. See <a href="#">IBM i PTFs</a> .
IBM i 7.1 or higher	Set the <b>delivery mode</b> to <b>asynchronous</b> , using the following command:  <pre>CHGASPSSN SSN(<i>yoursession</i>) OPTION(*CHGATTR) DELIVERY(*ASYN) MODE(*ASYN)</pre>

### Related information:

- [IBM i clustering for integrated servers](#)
- [Change ASP Session \(CHGASPSSN\)](#)
- [Implementing high availability](#)

## 7.4.6 Switching an iSCSI-attached VMware ESX server from one node to another

If your IBM i clustering environment uses one of the cross-site mirroring technologies (such as geographic mirroring) and includes VMware ESX servers, then there are some special considerations and procedures required when switching from the production node to the backup node.

**Important:** ESX drives have a signature that is based on the target and initiator iSCSI qualified names (IQNs) from the hosting IBM i system. The IQNs on the backup node are different than they are on the production node, so the signatures do not match after doing a switchover or failover to the backup node. This causes errors when the ESX server tries to access the storage.

To resolve the errors, see the following considerations and procedures for your configuration:

Configuration		Considerations and Procedures
System Drive NOT Mirrored	Shared ESX Embedded hypervisor	<p>The production and backup nodes use the same ESX Embedded hypervisor instance in flash memory (in the same System x or blade server hardware). There is no storage space to mirror for the ESX system drive, but the storage spaces for the virtual machines <b>are</b> mirrored.</p> <p><b>After a switchover or failover:</b>            You must remount the virtual machine drives. See <b>Mount a VMFS Datastore with an Existing Signature</b> section in:            -- <a href="#">vSphere Storage Guide</a> (for ESXi 5 servers)            -- <a href="#">ESXi Configuration Guide</a> (for ESXi 4 or ESX 4 servers)</p>
	Unique ESX server instances	<p>The production and backup nodes have unique ESX server instances (either embedded or non-embedded versions of ESX). The ESX system drive is <b>not</b> mirrored, but the storage spaces for the virtual machines <b>are</b> mirrored.</p> <p><b>After a switchover or failover:</b>            You must delete and re-add the virtual machines by getting their configurations from the disks. See <b>Return a Virtual Machine or Template to vCenter Server</b> in:            -- <a href="#">vSphere Virtual Machine Administration</a> (for ESXi 5 servers)            -- <a href="#">vSphere Basic System Administration</a> (for ESXi 4 or ESX 4 servers)</p>
System Drive Mirrored	Mirrored ESX server instance	<p>The production and backup nodes have mirrored ESX server instances (non-embedded versions of ESX). Therefore, all storage spaces are mirrored, including the ESX system drive.</p> <p><b>After a switchover or failover:</b></p> <p><b>Note:</b> For this configuration, the ESX server will fail to boot successfully after a switchover or failover to the backup node.</p> <p>You must perform the following procedures to recover the drives:</p> <ol style="list-style-type: none"> <li>1. Follow the instructions in VMware Knowledge Base Article <a href="#">ESX fails to boot when the disk containing the data store with esxconsole.vmdk is detected as a snapshot</a> to resignature the drives.</li> <li>2. You must delete and re-add the virtual machines by getting the configurations from the disks. See <b>Return a Virtual Machine or Template to vCenter Server</b> in:            -- <a href="#">vSphere Virtual Machine Administration</a> (for ESXi 5 servers)            -- <a href="#">vSphere Basic System Administration</a> (for ESXi 4 or ESX 4 servers)</li> </ol>

**Related information:**

- [IBM i clustering for integrated servers](#)
  - [Implementing high availability](#)
  - [vSphere Storage Guide](#)
- [vSphere Virtual Machine Administration](#)
  - [ESXi Configuration Guide](#)
  - [vSphere Basic System Administration](#)



## 7.5 Expanding a disk drive for an integrated server

The basic process for expanding an integrated server disk drive is to:

1. **From IBM i:** Expand the virtual storage space that contains the disk volume.
2. **From the server OS:** Extend the disk volume to include the unallocated storage.

The detailed procedure varies based on the type of volume and the [Server OS](#) version:

Volume Type	Server OS	Procedure
Data	ESX	<a href="#">Expanding a data drive for ESX Server</a>
	Windows	<a href="#">Expanding a data drive for Windows Server 2012 or 2008 or 2003</a>
System/Boot	WIN2012	<a href="#">Expanding a system drive for Windows Server 2012/2008</a>
	WIN2008	
	WIN2003	<a href="#">Expanding a system drive for Windows Server 2003</a>

### 7.5.1 Expanding a storage space from IBM i

**Attention:** You should back up your storage space before you expand it.

#### Notes:

- The storage space cannot be expanded from IBM i if it is currently in use by an active server, so if your server is active, then you must either shut down the server or dynamically unlink the storage space before expanding it.
- It can take a considerable amount of time to expand a storage space.

Use **one** of the following methods to expand the storage space from IBM i:

Method	Procedure
<b>Shut down server</b>	<p>This method expands the storage space while the server is shut down. Do the following:</p> <ol style="list-style-type: none"> <li>1. Shut down the server:               <ol style="list-style-type: none"> <li>a. Select <b>Integrated Server Administration</b> from the <a href="#">Web GUI</a> or <a href="#">System i Navigator</a>.</li> <li>b. Select <b>Servers</b>.</li> <li>c. Select the <b>Shut Down</b> action for the server.</li> <li>d. Click <b>Shut Down</b> on the confirmation page.</li> </ol> </li> <li>2. Expand the size of the storage space:               <ol style="list-style-type: none"> <li>a. Select <b>All Virtual Storage</b>.</li> <li>b. Select the <b>Properties</b> action for the storage space.</li> <li>c. Click on the <b>Capacity</b> tab of the virtual storage property sheet.</li> <li>d. Specify the increased virtual storage size in the <b>New capacity</b> field.</li> <li>e. Click <b>OK</b>.</li> </ol> </li> <li>3. Start the server:               <ol style="list-style-type: none"> <li>a. Select <b>Servers</b>.</li> <li>b. Select the <b>Start</b> action for the server.</li> </ol> </li> </ol>

Method	Procedure
Active server	<p>This method uses the capability to dynamically unlink and re-link the storage space to avoid shutting down the server.</p> <p><b>Note:</b> Not all storage spaces can be dynamically unlinked while the server is active, so this method does not work for all storage spaces. Common cases when dynamic unlinking is <b>not</b> allowed are:</p> <ul style="list-style-type: none"> <li>• For ESX servers, <b>no</b> storage spaces can be unlinked while the server is active.</li> <li>• For Windows servers, the storage to unlink cannot be a predefined storage space (the system or install drives), cannot be part of a volume set, and cannot be a volume mounted in a directory. Also, no users can currently be using a volume on the storage space.</li> </ul> <p>Do the following to expand the size of the storage space:</p> <ol style="list-style-type: none"> <li>1. Select <b>Integrated Server Administration</b> from the <a href="#">Web GUI</a> or <a href="#">System i Navigator</a>.</li> <li>2. Select <b>All Virtual Storage</b>.</li> <li>3. Select the <b>Properties</b> action for the storage space.</li> <li>4. Click on the <b>Capacity</b> tab of the virtual storage property sheet.</li> <li>5. Specify the increased virtual storage size in the <b>New capacity</b> field.</li> <li>6. Click <b>OK</b>.</li> <li>7. Click <b>Change</b> on the confirmation panel to confirm that it is acceptable to temporarily make the virtual storage unavailable to the server while the virtual storage is being expanded.</li> </ol> <p><b>Note:</b> The GUI dynamically unlinks the storage space before expanding it and then dynamically re-links the storage space after expanding it. If you do not use the GUI, then you will need to perform the unlink and re-link tasks separately.</p>

**Note** Expanding the storage space from IBM i adds unallocated disk space at the end of the storage space.

**Related information:**

- [IBM i configuration objects for integrated servers](#)
- [Dynamic virtual storage unlinking while server is active](#)

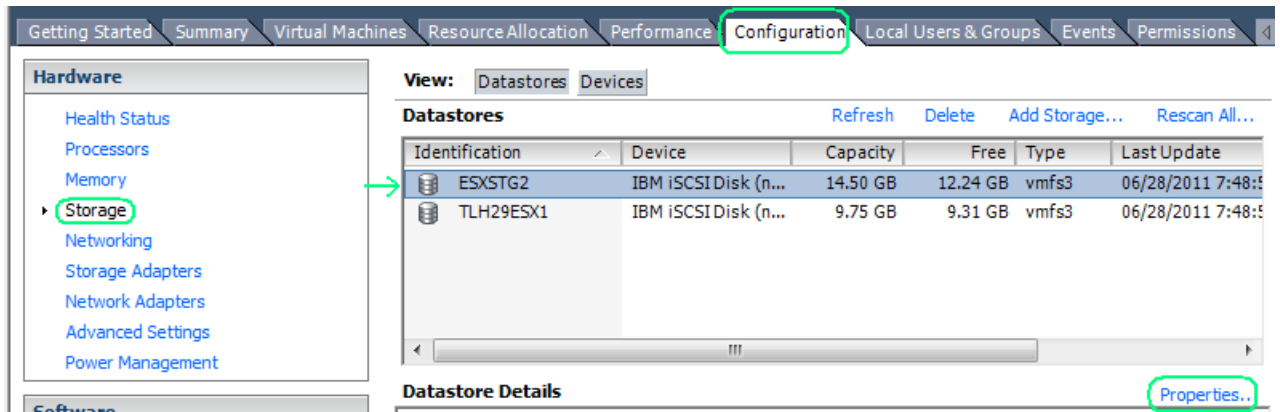
## 7.5.2 Expanding a data drive for ESX Server

To expand a data drive for ESX Server, do the following:

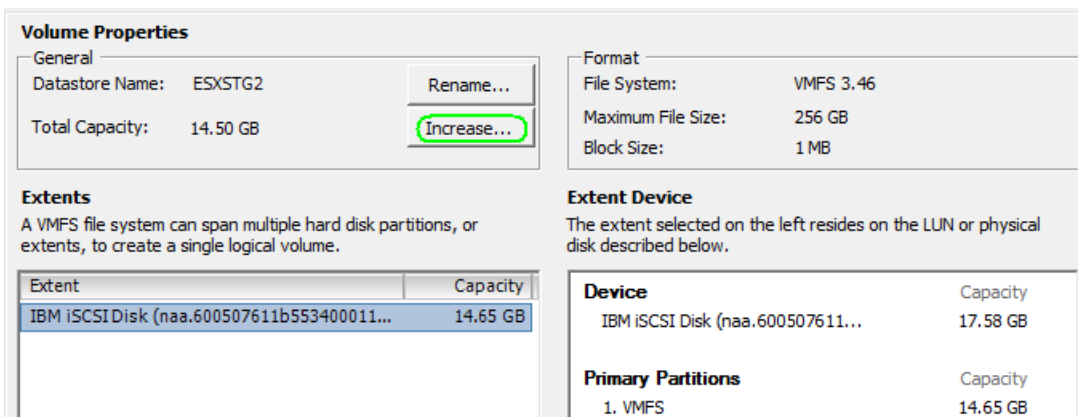
1. Perform the [Shut down server](#) method in the [Expanding a storage space from IBM i](#) section to add unallocated disk space at the end of the storage space.

**Note:** Storage spaces linked to ESX servers cannot be dynamically unlinked while the server is active. Therefore, the [Active server](#) method to expand the storage space from IBM i does **not** work for ESX servers.

2. On the **vSphere Client**, extend the datastore to use the unallocated disk space as follows:
  - a. Connect to the ESX host that uses the storage space.
  - b. Select the **Configuration** tab and then **Storage** hardware.
  - c. Select the Datastore to increase. For example:



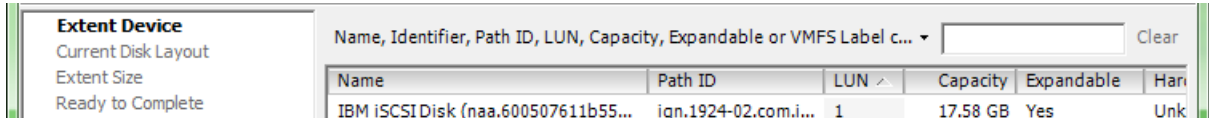
- d. Click **Properties...** to display the datastore properties. For example:



**Note:** In the above example, the device capacity is 17.58 GB, but the current VMFS partition capacity is 14.65 GB. This indicates that there is unallocated storage on the device.

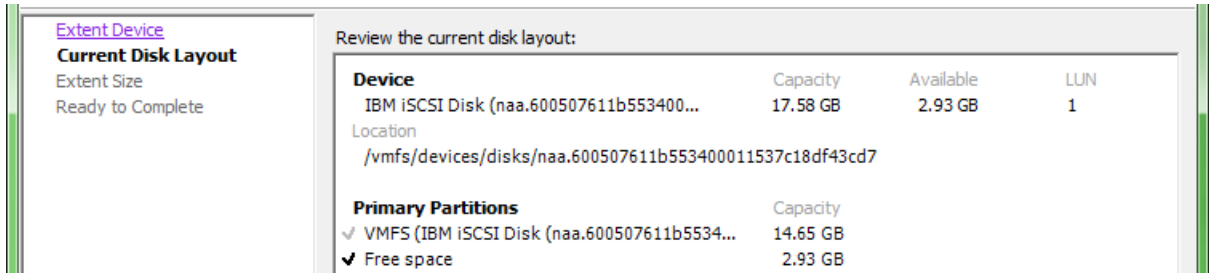
- e. Click **Increase...** to display the **Increase Datastore Capacity Wizard**.

- f. On the **Extent Device** page of the Wizard, select the device to use for extending this datastore and click **Next**. For example:



**Note:** For this scenario, choose the same device that currently contains the datastore so that the unallocated space at the end of the storage space can be used to extend the datastore.

- g. The **Current Disk Layout** page of the Wizard shows that the **Free Space** will be consumed to expand the volume. For example:



Click **Next**.

- h. The **Extent Size** defaults to maximum capacity, so just click **Next** on that page of the Wizard.
- i. On the **Ready to Complete** page of the Wizard, verify the changes to be made, then click **Finish**.
- j. The datastore now contains the previously unallocated disk space and is available to the server.

**Related information:**

- [IBM i configuration objects for integrated servers](#)

### 7.5.3 Expanding a data drive for Windows Server 2012 or 2008 or 2003

To expand a data drive for Windows Server 2012 or 2008 or 2003, do the following:

1. Perform **one** of the methods in the [Expanding a storage space from IBM i](#) section to add unallocated disk space at the end of the storage space.
2. On the Windows server console, extend the volume to use the unallocated disk space as follows:
  - a) Click the option for your Windows version:  
 WIN2012: **Start > Server Manager > Tools > Computer Management**  
 WIN2008: **Start > Administrative Tools > Server Manager**  
 WIN2003: **Start > Administrative Tools > Computer Management**

b) Expand **Storage** in the navigation pane. Then click **Disk Management**.

c) The volume that you want to expand should have some unallocated space immediately following the volume. See volume F: in the following example:



d) Do the appropriate procedure for your version of Windows to extend the volume:

Server OS	Procedure
WIN2012 or WIN2008	<p>Extend the volume using the <b>Extend Volume Wizard</b>:</p> <ol style="list-style-type: none"> <li>1. Right-click the graphical view of the volume that you want to expand in the <b>Disk Management</b> details pane. Then click <b>Extend Volume...</b> For example:               <div data-bbox="467 1186 1442 1449" style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p>The screenshot shows the same Disk Management view as above, but with a context menu open over the 'JAMW20083 (F:)' volume. The menu items are: Open, Explore, Mark Partition as Active, Change Drive Letter and Paths..., Format..., and <b>Extend Volume...</b> (highlighted in blue).</p> </div> </li> <li>2. Follow the instructions in the <b>Extend Volume Wizard</b> to extend the volume.</li> </ol>
WIN2003	<p>Extend the volume using the DISKPART utility:</p> <ol style="list-style-type: none"> <li>1. At a command prompt, type <b>diskpart</b> and press <b>Enter</b> to start the <b>diskpart</b> utility.</li> <li>2. Type <b>list volume</b> and press <b>Enter</b> to display the existing volumes. For example:</li> </ol>

Server OS	Procedure																																																
	<pre>DISKPART&gt; list volume</pre> <table border="1"> <thead> <tr> <th>Volume ###</th> <th>Ltr</th> <th>Label</th> <th>Fs</th> <th>Type</th> <th>Size</th> <th>Status</th> <th>Info</th> </tr> </thead> <tbody> <tr> <td>Volume 0</td> <td>E</td> <td></td> <td></td> <td>CD-ROM</td> <td>0 B</td> <td>Healthy</td> <td></td> </tr> <tr> <td>Volume 1</td> <td>F</td> <td></td> <td></td> <td>DUD-ROM</td> <td>0 B</td> <td>Healthy</td> <td></td> </tr> <tr> <td>Volume 2</td> <td>C</td> <td>JAMW20031</td> <td>NTFS</td> <td>Partition</td> <td>2047 MB</td> <td>Healthy</td> <td>System</td> </tr> <tr> <td>Volume 3</td> <td>D</td> <td>JAMW20032</td> <td>FAT</td> <td>Partition</td> <td>852 MB</td> <td>Healthy</td> <td></td> </tr> <tr> <td>Volume 4</td> <td>G</td> <td>JAMW2003A</td> <td>NTFS</td> <td>Partition</td> <td>1128 MB</td> <td>Healthy</td> <td></td> </tr> </tbody> </table> <p>3. Type <b>select volume &lt;number&gt;</b> and press <b>Enter</b>, where <b>&lt;number&gt;</b> is the number of the volume to be expanded.</p> <p>4. Type <b>extend</b> and press <b>Enter</b> to extend the volume to include any unallocated space immediately following the volume, while preserving the data.</p> <p>You should receive the following message:</p> <p><b>DiskPart successfully extended the volume.</b></p> <p>5. Type <b>exit</b> and press <b>Enter</b> to exit the <b>diskpart</b> utility.</p>	Volume ###	Ltr	Label	Fs	Type	Size	Status	Info	Volume 0	E			CD-ROM	0 B	Healthy		Volume 1	F			DUD-ROM	0 B	Healthy		Volume 2	C	JAMW20031	NTFS	Partition	2047 MB	Healthy	System	Volume 3	D	JAMW20032	FAT	Partition	852 MB	Healthy		Volume 4	G	JAMW2003A	NTFS	Partition	1128 MB	Healthy	
Volume ###	Ltr	Label	Fs	Type	Size	Status	Info																																										
Volume 0	E			CD-ROM	0 B	Healthy																																											
Volume 1	F			DUD-ROM	0 B	Healthy																																											
Volume 2	C	JAMW20031	NTFS	Partition	2047 MB	Healthy	System																																										
Volume 3	D	JAMW20032	FAT	Partition	852 MB	Healthy																																											
Volume 4	G	JAMW2003A	NTFS	Partition	1128 MB	Healthy																																											

- e) The volume now contains the previously unallocated disk space and is available to the server. For example:



**Related information:**

- [IBM i configuration objects for integrated servers](#)
- [Dynamic virtual storage unlinking while server is active](#)
- See the [Microsoft](#) Web page and search for "DISKPART"

### 7.5.4 Expanding a system drive for Windows Server 2012/2008

To expand a system drive for Windows Server 2012/2008, do the following:

1. Use the procedure documented in the [Expanding a data drive for Windows Server 2012 or 2008 or 2003](#) section. However, you **must** use the [Shut down server](#) method in the [Expanding a storage space from IBM i](#) section.

**Notes:**

- You can only extend the system drive boot partition in contiguous unallocated disk space.
- Since a system drive is always in use while the server is active, it cannot be dynamically unlinked while the server is active. Therefore, the [Active server](#) method to expand the storage space from IBM i does **not** work for a system drive.
- The expanded system drive is automatically available immediately after extending the volume. There is no requirement to restart the server.

**Related information:**

- [IBM i configuration objects for integrated servers](#)

## 7.5.5 Expanding a system drive for Windows Server 2003

### Notes:

- You can only extend the system drive boot partition in contiguous unallocated disk space.
- The storage space cannot be expanded from IBM i if it is currently in use by an active server. Since a system drive is always in use while the server is active, the server must be shut down while the system drive storage space is being expanded.
- The system drive for a Windows Server 2003 server (the **owning** server) cannot be extended while it is in use by the **owning** server. Therefore, the following procedure requires a **helper** server, which is an integrated Windows Server 2003 instance other than the **owning** server. The following procedure uses the “**owning** server” and “**helper** server” terms to distinguish which server is used in each step.

If you do not already have another Windows Server 2003 server that you can use as a *helper* server, then you must install another Windows Server 2003 server in order to expand the system drive for the *owning* server.

To expand a system drive for Windows Server 2003, do the following:

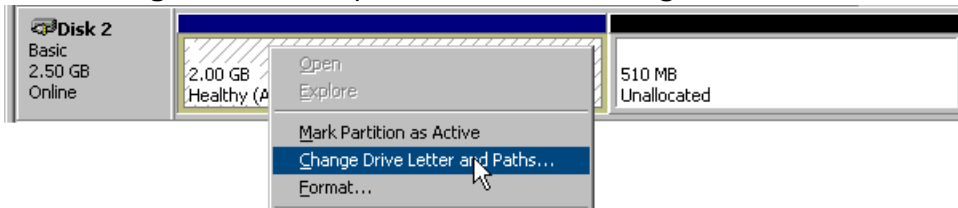
1. Shut down the *owning* server:
    - a) Select **Integrated Server Administration** from the [Web GUI](#) or [System i Navigator](#).
    - b) Select **Servers**.
    - c) Select the **Shut Down** action for the *owning* server.
    - d) Click **Shut Down** on the confirmation page.
  2. Unlink the system drive storage space from the *owning* server:
    - a) Select **All Virtual Storage**.
    - b) Select the **Remove link...** action for the storage space.
    - c) Click **Remove** on the confirmation page.
  3. Expand the size of the storage space:
    - a) Select the **Properties** action for the storage space.
    - b) Click on the **Capacity** tab of the virtual storage property sheet.
    - c) Specify the increased virtual storage size in the **New capacity** field.
    - d) Click **OK**.
- Note** Expanding the storage space from IBM i adds unallocated disk space at the end of the storage space.
4. Link the system drive storage space to the *helper* server as a data disk:
    - a) Select the **Add link...** action for the storage space.
    - b) Select the *helper* server.
    - c) Select sequence position **3** or higher.
    - d) Click **OK**.
  5. If the *helper* server is not already active, start it:
    - a) Select **Servers**.
    - b) Select the **Start** action for the *helper* server.

6. On the *helper* server Windows console, start the Windows **Disk Management** utility and ensure that the newly added system drive storage space from the *owning* server has a drive letter.
  - a) Click **Start > Administrative Tools > Computer Management**.
  - b) Expand **Storage** in the left navigation area and click **Disk Management**.

c) The system drive storage space from the *owning* server should have a partition that is **not** assigned a drive letter, followed by some unallocated space. For example:



d) **Assign** a drive letter to the volume. Right-click the graphical view of the first partition in the **Disk Management** details pane. Then click **Change Drive Letter and Paths...** For example:



On the next panel, click **Add...**, select **Assign the following drive letter**, select an unused drive letter, and then click **OK**.

The system drive storage space from the *owning* server should now have a drive letter assigned to the first partition. For example:



7. On the *helper* server Windows console, extend the partition using the DISKPART utility.
  - a. At a command prompt, type **diskpart** and press **Enter** to start the **diskpart** utility.
  - b. Type **list volume** and press **Enter** to display the existing volumes. For example:

```
DISKPART> list volume
```

Volume ###	Ltr	Label	Fs	Type	Size	Status	Info
Volume 0	E			CD-ROM	0 B	Healthy	
Volume 1	F			DUD-ROM	0 B	Healthy	
Volume 2	C	JAMW2K3H1	NTFS	Partition	2047 MB	Healthy	System
Volume 3	D	JAMW2K3H2	FAT	Partition	852 MB	Healthy	
Volume 4	G	JAMW20031	NTFS	Partition	2047 MB	Healthy	

- c. Type **select volume <number>** and press **Enter**, where **<number>** is the number of the volume to be expanded (the first partition on the system drive storage space from the *owning* server).
- d. Type **extend** and press **Enter** to extend the volume to include any unallocated space immediately following the volume, while preserving the data. You should receive the following message:  
**DiskPart successfully extended the volume.**



e. Type **exit** and press **Enter** to exit the **diskpart** utility.

8. The volume now contains the previously unallocated disk space. For example:



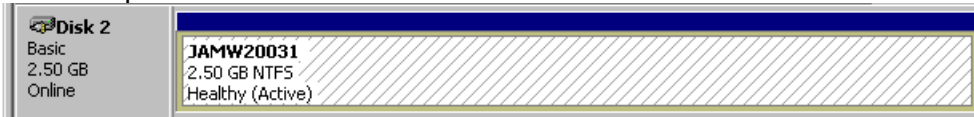
9. **Remove** the drive letter that was assigned to the volume in an earlier step.

**Note:** If you do not remove the drive letter that was assigned earlier (drive letter G: in the above examples), that drive letter will persist and is used for the system drive on the *owning* server.

Right-click the graphical view of the *owning* server system drive volume in the **Disk Management** details pane. Then click **Change Drive Letter and Paths...**

Then click **Remove** and click **Yes** on the confirm panel.

Now the system drive storage space from the *owning* server should no longer have a drive letter. For example:



10. (Optional) Shut down the *helper* server:

- Select **Integrated Server Administration** from the [Web GUI](#) or [System i Navigator](#).
- Select **Servers**.
- Select the **Shut Down** action for the *helper* server.
- Click **Shut Down** on the confirmation page.

11. Unlink the *owning* server's system drive storage space from the *helper* server:

- Select **All Virtual Storage**.
- Select the **Remove link...** action for the storage space.
- Click **Remove** on the confirmation page.

12. Link the expanded storage space to the *owning* server as the system drive:

- Select the **Add link...** action for the storage space.
- Select the *owning* server.
- Select sequence position **1**.
- Click **OK**.

**Note:** If you get a message indicating that the storage must be formatted, you can ignore it.

13. Start the *owning* server:

- Select **Servers**.
- Select the **Start** action for the *owning* server.

The expanded system drive is then available to the *owning* Windows Server 2003 server.

**Related information:**

- [IBM i configuration objects for integrated servers](#)
- See the [Microsoft](#) Web page and search for "DISKPART"

## 7.6 Managing iSCSI target and initiator usage

Use the tasks in the following sub-sections to manage iSCSI target and initiator usage for integrated servers.

### Section Table of Contents

7.6.1	Sharing an iSCSI target among multiple integrated servers .....	362
7.6.2	Distributing iSCSI network traffic between multiple iSCSI targets.....	363
7.6.3	Managing iSCSI initiator allocation at the Windows side of the iSCSI network.....	364
7.6.3.1	Display information about iSCSI initiator allocation.....	366

### 7.6.1 Sharing an iSCSI target among multiple integrated servers

A single iSCSI target installed in IBM i might be able to handle the workload for several servers that do not require high bandwidth for the SCSI and virtual Ethernet LAN traffic. For example, you can share an iSCSI target among several development and test servers if their workload is light.

There are limits to the number of storage and virtual Ethernet paths that an iSCSI target can support. Each active server storage path uses a file server resource in the network server host adapter (NWSH) object that corresponds to the iSCSI target. Likewise, each active server virtual Ethernet path uses a virtual Ethernet resource in the NWSH object. There is a limit to the number of file servers and virtual Ethernet resources that an NWSH can support. This restriction limits how many active servers can use the NWSH.

To see the NWSH file server and virtual Ethernet resource limits, follow these steps:

1. Select **Integrated Server Administration** from the [Web GUI](#) or [System i Navigator](#).
2. Select **Network Server Host Adapters**.
3. Select the **Properties** action for the network server host adapter.
4. Click the **Resource Usage** tab.

The table shows the active servers that are currently using the NWSH and the file server and virtual Ethernet resources that they are currently using. Below the table it shows how many file server and virtual Ethernet resources are still available for use by inactive servers and the total number of file server and virtual Ethernet resources that the NWSH supports.

5. Click **Cancel** on the NWSH properties panel to close the panel.

There is also a practical limit to the number of servers that an iSCSI target can support. The practical limit is determined by the available iSCSI target bandwidth and the workload that is run through the iSCSI target. The practical limit determines how many hosted systems the iSCSI target can support before the limits for the file server and virtual Ethernet resource are reached. The practical limits depend on your server configurations and workloads.

#### Related information:

➤ [Display Device Description \(DSPDEVD\)](#)

➤ [Work with Device Descriptions \(WRKDEVD\)](#)  
(use WRKDEVD \*NWSH)

## 7.6.2 Distributing iSCSI network traffic between multiple iSCSI targets

You can segment the network traffic by identifying which virtual disks and virtual Ethernet LANs require high bandwidth and which ones do not. For example, you can dedicate an iSCSI target to a disk that needs high bandwidth and share another iSCSI target among disks or other servers that do not require high bandwidth.

The way you spread a server's SCSI and virtual Ethernet workload over multiple iSCSI targets is to define multiple storage or virtual Ethernet paths in the network server description (NWSD) and assign which virtual disks and which virtual Ethernets use each path.

To define additional storage or virtual Ethernet paths, follow these steps:

1. Shut down the integrated server.
  - a. Select **Integrated Server Administration** from the [Web GUI](#) (7.2/7.1/6.1) or [System i Navigator](#) (5.4).
  - b. Select **Servers**.
  - c. Select the **Shut Down** action for the server.
  - d. Click **Shut Down** on the confirmation page.
2. Select the **Properties** action for the server.
3. Optional: To define additional storage paths, follow these steps:
  - a. Click the **Storage Paths** tab.
  - b. Click **Add** to define a new storage path.
  - c. Select the network server host adapter (NWSH) that corresponds to the iSCSI target that you want to use for the storage path.
  - d. Click **OK** to add the storage path to the server properties panel. Make note of the path number that is assigned to the new path. The path number is used to identify this path when linking disks later on.
4. Optional: To define additional virtual Ethernet paths, follow these steps:
  - a. Click the **Virtual Ethernets** tab.
  - b. Select the virtual Ethernet port that you want to use a new path for and click **Properties**.
  - c. Select the NWSH that you want to use for the virtual Ethernet port.
  - d. Click **OK** to update the virtual Ethernet port information about the server properties panel. The virtual Ethernet path for the port is implicitly updated as well.
5. On the server properties panel, click **OK** to save the updated storage and virtual Ethernet paths in the NWSD.

If a new storage path was defined, you need to re-link one or more of the server's virtual disks to use the new storage path:

1. First unlink the disk:
  - a. Select **Integrated Server Administration** from the [Web GUI](#) (7.2/7.1/6.1) or [System i Navigator](#) (5.4).
  - b. Select **All Virtual Storage**.
  - c. Select the **Remove link...** action for the storage space.
  - d. Click **Remove** on the confirmation page.
2. Then link the disk to the server again:
  - a. Select the **Add link...** action for the storage space.
  - b. Select the server.
  - c. Select the new storage path number that was added above.
  - d. Click **OK**.

**Related information:**

- [Configuring IBM i for multipath I/O](#)
- [Work with Network Servers \(WRKNWSD\)](#)
- [Change Network Server Desc \(CHGNWSD\)](#)  
(see the STGPTH and VRTETHPTH keywords)

### 7.6.3 Managing iSCSI initiator allocation at the Windows side of the iSCSI network

Use these tasks to configure iSCSI initiator ports and virtual Ethernet information from the Windows operating system.

An iSCSI-attached integrated Windows server can use multiple physical iSCSI initiator ports. An iSCSI initiator port can carry traffic for IBM i storage paths and virtual Ethernet networks. Several factors influence the nature of the traffic that flows through each iSCSI initiator port for the Windows server.

Factors	Description
IP addresses	iSCSI initiator ports can have a SCSI IP address, a LAN IP address, or both. A port with a SCSI IP address can carry storage traffic. A port with a LAN IP address can carry virtual Ethernet traffic. A port with both addresses can carry both types of traffic.
Boot storage configuration	You select the iSCSI initiator port that is used to boot Windows with the iSCSI initiator configuration utility. After the Windows Server has started, the selected iSCSI initiator port continues to provide a connection to the IBM i storage path that corresponds to the system drive.

Factors	Description
Automatic allocation of iSCSI initiator ports to virtual Ethernet and non-boot storage paths	<p>IBM i Integrated Server Support includes several applications for Microsoft Windows. These applications automatically read the IBM i objects that contain the server configuration information. These programs automatically allocate the iSCSI initiator ports to virtual Ethernet and non-boot storage paths.</p> <p>The following conditions will cause Virtual Ethernet ports to be automatically allocated:</p> <ul style="list-style-type: none"> <li>• You start the server (vary on the NWSD).</li> <li>• You restart the Windows server.</li> <li>• You restart the <b>IBM i Virtual Ethernet Manager</b> service from <b>Control Panel &gt; Administrative Tools &gt; Services</b>.</li> <li>• You run the <b>qvndvimir /restart</b> command at a Windows command prompt.</li> <li>• A connection fails. In this case, the affected virtual Ethernet connections are automatically assigned to a different iSCSI initiator port at the hosted system if another initiator is available. Virtual Ethernet uses the failed connection again after the cause of the failure is corrected and one of these conditions for virtual Ethernet automatic allocation occurs.</li> </ul> <p>Any of the following things cause non-boot storage path automatic allocation to occur:</p> <ul style="list-style-type: none"> <li>• You start the server (vary on the NWSD).</li> <li>• You restart Windows.</li> <li>• You restart the <b>IBM Integration Manager</b> service from <b>Control Panel &gt; Administrative Tools &gt; Services</b>.</li> <li>• You run the <b>lvmaster /restart</b> command at a Windows command prompt.</li> </ul>
Manual allocation of storage to a physical iSCSI initiator port	<p>You can manually allocate storage to a physical iSCSI initiator port. You must have a Windows server with multiple iSCSI initiator ports and an IBM i system with multiple iSCSI targets. This task affects iSCSI port usage at both sides of the iSCSI network.</p> <p>Run the <b>qvnimap</b> command at the integrated server console to generate a <b>Storage Device Connection</b> table. In the table look for all rows that show a physical connection to the desired iSCSI initiator port at the Windows server. Note the path numbers in these rows. If there is more than one path number, decide which one you want to use. Then relink the storage space to that path.</p>
Manual allocation of a virtual Ethernet adapter to a physical iSCSI initiator port	<p>If you want to override automatic allocation for virtual Ethernet, you can manually allocate an iSCSI initiator port. At the integrated server console, complete these steps:</p> <ol style="list-style-type: none"> <li>1. Navigate to the <b>Network Connections</b> window.</li> <li>2. Double-click the <b>IBM Virtual Ethernet x</b> adapter that you want to configure.</li> <li>3. Click <b>Properties</b>.</li> <li>4. Click <b>Configure</b>.</li> <li>5. Click <b>Advanced</b>.</li> <li>6. Click <b>Initiator LAN IP Address</b>.</li> <li>7. In Windows, enter the IP address of the iSCSI initiator port that you want the virtual Ethernet adapter to use for its physical connection.</li> </ol> <p>You can use the <b>qvnimap</b> and <b>qvndvimir</b> commands at the Windows console to view more information about iSCSI initiator allocation.</p>

### 7.6.3.1 Display information about iSCSI initiator allocation

You can use the `qvnimap` command to display how iSCSI initiators are being used for a particular Windows server. Make sure you have administrator rights on the integrated server and run the following command at a Windows command prompt on that server.

**qvnimap**

The output consists of several tables. You can also run the following command for a list of options that you can use with the `qvnimap` command.

**qvnimap /?**

There are two types of connection tables, one for storage devices and one for virtual Ethernet networks. In connection tables, an **X** represents a physical connection that is used by the storage device and path or is used by the virtual Ethernet described to the left of the **X**. The two endpoints of the physical connection are the initiator port identified above the **X**, and the target NWSH identified to the immediate left of the **X**. By looking for all occurrences of **X** in a column, you can determine how a particular initiator port is being used.

The **Storage Device Connections** table also shows relationships between storage devices and paths. If you have not assigned a drive letter to a storage space in Microsoft Windows, a blank will appear in the drive column. If a storage space is being used to provide multiple drives, there will be a row for each drive. Logically connected storage paths that are not currently used by any storage device are displayed with a disk value of **None**.

In addition to the connection tables, there are other tables that provide details about the following things:

- iSCSI initiator ports, identified by names such as P1 and P2
- Windows-side Virtual Ethernet port, identified by names such as VRTETHPTP and VRTETH0
- iSCSI targets, identified by NWSH name

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

- "Unknown" for an entire column of a table
- "Unknown" for all virtual Ethernet information
- "RMTIFC MAC address not found" for all configured SCSI MAC addresses

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

Condition	Possible causes
RMTIFC MAC address not found	Incorrect MAC address in the remote system configuration object.
Not operational	The corresponding LAN or virtual Ethernet driver might be disabled or is not installed.
Link down	<p>On a physical port, such as P1, this might be a cable or switch problem.</p> <p>On a virtual Ethernet port, such as VRTETHPTP, this might be caused by one of the following things:</p> <ul style="list-style-type: none"> <li>• A physical port, network, or network server host adapter (NWSH) problem.</li> <li>• The target and initiator might be on different LAN IP subnets without a router.</li> <li>• The IBM i Integration Manager, IBM i Shutdown Manager, or IBM i Virtual Ethernet Manager service might not be started in Windows.</li> </ul>

## 7.7 Additional integrated Windows server topics

Use these tasks to manage integrated servers running Windows Server.

### Section Table of Contents

7.7.1	Formatting storage for Windows servers.....	368
7.7.2	Enabling Windows share names for file level backup from IBM i.....	369
7.7.3	Managing virtual Ethernet networks.....	371
7.7.3.1	Display information about virtual Ethernet adapters.....	371
7.7.3.2	Configuring IP address, gateway, and MTU values for integrated servers.....	371
7.7.3.2.1	Configuring VE for applications that support frame sizes larger than 1500 bytes	371
7.7.3.2.2	Configuring VE for iSCSI networks with a frame size less than 1500 bytes.....	372
7.7.3.2.3	Configuring VE to support non-TCP applications that do not negotiate MTU.....	372
7.7.3.3	Configuring virtual Ethernet networks between integrated Windows servers.....	373
7.7.3.4	Configuring inter-partition virtual Ethernet for integrated Windows servers.....	374
7.7.3.5	Managing point-to-point virtual Ethernet networks for integrated Windows servers	375
7.7.3.5.1	Viewing point-to-point (PTP) virtual Ethernet connections from IBM i.....	375
7.7.3.5.2	Viewing PTP virtual Ethernets from the integrated Windows server console.....	376
7.7.4	Sharing tape and optical devices between IBM i and integrated Windows servers.....	377
7.7.4.1	Using IBM i tape devices with integrated Windows servers.....	377
7.7.4.1.1	Installing tape device drivers on Windows.....	377
7.7.4.1.2	Formatting an IBM i tape for use with an integrated Windows server.....	378
7.7.4.1.3	Transferring an IBM i tape device to an integrated Windows server.....	378
7.7.4.1.4	Transferring a tape device from integrated Windows server to IBM i.....	379
7.7.4.1.5	Identifying IBM i tape devices to Windows applications.....	380
7.7.4.2	Using IBM i optical devices with integrated Windows servers.....	381
7.7.4.2.1	Transferring an optical device from IBM i to an integrated Windows server.....	381
7.7.4.2.2	Transferring an optical device from an integrated Windows server to IBM i.....	382
7.7.4.3	Transferring IBM i tape and optical devices between integrated Windows servers.....	382
7.7.4.4	Restricting IBM i tape and optical devices from integrated Windows servers.....	383
7.7.5	Printing to IBM i printers from integrated Windows servers.....	384
7.7.6	Running integrated Windows server commands remotely.....	385
7.7.6.1	Guidelines for running remote commands on an integrated Windows server.....	386
7.7.6.1.1	SBMNWSCMD and file level backup support for Kerberos V5 and EIM.....	388
7.7.7	Configuring time synchronization for integrated Windows server.....	389
7.7.8	Firewall considerations for Windows servers.....	390
7.7.9	Windows Server 2003 topics.....	392
7.7.9.1	Integrating a service pack with Windows Server 2003.....	392
7.7.9.2	Windows Server 2003 Service Pack 1.....	393
7.7.9.3	Using IBM i virtual optical support for Windows Server 2003 installations.....	393
7.7.9.4	Creating a Windows Server 2003 install CD image in IFS.....	395
7.7.9.5	Using the Windows Server 2003 Backup utility with integrated servers.....	396
7.7.9.6	Migrating IXS/IXA Windows Server 2003 to iSCSI.....	396

## 7.7.1 Formatting storage for Windows servers

Do these steps to format virtual storage for an integrated server with the Windows operating system.

1. On the integrated Windows server console, select:  
WIN2012: **Start >Server Manager >Tools > Computer Management**  
WIN2008: **Start > Administrative Tools > Server Manager.**  
WIN2003: **Start > All Programs > Administrative Tools > Computer Management.**
2. Expand **Storage** in the navigation pane. Then click **Disk Management**.
3. 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**.
4. 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 virtual storage.
  - c. Select the quick format for a storage space that has just been created. It has already been low level formatted by IBM i when it was allocated.

### Related information:

➤ [Virtual storage formatting](#)

➤ [Storage alignment considerations for multiple partitions](#)



## 7.7.2 Enabling Windows share names for file level backup from IBM i

To enable Windows file-level backup and recovery from IBM i, you must list the Windows share names that are enabled for backup in a member of the IBM i QAZLCSAVL file in the QUSRSYS library.

### Notes:

1. Use normal Windows operating system methods to create the share names on Windows. This is usually done before the share names are enabled from IBM i, but that is not a requirement.
2. Windows share names can be quite long. However, share names that are visible in the IBM i QNTC file system are restricted to 12 characters or less. Keep this in mind when defining share names on Windows, if you want to enable them for backup from IBM i.
3. Share names can have embedded blanks.
4. You can see the valid share names under the /QNTC/*servername* directory in the IFS. The server must be active in order for the share names to be visible in the QNTC file system.
5. The IBM i user who views the share names under the /QNTC/*servername* directory must be authorized to the share names in Windows, either via public or explicit authority.
6. If you enable multiple share names for backup that point to the same Windows server directory, IBM i saves the data multiple times for a "save all" request. To avoid duplicating data when you save it, do not enable multiple shares that include the same Windows directory or data.

Choose **one** of the following methods to enable Windows share names for backup from IBM i:

IBM i	Method	Tasks
i 7.2 i 7.1 i 6.1	<a href="#">Web GUI</a> <b>Server Properties task</b>	<p>Perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Using the IBM i <a href="#">Web GUI</a>, select <b>Servers</b>.</li> <li>2. Display the properties for the appropriate Windows server.</li> <li>3. Click on the <b>File Level Backup</b> tab in the server properties.</li> <li>4. Put a check mark next to the share names to enable for backup. <p><b>Note:</b> The server must be active in order for the share names to be automatically listed on the <b>File Level Backup</b> tab in the server properties. If the server is not currently active when you display the server properties, then you can use <b>Insert...</b> to manually insert share names to enable for backup.</p> </li> <li>5. Click <b>OK</b> to save the changes. <p><b>Note:</b> This adds a member to the QAZLCSAVL file, if necessary, and updates it to list the share names that you enabled for backup.</p> </li> </ol>

IBM i	Method	Tasks
All	<p><b>Manually Create and Edit the QAZLCSAVL file member</b></p>	<p>Perform the following steps:</p> <ol style="list-style-type: none"> <li>On the IBM i command line, use the Add Physical File Member (ADDPFM) command to add a file member, if necessary: <pre>ADDPFM FILE(QUSRSYS/QAZLCSAVL) MBR(<i>nwsdname</i>) TEXT('description') EXPDATE(*NONE) SHARE(*NO) SRCTYPE(TXT)</pre> <p>where <i>nwsdname</i> is the NWSD name for the server and <i>description</i> is a short description of your choice.</p> </li> <li>Using an editor of your choice, edit the file member created above.</li> <li>List the share names to enable for backup, one share name per record of the member. <p>For example, if you defined cshare, dshare, eshare, fshare, gshare, and my share as share names on the Windows server, then the records in the QAZLCSAVL file member would look like this:</p> <pre>0001.00 cshare 0002.00 dshare 0003.00 eshare 0004.00 fshare 0005.00 gshare 0006.00 my share</pre> </li> <li>Save the updates to the QAZLCSAVL file member.</li> </ol>

**Related information:**

- [Backup and recovery concepts](#)

## 7.7.3 Managing virtual Ethernet networks

Use these tasks to configure and manage the virtual Ethernet networks for integrated Windows servers.

### 7.7.3.1 Display information about virtual Ethernet adapters

To display information, such as UDP port numbers, for virtual Ethernet adapters on a particular Windows server, run the following command at a Windows command prompt on that server.

```
qvndvivr /status
```

### 7.7.3.2 Configuring IP address, gateway, and MTU values for integrated servers

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

- The IP address and subnet mask are automatically assigned when a virtual Ethernet line is added to an existing server and the server is restarted. After the server is restarted, these values can only be changed from within the Windows operating system.
- Configure virtual Ethernet point-to-point IP address changes in both the Windows operating system and IBM i. For more information, go to the [Troubleshooting](#) Web page and search for **Point to point virtual Ethernet IP address conflicts**.
- When using iSCSI hardware initiators, the virtual Ethernet MTU size is configured using the appropriate iSCSI initiator configuration utility. See [Changing the iSCSI initiator MTU](#).

#### 7.7.3.2.1 *Configuring VE for applications that support frame sizes larger than 1500 bytes*

Do these steps to configure virtual Ethernet (VE) to support jumbo frames for an integrated server.

For information about configuring the virtual Ethernet frame size for your iSCSI initiator adapters, see [Changing the iSCSI initiator MTU](#).

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

- For Windows virtual Ethernet adapters, Maximum Frame Size defaults to Auto. This value causes virtual Ethernet to calculate a maximum frame size based on the Ethernet Frame Size of the iSCSI initiator adapter port used. See [Managing iSCSI initiator allocation at the Windows side of the iSCSI network](#) for an explanation of iSCSI initiator adapter port usage.
- In IBM i virtual Ethernet line descriptions, **Maximum frame size (MAXFRAME)** defaults to **8996**.
- In IBM i TCP/IP interfaces for virtual Ethernet, **Maximum transmission unit (MTU)** defaults to **\*LIND**.

### **7.7.3.2.2 Configuring VE for iSCSI networks with a frame size less than 1500 bytes**

Do these steps to configure virtual Ethernet (VE) for iSCSI networks that have a maximum frame size that is less than 1500 bytes.

At the Windows console, perform the following steps:

1. Navigate to the **Network Connections** Window.
2. Double click the **IBM Virtual Ethernet x** adapter that will use an iSCSI initiator adapter connected to the iSCSI network having a maximum frame size less than 1500 bytes.
3. Click on **Properties**.
4. Click on **Configure**.
5. Click on **Advanced**.
6. Click on **Maximum Frame Size**.
7. Select a value that is as large as possible without exceeding the maximum frame size of the iSCSI network.

### **7.7.3.2.3 Configuring VE to support non-TCP applications that do not negotiate MTU**

Do these steps to configure virtual Ethernet (VE) for an integrated Windows server to support applications that do not use TCP and do not negotiate maximum transmission unit (MTU).

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

1. Do **one** of the following steps:
  - a. If all Windows endpoints use an iSCSI network having a maximum frame size of 1500 bytes or greater, configure the iSCSI initiator adapter Ethernet frame size at all Windows endpoints to a value as large as possible without exceeding the maximum frame size of the most constrained iSCSI network.
  - b. If any Windows endpoint uses an iSCSI network having a maximum frame size less than 1500 bytes, configure the virtual Ethernet Maximum frame size at all Windows endpoints to a value as large as possible without exceeding the maximum frame size of the most constrained iSCSI network.
2. At other endpoints, set the MTU to a value determined by subtracting **116** from the smaller of the Windows iSCSI initiator adapter Ethernet frame size and the virtual Ethernet Maximum frame size.

For IBM i endpoints, you can accomplish this by performing the following procedure:

- a. Select **Network** from the [Web GUI](#) or [System i Navigator](#).

- b. **Web GUI only:** Click **Show All Network Tasks**.
- c. Select **Network > TCP/IP Configuration > IPv4 > Interfaces**.
- d. Click the menu icon for the interface with the IP address and line description name of interest and select **Properties**.
- e. On the **Advanced** tab, type the calculated value in the Maximum transmission unit field and click **OK** to save the change.

**Related information:**

- [Configure TCP/IP \(CFGTCP\)](#) (use CFGTCP, then option 1)

### 7.7.3.3 Configuring virtual Ethernet networks between integrated Windows servers

Do these steps to configure a virtual Ethernet network between integrated Windows servers that are configured in the same logical partition.

1. Configure a virtual Ethernet port and line description for the integrated server.
  - a. Select **Integrated Server Administration** from the [Web GUI](#) or [System i Navigator](#).
  - b. Select **Servers**.
  - c. Click the menu icon for the integrated server and select **Properties**.
  - d. On the server properties panel, click the **Virtual Ethernet** tab.
  - e. Click **Add...** to add a new virtual Ethernet port.
  - f. On the virtual Ethernet properties panel, specify the values for the new virtual Ethernet port
    - A. Select the virtual Ethernet port number.
    - B. Type the IP address that the integrated server will use.
    - C. Type the subnet mask that the integrated server will use.
    - D. 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*.
    - E. Leave the associated port set to **None**.
    - F. Leave the maximum frame size set to the default **8996**.
    - G. Select the network server host adapter corresponding to the iSCSI target adapter port that you want IBM® i to use for this virtual Ethernet configuration to reach the hosted system.
    - H. Click **OK** to add the new port to the **Virtual Ethernet** tab on the server properties panel.

- g. 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.
  - h. 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.

### 7.7.3.4 Configuring inter-partition virtual Ethernet for integrated Windows servers

If you want an integrated Windows server to communicate with other logical partitions, or with integrated servers controlled by other IBM i partitions, you need to configure one or more inter-partition networks.

Inter-partition connections exist between partitions or integrated servers using the same VLAN ID. Participating integrated servers do not support VLAN IDs directly. Instead, each participating integrated server needs an Ethernet line description that associates a virtual Ethernet port value with a virtual adapter having a VLAN ID. The configuration procedure consists of the following steps:

1. Create a virtual Ethernet adapter for each partition and each integrated server that will participate in the inter-partition network. For more information, see [Logical partitioning](#) in the IBM Systems Hardware Information Center. For each virtual adapter that will connect an integrated server or IBM i 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 [Configuring virtual Ethernet networks between integrated Windows servers](#). Select an associated port name (Cmnxx) for the appropriate 268C resource.
3. Continue with step 2 of [Configuring virtual Ethernet networks between integrated Windows servers](#) (in all IBM i partitions that control a participating integrated server), and step 3 of [Configuring virtual Ethernet networks between integrated Windows servers](#).
4. For a partition to fully participate, you will need to appropriately configure the protocol(s) within the partition. In each IBM i partition, create an Ethernet line description on the appropriate dedicated 268C port resource and configure a TCP/IP interface that references the line description. Configure an appropriate unique IP address in each partition that will participate in TCP/IP communications.
5. Test to see if the inter-partition network is functioning. For example, ping between connected integrated servers and partitions.

### 7.7.3.5 Managing point-to-point virtual Ethernet networks for integrated Windows servers

Each integrated Windows server has a point-to-point (PTP) virtual Ethernet network connection with IBM i, which allows IBM i to do management tasks on the integrated server.

These connections are automatically configured during installation. You can view and manage these connections from IBM i or the integrated Windows server console.

#### 7.7.3.5.1 Viewing point-to-point (PTP) virtual Ethernet connections from IBM i

Point to point virtual Ethernet connections in IBM i are composed of a line description and an entry in an integrated server NWSD.

1. To view the line description issue the command `WRKCFGSTS *NWS` from the IBM i 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 NWSD. Issue the command `WRKNWSD`. Find your integrated server 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.

#### Related information:

- [Work with Configuration Status \(WRKCFGSTS\)](#)
- [Work with Network Servers \(WRKNWSD\)](#)
- [Configure TCP/IP \(CFGTCP\)](#)

### **7.7.3.5.2 Viewing PTP virtual Ethernets from the integrated Windows server console**

To view point-to-point (PTP) virtual Ethernet connections:

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 IBM i 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 IBM i 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 IBM i 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 IBM i command to ping the integrated server. For example, enter `ping '192.168.3.2'`.



## 7.7.4 Sharing tape and optical devices between IBM i and integrated Windows servers

Use these tasks to configure an integrated Windows server to use IBM i tape and optical devices.

### 7.7.4.1 Using IBM i tape devices with integrated Windows servers

IBM i tape drives can perform faster than drives you normally attach to an IBM BladeCenter or System x server. You can allocate IBM i tape drives to integrated Windows servers, therefore providing a faster tape access method than available to stand-alone servers.

Because multiple integrated Windows servers in the same IBM i partition can all access the same tape drive (although not at the same time), one tape drive can be shared among multiple integrated Windows servers.

#### Notes:

1. Although you can use IBM i tape drives from both the integrated server and from IBM i, 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 Windows server and on IBM i without reformatting it.
2. If you have logical partitions on your Power server, the tape drive is allocated to a single partition. It cannot be shared by integrated Windows servers that are in other partitions.
3. See the following sections for information about which IBM i tape devices are supported for use with each Windows operating system version:
  - [IBM i tape devices for Windows Server 2008/2012](#)
  - [IBM i tape devices for Windows Server 2003](#)

To use an IBM i tape drive from an integrated Windows server, see the tasks in the following sub-sections.

#### 7.7.4.1.1 *Installing tape device drivers on Windows*

Download and install Windows device drivers for tape devices. For information about supported tape device drivers, see the appropriate section below for your Windows operating system version:

- [IBM i tape devices for Windows Server 2008/2012](#)
- [IBM i tape devices for Windows Server 2003](#)

Install the tape device driver using the instructions provided by the driver provider. Review the readme file for the device driver. Make sure to install the driver using the nonexclusive option for use with Microsoft Removable Storage Manager.

Using the new tape drivers, the tape drives look identical to drives available for System x or BladeCenter blade hardware. The devices are listed by type-model number in the device locking/unlocking utility.

### 7.7.4.1.2 **Formatting an IBM i tape for use with an integrated Windows server**

Use the IBM i Initialize tape (INZTAP) command to format IBM i tape media to work with your integrated Windows servers.

To format a tape, do the following steps:

1. Insert a tape in the IBM i tape drive.
2. At the IBM i command line, enter:

```
INZTAP DEV(tap01) NEWVOL(*NONE) NEWOWNID(*BLANK) VOL(*MOUNTED) CHECK(*NO)
DENSITY(*CTGTYPE) CODE(*EBCDIC)
```

where *tap01* is the name of your tape drive.

3. Press **Enter**.

### 7.7.4.1.3 **Transferring an IBM i tape device to an integrated Windows server**

Do these steps to allocate an IBM i tape device to an integrated Windows server.

**Note:**

Some tape devices report in under more than one device description. Tape libraries (3590, 3570, and so on) report in as devices (TAPxx) as well as tape libraries (TAPMLBxx), where xx is a number. IBM i 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 Windows server.

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

1. Vary off the tape device on IBM i.
  - a. At the IBM i command line, type `WRKCFGSTS *DEV *TAP` and press **Enter**. The **Work with Configuration Status** display appears.

**Note:** `WRKCFGSTS *DEV *TAPMLB` displays a list of the tape library devices.
  - b. In the **Opt** column next to the device name of your tape device, type **2** to vary off the tape device.
  - c. Press **Enter**. The tape device varies off.
2. Lock the tape device from the integrated Windows server console:
  - a. i 7.2 or 7.1: Click **Start > All Programs > IBM i > IBM i Integrated Server Support**  
i 6.1 or 5.4: Click **Start > All Programs > IBM iSeries > IBM iSeries Integrated Server Support**
  - b. Expand **Integrated Server Support**
  - c. Expand the network server description name.

- d. Select **i5/OS Devices**.
- e. Right-click the device and select **All Tasks > Lock Device**.

If you need other information about the tape device to enable an application to recognize it, see [Identifying IBM i tape devices to Windows applications](#).

#### **7.7.4.1.4 Transferring a tape device from integrated Windows server to IBM i**

For IBM i to use a tape device currently locked on an integrated Windows server, you must first unlock it from the integrated server and then vary it on from IBM i.

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

To transfer control of an IBM i tape device from an integrated Windows server to IBM i, follow these steps:

1. Unlock the tape device from the integrated Windows server console:
  - a. i 7.2 or 7.1: Click **Start > All Programs > IBM i > IBM i Integrated Server Support**  
i 6.1 or 5.4: Click **Start > All Programs > IBM iSeries > IBM iSeries Integrated Server Support**
  - b. Expand **Integrated Server Support**
  - c. Expand the network server description name.
  - d. Select **i5/OS Devices**.
  - e. Right-click the device and select **All Tasks > Unlock Device**.
2. Make the device available to IBM i. From the IBM i 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 device name (for example, TAP01), type **1** to vary on the tape device.
  - c. Press **Enter**. The tape device varies on.
  - d. Change the tape to one formatted for IBM i.

### 7.7.4.1.5 *Identifying IBM i tape devices to Windows applications*

Do these steps to identify an IBM i tape device to Windows applications.

Windows applications do not refer to tape devices by device description or hardware resource name as IBM i 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 > All 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 IBM i 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.

## 7.7.4.2 Using IBM i optical devices with integrated Windows servers

Configure your integrated Windows server to use IBM i optical devices.

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

If you have logical partitions on your Power server, 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 an NWSD to be used.

To use an IBM i optical device from an integrated Windows server, see the tasks in the following subsections.

### 7.7.4.2.1 *Transferring an optical device from IBM i to an integrated Windows server*

The IBM i optical device must be varied on before you can allocate it to an integrated Windows server.

To transfer control of an IBM i optical device to an integrated Windows server, follow these steps:

1. If the optical device is not varied on in IBM i, vary it on.
  - a. At the IBM i 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 device.
  - c. Press **Enter** and the optical device varies on.
2. On the integrated Windows server console, lock the optical device:
  - a. i 7.2 or 7.1: Click **Start > All Programs > IBM i > IBM i Integrated Server Support**  
i 6.1 or 5.4: Click **Start > All Programs > IBM iSeries > IBM iSeries Integrated Server Support**
  - b. Expand **Integrated Server Support**
  - c. Expand the network server description name.
  - d. Select **i5/OS Devices**.
  - e. Right-click the device and select **All Tasks > Lock Device**.

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

### 7.7.4.2.2 *Transferring an optical device from an integrated Windows server to IBM i*

To use the optical device from IBM i, you must first unlock it from the integrated server.

**Note:** To unlock the optical device from the integrated server, you must either be the person who originally locked the device or have **Administrator** or **Backup Operator** authority.

On the integrated Windows server console, unlock the optical device:

1. i 7.2 or 7.1: Click **Start > All Programs > IBM i > IBM i Integrated Server Support**  
i 6.1 or 5.4: Click **Start > All Programs > IBM iSeries > IBM iSeries Integrated Server Support**
2. Expand **Integrated Server Support**
3. Expand the network server description name.
4. Select **i5/OS Devices**.
5. Right-click the device and select **All Tasks > Unlock Device**.

**Note:** No action is required on IBM i, since the IBM i optical device is already varied on.

### 7.7.4.3 **Transferring IBM i tape and optical devices between integrated Windows servers**

IBM i tape and optical devices can only be used by one integrated Windows server at a time. Do these steps to transfer IBM i tape and optical devices between integrated servers.

To transfer control of tape and optical devices 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 Power server, the tape or optical device is allocated to a single partition and cannot be shared by integrated servers that are in other partitions.

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

1. On the console of the integrated Windows server that has control of the device, unlock the device:
  - a. i 7.2 or 7.1: Click **Start > All Programs > IBM i > IBM i Integrated Server Support**  
i 6.1 or 5.4: Click **Start > All Programs > IBM iSeries > IBM iSeries Integrated Server Support**
  - b. Expand **Integrated Server Support**
  - c. Expand the network server description name.
  - d. Select **i5/OS Devices**.
  - e. Right-click the device and select **All Tasks > Unlock Device**.

2. On the console of the integrated Windows server that you want to give control of the device, lock the device:
  - a. i 7.2 or 7.1: Click **Start > All Programs > IBM i > IBM i Integrated Server Support**  
i 6.1 or 5.4: Click **Start > All Programs > IBM iSeries > IBM iSeries Integrated Server Support**
  - b. Expand **Integrated Server Support**
  - c. Expand the network server description name.
  - d. Select **i5/OS Devices**.
  - e. Right-click the device and select **All Tasks > Lock Device**.

#### 7.7.4.4 Restricting IBM i tape and optical devices from integrated Windows servers

You can prevent an integrated Windows server from using a particular tape or optical device by specifying the tape or optical device as a restricted resource in the NWSD for the server.

Shut down the integrated server:

1. Select **Integrated Server Administration** from the [Web GUI](#) or [System i Navigator](#).
2. Select **Servers**.
3. Select the **Shut Down** action for the server.
4. Click **Shut Down** on the confirmation page.

Do these steps to make IBM i devices inaccessible to an integrated server.

1. Select the **Properties** action for the server.
2. Select the **System** tab.
3. Click **Advanced**.
4. Go to the **Restricted Devices** tab and select the devices you want to restrict.
5. Click **OK** to return to the server properties page.
6. Click **OK** again to save the server properties.

Start the integrated server:

1. Select the **Start** action for the server.

**Related information:**

➤ [Work with Network Servers \(WRKNWSD\)](#)

➤ [Change Network Server Desc \(CHGNWSD\)](#)

## 7.7.5 Printing to IBM i printers from integrated Windows servers

Do these steps to configure an integrated Windows server to print to an IBM i printer.

To send a print job to IBM i, you must set up the IBM i 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 IBM i printers, perform these tasks:

1. Set up the IBM i printer for TCP/IP printing. For more information, see the [TCP/IP Setup](#) topic collection.
2. Set up the integrated server to print to IBM i printers:
  - a. From the **Start** menu on Windows, click **Printers and Faxes**. The **Printers and Faxes** window appears.
  - b. Double-click the **Add Printer** icon. The **Add Printer Wizard** starts.
  - c. Click **Network Printer**.
  - d. On the **Locate your Printer** panel, type the printer name or click **Next** to browse for the printer.



## 7.7.6 Running integrated Windows server commands remotely

You can use IBM i to remotely submit integrated Windows server batch commands. Windows server commands that can run in batch mode without user interaction will work.

Before submitting a remote command verify that the following are true:

- The server is an Integrated Windows Server on this IBM i system 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 LCLPDMGT 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 LCLPDMGT value is \*NO, then network authentication (Kerberos) is used. The user must access the IBM i operation through Kerberos enabled applications. See [Guidelines for running remote commands on an integrated Windows server](#).
- The IBM i user profile password, and Windows password must be equivalent. The easiest way to keep them consistent is to use User and Group enrollment.

To run integrated Windows server commands:

1. Select **Integrated Server Administration** from the [Web GUI](#) or [System i Navigator](#).
2. Select **Servers**.
3. Select the **Run command** action for the integrated Windows server on which to run the batch command.
4. 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.

5. 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 IBM i 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 name for the server you want to run the command on and press **Enter**.
5. The IBM i user profile 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 is displayed on the console. Press F10 to see all messages.

### 7.7.6.1 Guidelines for running remote commands on an integrated Windows server

The environment, user, and interface must be configured to run remote commands on an integrated Windows server.

**Note:** Many of the Submit Network Server Command (SBMNWSCMD) CL command parameters listed in this section are not available when running Windows commands from the IBM i GUI. If you need to use a parameter that the GUI 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 LCLPDMGT user profile attribute is \*NO. See [SBMNWSCMD and file level backup support for Kerberos V5 and EIM](#).
- 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 code sets. 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 IBM i, 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 IBM i 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.

### **7.7.6.1.1 SBMNWSCMD and file level backup support for Kerberos V5 and EIM**

You can use Kerberos V5 for some types of remote commands and backup.

File level backup operations to an integrated Windows server utilize the IBM i NetClient and Submit Network Server Command (SBMNWSCMD) functions. These functions provide limited Kerberos v5 support (also known as IBM 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 IBM i to use Kerberos authentication, you must configure these things on IBM i:
  - [Network authentication service](#)
  - [Enterprise Identity Mapping](#)
  - [Network authentication service planning work sheets](#)
2. IBM i NetServer should be configured to use Password/Kerberos v5 authentication and NetServer must be active.
3. The Kerberos KDC must be a Windows Active Directory domain controller.
4. Kerberos authentication will only be used when the user profile associated with the IBM i job 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 IBM i profile name. Thus, user enrollment can look for an EIM registry which is named for the Windows Active Directory domain name, or for an 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 IBM i 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 IBM i profile name.

- 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, 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**.

### 7.7.7 Configuring time synchronization for integrated Windows server

Time synchronization for your integrated Windows server needs to be configured both in IBM i and the integrated Windows server operating system.

To keep the time on IBM i and the integrated Windows server synchronized, do the following steps:

- Select **Integrated Server Administration** from the [Web GUI](#) or [System i Navigator](#).
- Select **Servers**.
- Select the **Properties** action for the server.
- Select the **System** tab.
- Click **Advanced**.
- On the **Configuration** tab, select the **Synchronize integrated server date and time with host** option that you want. Possible values include:

Option	Description
<b>Every 30 minutes while the server is active</b>	The system synchronizes the time between IBM i and the integrated Windows server every 30 minutes.
<b>Once every time the server is started</b>	The system synchronizes the date and time only when the integrated Windows server is started.
<b>Do not synchronize date and time</b>	The system does not synchronize the date and time for the integrated Windows server.

- Click **OK** to return to the server properties page.
- Click **OK** again to save the server properties.
- Ensure that the IBM i time, date, and time zone are correct. Once these values are set, they are automatically updated every six months for daylight saving time adjustments. See [Time management](#) for more information.

After you complete the server installation, you need to configure additional settings at the integrated server console.

If you have problems with time synchronization, check the IBM i system value for LOCALE to make sure that it is set properly.

**Related information:**

- [Work with Network Servers \(WRKNWSD\)](#)
- [Change Network Server Desc \(CHGNWSD\)](#)

## 7.7.8 Firewall considerations for Windows servers

This section addresses using an iSCSI attached Windows server as a firewall to protect your internal network.

There are also some special considerations when using the **Windows Firewall** function that was introduced with Windows Server 2003 Service Pack 1 (SP1) to protect the Windows server itself. See [Windows Server 2003 Service Pack 1](#) for more information.

**Note:** The Windows Server 2003 SP1 security changes are also included in later Windows Server 2003 service packs (for example, SP2) and in later Windows Server versions such as Windows Server 2003 R2, Windows Server 2008 and Windows Server 2012. The SP1 considerations listed below also apply to later Windows Server versions.

### Hardware:

In order to use an integrated Windows server as a firewall, at least two LAN adapters are required on the server; one for the secure subnet and the other for the perimeter or public network.

### Hardening:

If you choose to harden your firewall system, there are a few considerations to keep in mind. Hardening your system turns off the **Workstation** and **Server** services. These services are used by some of the IBM i Integrated Server Support code, so the following restrictions apply on a hardened system:

1. When you install an IBM i Integrated Server Support service pack, you must temporarily turn on the **Workstation** service.
  - a) Go to the **Services** icon on your Windows server.
  - b) Look for the **Workstation** service. If it is disabled, highlight it and click **Startup**. Change the **Startup Type** to **Manual**.
  - c) Highlight the **Workstation** service and click **Start** if it is not already started.
  - d) Install the IBM i Integrated Server Support service pack.
  - e) When the service pack installation has completed, you can go back to **Services**, click **Startup** for the **Workstation** service and change the **Startup Type** back to **Disabled**.
2. When using the [Web GUI](#) or [System i Navigator](#) GUI to view the server properties, or option 5 of the Work with Network Server Status (WRKNWSSTS) command, the following field restrictions apply:
  - a) The Windows Domain name will be blank.
  - b) The Server description text will be blank.
3. User enrollment to the local server is still allowed, but user enrollment to the primary domain of the server is not allowed.

4. A 5-minute delay has been added to wait for the **Server** service to start, and a 5-minute delay to wait for the **Workstation** service to start.<sup>1</sup> If you have hardened your firewall system and plan to leave the **Workstation** and **Server** service turned off, you can shorten these waits. To do so:
  - a) Run regedt32.exe on your Windows system.<sup>2</sup>
  - b) Open the key: HKEY\_LOCAL\_MACHINE\SOFTWARE\IBM\AS400NT\UserAdmin
  - c) Double-click the **ServerWait** value and change it from 300 seconds to 2 seconds.
  - d) Double-click the **WorkstationWait** value and change it from 300 seconds to 2 seconds.
5. If you wish to run Submit Network Server Command (SBMNWSCMD) or do a Windows file level backup from IBM i, you will need to start the **Server** and **Workstation** services on your Windows server.

**Notes:**

<sup>1</sup> If you choose to leave the two 5-minute delays, remember to do a shutdown of the Windows server prior to doing a vary off from IBM i if you vary it off immediately (within 10 minutes) after varying it on.

<sup>2</sup> Be careful when editing the Windows registry as it can damage your system if you edit the wrong key. You should back up your server prior to editing the registry.

See Chapter 8 of Redbook [SG24-5643 - AS/400 Mail: Multiple SMTP Domains Behind a Firewall](#) (PDF, 6.2MB) for more information regarding setting up an integrated server to support a Windows firewall.

## 7.7.9 Windows Server 2003 topics

The following sub-sections contain topics that are unique to Windows Server 2003.

### 7.7.9.1 Integrating a service pack with Windows Server 2003

This section describes how to create an integrated install image that contains Microsoft Windows Server 2003 with Service Pack 1 (SP1) or later applied. The integrated install image can be used when installing the integrated server from IBM i.

To create an integrated install image, use the instructions in the **Microsoft TechNet** article titled [Windows Server 2003 Service Pack 2 Installation and Deployment Guide](#). Detailed instructions for integrating the service pack are found in section:

**The Integrated Installation** > *Scenario 1: Creating an integrated installation.*

#### Notes:

- Use the instructions for 32-bit versions of Windows Server 2003.
- In the commands shown in the TechNet article, *Drive:* is a mapped network drive where the integrated install image will be stored. *LLL* in the install file name (for example, WindowsServer2003-KB889101-SP1-x86-LLL.exe for SP1) is the language version (for example, ENU for English) of the service pack to integrate with the base Windows Server 2003 install image.
- If your service pack CD image does not contain the required install file referenced in the TechNet article, then you need to download the appropriate version of the install file from the Microsoft [Windows Server 2003 Downloads](#) web page. Download the service pack version that is used for installing on multiple servers.
- It is also possible to integrate additional updates besides the service pack into the install image. See the **Microsoft TechNet** article titled [Installing and Deploying Updates for Microsoft Windows Server 2003](#) for details.

Save the resulting integrated install image one of the following ways:

1. Burn the integrated install image onto a CD. The CD is used in the IBM i optical drive when installing the server (for example, using the INSWNTSVR command).
2. Store an ISO file containing the integrated install image in the IBM i Integrated File System (IFS). Then create a virtual optical device on IBM i and mount the ISO image in the virtual optical device.
3. Copy the integrated install image to an IBM i Integrated File System (IFS) directory. See [Creating a Windows Server 2003 install CD image in IFS](#). The IFS directory is used on the *Windows source directory* (WNTSRCDIR) parameter when running the INSWNTSVR command.

**Note:** This method does **NOT** work with the **Create Server** [Web GUI](#) task.



## 7.7.9.2 Windows Server 2003 Service Pack 1

Microsoft Windows Server 2003 Service Pack 1 (SP1) introduced some security changes that affect how the server interacts with network connections. For example, SP1 provides the Windows Firewall.

**Note:** The Windows Server 2003 SP1 security changes are also included in later Windows Server 2003 service packs (for example, SP2) and in later Windows Server versions (for example, Windows Server 2003 R2). The SP1 considerations listed below also apply to Windows servers with that software installed.

The IBM i integration support for Windows uses a private point-to-point (PTP) virtual Ethernet LAN to communicate between IBM i and Windows to perform various integration functions such as user enrollment, file level backup, serviceability, remote command, etc. The security changes introduced by SP1 affect these integration functions. When using SP1 on an integrated Windows server, follow the instructions below to allow the IBM i integration support to communicate over the private PTP virtual Ethernet LAN.

Included in Windows Server 2003 Service pack 1 is a software firewall, called Windows Firewall. This feature is not installed by default, but can be turned on by the customer after they have applied Service Pack 1 to their server. If enabled, the default configuration is to block all incoming connections on all network interfaces on the Server. Leaving the firewall in this configuration will prevent essential IBM i integration services (like user enrollment, file level backup, serviceability, remote command, etc.) from connecting to IBM i.

If the Windows Firewall is used, **it must be disabled for the entire Virtual Ethernet PTP interface.**

**Note:** Since there are only two systems connected to the Virtual Ethernet PTP LAN (the IBM i logical partition and the Windows server), it is inherently secure by design. The Virtual Ethernet PTP LAN should not be bridged or routed to other LANs, so no traffic but the IBM i integration functions flow on this LAN.

Here is a link to the Microsoft web site that describes how to disable the firewall for a specific interface/connection: [Turn Windows Firewall On or Off for a Specific Connection](#).

Here is a link to the Microsoft web site which describes the Windows Firewall in General: [Windows Firewall Operations Guide](#).

## 7.7.9.3 Using IBM i virtual optical support for Windows Server 2003 installations

As an alternative to using a physical installation CD, you can install Windows Server 2003 on an integrated server using an ISO image of the CD located somewhere in the IBM i Integrated File System (IFS) and mounting that ISO image in an IBM i virtual optical device.

This method has several advantages:

- There is no need to load physical install media in the IBM i optical drive.
- The installation using an ISO image in IFS is relatively quick compared to using a CD.

### Notes:

- This method **does** work with the **Create Server Wizard**, which uses the default INSWNTSVR CD search method and looks for the first mounted physical or virtual optical device with an i386

directory.

- If the **one-time setup** procedure below has previously been performed, then you can skip to the **load the image catalog into the virtual optical device** procedure.
- In the following procedures, example names are used:  
**WS03SP1\_EN** is the name of the Windows Server 2003 installation CD ISO image.  
**/ISO9660** is the IFS directory where ISO images are stored.  
**MYCATALOG** is the name of the image catalog.  
**OPTVRT01** is the name of the IBM i virtual optical device description.  
You may substitute names of your choosing for any of these items.

**One-time setup:** Create an image catalog containing the Windows Server 2003 image:

1. Use the following command to create an IFS directory to contain ISO images:

```
MKDIR DIR('/ISO9660')
```

2. Create an ISO image that contains the Windows Server 2003 install image that includes service pack 1 (SP1) or later. See [Integrating a service pack with Windows Server 2003](#).
3. Send the ISO image to the IBM i system using binary FTP transfer to '/ISO9660/WS03SP1\_EN'.
4. Verify that the ISO image exists in IFS with:

```
WRKLNK '/ISO9660/*'
```

5. If an image catalog does not already exist, create one:

```
CRTIMGCLG IMGCLG(MYCATALOG) DIR('/ISO9660') TYPE(*OPT) CRTDIR(*YES)
```

6. Add the Windows Server 2003 ISO image to the image catalog:

```
ADDIMGCLGE IMGCLG(MYCATALOG) FROMFILE('/ISO9660/WS03SP1_EN')  
TOFILE(*FROMFILE)
```

7. If an IBM i virtual optical device does not already exist, create one:

```
CRTDEVOPT DEVD(OPTVRT01) RSRNAME(*VRT) ONLINE(*YES)  
TEXT('Virtual CD Device')
```

**Load the image catalog into the virtual optical device:**

1. If the virtual optical device created in the **one-time setup** above is not active, vary it on:

```
VRYCFG CFGOBJ(OPTVRT01) CFGTYPE(*DEV) STATUS(*ON)
```

2. Load the image catalog containing the Windows Server 2003 ISO image into the virtual optical device created in the **one-time setup** above:

```
LODIMGCLG IMGCLG(MYCATALOG) DEV(OPTVRT01)
```

The virtual optical device containing the Windows Server 2003 ISO image can then be used when installing an integrated Windows Server 2003 server using either the [Web GUI Create Server Wizard](#) or the **INSWNTSVR** CL command (you can use the default *Windows source directory* (WNTSRCDIR) parameter value).

## 7.7.9.4 Creating a Windows Server 2003 install CD image in IFS

**Note:** This method does **NOT** work with the **Create Server Wizard**, which uses the default INSWNTSVR CD search method and only looks for the first mounted physical or virtual optical device with an i386 directory.

As an alternative to using a physical installation CD, you can install Windows Server 2003 on an integrated server using an image of the CD located somewhere in the IBM i Integrated File System (IFS). This method requires that the Windows source directory (WNTSRCDIR) parameter of the Install Windows Server (INSWNTSVR) command is used to point to the appropriate IFS directory instead of using an optical device.

This method has several advantages:

- There is no need to load physical install media in the IBM i optical drive.
- The installation using an IFS source directory is relatively quick compared to using a CD.

The following steps use IBM i NetServer to define a shared folder in IFS. The shared folder is used to store the install CD image, which can then be used to install Windows Server 2003.

1. From the IBM i command line, create an IFS directory (folder) to hold CD images:

```
MKDIR DIR('/cdimages')
```

2. From the IBM i command line, create a read/write share for the IFS directory (folder) created above:

```
CALL QZLSADFS PARM(cdimages '/cdimages' x'00000009' x'00000000' 'CD  
images' x'00000002' x'ffffffff' x'00000000')
```

3. From a Windows PC command line, map a drive to the share created above:

```
C:\> NET USE x: \\ ibmihost\cdimages  
where x: is the mapped drive letter and ibmihost is the name of the IBM i system.
```

4. From the Windows PC command line, create a directory (folder) to hold the Windows Server CD image:

```
C:\> x:  
where x: is the mapped drive letter.
```

```
x:\> mkdir ws2003  
where ws2003 is the directory that will hold the CD image.
```

5. From the Windows PC, copy the i386 directory, its contents, and all subdirectories from the Windows Server 2003 CD-ROM to the mapped IFS drive/directory that was created above.

```
For example, you could copy the i386 directory from the CD to directory  
x:\ws2003
```

```
which would place the i386 directory and its contents in IFS directory  
/cdimages/ws2003
```

You should end up with a /cdimages/ws2003/i386 directory with a bunch of files and directories under it.

6. You can then use the install CD image stored in IFS to install a Windows Server 2003 server. From the IBM i command line, perform a \*FULL Windows install, specifying the above IFS directory in the INSWNTSVR command *Windows source directory* (WNTSRCDIR) parameter:

```
INSWNTSVR INSTYPE(*FULL) WNTSRCDIR('/cdimages/ws2003') ...
```

### 7.7.9.5 Using the Windows Server 2003 Backup utility with integrated servers

You can use the Windows Server 2003 Backup utility and an IBM i tape drive to do backups from the integrated server.

You can use the Windows backup utility to save data to CD, DVDs or the virtual disks for the integrated server.

Integrated servers running Windows Server 2003 can also use tape or shared IBM i tape devices with the Windows backup utility. See [Using IBM i tape devices with integrated Windows servers](#).

To start the **Backup** utility:

1. On the integrated server console, click **Start**
2. Select **Accessories > System Tools > Backup**.

For information about backup or recovery by using LAN-connected mass storage devices, refer to your Windows server documentation from Microsoft.

### 7.7.9.6 Migrating IXS/IXA Windows Server 2003 to iSCSI

IBM Lab Services is offering a migration utility that can convert an Integrated xSeries Server (IXS) or Integrated xSeries Adapter (IXA) based Windows Server 2003 image to an iSCSI based image. The migration utility saves you from having to do a new Windows Server 2003 install, reinstalling your applications and reconfiguring your server back to its previous state.

If you are interesting in taking advantage of this utility, send an e-mail to [intwin@us.ibm.com](mailto:intwin@us.ibm.com).

## 7.8 Additional integrated VMware ESX server topics

Use these tasks to manage integrated servers running VMware ESX Server.

### Section Table of Contents

7.8.1	VMware ESX documentation and management tools.....	398
7.8.2	Tasks for ESX Management server based infrastructure.....	398
7.8.2.1	Configuring the QVMWINT user for integrated VMware ESX server management.....	398
7.8.2.2	Managing connections for integrated VMware ESX servers.....	400
7.8.2.2.1	Adding connection information .....	401
7.8.2.2.2	Listing connection information .....	402
7.8.2.2.3	Verifying connection information .....	402
7.8.2.2.4	Changing connection information .....	403
7.8.2.2.5	Overriding management of a connection.....	403
7.8.2.2.6	Deleting connection information .....	404
7.8.3	Switching between ESX 4 server management infrastructures on i 6.1.....	405
7.8.4	Save While Active (SWA) for integrated VMware ESX servers on i 7.1 or higher .....	406
7.8.4.1	Reverting to a consistent SWA virtual machine snapshot after restore .....	406
7.8.4.2	Deleting the SWA virtual machine snapshot without reverting.....	407
7.8.5	ESX migration and upgrade scenarios.....	408
7.8.5.1	Migrating VMware ESX servers to i 7.1 or higher .....	408
7.8.5.2	Migrating VMware ESX servers to i 6.1 .....	412
7.8.5.3	Upgrading VMware ESX 3 to VMware ESX 4.....	414
7.8.5.3.1	Upgrading an existing VMware ESX 3.x server to VMware ESX 4 .....	415

## 7.8.1 VMware ESX documentation and management tools

To configure your VMware ESX environment, you need to use management tools and associated documentation that is provided by VMware. The information you need depends on the version of ESX that you are using on your integrated server:

Server OS	Documentation
ESXi5	<a href="#">VMware vSphere Documentation</a>
ESXi4 ESX4	<a href="#">VMware vSphere 4 Documentation</a>
ESX3.5	<a href="#">VMware Infrastructure 3 Documentation</a>

## 7.8.2 Tasks for ESX Management server based infrastructure

### 7.8.2.1 Configuring the QVMWINT user for integrated VMware ESX server management

When using the [Management server based infrastructure](#), you need to set up the **QVMWINT** user in order to perform IBM i management tasks, such as shutting down the integrated VMware ESX server and linking storage to the ESX server while it is active.

To set up the QVMWINT user, follow these steps:

1. Enable the IBM i QVMWINT user profile.
  - a. Select **Users and Groups** from the [Web GUI](#) or [System i Navigator](#).
  - b. Select **Users**.
  - c. Select the **Properties** action for the **QVMWINT** user profile.

**Note:** If the **QVMWINT** user profile does not exist in the **Users** list, then run the following command from an IBM i command session to create it:

```
QSYS/CRTUSRPRF USRPRF(QVMWINT) PASSWORD(*NONE) STATUS(*DISABLED)  
USRCLS(*USER) SPCAUT(*NONE) AUT(*EXCLUDE) GRPPRF(*NONE)  
SUPGRPPRF(*NONE) JOBD(QDFTJOB) OWNER(*USRPRF)  
TEXT('IBM-supplied User Profile')
```

Then refresh the **Users** list and continue with this procedure.

- d. Select the **Enable for processing** check box.
- e. Set the password for user QVMWINT to a value that is valid on Windows.
- f. Click **OK** to save the change.

2. Enroll the QVMWINT user profile to the integrated Windows server that serves as the management server for the VMware ESX server. The QVMWINT user must have administrative rights on the Windows server, so specify **Administrator** for the user template when enrolling QVMWINT. See [Enrolling IBM i users to integrated Windows servers](#) for more information.

**Note:** At IBM i password level (QPWDLVL) 0 or 1, the IBM i QVMWINT password is converted to all lower case characters when it is set on the integrated Windows server.

3. Create a QVMWINT user profile on either your VMware ESX server or your ESX platform manager (vCenter Server), if one is used.
  - a. If you have not already done so, install the **VMware vSphere Client** on a Windows system. Refer to your VMware documentation for instructions.
  - b. Launch the **VMware vSphere Client** and log into the ESX host or the ESX platform manager (vCenter Server). Then select the **Local Users & Groups** tab.
  - c. Right click in the users list and select **Add...**
  - d. Add the QVMWINT user.

**Notes:**

- The **QVMWINT** user login name on the VMware ESX server or vCenter Server must be all **UPPER CASE** letters.
  - The **password** on the VMware ESX server or vCenter Server must match the password that is used for the IBM i QVMWINT user profile.
  - If your IBM i password level is 0 or 1, the **password** on the VMware ESX server or vCenter Server must use **lower case** letters (no upper case letters).
  - If you need detailed instructions, refer to the section titled **Managing Users, Groups, Roles and Permissions** in the **vSphere Security Guide** found under the **VMware vSphere** link on the [VMware Documentation](#) Web page.
- e. Select the **Permissions** tab.
  - f. Right click on an open area of the **User/Group** list and select **Add Permission...**
  - g. On the **Assign Permissions** panel, click **Add...** and follow the prompts to add the QVMWINT user to the **Users and Groups** list. Then select **Administrator** for the **Assigned Role**. Finally, click **OK** to save the changes.

**Note:** The QVMWINT user on the VMware ESX server or vCenter Server must have explicit **Administrator** permissions. Assigning the QVMWINT user to a group that has **Administrator** permissions does **not** provide the required permissions.

## 7.8.2.2 Managing connections for integrated VMware ESX servers

When using the [Management server based infrastructure](#), the **IBM i connection utility for virtualization hosts** (`ibmvmcon.exe`) is used to define connection information so that IBM i can manage integrated VMware ESX servers.

The connection utility runs on the integrated Windows server that serves as the management server for the VMware ESX server. The connection utility can be run a couple of ways:

Method	Task
Interactive	<p>Click <b>Start &gt; All Programs &gt; IBM i &gt; IBM i connection utility for virtualization hosts</b></p> <p>Or, type <code>ibmvmcon</code> at the Windows command line and press <b>Enter</b>.</p> <p>The connection utility shows a series of menus to step you through the various connection configuration tasks. The connection configuration tasks are described in the following sections.</p>
Non-interactive	<p>Type <code>ibmvmcon</code> and the command options at the Windows command line and press <b>Enter</b>.</p> <p>The command runs immediately, without showing any menus.</p> <p><b>Tip:</b> To see the <code>ibmvmcon</code> command syntax and the available command options, type <code>ibmvmcon help</code> at the Windows command line and press <b>Enter</b>.</p>



### 7.8.2.2.1 Adding connection information

Add connection information that is necessary for administrative communication between an integrated VMware ESX server NWSD on IBM i and the ESX host or ESX platform manager (VMware vCenter).

**Tip:** This task automatically verifies the connection information. The ESX server must be active while performing this task and a network connection to the ESX server must be available. If a platform manager is specified, then the platform manager must also be active and connected to the network.

**Note:** If you are using the [IBM i iSCSI Solution Work Sheets](#), use the following work sheet to help you do this task:

- **Integrated VMware ESX server management**

Do these steps on the management server (integrated Windows server):

1. Click **Start > All Programs > IBM i > IBM i connection utility for virtualization hosts** to show the connection utility menu.
2. Type **1** (Add connection information) and press **Enter**.

A numbered list of network server descriptions (NWSDs) that exist on the IBM i partition is shown.

3. Type the number corresponding to the ESX server NWSD and press **Enter**.
4. Type the ESX server IP address or host name and press **Enter**.
5. Type the platform manager IP address or host name, or leave blank and press **Enter**.

**Note:** If you specify a platform manager, the management server communicates IBM i requests to the vCenter server, which then forwards the requests to the ESX host. If an ESX platform manager is not specified, the management server communicates IBM i requests directly to the ESX host.

The connection information is displayed again and then the results of the task are shown.

6. Press **Enter** to return to the connection utility menu.
7. If you are done working with connections, type **7** (Exit) and press **Enter**.

**Tip:** Use the following command to perform this task without using the connection utility menu interface:

```
ibmvmcon add -n nwsd -h host [-pm platformmanager]
```

Where *nwsd* is the ESX server NWSD name, *host* is the ESX server IP address or host name, and *platformmanager* is the optional vCenter server IP address or host name.

### 7.8.2.2 Listing connection information

List the integrated VMware ESX server connection information and the management server that is currently managing the connection.

Do these steps on the management server (integrated Windows server):

1. Click **Start > All Programs > IBM i > IBM i connection utility for virtualization hosts** to show the connection utility menu.
2. Type **3** (List connection information) and press **Enter**.  
The list of connections is shown.
3. Press **Enter** to return to the connection utility menu.
4. If you are done working with connections, type **7** (Exit) and press **Enter**.

**Tip:** Use the following command to perform this task without using the connection utility menu interface:

```
ibmvmcon list
```

### 7.8.2.3 Verifying connection information

Verify the integrated VMware ESX server connection information that is configured on the management server. Verifying the connection can help resolve connection problems.

The verify option determines if the management server can communicate with IBM i and the ESX host or platform manager.

Do these steps on the management server (integrated Windows server):

1. Click **Start > All Programs > IBM i > IBM i connection utility for virtualization hosts** to show the connection utility menu.
2. Type **4** (Verify connection information) and press **Enter**.

A numbered list of connections for ESX server NWSDs is shown.

3. Type the number corresponding to the ESX server NWSD or the number of the entry labeled **All** and press **Enter**.

The connections for the selected ESX server NWSDs are verified and the results are shown.

4. Press **Enter** to return to the connection utility menu.
5. If you are done working with connections, type **7** (Exit) and press **Enter**.

**Tip:** Use the following command to perform this task without using the connection utility menu interface:

```
ibmvmcon verify -n nwsd
```

Where *nwsd* is the ESX server NWSD name. Specify \*ALL for the NWSD name to verify connections for all ESX server NWSDs that have connections defined on the management server.

#### **7.8.2.2.4 Changing connection information**

It might be necessary to update the connection information for an integrated VMware ESX server if your environment has changed.

For example, you need to update the connection information for an integrated VMware ESX server if the IP address of the ESX server or platform manager has changed, or you want to start using or discontinue using a platform manager.

Do these steps on the management server (integrated Windows server):

1. Delete the existing connection information for the ESX server.  
See [Deleting connection information](#).
2. Add the new connection information for the ESX server.  
See [Adding connection information](#).

#### **7.8.2.2.5 Overriding management of a connection**

Override management of an integrated VMware ESX server administrative connection.

Integrated VMware ESX server connection information might be configured on multiple management servers. However, only one management server can manage the connection at a time. Connections are normally managed automatically by management servers on a first come, first serve basis. This task overrides the current management server for the connection.

Do these steps on the management server (integrated Windows server) that is to take over the connection:

1. Click **Start > All Programs > IBM i > IBM i connection utility for virtualization hosts** to show the connection utility menu.
2. Type **5** (Manage connection) and press **Enter**.

A numbered list of connections for ESX server NWSDs is shown.

3. Type the number corresponding to the ESX server NWSD or the number of the entry labeled All and press **Enter**.

The local management server takes over management of the connections for the selected ESX server NWSDs.

4. Press **Enter** to return to the connection utility menu.
5. If you are done working with connections, type **7** (Exit) and press **Enter**.

**Tip:** Use the following command to perform this task without using the connection utility menu interface:

```
ibmvmcon manage -n nwsd
```

Where *nwsd* is the ESX server NWSD name. Specify \*ALL for the NWSD name to manage connections for all ESX server NWSDs that have connections defined on the local management server.

### 7.8.2.2.6 **Deleting connection information**

Deletes integrated VMware ESX server connection information on the local management server. When the connection information is deleted, the local management server can no longer manage the connection.

#### **CAUTION:**

If there is only one management server configured to manage the connection to be deleted, administrative communication is lost between IBM i and the ESX server. If administrative communication is lost, varying off the ESX NWSD on IBM i might cause an unclean shutdown of the ESX server.

Do these steps on the management server (integrated Windows server):

1. Click **Start > All Programs > IBM i > IBM i connection utility for virtualization hosts** to show the connection utility menu.
2. Type **2** (Delete connection information) and press **Enter**.

A numbered list of connections for ESX server NWSDs is shown.

3. Type the number corresponding to the ESX server NWSD or the number of the entry labeled **All** and press **Enter**.
4. Respond to the confirmation message with one of the following choices:
  - Type **1** (yes) and press **Enter** to confirm the delete operation.  
The connections for the selected ESX server NWSDs are deleted.
  - Type **2** (no) and press **Enter** to cancel the delete operation.
5. Press **Enter** to return to the connection utility menu.

6. If you are done working with connections, type **7** (Exit) and press **Enter**.

**Tip:** Use the following command to perform this task without using the connection utility menu interface:

```
ibmvmcon delete -n nwsd
```

Where *nwsd* is the ESX server NWSD name. Specify \*ALL for the NWSD name to delete the connections for all ESX server NWSDs that have connections defined on the local management server.

### 7.8.3 Switching between ESX 4 server management infrastructures on i 6.1

With IBM i 6.1, ESX 4.0 servers can be managed using either of the two IBM i ESX server management infrastructures. If at some point you need to switch from one IBM i ESX 4 server management infrastructure to the other, follow the appropriate steps below.

Current Infrastructure	Target Infrastructure	Tasks
<a href="#">Service console based infrastructure</a>	<a href="#">Management server based infrastructure</a>	<ol style="list-style-type: none"> <li>1. Remove the Integrated Server Support service console programs.               <ol style="list-style-type: none"> <li>a. Log on to the ESX console and mount the install device. Follow steps 1 - 4 in <a href="#">Completing the ESX installation – Service console based infrastructure</a>.</li> <li>b. Run the uninstall utility:                   <pre style="margin-left: 40px;">\mnt\ibm1sv\install\ibmunins</pre> </li> </ol> </li> <li>2. Follow the steps in section <a href="#">Completing the ESX installation – Management server based infrastructure</a>.</li> </ol>
<a href="#">Management server based infrastructure</a>	<a href="#">Service console based infrastructure</a>	<ol style="list-style-type: none"> <li>1. Log on to the Management server (Windows) as a user with Administrator authority.</li> <li>2. Use the <b>IBM i connection utility for virtualization hosts</b> (ibmvmcon.exe) to delete connection information associated with the ESX server. Follow the steps in <a href="#">Deleting connection information</a>.</li> <li>3. Follow the steps in <a href="#">Completing the ESX installation – Service console based infrastructure</a>.</li> </ol>

## 7.8.4 Save While Active (SWA) for integrated VMware ESX servers on i 7.1 or higher

With **IBM i 7.1** or higher, virtual storage spaces for **active** integrated VMware ESX servers can be included in your IBM i backups. When this is done, the save process automatically uses VMware ESX utilities to create a virtual machine snapshot named **IBMi\_NWSSTG\_SWA** that can be used as a safe and consistent recovery point.

If you later restore the storage space, you must revert to the virtual machine **IBMi\_NWSSTG\_SWA** snapshot in order to ensure that the virtual machine data is in a consistent state. See [Reverting to a consistent SWA virtual machine snapshot after restore](#).

**Note:** Normally, once the IBM i save processing is completed, the **IBMi\_NWSSTG\_SWA** snapshot is automatically deleted, which merges the changes made since the snapshot into the parent disk. However, if the VMware ESX server is shut down before the IBM i save processing is completed, then the **IBMi\_NWSSTG\_SWA** snapshot is not automatically deleted. If this happens, you should manually delete the **IBMi\_NWSSTG\_SWA** snapshot once the ESX server is active again. See [Deleting the SWA virtual machine snapshot without reverting](#).

### Related information:

- [Backup and recovery concepts](#)

### 7.8.4.1 Reverting to a consistent SWA virtual machine snapshot after restore

After restoring a VMware ESX storage space that was saved while the ESX server was active, you must revert to the virtual machine **IBMi\_NWSSTG\_SWA** snapshot that was taken when the storage space was saved in order to ensure that the virtual machine data is in a consistent state.

To revert back to that point and essentially undo any writes to storage that occurred during the save while active process, do the following:

1. Right-click on the virtual machine using the **vSphere Client** and select:  
**Snapshot > Snapshot Manager**
2. Select the **IBMi\_NWSSTG\_SWA** snapshot in the tree of snapshots above the **You are here** item and then select **Go to**.

When selecting to “Go to” this snapshot, a confirmation message is displayed which states that the current state of the virtual machine will be lost when reverting to a snapshot. This is exactly what is required when reverting to the a known recovery point, such as **IBMi\_NWSSTG\_SWA**.

3. Select **Yes** for the confirmation message to revert to the **IBMi\_NWSSTG\_SWA** snapshot.

This reverts the virtual machine to the point in time that the storage space was saved from IBM i.

4. Select the **IBMi\_NWSSTG\_SWA** snapshot again and then select **Delete** to remove the snapshot file.

This merges all changes made since the snapshot into the parent disk and removes the **IBMi\_NWSSTG\_SWA** snapshot from the **Snapshot Manager**.

**Note:** Deleting the snapshot is now safe to do since no unknown changes will be merged into the parent disk data.

**Related information:**

➤ [Backup and recovery concepts](#)

## 7.8.4.2 Deleting the SWA virtual machine snapshot without reverting

If a storage space for a virtual machine was **not** recently restored from backup and has information that must not be lost by reverting to the IBMi\_NWSSTG\_SWA snapshot, then do **not** revert to that snapshot. In this scenario the snapshot file is not needed, so delete the snapshot file, which merges the changes made since the snapshot into the parent disk.

To delete the IBMi\_NWSSTG\_SWA snapshot, do the following:

1. Right-click on the virtual machine using the **vSphere Client** and select:  
**Snapshot > Snapshot Manager**
2. Select the **IBMi\_NWSSTG\_SWA** snapshot in the tree of snapshots above the **You are here** item and then select **Delete** to remove the snapshot file.

This merges all changes made since the snapshot into the parent disk and removes the IBMi\_NWSSTG\_SWA snapshot from the **Snapshot Manager**.

**Related information:**

➤ [Backup and recovery concepts](#)

## 7.8.5 ESX migration and upgrade scenarios

The following sections provide information on how to migrate or upgrade your integrated servers for various scenarios.

### 7.8.5.1 Migrating VMware ESX servers to i 7.1 or higher

In IBM i 7.1 or higher, support for running VMware ESX Server on integrated BladeCenter blade or System x servers uses a different IBM i infrastructure than it did in previous IBM i releases. The new i 7.1 infrastructure for VMware ESX must be used and includes the following.

- New network server description (NWSD) types are provided for VMware ESX/ESXi servers. The new NWSD types eliminate the requirement for an "install" drive (the second drive) on VMware ESX servers. For VMware ESXi Embedded servers, the "system" drive (the first drive) is also no longer required.
- Integrated server support for VMware ESX/ESXi runs on an integrated Windows Server. The integrated Windows server manages administrative communication from IBM i to the VMware ESX/ESXi server.
- Integrated server support for VMware ESX/ESXi is updated automatically when updating integrated server support on the Windows management server.

This section describes the process required to migrate integrated VMware ESX servers that were originally installed on previous IBM i releases to the new IBM i 7.1 infrastructure for VMware ESX. The migration process described below preserves the VMware ESX disks, except for disks that are no longer needed. After upgrading to IBM i 7.1 or higher, the steps described below must be performed before IBM will provide service support for VMware ESX servers that were originally installed on previous IBM i releases.

**Note:** The IBM i command examples in the sections below use **myesx** as the name of the network server description (NWSD) which has a system drive named **myesx1** and an install drive named **myesx2**. An example tape device with device description name **tap01** is also used. When performing the steps below, you need to replace these items with ones that are appropriate for your environment.

**Important:** There must be **no** customer applications or data stored on the "install" drive (the second linked storage space, which is device **/mnt/sdb1** when viewed from VMware ESX). The install drive is removed during the following migration process. Any customer applications or data stored on the install drive will be lost during the migration, so you must move them to a different drive before continuing with this migration process. Also, for ESXi embedded servers, the "system" drive (the first linked storage space) is also removed.

**Important:** With IBM i 7.1 or higher, an iSCSI-attached integrated Windows server is required to perform management functions for VMware ESX servers (for example, to shut down the ESX server).

- If your IBM i 7.1 or higher system does not already have an iSCSI-attached integrated server running Windows Server 2003 or Windows Server 2008 or Windows Server 2012, then you must install one before performing the following ESX server migration procedure. To install the Windows server, follow the [Server installation road map and checklist](#).



- If you have migrated an iSCSI-attached integrated Windows server from a prior IBM i release to IBM i 7.1 or higher, you must also synchronize the integration software. See [Updating the integration software: Windows server console](#).

Perform these steps on your IBM i system after upgrading to IBM i 7.1 or higher.

### A. Install and update IBM i software

1. Make sure that all of the IBM i software listed in [IBM i products and options](#) is installed.
2. Apply the latest integrated server PTFs to your IBM i system. See the [IBM i PTFs](#) page.

### B. Save required information from the network server

1. Run the following command and record the link information (link type and sequence) of all storage spaces associated with your VMware ESX server:

```
WRKNWSSTG NWS(myesx)
```

2. Back up the system and install drive storage spaces associated with your VMware ESX server as follows:

```
SAV DEV('/QSYS.LIB/tap01.DEVD') OBJ((' /QFPNWSSTG/myesx1'))
```

```
SAV DEV('/QSYS.LIB/tap01.DEVD') OBJ((' /QFPNWSSTG/myesx2'))
```

**Note:** In this example, storage spaces `myesx1` and `myesx2` are saved to tape. Alternatively, you could save the storage spaces to a save file or to a virtual tape. The SAV command in this step and the RST command in the restore step later on would then refer to the save file or virtual tape instead of the physical tape device description.

### C. Create a new network server description and link storage

1. Delete your VMware ESX server NWS and associated objects that you installed on the previous IBM i release with the following command:

```
DLTINTSVR NWS(myesx)
```

**Note:** Make sure you have saved your VMware ESX server system and install drive storage spaces as described previously, since this command deletes them.

2. Run the INSINTSVR command using the original NWS name to create a new NWS.

#### Notes:

- Use the appropriate operating system type (OSTYPE) value:
  - \*ESXII For VMware ESXi Installable 5.x or 4.x
  - \*ESXIE For VMware ESXi Embedded 5.x or 4.x
  - \*ESX4 For VMware ESX 4 (Also use this value if you are migrating an ESX 3 server.)
- Use the minimum system storage space size, since later you will restore the storage space previously saved.
- When INSINTSVR completes, it varies on the server. You must then vary off the server.

3. Unlink the newly created system storage space, then delete it as follows:

```
RMVNWSTGL NWSSTG(myesx1) NWSSTG(myesx) RENUMBER(*NO)
DLTNWSTGL NWSSTG(myesx1)
```

**Note:** This step does not apply to ESXi Embedded servers, since a system storage space is not created for ESXi Embedded servers.

4. Restore your VMware ESX server's original system and install storage spaces, then link them to the NWSSTG as follows:

```
RST DEV('/QSYS.LIB/tap01.DEVD') OBJ('/QFPNWSSTG/myesx1') ALWOBJDIF(*ALL)
RST DEV('/QSYS.LIB/tap01.DEVD') OBJ('/QFPNWSSTG/myesx2') ALWOBJDIF(*ALL)
ADDNWSSTGL NWSSTG(myesx1) NWSSTG(myesx)
ADDNWSSTGL NWSSTG(myesx2) NWSSTG(myesx)
```

5. If necessary, use the ADDNWSSTGL command to link any additional storage spaces that you originally had linked into your VMware ESX server.

**Notes:**

- Make sure that each storage space is linked with the same link type and sequence parameters as before. Otherwise your VMware ESX server may not boot. See the information you recorded in step **B-1** above.
- In order to take advantage of advanced VMware ESX functions such as VMware VMotion, VMware HA and VMware DRS, the additional storage spaces should be linked using **shared update** access mode instead of exclusive update. The ADDNWSSTGL command parameter value to use for shared update access is: **ACCESS(\*SHRUPD)**

#### D. Upgrade VMware ESX 3 to ESX 4

VMware ESX 3 servers are not supported on i 7.1 or higher and need to be upgraded to ESX 4.

If you are migrating an ESX 3 server, perform the steps in the [Upgrading VMware ESX 3 to VMware ESX 4](#) section before continuing with the migration sections below.

#### E. Set up IBM i integrated server administration for VMware ESX

**Note:** If prior to upgrading to i 7.1 or higher you had already set up a Windows management server and ESX connection information on i 6.1, and you plan to use the same Windows management server and ESX connection information on i 7.1 or higher, then you can skip the following steps.

1. If you do not already have an iSCSI-attached integrated server running Windows Server 2003 or Windows Server 2008 or Windows Server 2012, you must install one. To install the Windows server, follow the [Server installation road map and checklist](#).
2. If you have migrated an iSCSI-attached integrated Windows server to IBM i 7.1 or higher, you must also synchronize the integration software. See [Updating the integration software: Windows server console](#).
3. Follow the steps listed in section [Complete the integrated server installation](#) in the Installation road map.

## F. Remove previous IBM i release integrated server support from the VMware ESX console

**Note:** If you are migrating an ESXi Embedded or ESXi Installable server, then you can skip the following steps.

1. Log on to the ESX console as root.
2. Download the uninstall utility, **ibmunins**. To do this, run the following commands:

```
esxcfg-firewall --allowOutgoing
ftp address
(where address is the IP address or host name of your IBM i system)
cd /QIBM/ProdData/NTAP/ESXmigration
bin
get ibmunins
quit
esxcfg-firewall -r
```

3. Make the **ibmunins** utility executable by running the following command:

```
chmod +x ibmunins
```

4. Run the uninstall utility as follows.

```
ibmunins
```

## G. Delete unnecessary storage spaces

**Note:** Once the migration to the new NWS type is complete:

- The install drive **myesx2** is no longer needed.
- For ESXi Embedded servers, the system drive **myesx1** also is no longer needed, since ESXi Embedded servers boot from flash memory.

Delete the unnecessary storage spaces at your convenience as follows.

1. Vary off the ESX server with the following command.

```
VRVCFG CFGOBJ(myesx) CFGTYPE(*NWS) STATUS(*OFF)
```

2. Unlink the install drive and delete it with the following commands.

```
RMVNWSSTGL NWSSTG(myesx2) NWS(myesx)
```

```
DLTNWSSTG NWSSTG(myesx2)
```

3. **Only for ESXi Embedded servers:** Unlink the system drive and delete it with the following commands.

```
RMVNWSSTGL NWSSTG(myesx1) NWS(myesx)
```

```
DLTNWSSTG NWSSTG(myesx1)
```

4. Vary on the ESX server with the following command to resume normal operation.

```
VRVCFG CFGOBJ(myesx) CFGTYPE(*NWS) STATUS(*ON)
```

## 7.8.5.2 Migrating VMware ESX servers to i 6.1

In IBM i 6.1, support for running VMware ESX Server on integrated BladeCenter blade or System x servers uses a different IBM i infrastructure than it did in i 5.4. The new i 6.1 infrastructure for VMware ESX must be used in i 6.1 and provides the following benefits:

- The integrated server code running on your VMware ESX server can be serviced.
- Shared storage can be linked to your integrated VMware ESX Server. Shared storage is required for advanced VMware ESX functions such as VMware VMotion, VMware HA and VMware DRS.

This section describes the process required to migrate integrated VMware ESX servers that were originally installed on i 5.4 to the new IBM i 6.1 infrastructure for VMware ESX. The migration process described below preserves the VMware ESX server disk drives, including the applications and data that are installed. After upgrading IBM i from i 5.4 to i 6.1, the steps described below must be performed before IBM will provide service support for VMware ESX servers that were originally installed on i 5.4.

**Note:** The IBM i command examples in the sections below use **myesx** as the name of the network server description (NWSD) which has a system drive named **myesx1** and an install drive named **myesx2**. An example tape device with device description name **tap01** is also used. When performing the steps below, you need to replace these items with ones that are appropriate for your environment.

**Important:** There must be **no** customer applications or data stored on the "install" drive (the second linked storage space, which is device **/mnt/sdb1** when viewed from VMware ESX). The install drive is reserved for use by the VMware ESX integration support and will be replaced during the following migration process. Any customer applications or data stored on the install drive will be lost during the migration, so you must move them to a different drive before continuing with this migration process.

Perform these steps on your IBM i system after upgrading to IBM i 6.1.

### A. Install and update IBM i software

1. Make sure the following IBM i software is installed:
  - 5761-SS1 option 29: Integrated Server Support
  - 5761-LSV: Extended Integrated Server Support
2. Apply the latest integrated server PTFs to your IBM i system. See the [IBM i PTFs](#) page.

### B. Save required information from the network server

1. Run the following command and record the link information (link type and sequence) of all storage spaces associated with your VMware ESX server:

```
WRKNWSSTG NWSD(myesx)
```

2. Run the following command to print the NWSD attributes:

```
DSPNWSD NWSD(myesx) OUTPUT(*PRINT)
```

When you run the INSLNXSVR command in step 7, use this as a reference for the values to specify.

3. Back up the system drive storage space associated with your VMware ESX server as follows:

```
SAV DEV('/QSYS.LIB/tap01.DEVD') OBJ('/QFPNWSSTG/myesx1')
```

**Note:** In this example, storage space **myesx1** is saved to tape. Alternatively, you could save the storage space to a save file or to a virtual tape. The SAV command in this step and the RST command in the restore step later on would then refer to the save file or virtual tape instead of the physical tape device description.

### C. Create a new network server description and link storage

1. Delete your VMware ESX server NWSD and associated objects. The easiest way to do this is to delete the VMware ESX server with the following command:

```
DLTLNXSVR NWSD(myesx)
```

**Note:** Make sure you have saved your VMware ESX server system drive storage space as described previously, since this command deletes it.

2. Run the INSLNXSVR command, using the original NWSD name to create a new NWSD and associated objects.

**Notes:**

- Use the minimum system storage space size of 1024 MB.
- When the INSLNXSVR prompts to vary on your server, enter C to cancel. Your server will not vary on.
- You do not need to complete the install on the VMware ESX server console, since the server's system storage space will be replaced with the original system storage space as described below.

3. Unlink the newly created system storage space then delete it as follows:

```
RMVNWSSTGL NWSSTG(myesx1) NWSD(myesx) RENUMBER(*NO)
```

```
DLTNWSSTG NWSSTG(myesx1)
```

**Note:** Do **not** unlink and delete the server's new install storage space **myesx2**.

4. Restore your VMware ESX server's original system storage space, then link it to the NWSD as follows:

```
RST DEV('/QSYS.LIB/tap01.DEVD') OBJ('/QFPNWSSTG/myesx1') ALWOBJDIF(*ALL)
```

```
ADDNWSSTGL NWSSTG(myesx1) NWSD(myesx)
```

**Note:** Do **not** restore and link the server's original install storage space **myesx2**.

5. If necessary, use the ADDNWSSTGL command to link any additional storage spaces (except the install storage space **myesx2**) that you originally had linked into your VMware ESX server.

**Notes:**

- Make sure that each storage space is linked with the same link type and sequence parameters as before. Otherwise your VMware ESX server may not boot. See the information you recorded in step 3 above.

- In order to take advantage of advanced VMware ESX functions such as VMware VMotion, VMware HA and VMware DRS, the additional storage spaces should be linked using **shared update** access mode instead of exclusive update. The ADDNWSSTGL command parameter value to use for shared update access is: **ACCESS(\*SHRUPD)**

#### D. Set up IBM i integrated server administration for VMware ESX

1. Vary on your VMware ESX Server and sign on to the ESX console as **root**.
2. From the shell prompt, run the following commands to unmount the i 5.4 mount point for the install drive, create the mount point required for i 6.1 and mount the install drive with the i 6.1 mount point:

```
umount /mnt/sdb1
mkdir /mnt/ibmlsv
mount /dev/sdb1 /mnt/ibmlsv
```

3. From the shell prompt, run the following i 6.1 post install utility command to update the VMware ESX server with i 6.1 code and complete the migration:

```
/mnt/ibmlsv/install/ibmsetup.sh address
```

**Note:** In this command, replace *address* with the IP address or host name of your IBM i system.

#### 7.8.5.3 Upgrading VMware ESX 3 to VMware ESX 4

The process of upgrading VMware ESX 3 to VMware ESX 4 is referred to by VMware as a **Host Upgrade**. Some specific steps are discussed below that apply for integrated servers when performing the Host Upgrade.

The **vSphere Upgrade Guide** describes how to upgrade from earlier versions of VMware ESX/ESXi and VirtualCenter to ESX/ESXi 4 and vCenter Server 4. There are a number of upgrade scenarios to consider and you should read about the upgrade process before attempting an upgrade. If you do not follow the appropriate safeguards, you might lose data and access to your servers. The upgrade process is documented in the **vSphere Upgrade Guide** under the VMware vSphere section on the [VMware Documentation](#) Web page.

The **vSphere Upgrade Guide** details a number of upgrade scenarios. The Host Upgrade process falls into two main categories. Choose one of the following methods to perform the upgrade:

1. Install a new VMware ESX 4 server, then migrate the Virtual Machines from the VMware ESX 3.x server.
  - To install the new VMware ESX 4 server, perform the steps in the [Server installation road map and checklist](#).
  - After you have completed the VMware ESX 4 installation, follow the steps provided in the **vSphere Upgrade Guide** to move the Virtual Machines.
2. Upgrade the existing VMware ESX 3.x server to VMware ESX 4 using the steps in the following section.

### 7.8.5.3.1 Upgrading an existing VMware ESX 3.x server to VMware ESX 4

#### A. Prior to performing the Host Upgrade

**Note:** The IBM i command examples below use **myesx** as the name of the network server description (NWS), which has a system drive named **myesx1**. An example tape device with device description name **tap01** is also used. When performing the steps below, you need to replace these items with ones that are appropriate for your environment.

1. Back up the system drive of the existing VMware ESX 3 server as follows:

```
SAV DEV('/QSYS.LIB/tap01.DEVD') OBJ((' /QFPNWSSTG/myesx1'))
```

**Note:** This is a precautionary step that is optional, but highly recommended.

2. Set the NWS **Restricted device resources** (RSTDDEVRSC) parameter to \*ALL as follows:

```
CHGNWS NWS(myesx) RSTDDEVRSC(*ALL)
```

**Note:** If RSTDDEVRSC is not set to \*ALL, the **Host Upgrade** may fail in a later step.

3. Create a new storage space for the VMware ESX 4 upgrade. This storage space should be at least 15000MB. This value is based on needs for integrated server support and the ESX partition requirements documented in the ESX and vCenter Server Installation Guide from the [VMware Documentation](#) Web page. Below is an example IBM i command to create a storage space named **myesxdsk**:

```
CRTNWSSTG NWSSTG(myesxdsk) NWSSIZE(15000) FORMAT(*OPEN)
```

4. Link the new storage space **myesxdsk** for the VMware ESX 4 upgrade to the NWS **myesx**. The storage space **myesxdsk** must be linked with exclusive update (\*UPDATE) access type. The sequence number on IBM i 7.1 or higher must be 2 or greater, while on IBM i 6.1 it must be 3 or greater. The integrated server **myesx** system drive **myesx1** must remain linked with exclusive update (\*UPDATE) access type and storage space sequence 1.

Below is an example IBM i command to link the storage space **myesxdsk** to the Network Server Description named **myesx**. Notice that a link sequence number is not specified, so the command will calculate the next available sequence number to use.

```
ADDNWSSTGL NWSSTG(myesxdsk) NWS(myesx) ACCESS(*UPDATE)
```

5. Record the storage space sequence of the VMware ESX 4 upgrade disk. The following command will display all the storage spaces linked to **myesx**. Record the storage space sequence for **myesxdsk**.

```
WRKNWSSTG NWS(myesx)
```

6. Start the integrated server running VMware ESX 3. Below is an example IBM i command to vary on the server.

```
VRYCFG CFGOBJ(myesx) CFGTYPE(*NWS) STATUS(*ON)
```

7. Create the VMFS datastore on the ESX 4 system disk.
  - a. Use the vSphere Client to connect to your VMware ESX 3 server.
  - b. Click on the **Configuration** tab.
  - c. Click on **Storage** under the **Hardware** list.
  - d. Click on **Add Storage**. This will start the **Add Storage Wizard**.
  - e. Select **Disk/LUN** for the **Storage Type**.
  - f. Select the device for the storage space created in step 3 above for the ESX 4 system disk.  
The device name format is: vmhba#:Channel:ID:LUN  
The LUN number is always one less than the storage space sequence number.  
  
**Note:** If you linked myesxdsk to NWSD myesx while it was active, you must then rescan the iSCSI initiator under **Storage Adapters** on the **Configuration** tab before the device will show up here.
  - g. Continue with the rest of the panels on the **Add Storage Wizard**.

## B. Performing the Host Upgrade

Refer to the **vSphere Upgrade Guide** for the upgrade scenarios, requirements and procedures that apply to your environment.

During the Host Upgrade process, you might see the following message on the server console:

```
Installing GRUB to the MBR of a disk that was not the first disk
reported by the BIOS. User must change their BIOS settings if they
want to boot from this disk.
```

You can ignore this message, since you do not need to modify the BIOS settings.  
When the upgrade is 100% complete, you might have to press **Enter** to reboot the server.

The Host Upgrade process does not remove the VMware ESX 3 system partitions. After the Host Upgrade is complete, you will see options in the boot menu for VMware ESX 4 and VMware ESX 3. This allows you to boot either ESX version, which can be used to troubleshoot upgrade problems.

## C. After the Host Upgrade

After the VMware ESX 4 upgrade process is complete, perform the steps in section [Complete the integrated server installation](#) in the Installation road map.



# 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:

Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan, Ltd.  
3-2-12, Roppongi, Minato-ku, Tokyo 106-8711

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

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

measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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

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

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.

Intel is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered 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.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

## Terms and conditions

Permissions for the use of this publication 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.

End of Document