



IBM Systems - iSeries

Windows-Umgebung auf iSeries





IBM Systems - iSeries

Windows-Umgebung auf iSeries

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die allgemeinen Informationen unter „Bemerkungen“, auf Seite 279 gelesen werden.

Zehnte Ausgabe (Februar 2006)

Diese Ausgabe bezieht sich auf Version 5, Release 4, Modifikation 0 von IBM i5/OS (Produktnummer 5722-SS1) und alle nachfolgenden Releases und Modifikationen, es sei denn, es erfolgen anders lautende Angaben in neuen Ausgaben. Diese Version kann nicht auf allen RISC-Modellen (Reduced Instruction Set Computer) ausgeführt werden. Auf CICS-Modellen ist sie nicht ausführbar.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Systems - iSeries Windows Environment on iSeries,
herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 1998, 2006
© Copyright IBM Deutschland GmbH 1998, 2006

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
Februar 2006

Inhaltsverzeichnis

Kapitel 1. Windows-Umgebung auf iSeries.	1	Konfiguration für Verbindungssicherheit.	49
		Zertifikatsspeicher	49
Kapitel 2. Neuerungen in V5R4	3	Konzepte für Hochverfügbarkeit	50
Kapitel 3. Druckbare PDF	5	Sicherheitskonzepte.	51
Kapitel 4. Konzepte	7	Sicherheit für IXS und Systeme mit IXA-Anschluss	51
Integrierter Server - Übersicht	8	Sicherheit für Systeme mit iSCSI-Anschluss.	51
Vorteile	9	Konzepte für Benutzer und Gruppen	54
Terminologie	10	Arten von Benutzerkonfigurationen	56
Hardwarekonzepte	14	Schablonen für die Benutzerregistrierung	58
IXS und Server mit IXA-Anschluss	16	Überlegungen zu Kennwörtern	59
Server mit iSCSI-Anschluss	18	Kapitel 5. Windows-Umgebung auf der	iSeries installieren und konfigurieren . 61
Server mit iSCSI-Anschluss - Übersicht	19	Hardwarevoraussetzungen	62
Basisunterstützung für Einzelserver	19	Softwarevoraussetzungen.	64
Unterstützung für mehrere Server	21	Installation von integrierten Windows-Servern vorbereiten.	64
Erweiterte iSCSI-Unterstützung.	22	Maschinenpoolvoraussetzungen	66
Booten über iSCSI ohne Plattenspeicher	23	Zeitsynchronisation.	67
Windows-Konsole	24	i5/OS-TCP/IP für integrierte Windows-Server.	67
Überlegungen	25	iSeries Access für Windows auf integrierten Windows-Servern.	68
Leistungsverhalten	26	iSeries NetServer aktivieren	68
iSeries-Speicherbereiche im Vergleich zu dedizierten Festplatten	26	Gastbenutzerprofil für iSeries NetServer erstellen	68
Lastausgleich des Speicherbereichs	27	IBM i5/OS Integrated Server Support installieren.	69
Server mit iSCSI-Anschluss - Serverleistung	28	Installation des Windows-Servers planen	70
Virtual Ethernet	29	Installation der iSCSI-Hardware planen	70
Konzepte für den Netzwerkbetrieb	29	Bootmodus für Hosted System planen	70
Serviceprozessorverbindung.	30	Konfiguration des Serviceprozessors und des fernen Systems erstellen	71
iSCSI-Netzwerk	30	Serviceprozessorverbindung planen	72
Virtual Ethernet-Punkt-zu-Punkt	33	Erkennungsmethode für Serviceprozessor auf dem iSeries-Server konfigurieren	72
Virtual Ethernet-Netzwerke	33	NWS-Beschreibungen	73
Externe Netzwerke	38	Installationsarbeitsblatt für i5/OS-Parameter	73
Softwarekonzepte	38	Vergleich der Dateisysteme FAT, FAT32 und NTFS	96
Integrierter xSeries-Server (IXS) und über integrierten xSeries-Adapter (IXA) angeschlossene xSeries-Server	39	Tipp: Ressourcennamen bei mehreren integrierten Servern suchen	97
NWS-Beschreibung	41	Unterstützte Sprachversionen	97
Name der Hardwareressource	41	Windows 2000 Server oder Windows Server 2003 installieren.	98
NWS-Speicherbereiche.	42	iSCSI-Hardware für Windows-Installation vorbereiten	99
Virtual Ethernet-Leitungsbeschreibungen	42	Serviceprozessorsicherheit initialisieren	99
TCP/IP-Schnittstellen	43	NWS-Hostadapter erstellen und starten	99
Systembus- und HSL-Datenfluss	43	Installation über die i5/OS-Konsole starten	100
xSeries- und IBM BladeCenter-Server mit iSCSI-Anschluss	43	Installation über die Konsole des integrierten Windows-Servers fortsetzen	103
NWS-Hostadapter	45	Serverinstallation abschließen	104
Konfiguration des fernen Systems	45	Upgrade des Lizenzprogramms IBM iSeries Integration für Windows-Server durchführen.	105
Konfiguration für Serviceprozessor	46		
NWS-Beschreibung	46		
NWS-Speicherbereiche.	47		
Datenfluss.	47		
Über iSCSI angeschlossene xSeries- und BladeCenter-Server mit Netzsicherheit	48		
Konfiguration des fernen Systems	49		
Konfiguration für Serviceprozessor	49		

Upgrade von IBM i5/OS Integrated Server Support auf der Seite des integrierten Servers durchführen	107	Mit iSCSI-Konfigurationsobjekten arbeiten	127
Hardware des integrierten xSeries-Servers von 285x oder 661x auf 2890 migrieren	108	NWS-Hostadapter verwalten	127
Migration auf Server mit iSCSI-Anschluss durchführen	108	NWS-Hostadapterobjekt erstellen	127
Windows-Clusterdienst	108	Ein NWS-Hostadapterobjekt auf der Basis eines anderen erstellen	128
Windows-Clusterdienst installieren	109	Eigenschaften des NWS-Hostadapters anzeigen	128
Windows-Clusterdienst auf einem neuen integrierten Windows-Server installieren	109	Eigenschaften des NWS-Hostadapters ändern	129
Windows-Clusterdienst auf einem vorhandenen Server installieren	110	NWS-Hostadapter starten	129
Windows für die Installation des Windows-Clusterdienstes vorbereiten	111	NWS-Hostadapter stoppen	129
Windows-Clusterdienst unter Windows installieren	112	NWS-Hostadapter löschen	130
Windows-Clusterdienst unter Windows 2000 Server installieren	113	Konfigurationen von Netzwerkservers fernere Systeme verwalten	130
Windows-Clusterdienst unter Windows Server 2003 installieren	113	Konfigurationsobjekt für ein fernes System erstellen	130
Kerberos für Windows Server 2003 Active Directory Server aktivieren	115	Konfigurationsobjekt des fernen Systems auf der Basis eines anderen erstellen	131
ATI Radeon 7000M-Bildschirmeinheitentreiber für Windows 2000 auf dem integrierten xSeries-Server 2892-002 oder 4812-001 installieren	115	Konfigurationseigenschaften des fernen Systems anzeigen	131
Hardwarebeschleunigung für Windows Server 2003 auf dem integrierten xSeries-Server 2892-002 oder 4812-001 anpassen	116	Konfigurationseigenschaften des fernen Systems ändern	132
Fehlernachrichten während der Installation beantworten	116	Status des fernen Systems anzeigen	132
Integrierten Windows-Server für automatisches Anhängen mit TCP/IP einstellen	117	Konfigurationsobjekt für ein fernes System löschen	132
Codekorrekturen	117	Netzwerkserverkonfigurationen des Serviceprozessors verwalten	133
Arten von Codekorrekturen	118	Konfigurationsobjekt für einen Serviceprozessor erstellen	133
Level der Integrationssoftware über die Konsole des integrierten Windows-Servers synchronisieren	119	Konfigurationsobjekt des Serviceprozessors auf der Basis eines anderen erstellen	134
Level der Integrationssoftware mit iSeries Navigator synchronisieren	119	Konfigurationseigenschaften des Serviceprozessors anzeigen	134
Level der Integrationssoftware mit einem fernen Befehl synchronisieren	119	Konfigurationseigenschaften des Serviceprozessors ändern	134
Kapitel 6. Virtual Ethernet- und externe Netzwerke verwalten.	121	Serviceprozessor initialisieren	135
IP-Adresse, Gateway und MTU-Werte konfigurieren	121	Konfigurationsobjekt für einen Serviceprozessor löschen	135
Virtual Ethernet-Netzwerke konfigurieren	121	Netzwerkserverkonfigurationen für Verbindungssicherheit verwalten	135
Partitionsübergreifende Virtual Ethernet-Netzwerke konfigurieren	122	Verbindungssicherheitskonfigurationsobjekt erstellen	136
Virtual Ethernet-Punkt-zu-Punkt-Netzwerke anzeigen und ändern	123	Objekt der Verbindungssicherheitskonfiguration auf der Basis eines anderen erstellen	136
Externe Netzwerke	125	Konfigurationseigenschaften der Verbindungssicherheit anzeigen	137
Einheitentreiber für Netzwerkadapter installieren und Adressinformationen des Adapters zum integrierten Windows-Server hinzufügen	125	Konfigurationseigenschaften der Verbindungssicherheit ändern	137
Netzwerkadapter entfernen	126	Verbindungssicherheitsobjekt löschen	138
Kapitel 7. Verbindungen der Server mit iSCSI-Anschluss verwalten.	127	Sicherheit zwischen i5/OS und Hosted Systemen konfigurieren	138
		CHAP konfigurieren	138
		IPSec konfigurieren	139
		Serviceprozessor-SSL konfigurieren	140
		Automatische SSL-Initialisierung	140
		Manuelle SSL-Initialisierung	141
		Serviceprozessorkennwort	142
		Firewall konfigurieren	142
		iSCSI-Hostbusadapter verwalten	143
		Hot-Spare zwischen lokalen iSCSI-Hostadapters	143
		iSCSI-HBA-Nutzung verwalten	144

Einigen iSCSI-HBA mit mehreren Hosted Servern gemeinsam benutzen	144
Workload über mehrere iSCSI-HBAs verteilen	145
Mehrere iSCSI-HBAs für Redundanz verwenden.	146
iSCSI-HBA-Zuordnung auf der Windows-Seite des iSCSI-Netzwerks verwalten . . .	147
Überlegungen zur größten zu übertragenden Einheit (MTU)	147
Virtual Ethernet für maximale Leistung auf iSCSI-Netzwerken konfigurieren, die Rahmen über 1500 Byte unterstützen	148
Virtual Ethernet für iSCSI-Netzwerk konfigurieren, deren maximale Rahmengröße geringer als 1500 Byte ist	148
Virtual Ethernet so konfigurieren, dass ungewöhnliche Nicht-TCP-Anwendungen unterstützt werden, die keine MTU vereinbaren	149
Integrierter DHCP-Server	149
Fernen Server erkennen und verwalten	150
IBM Director installieren und konfigurieren . . .	150
Fernen Server und Serviceprozessor erkennen	151
Erkennungskonfiguration für Serviceprozessor.	151
Dynamische IP-Adressierung (DHCP)	153
Erkennungsmethode für Serviceprozessor	153
Service Location Protocol (SLP) mit Multicastadressierung	153
Erkennung durch IP-Adresse	154
Erkennung durch Hostname	155
Managementmodul- oder RSA II-Webschnittstelle verwenden	155

Kapitel 8. Integrierte Windows-Server verwalten 157

Integrierten Server starten und stoppen	157
Integrierten Windows-Server mit iSeries Navigator starten und stoppen	157
Integrierten Windows-Server über die zeichenorientierte Schnittstelle starten und stoppen . . .	158
Integrierten Server über die Konsole des Windows-Servers beenden	158
iSeries mit integrierten Windows-Servern sicher herunterfahren	158
Verbindung zur virtuellen seriellen Konsole für IXS Modell 4812 herstellen	159
Konfigurationsdaten des integrierten Windows-Servers anzeigen oder ändern	160
Nachrichtenprotokollierung	161
Befehle für den integrierten Windows-Server im Fernzugriff ausführen	161
Richtlinien für die Übergabe ferner Befehle . . .	163
Unterstützung des Befehls SBMNWSCMD und der Sicherung auf Dateiebene für Kerberos V5 und EIM	165
Hot-Spare zwischen Server-Hardware	166

Kapitel 9. Speicherverwaltung 167

i5/OS-Speicherverwaltung	167
Plattenlaufwerke für integrierte Windows-Server	168

Vordefinierte Plattenlaufwerke für integrierte Windows-Server	171
Plattenlaufwerke des integrierten Windows-Servers unter i5/OS verwalten	172
Vom integrierten Server auf das i5/OS-Dateisystem zugreifen	172
Informationen zu Plattenlaufwerken des integrierten Servers abrufen	172
Plattenlaufwerke zu integrierten Windows-Servern hinzufügen	172
Plattenlaufwerk für integrierten Server erstellen	173
Plattenlaufwerk mit einem integrierten Server verbinden	173
Plattenlaufwerke für integrierten Server formatieren	175
Plattenlaufwerk kopieren	175
Plattenlaufwerk erweitern	176
Systemlaufwerk erweitern	177
Verbindung von Plattenlaufwerken für integrierten Windows-Server aufheben	177
Plattenlaufwerke für integrierten Windows-Server löschen	178
Windows-Programme zur Datenträgerverwaltung mit integrierten Windows-Servern verwenden . . .	178

Kapitel 10. Einheiten gemeinsam benutzen 179

Einheitenbeschreibung und Hardwareressourcenamen für iSeries-Einheiten bestimmen.	179
Optische iSeries-Laufwerke mit integrierten Windows-Servern verwenden	179
iSeries-Bandlaufwerke mit integrierten Windows-Servern verwenden	180
Bandeinheitentreiber installieren	181
Band unter i5/OS für integrierte Windows-Server formatieren.	181
iSeries-Bandlaufwerk einem integrierten Windows-Server zuordnen	182
Steuerung eines Bandlaufwerks vom integrierten Windows-Server an die iSeries zurückgeben . . .	182
Unterstützte iSeries-Bandlaufwerke	183
iSeries-Bandlaufwerke für Anwendungen identifizieren	183
Steuerung von optischen Laufwerken und Bandlaufwerken der iSeries zwischen integrierten Windows-Servern übertragen	184
Vom integrierten Windows-Server auf iSeries-Druckern drucken	185

Kapitel 11. Benutzer des integrierten Windows-Servers unter i5/OS verwalten 187

Einzelnen i5/OS-Benutzer mit iSeries Navigator in der Windows-Umgebung registrieren	187
i5/OS-Gruppe mit iSeries Navigator in der Windows-Umgebung registrieren	188
i5/OS-Benutzer über die zeichenorientierte Schnittstelle in der Windows-Umgebung registrieren . . .	188
Benutzerschemata erstellen	189

Ausgangsverzeichnis in einer Schablone angeben	190
Benutzerprofilattribut LCLPWDMGT ändern	190
EIM (Enterprise Identity Mapping)	191
Benutzerregistrierung in der Windows-Umgebung beenden	192
Gruppenregistrierung in der Windows-Umgebung beenden	193
Benutzer QAS400NT	193
Registrierung und Weitergabe auf einem integrierten Windows-Server verhindern	196

Kapitel 12. Integrierte Windows-Server sichern und zurückspeichern 199

Einem integrierten Windows-Server zugeordnete NWS-Beschreibungen und andere Objekte sichern	199
NWS-Beschreibung eines integrierten Windows-Servers sichern	200
NWSH-Konfiguration eines Windows-Servers mit iSCSI-Anschluss sichern	200
iSCSI-NWSCFGs und Prüflisten sichern	200
Vordefinierte Plattenlaufwerke für integrierte Windows-Server sichern	201
Benutzerdefinierte Plattenlaufwerke für einen integrierten Windows-Server sichern	202
Benutzerregistrierungsdaten sichern und zurückspeichern	203
Zu sichernde Objekte und ihre Positionen unter i5/OS	203
Einzelne Dateien und Verzeichnisse des integrierten Windows-Servers sichern	205
Einschränkungen für Sicherungen auf Dateiebene	205
Vorbereitende Konfigurationsaufgaben	206
Freigaben auf integrierten Windows-Servern erstellen	207
Teildateien zur Datei QAZLCSAVL hinzufügen	207
Zugehörigkeit von iSeries NetServer und integriertem Windows-Server zur selben Domäne sicherstellen	207
Dateien sichern	208
Beispiele: Komponenten eines integrierten Windows-Servers angeben	208
Windows-Sicherungsdienstprogramm	209
NWS-Beschreibung und Plattenlaufwerke eines integrierten Windows-Servers zurückspeichern	209
Vordefinierte Plattenlaufwerke für integrierte Windows-Server zurückspeichern	210
Benutzerdefinierte Plattenlaufwerke für integrierte Windows-Server zurückspeichern	211
NWS-Beschreibungen von integrierten Windows-Servern zurückspeichern	212
NWSHs von integrierten Windows-Servern zurückspeichern	213
NWSCFGs von integrierten Windows-Servern für Server zurückspeichern, die über iSCSI angeschlossen sind	213
Dateien des integrierten Windows-Servers zurückspeichern	214

Kapitel 13. Betriebssystem des Windows-Servers von der Hardware des integrierten Servers deinstallieren . . . 215

NWS-Beschreibung eines integrierten Servers löschen	215
Leitungsbeschreibungen eines integrierten Servers löschen	216
TCP/IP-Schnittstellen löschen, die einem integrierten Windows-Server zugeordnet sind	216
Einem integrierten Windows-Server zugeordnete Controllerbeschreibungen löschen	217
Einem integrierten Windows-Server zugeordnete Einheitenbeschreibungen löschen	217
Einem integrierten iSCSI Windows-Server zugeordnete NWS-Konfigurationen löschen	217
IBM i5/OS Integrated Server Support, i5/OS-Option 29 (5722-SS1) löschen	218

Kapitel 14. Fehlerbehebung bei integrierten Windows-Servern 219

Nachrichten und Jobprotokolle prüfen	219
Überwachungsjob	221
Zusätzliche Protokolle und Nachrichten für Server mit iSCSI-Anschluss	221
Fehler auf integrierten Windows-Servern	222
STOP oder Blue-Screen-Fehler	223
Zu wenig Speicherplatz auf dem Systemlaufwerk des integrierten Servers	223
Fehler bei optischen Einheiten	224
Sperrung der optischen Einheit bei ausgefallenem Server	225
Bandfehler	225
Prüfen, ob der Einheits-treiber für Bandlaufwerke geladen ist	226
Fehler beim Starten eines integrierten Windows-Servers	227
Fehler beim Hot-Sparing zwischen Servern	228
Fehler bei der gemeinsamen Nutzung von Hardware für Hosted Systeme	229
Mehrere NWSDs für gemeinsame Nutzung von Hardware für Hosted Systeme definiert	229
Besonderheiten bei Systemen mit iSCSI-Anschluss	230
Fehler in der NWSD-Konfigurationsdatei	231
NWSD-Konfigurationsdatei korrigieren	231
NWSD-Konfigurationsdateiparameter zurücksetzen	231
Frühere Version der Datei des integrierten Servers verwenden	231
DASD in Servern mit IXa- oder iSCSI-Anschluss	232
Fehler bei der Benutzer- und Gruppenregistrierung	232
Berechtigungsfehler bei der Benutzerregistrierung	233
Kennwortfehler	234
Snap-in-Programm von IBM iSeries Integrated Server Support	235
Fehler auf Servern mit iSCSI-Anschluss	236
Netzplananalyse für Boot- und Speicherpfade	238
Pfadzertifikate verwalten	238

Fehlerbehebung für IBM Director	239	Schlüsselwort TARGETDIR	264
Fehler bei der Erkennung	240	Schlüsselwort TARGETFILE	264
Fehler bei SSL-Verbindungen	240	Datei eines integrierten Servers mit Eintragsart	
Virtual Ethernet-Fehler bei Servern mit iSCSI-		ADDCONFIG ändern	264
Anschluss	242	Schlüsselwort VAR	265
Virtual Ethernet-Fehler bei IXS und Servern mit		Schlüsselwort ADDSTR	265
IXA-Anschluss	244	Schlüsselwort ADDWHEN	266
Sowohl Leitungsbeschreibung als auch Sym-		Ausdrucksoperatoren ADDWHEN und	
bol sind vorhanden	245	DELETEWHEN	266
Leitungsbeschreibung ist vorhanden und		Schlüsselwort DELETEWHEN	267
Symbol fehlt.	246	Schlüsselwort LINECOMMENT	267
Leitungsbeschreibung fehlt und Symbol ist		Schlüsselwort LOCATION	267
vorhanden	247	Schlüsselwort LINESEARCHPOS	267
Sowohl Leitungsbeschreibung als auch Sym-		Schlüsselwort LINESEARCHSTR	267
bol fehlen	247	Schlüsselwort LINELOCATION	267
Fehler bei externen Netzwerken	248	Schlüsselwort FILESEARCHPOS (Eintragsart	
LAN-Treiber auf dem integrierten Windows-		ADDCONFIG)	268
Server manuell aktualisieren	249	Schlüsselwort FILESEARCHSTR	268
Installation oder Aktualisierung des LAN-		Schlüsselwort FILESEARCHSTROCC	268
Treibers beginnen	249	Schlüsselwort REPLACEOCC	268
Zu installierenden oder zu aktualisierenden		Schlüsselwort TARGETDIR	269
Adapter auswählen	249	Schlüsselwort TARGETFILE	269
Installation oder Aktualisierung des LAN-		Schlüsselwort UNIQUE	269
Treibers abschließen	249	Schlüsselwort VAROCC	269
IP-Adressenkonflikte bei Virtual Ethernet-Punkt-		Schlüsselwort VARVALUE	269
zu-Punkt	251	Datei des integrierten Windows-Servers mit	
IP-Adressen für Virtual Ethernet-Punkt-zu-		Eintragsart UPDATECONFIG ändern	270
Punkt zuordnen	252	Schlüsselwort FILESEARCHPOS (Eintragsart	
Fehler bei TCP/IP über Virtual Ethernet	253	UPDATECONFIG).	271
Fehler beim Zugriff auf Freigaben von Windows		Schlüsselwort FILESEARCHSTR (Eintragsart	
Server 2003 mit dem Dateisystem QNTC	254	UPDATECONFIG).	271
IFS-Zugriffsfehler	254	Schlüsselwort FILESEARCHSTROCC (Eintrags-	
Fehler beim Sichern von Dateien des integrier-		art UPDATECONFIG)	271
ten Windows-Servers	254	Konfigurationsstandardwerte mit der Eintragsart	
Nicht lesbare Nachrichten in der Servernach-		SETDEFAULTS festlegen	271
richtenwarteschlange	255	ADDWHEN	272
Fehler beim Erstellen eines Windows-System-		DELETEWHEN	272
speicherauszugs	256	Schlüsselwort FILESEARCHPOS (Eintragsart	
Integrierten Windows-Server erneut installieren	257	SETDEFAULTS)	273
Servicedaten des integrierten Windows-Servers		Schlüsselwort FILESEARCHSTR (Eintragsart	
erfassen	257	SETDEFAULTS)	273
Hauptspeicherauszug für einen integrierten		TARGETDIR	273
Windows-Server unter i5/OS erstellen	258	TARGETFILE	273
NWSD-Speicherauszugstool unter i5/OS ver-		Substitutionsvariablen für Schlüsselwortwerte ver-	
wenden	258	wenden	274
Kapitel 15. Konfigurationsdateien für		Kapitel 16. Referenzinformationen	277
NWSD-Beschreibung (NWSD)	261	Anhang. Bemerkungen	279
Format der NWSD-Konfigurationsdatei.	261	Marken	280
NWSD-Konfigurationsdatei erstellen	262	Bedingungen	281
Beispiel: NWSD-Konfigurationsdatei.	263		
Zeilen aus einer bestehenden Datei eines integrier-			
ten Servers mit der Eintragsart CLEARCONFIG			
entfernen	264		

Kapitel 1. Windows-Umgebung auf iSeries

Mehr als jede andere Hardware- oder Softwarekomponente ist die Windows-Umgebung auf iSeries im Grunde genommen eine Konzeption. Sie ermöglicht die Zusammenarbeit von iSeries-Servern und Personal Computern (PCs) und darüber hinaus die Steuerung von PCs durch den iSeries-Server mit dem Ziel, deren Verwaltung zu vereinfachen.

Die erste Komponente der Windows-Umgebung auf der iSeries ist die PC-Hardware, die zur iSeries hinzugefügt werden muss. Hierfür gibt es drei grundlegende Methoden.

- Durch die Verwendung eines *integrierten xSeries-Adapters (IXA)* kann die iSeries die IBM xSeries-Server steuern. IBM verwendet die Bezeichnung *xSeries-Server* für seine PC-Reihe.
- Durch die Verwendung eines *Internet SCSI-Hostbusadapters (iSCSI-HBA)* kann der iSeries-Server eine Verbindung über Ethernet herstellen und IBM xSeries- oder IBM BladeCenter-Server steuern.
- Ein *integrierter xSeries-Server (IXS)* ist eine iSeries-Erweiterungskarte, die Arbeitsspeicher (Random Access Memory - RAM) sowie einen Intel-Prozessor enthält. Den IXS kann man sich als PC vorstellen, der in das Gehäuse eines iSeries-Servers eingegliedert wurde.

Die zweite Komponente ist IBM i5/OS-Option 29 (5722-SS1), die auf dem iSeries-Server installiert ist, damit er die Befähigung erhält, PCs zu steuern. Diese PCs werden dann als integrierte Windows-Server bezeichnet.

Schließlich muss die Microsoft-Software Windows 2000 Server oder Windows Server 2003 installiert sein.

Das vorliegende Dokument ist in die folgenden Kapitel gegliedert:

Kapitel 2, „Neuerungen in V5R4“, auf Seite 3

In diesem Kapitel werden die Änderungen und Erweiterungen vorgestellt, die an diesem Release vorgenommen wurden.

Kapitel 3, „Druckbare PDF“, auf Seite 5

Hier wird beschrieben, wie Sie eine PDF-Version dieses Dokuments drucken können.

Kapitel 4, „Konzepte“, auf Seite 7

Dieses Kapitel enthält Wissenswertes zur Lösung für die Windows-Umgebung auf der iSeries.

Kapitel 5, „Windows-Umgebung auf der iSeries installieren und konfigurieren“, auf Seite 61

Die Anweisungen in diesem Kapitel beschreiben, wie Sie einen integrierten Windows-Server neu installieren.

Kapitel 6, „Virtual Ethernet- und externe Netzwerke verwalten“, auf Seite 121

In diesem Kapitel erfahren Sie, wie Sie die drei unterschiedlichen Netzwerkkarten verwenden, die für integrierte Server zur Verfügung stehen.

Kapitel 7, „Verbindungen der Server mit iSCSI-Anschluss verwalten“, auf Seite 127

Hier wird beschrieben, wie Sie die iSeries mit Hilfe von iSCSI für die Verbindung zu xSeries- oder IBM BladeCenter-Servern konfigurieren.

Kapitel 8, „Integrierte Windows-Server verwalten“, auf Seite 157

Hier wird beschrieben, wie Sie den Server starten und stoppen, Befehle für den integrierten Server im Fernzugriff ausführen, Konfigurationsdaten anzeigen und ändern sowie Nachrichten- und Fehlerprotokolle überwachen.

Kapitel 9, „Speicherverwaltung“, auf Seite 167

Dieses Kapitel enthält Informationen zu Festplatten für integrierte Server.

Kapitel 10, „Einheiten gemeinsam benutzen“, auf Seite 179

In diesem Kapitel wird die Verwendung von iSeries-Einheiten auf integrierten Servern beschrieben.

Kapitel 11, „Benutzer des integrierten Windows-Servers unter i5/OS verwalten“, auf Seite 187

Hier wird erläutert, wie i5/OS-Benutzer in die Windows-Umgebung integriert werden.

Kapitel 12, „Integrierte Windows-Server sichern und zurückspeichern“, auf Seite 199

In diesem Kapitel werden Methoden beschrieben, wie Dateien integrierter Server auf Bandlaufwerke oder iSeries-Festplatten gesichert werden können.

Kapitel 13, „Betriebssystem des Windows-Servers von der Hardware des integrierten Servers deinstallieren“, auf Seite 215

In diesem Kapitel finden Sie alle Informationen, die Sie zum Entfernen der Software für den integrierten Server von Ihrem System benötigen.

Kapitel 14, „Fehlerbehebung bei integrierten Windows-Servern“, auf Seite 219

In diesem Kapitel werden häufig gestellte Fragen beantwortet.

Kapitel 15, „Konfigurationsdateien für NWS-Beschreibung (NWSD)“, auf Seite 261

Hier wird erläutert, wie Sie Ihre integrierten Server durch die Erstellung eigener Konfigurationsdateien anpassen können.

Kapitel 16, „Referenzinformationen“, auf Seite 277

Kapitel 2. Neuerungen in V5R4

In V5R4 wurde die Windows-Umgebung auf der iSeries mit mehreren neuen Funktionen ausgestattet:



- Unterstützung für die Integration von xSeries- und IBM BladeCenter-Systemen in den iSeries-Server via iSCSI-Hostbusadapter (iSCSI-HBAs). Diese Technologie der Serverintegration ergänzt die vorhandenen Technologien der integrierten xSeries-Server und integrierten xSeries-Adapter. Sowohl die iSeries- als auch die xSeries-Server unterstützen Server, die über ein skalierbares Gigabit-Ethernet-Netzwerk unter Verwendung des iSCSI-Protokolls und unterstützter Adapter angeschlossen sind. Informationen darüber, wie die iSCSI-Technologie für die Integration von IBM xSeries- und BladeCenter-Systemen in den iSeries-Server eingesetzt wird, finden Sie in Kapitel 4, „Konzepte“, auf Seite 7. Informationen über die Verwaltung und Konfiguration von Servern mit iSCSI-Anschluss finden Sie in Kapitel 7, „Verbindungen der Server mit iSCSI-Anschluss verwalten“, auf Seite 127 und Kapitel 8, „Integrierte Windows-Server verwalten“, auf Seite 157.
- Das Produkt IBM iSeries Integration für Windows Server (5722-WSV) wurde als i5/OS Integrated Server Support (5722-SS1 Option 29) neu konfektioniert.

Anmerkung: Wenn Sie ein Upgrade von einem früheren Release auf i5/OS V5R4 vornehmen, wird Produkt 5722-WSV automatisch entfernt und stattdessen Produkt 5722-SS1 Option 29 installiert.

- Erweiterte Speicherkapazität für Windows-Server mit iSCSI-Anschluss. An einen Windows-Server mit iSCSI-Anschluss können bis zu 64 Plattenlaufwerke (NWS-Speicherbereiche) angeschlossen werden, was mehr als 60 TB an Plattenspeicher pro Server bedeutet.
- Die Unterstützung für die Erweiterung von Plattenlaufwerken (NWS-Speicherbereichen) wurde hinzugefügt. Weitere Informationen finden Sie unter „Plattenlaufwerk erweitern“ auf Seite 176.
- Die Unterstützung für Volume Shadow Copy Service (VSS) von Windows Server 2003 wurde hinzugefügt. VSS kann von Backup-Anwendungen genutzt werden, die unter Windows ausgeführt werden. Daten für Anwendungen, die Volume Shadow Copy Service (VSS) von Windows Server 2003 unterstützen, können ohne Stoppen der Anwendung gesichert werden, was wiederum die Anwendungsverfügbarkeit erhöht. Weitere Informationen finden Sie in Kapitel 12, „Integrierte Windows-Server sichern und zurückspeichern“, auf Seite 199.
- Zusätzliche iSeries Navigator GUI-Unterstützung. Dazu gehören die Unterstützung für die Verwaltung von Servern mit iSCSI-Anschluss, die Verwaltung integrierter Linux- und AIX-Server sowie die Konfiguration von Virtual Ethernet-Ports für integrierte Server.
- Die Unterstützung für den IBM Integrierten PC-Server für AS/400 (IPCS) mit 200 MHz und 333 MHz und die Unterstützung für den IBM Integrierten Netfinity-Server für AS/400 (INS) wurde zurückgezogen. Die zurückgezogenen IPCS- und INS-Hardwareressourcentypen sind 6617 und 2850 mit den Feature-Codes 2854, 2857, 2865, 2866, 6617 und 6618. Da die IPCS- und INS-Server die einzigen integrierten Servertypen waren, die Host-LAN-Unterstützung boten (gemeinsame Nutzung von LAN-Adaptoren in i5/OS und Windows), wurde die Host-LAN-Funktion ebenfalls zurückgezogen.
- Die bisher in diesem Dokument enthaltenen Informationen über Windows NT 4.0-Server (die ab V5R3 nicht mehr unterstützt werden), IPCS- oder INS-Hardware (Typen 6617 und 2850), gemeinsam genutzte Netzwerkadapter (Host-LAN) sowie Informationen über Server, die vor V4R5 installiert wurden, wurden gelöscht. Diese Informationen finden Sie weiterhin unter dem Thema zur Windows-Umgebung auf iSeries im iSeries Information Center für V5R3.

Neuerungen oder Änderungen erkennen

Damit Sie einfacher feststellen können, an welchen Stellen technische Änderungen vorgenommen wurden, wird im vorliegenden Dokument die folgende Kennzeichnung verwendet:

- Das Symbol  kennzeichnet den Beginn von neuen oder geänderten Informationen.
- Das Symbol  kennzeichnet das Ende von neuen oder geänderten Informationen.

Weitere Informationen über Neuerungen oder Änderungen in diesem Release finden Sie im Memorandum für Benutzer.

Kapitel 3. Druckbare PDF

Wählen Sie zum Anzeigen oder Herunterladen der PDF-Version dieses Dokuments Windows-Umgebung auf iSeries aus (ca. 4,2 MB).


Die in Kapitel 16, „Referenzinformationen“, auf Seite 277 aufgeführten zugehörigen Handbücher und Redbooks können Sie als PDF anzeigen oder drucken.

PDF-Dateien speichern

So können Sie eine PDF-Datei zum Anzeigen oder Drucken auf Ihrer Workstation speichern:

1. Klicken Sie in Ihrem Browser mit der rechten Maustaste auf die PDF-Datei (klicken Sie mit der rechten Maustaste auf den obigen Link).
2. Klicken Sie bei Verwendung des Internet Explorers auf die Option für das Speichern des Ziels. Klicken Sie bei Verwendung von Netscape Communicator auf die Option für das Speichern des Links.
3. Navigieren Sie zu dem Verzeichnis, in dem Sie die PDF-Datei speichern möchten.
4. Klicken Sie auf **Speichern**.

Adobe Reader herunterladen

- | Zum Anzeigen oder Drucken der PDF-Dateien benötigen Sie das Programm Adobe Reader. Von der Adobe-Website (www.adobe.com/products/acrobat/readstep.html)  können Sie eine kostenfreie Kopie dieses Programms herunterladen.

Kapitel 4. Konzepte

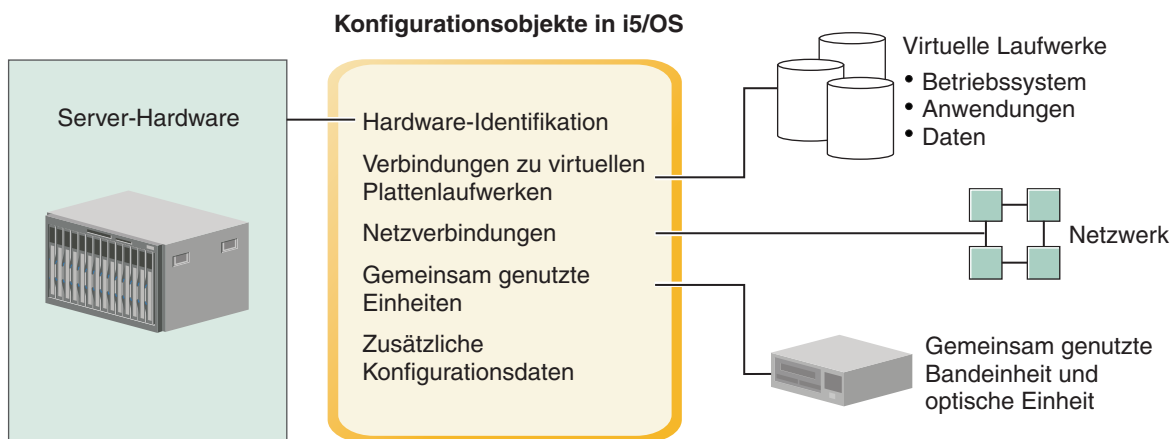
| In diesem Dokument bezeichnet der Begriff *Integrierter Windows-Server* (kurz: *Integrierter Server*) eine
| Instanz von Microsoft Windows 2000 Server oder Windows Server 2003, die auf einem integrierten xSe-
| ries-Server, auf einem xSeries-Server, der mit einem integrierten xSeries-Adapter an eine iSeries ange-
| schlossen ist, oder auf einem xSeries- oder IBM BladeCenter-Server, der mit einem iSCSI-Hostbusadapter
| an einen iSeries-Server angeschlossen ist, ausgeführt wird. Analog zum Begriff "PC", der häufig verwen-
| det wird, um auf die Software des Microsoft-Betriebssystems und den zugehörigen Intel-Mikroprozessor
| sowie die zugehörige Hardware zu verweisen, wird der Terminus "integrierter Windows-Server" hier ver-
| wendet, um die Kombination aus Hardware und Software zu bezeichnen, aus der sich das Gesamt-
| produkt zusammensetzt.

Die folgenden Abschnitte enthalten konzeptbezogene Informationen:

- „Integrierter Server - Übersicht“ auf Seite 8
- „Vorteile“ auf Seite 9
- „Terminologie“ auf Seite 10
- „Hardwarekonzepte“ auf Seite 14
- „Überlegungen“ auf Seite 25
- | • „Leistungsverhalten“ auf Seite 26
- „Konzepte für den Netzwerkbetrieb“ auf Seite 29
- „Softwarekonzepte“ auf Seite 38
- | • „Konzepte für Hochverfügbarkeit“ auf Seite 50
- | • „Sicherheitskonzepte“ auf Seite 51
- „Konzepte für Benutzer und Gruppen“ auf Seite 54

Integrierter Server - Übersicht

Ein integrierter Server besteht aus einer Kombination mehrerer Hardware- und Softwarekomponenten.



RZAHQ507-1

Abbildung 1. Integrierter Server - Übersicht

Die **Server-Hardware** ist die physische Hardware (z. B. Prozessor und Speicher), auf der der Server läuft. Je nach individuellem Bedarf, können mehrere Typen von Server-Hardware für integrierte Server verwendet werden. Die Server-Hardware kann in Form einer Karte vorliegen, die in Ihren iSeries-Server integriert wird, es kann sich um einen externen IBM xSeries-Server handeln, der an einen iSeries-Server mit einem integrierten xSeries-Adapter angeschlossen wird, oder bei der Hardware kann es sich um einen IBM xSeries- oder IBM BladeCenter-Server handeln, der mit einem iSCSI-Hostbusadapter an den iSeries-Server angeschlossen wird. Der integrierte Server kann außerdem Bandoeinheiten und optische Einheiten verwenden, die an die i5/OS-Hosting-Partition angeschlossen sind. Weitere Informationen über die Hardwaretypen, die für integrierte Server verwendet werden können, finden Sie unter „Hardwarekonzepte“ auf Seite 14.

Jeder integrierte Server verfügt über mindestens eine Verbindung zu einem **Netzwerk**. Es werden sowohl physische Netzverbindungen mit einem Netzadapter als auch Virtual iSeries Ethernet-Netzverbindungen unterstützt. Weitere Informationen über die Netzverbindungen, die für integrierte Server verwendet werden können, finden Sie unter „Konzepte für den Netzwerkbetrieb“ auf Seite 29.

Jeder integrierte Server verwendet **virtuelle Plattenlaufwerke**, die das Betriebssystem des Servers, Anwendungen und Daten enthalten. Diese virtuellen Plattenlaufwerke werden aus dem i5/OS-Plattenspeicher heraus zugeordnet. Der integrierte Server behandelt diese Laufwerke wie physische Plattenlaufwerke, die sich innerhalb des Servers befinden. Der integrierte Server verfügt jedoch nicht wirklich über eigene physische Plattenlaufwerke. Weitere Informationen über virtuelle Plattenlaufwerke finden Sie unter „Softwarekonzepte“ auf Seite 38.

Zu den **gemeinsam genutzten Einheiten** gehören alle unterstützten Bandlaufwerke und optische Einheiten, auf die der integrierte Server so zugreifen kann, als wären sie lokale Servereinheiten. Standardmäßig hat der integrierte Server automatisch Zugriff auf alle Bandoeinheiten und optische Einheiten der iSeries. Sie können angeben, für welche dieser iSeries-Einheiten der integrierte Server zugriffsberechtigt sein soll.

| **Konfigurationsobjekte in i5/OS** beschreiben jeden einzelnen integrierten Server. Die i5/OS-Konfigurationsobjekte identifizieren die Hardware, auf der der integrierte Server läuft, die virtuellen Plattenlaufwerke und die Virtual Ethernet-Verbindungen, die der integrierte Server verwendet, sowie zahlreiche weitere Server-Attribute. Weitere Informationen über die i5/OS-Konfigurationsobjekte, die einen integrierten Server beschreiben, finden Sie unter „Softwarekonzepte“ auf Seite 38.

Vorteile

Die Windows-Umgebung auf der iSeries stellt die meisten Funktionen bereit, die auch bei der Ausführung von Microsoft Windows auf einem PC-basierten Server verfügbar sind, und bietet gegenüber anderen Datenverarbeitungssystemen die folgenden Vorteile:

Kleinere Stellfläche

- Sie müssen weniger Hardwarekomponenten verwalten, die weniger Platz benötigen.

Besserer Zugriff auf Daten und besserer Datenschutz

- Ein integrierter Windows-Server verwendet iSeries-Plattenspeicher, der im Allgemeinen zuverlässiger als Festplatten auf einem PC-Server ist.
- Sie können auf die schnelleren iSeries-Bandlaufwerke für die Sicherungen der integrierten Server zugreifen.
- | • Sie können den gesamten Windows-Server im Rahmen Ihres iSeries-Server-Backups sichern. Auf diese Weise können Sie einen ausgefallenen Server viel schneller und einfacher wiederherstellen als mit der normalen Wiederherstellung auf Dateiebene unter Windows.
- | • Integrierte Server nutzen implizit die Datenschutzpläne für den übergeordneten Datenschutz aus i5/OS, wie beispielsweise RAID oder die Spiegelungstechnologie für Laufwerke.
- | • Bei typischen Konfigurationen integrierter Server werden Speicherbereichsdaten über mehr iSeries-Plattenlaufwerke verteilt als bei standalone (nicht integrierten) Windows-Server-Installationen. Dadurch kann häufig eine bessere maximale Platten-E/A-Kapazität erzielt werden, da die einzelnen Server nicht auf wenige zugeordnete Laufwerke beschränkt sind.
- | • Sie können integrierten Servern zusätzlichen Plattenspeicher hinzufügen, ohne die Server beenden zu müssen.
- | • Mit iSeries Access können Sie über einen erweiterten ODBC-Einheitentreiber auf Daten von DB2 UDB für iSeries zugreifen. Mit diesem Einheitentreiber sind Server-zu-Server-Anwendungen zwischen integrierten Servern und i5/OS möglich.
- | • Sie können einen integrierten Server als zweite Stufe in einer dreistufigen Client/Server-Anwendung einsetzen.
- | • Für den virtuellen Netzwerkbetrieb wird keine zusätzliche LAN-Hardware benötigt; er ermöglicht die Übertragung zwischen logischen Partitionen der iSeries, integrierten xSeries-Servern (IXS), integrierten xSeries-Adaptern (IXA) und iSCSI-HBAs.

Vereinfachte Verwaltung

- Benutzerparameter, wie z. B. Kennwörter, können unter i5/OS einfacher verwaltet werden. Sie können Benutzer und Gruppen unter i5/OS für integrierte Server erstellen und registrieren. Dies vereinfacht die Aktualisierung von Kennwörtern und anderen Benutzerinformationen unter i5/OS.
- Dank der Integration von Benutzeradministrationsfunktion, Sicherheit, Server-Management sowie Sicherungs- und Wiederherstellungsplänen zwischen den Umgebungen von i5/OS und Microsoft Windows ist Ihr Datenverarbeitungssystem einfacher strukturiert. Sie können die Daten Ihres integrierten Servers gemeinsam mit anderen i5/OS-Daten auf einem Datenträger speichern und einzelne Dateien sowie i5/OS-Objekte zurückspeichern.

Fernverwaltung und -fehleranalyse

- Sie haben die Möglichkeit, sich von einem fernen Standort aus an i5/OS anzumelden, um den integrierten Server zu beenden bzw. erneut zu starten.
- Da Sie Informationen im Ereignisprotokoll des integrierten Servers nach i5/OS spiegeln können, können Sie Fehler von Microsoft im Fernzugriff analysieren.

| Über integrierten xSeries-Adapter (IXA) oder iSCSI-HBA angeschlossener xSeries-Server

- Sie sind wesentlich flexibler beim Konfigurieren eines eigenständigen xSeries-Servers im Vergleich zur Konfiguration eines IXS, also eines xSeries-Servers auf einer Karte.
- Für eigenständige xSeries-Modelle gibt es häufiger neue Releases. Dies bedeutet, dass Sie die aktuellsten Intel-Prozessoren und andere Hardware erhalten können.
- Für eigenständige xSeries-Server sind mehr PCI-Featurekarten verfügbar als für IXS-Modelle.

| Über einen iSCSI-Hostbusadapter angeschlossener IBM BladeCenter-Server

- Dichte IBM BladeCenter-Konfektionierung
- Für neue IBM BladeCenter-Modelle gibt es häufiger neue Releases als für IXS.

Mehrere Server

- Mit Hilfe des Microsoft Clusterdienstes können Sie mehrere Server zu Server-Clustern verbinden. Server-Cluster bieten Hochverfügbarkeit und einfache Verwaltungsfunktionen für Daten und Programme innerhalb des Clusters.
- Server und logische Partitionen, die auf der gleichen iSeries ausgeführt werden, bieten - ohne Verwendung von LAN-Hardware - eine leistungsfähige und gesicherte Übertragung in virtuellen Netzwerken.
- Sie können mehrere integrierte Server auf der gleichen iSeries ausführen. Dies ist nicht nur bequem und effizient, sondern ermöglicht Ihnen bei einem Hardwarefehler außerdem den einfachen Wechsel auf einen anderen, betriebsbereiten und aktiven Server.
- Wenn auf Ihrer iSeries mehrere integrierte Server installiert sind, können Sie deren Windows-Domänenaufgabenbereiche so definieren, dass die Benutzerregistrierung und der Zugriff erleichtert werden. Sie können beispielsweise einen dieser Server als Domänencontroller konfigurieren. Dann müssen Sie lediglich Benutzer für den Domänencontroller registrieren, damit sich die Benutzer auf einer beliebigen Maschine mit Microsoft Windows an dieser Domäne anmelden können.
- Die optischen Laufwerke und die Bandlaufwerke eines iSeries-Servers können mit integrierten Servern, die auf der iSeries ausgeführt werden, gemeinsam genutzt werden.

| Hot-Spare-Unterstützung

- Serverintegration und Speichervirtualisierung sind innovative Optionen für höhere Zuverlässigkeit und bessere Wiederherstellbarkeit der Windows-Server-Umgebung.
- Bei einem Hardwarefehler des Windows-Servers kann die Konfiguration des Servers schnell und ohne großen Aufwand auf einen anderen xSeries- oder IBM BladeCenter-Server (den sog. Hot-Spare-Server) umgeschaltet werden, ohne den iSeries-Server erneut starten zu müssen. Dadurch kann die Gesamtmenge der für die höhere Verfügbarkeit benötigten PC-Server reduziert werden.
- Die Hot-Spare-Unterstützung erhöht außerdem die Flexibilität, da ein Ersatzserver zum Schutz mehrerer Produktionsserver eingesetzt wird.

Terminologie

Die folgenden Begriffe werden im Zusammenhang mit der Windows-Umgebung auf der iSeries verwendet. Andere Begriffe und Begriffsbestimmungen für die iSeries können Sie im Glossar des Information Centers nachlesen.

- **Baseboard Management Controller (BMC).** Ein Basisserviceprozessor mit geringem Funktionsumfang, der zur Steuerung von xSeries-Systemen dient.

| **Challenge Handshake Authentication Protocol (CHAP).** Ein Authentifizierungsprotokoll, das einen geheimen Schlüssel beinhaltet, der sowohl dem Authentifikator als auch demjenigen, der authentifiziert wird, bekannt ist. Der geheime Schlüssel ist während der Übertragung abhörsicher.

Enterprise Identity Mapping (EIM). Eine Methode für die Zuordnung einer Person oder einer Definitionseinheit zu den korrekten Benutzeridentitäten in unterschiedlichen Registern auf unterschiedlichen Betriebssystemen. Die Benutzeradministrationsfunktion bietet Unterstützung für die automatische Erstellung von EIM-Quellenzuordnungen für Windows und integriert damit die Benutzerregistrierung in EIM. Außerdem können sich bei registrierten i5/OS-Benutzerprofilen die Windows-Benutzerprofile vom i5/OS-Benutzerprofil unterscheiden, wenn der Administrator die EIM-Quellenzuordnung für Windows manuell definiert hat.

EIM-Kennung. Repräsentiert eine tatsächliche Person oder eine Definitionseinheit in EIM. Wenn Sie eine EIM-Kennung erstellen, ordnen Sie sie der Benutzeridentität für die entsprechende Person zu.

EIM-Zuordnungen für Identitätsabgleich. Eine Umgebung für die Einzelanmeldung wird dadurch ermöglicht, dass der Benutzeridentität in einem Register eine EIM-Kennung zugeordnet wird. Es gibt 3 Arten von Zuordnungen, nämlich die Quellenzuordnung, die Zielzuordnung und die administrative Zuordnung. Die Integration der Benutzerregistrierung in EIM erfolgt, wenn eine Zielzuordnung für i5/OS und eine Quellenzuordnung für Windows definiert wird. Die Zuordnungen können entweder unter Verwendung des Benutzerprofilattributs EIMASSOC automatisch oder mit iSeries Navigator manuell definiert werden. Zielzuordnungen werden hauptsächlich zum Schutz von vorhandenen Daten verwendet. Quellenzuordnungen dienen primär zu Authentifizierungszwecken.

| **Externes Netzwerk.** Netzwerk, auf das integrierte Server mittels physischer Netzwerkhardware zugreifen. Siehe auch **virtuelles Netzwerk**.

| **Ferne Schnittstelle.** Die ferne Schnittstelle stellt die Konfigurationsparameter dar, die den iSCSI-Initiatoradapter beschreiben, der sich im xSeries-Server oder im IBM BladeCenter-Server befindet. Die ferne Schnittstelle enthält sowohl Parameter für die SCSI- als auch für die LAN-Funktionen des Adapters.

| **Gehäuseidentifikation.** Seriennummer, Typ und Modell des Gehäuses, das den Serviceprozessor enthält. Bei einem xSeries-Standardserver haben Serviceprozessor und xSeries-Server eine gemeinsame Gehäuseidentifikation. Bei einem IBM BladeCenter-Server kennzeichnet die Gehäuseidentifikation das Managementmodul, das die von ihm gesteuerten IBM BladeCenter-Server enthält.

| **Hostbusadapter (HBA).** Ein Hostbusadapter (HBA) ist eine Adapterkarte, die in den Bus des Hostsystems integriert wird. Z. B. ein Ethernet-Adapter oder ein iSCSI-Adapter.

| **Hot-Spare.** Hot-Spare bietet die Möglichkeit, Ersatz-Server-Hardware (z. B. einen inaktiven IXS) als Backup für die Server-Hardware zu reservieren, die von einem oder mehreren aktiven Servern genutzt wird. Wenn bei einem der aktiven Server ein Hardwarefehler auftritt, kann schnell auf die Ersatz-Server-Hardware gewechselt und der Server erneut gestartet werden. Auf diese Weise wird die normalerweise bei einem Hardwarefehler zu verzeichnende Ausfallzeit des Servers drastisch reduziert. Weitere Informationen finden Sie unter „Hot-Spare zwischen Server-Hardware“ auf Seite 166.

| **IBM Director.** Eine Anwendung, die die Erkennung, Leistungssteuerung und Verwaltung von xSeries- und IBM BladeCenter-Servern über Remotezugriff ermöglicht. IBM Director wird mit der Standardauflage von Virtualization Engine geliefert. Bei iSeries-Servern mit iSCSI-Anschluss ist dies nur der Hostteil von IBM Director, der auf der i5/OS-Partition ausgeführt wird, die den Hosting-Service für die Server mit iSCSI-Anschluss bereitstellt.

IBM i5/OS Integrated Server Support. Eine Erweiterung des Betriebssystems i5/OS, die auf der iSeries installiert wird und die Zusammenarbeit mit integrierten Windows- und Linux-Servern ermöglicht. Es gibt außerdem eine Komponente des Produkts, die auf dem integrierten Server ausgeführt wird.

| **ID des fernen Systems.** Seriennummer, Typ und Modell des xSeries-Servers oder des IBM BladeCenter-Servers. Bei einem xSeries-Standardserver haben Serviceprozessor und xSeries-Server eine gemeinsame ID. Bei einem IBM BladeCenter-Server kennzeichnet diese ID den Server innerhalb eines Gehäuses.

Integrierter Windows-Server. Wird auch als *integrierter Server* bezeichnet. Eine Instanz von Windows 2000 Server oder Windows Server 2003, die auf einem IXS, einem xSeries-Server mit IXA-Anschluss oder einem xSeries- oder IBM BladeCenter-Server mit iSCSI-HBA-Anschluss ausgeführt wird.

Integrierter xSeries-Server (IXS). Ein PC (Intel-basierter Computer) auf einer PCI-Erweiterungskarte, der in einem iSeries-Server installiert wird.

Integrierter xSeries-Adapter (IXA). Eine PCI-Erweiterungskarte, die in ausgewählten Modellen von IBM eServer xSeries-Servern installiert wird und eine HSL-Verbindung (HSL = High-Speed Link) zu einem iSeries-Server ermöglicht.

| **Internet Protocol Security (IPSec).** Verschlüsselt Datenverkehr auf dem iSCSI-Netzwerk.

| **IP Multicast.** Übertragung eines Internet Protocol (IP)-Datenpakets an eine Gruppe von Systemen, die zusammen eine einzelne Multicastgruppe bilden.

| **IPSec.** Siehe Internet Protocol Security.

| **IQN.** Siehe qualifizierter iSCSI-Name.

| **iSCSI.** Internet-SCSI. Kapselung des SCSI-Protokolls innerhalb von TCP/IP-Paketen. Bietet eine interoperable Lösung, die die vorhandene Infrastruktur und die Verwaltungsfunktionen des Internet nutzen und mehr Server über weitere Entfernungen verbinden kann.

| **iSCSI-Verbindung.** Eine iSCSI-Verbindung ist eine TCP-Verbindung. Die Kommunikation zwischen dem Initiator und dem Ziel findet über eine oder mehrere TCP-Verbindungen statt.

| **iSCSI-Initiator-Adapter.** Ein Hostbusadapter (HBA), der iSCSI-Anforderungen initiiert. iSCSI-Initiatoren geben SCSI-Befehle aus, um Services von Komponenten oder logischen Einheiten eines Servers anzufordern, der als **Ziel** bezeichnet wird. Der iSCSI-Initiator ist der iSCSI-HBA im xSeries- oder BladeCenter-Server.

| **iSCSI-Zieladapter.** Ein Hostbusadapter (HBA), der iSCSI-Initiatoranforderungen bedient. Ein iSCSI-Ziel dient als Speichercontroller, der die logischen Einheiten (LUNs) betreibt. Im Zusammenhang mit iSeries-Servern mit iSCSI-Anschluss ist das iSCSI-Ziel der iSCSI-HBA für iSeries.

Kerberos. Ein vom MIT erstelltes Sicherheitsprotokoll für Netzwerke. Es stellt Tools für die Authentifizierung und die strenge Verschlüsselung im Netzwerk bereit und verbessert den Schutz der Informationssysteme in Ihrem gesamten Unternehmen. iSeries Navigator verwendet eine über Kerberos authentifizierte Anmeldung. Die Benutzeradministration unterstützt die Umgebung für die Einzelanmeldung, indem die Definition von Kennwörtern für i5/OS-Benutzerprofile mit *NONE zugelassen wird und registrierte Windows-Benutzer ihre Kennwörter unter Windows festlegen können. Diese Unterstützung wird bereitgestellt, wenn das Attribut für ein registriertes Benutzerprofil mit LCLPWDMGT(*NO) angegeben wird.

| **Lokale Schnittstelle.** Die lokale Schnittstelle stellt die Konfigurationsparameter dar, die den iSCSI-Zieladapter beschreiben, der sich im iSeries-Server befindet.

| **MAC.** Siehe Media Access Control.

| **Managementmodul.** Ein mit zahlreichen Funktionen ausgestatteter Serviceprozessor für die Steuerung eines IBM BladeCenter-Chassis und die darin enthaltenen einzelnen Server.

| **Media Access Control (MAC).** In einem lokalen Netz das Protokoll, das bestimmt, welche Einheit zu einem bestimmten Zeitpunkt Zugriff auf das Übertragungsmedium erhält.

Microsoft Windows-Clusterdienst (MSCS). Ein Dienst von Microsoft Windows, der einzelne Server miteinander verbindet, damit diese gemeinsam Aufgaben ausführen können.

| **Netzwerkserverkonfiguration für Verbindungssicherheit.** Ein i5/OS-Konfigurationsobjekt, mit dem sicherheitsrelevante Werte konfiguriert werden, die steuern, wie die iSCSI-HBA- und Virtual Ethernet-LAN-Daten auf dem Netzwerk geschützt werden. Der entsprechende i5/OS-Objektyp ist *NWSCFG mit dem Subtyp *CNNSEC. Dieses Objekt wird auch als **Verbindungssicherheitskonfiguration** bezeichnet.

| **NWS-Konfiguration (NWSCFG).** Ein i5/OS-Konfigurationsobjekt, das Attribute beschreibt, die für einen fernen integrierten Server mit iSCSI-Anschluss verwendet werden. Zu diesen Attributen gehören das ferne System (*RMTSYS), der Serviceprozessor auf dem fernen System (*SRVPRC) und die Konfigurationssicherheitswerte, die für die Kommunikation mit dem Server verwendet werden (*CNNSEC). Der entsprechende i5/OS-Objektyp ist *NWSCFG.

NWS-Beschreibung (NWSD). Ein i5/OS-Konfigurationsobjekt, das einen integrierten Server beschreibt. Der entsprechende i5/OS-Objektyp ist *NWSD.

| **NWS-Hostadapter (NWSH).** Ein NWS-Hostadapter (NWSH) ist ein i5/OS-Konfigurationsobjekt, mit dem die iSCSI-HBA-Einheit im iSeries-Server konfiguriert wird. Der entsprechende i5/OS-Einheitentyp ist *NWSH.

| **NWS-Speicherbereich (NWSSTG).** i5/OS-Plattenspeicher, der einem integrierten Server zugeordnet ist.

| **NWSH.** Siehe NWS-Hostadapter (NWSH).

| **NWS-Konfiguration des fernen Systems.** Ein i5/OS-Konfigurationsobjekt, mit dem spezielle Attribute für einen bestimmten fernen xSeries- oder IBM BladeCenter-Server konfiguriert werden. Dazu gehören Informationen, die für die Identifikation und das Booten des fernen Systems erforderlich sind, sowie Informationen über die von dem fernen System verwendeten iSCSI-Initiatoradapter. Der entsprechende i5/OS-Objektyp ist *NWSCFG mit dem Subtyp *RMTSYS. Dieses Objekt wird auch als **Konfiguration des fernen Systems** bezeichnet.

| **NWS-Konfiguration des Serviceprozessors.** Ein i5/OS-Konfigurationsobjekt, das die Parameter beinhaltet, die sich auf den Serviceprozessor auf dem fernen System beziehen. Bei IBM BladeCenter-Servern ist dies das IBM BladeCenter-Gehäuse. Der entsprechende i5/OS-Objektyp ist *NWSCFG mit dem Subtyp SRVPRC. Dieses Objekt wird auch als **Serviceprozessorkonfiguration** bezeichnet.

| **Qualifizierter iSCSI-Name (IQN).** Ein eindeutiger Name, der einen iSCSI-Zieladapter oder einen iSCSI-Initiatoradapter nach iSCSI-Standard (RFC 3722) identifiziert.

| **Remote Supervisor Adapter (RSA).** Ein mit zahlreichen Funktionen ausgestatteter Serviceprozessor, der zur Steuerung von xSeries-Systemen dient.

| **Serviceprozessor.** Ein von der Haupt-CPU des Systems unabhängiger Prozessor. Der Serviceprozessor wird für die Leistungssteuerung sowie weiterer Verwaltungs- und Diagnosefunktionen des Systems verwendet. Für integrierte xSeries- und IBM BladeCenter-Systeme stehen mehrere verschiedene Typen von Serviceprozessoren zur Verfügung. Siehe **Remote Supervisor Adapter (RSA)**, **Baseboard Management Controller (BMC)** und **Managementmodul**.

| **Speicherpfad.** Der Speicherpfad definiert, welcher NWS-Hostadapter (NWSH) von den Speicherbereichen benutzt werden kann, sowie die IP-Sicherheitsregel für den Datenverkehr.

| **Unicast.** Die Übertragung von Daten an eine einzige Zieladresse.

| **Virtual Ethernet-Punkt-zu-Punkt (Virtual Ethernet-PTP).** Ein Virtual Ethernet-Netzwerk, das zwischen einer iSeries und einem integrierten Windows-Server während dessen Installation konfiguriert wird. Es handelt sich hierbei um die Verbindung, die für die Übertragung zwischen der iSeries und dem integrierten Server verwendet wird.

| **Virtuelles Netzwerk.** Ein Ethernet-Netzwerk, das auf der iSeries emuliert wird, damit Netzwerke zwischen logischen i5/OS-Partitionen, logischen Linux-Partitionen und integrierten Windows-Servern erstellt werden können.

| **Volume Shadow Copy Service (VSS) von Windows Server 2003.** Eine Unterstützung, die ermöglicht, dass Anwendungsdaten ohne Beenden der Anwendung gesichert werden können. Dieser Service verbessert die Anwendungsverfügbarkeit.

| **Windows-Server.** Microsoft Windows 2000 Server oder Windows Server 2003


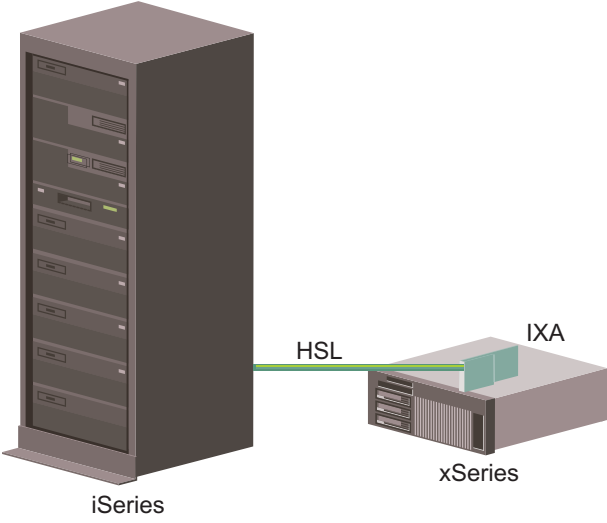
| **Zertifikat.** Ein Standardformat für die Kombination einer Identität mit einem öffentlichen Schlüssel, das von einer Zertifizierungsstelle signiert wird, und innerhalb eines bestimmten Zeitraums (Startdatum/-uhrzeit bis Enddatum/-uhrzeit) gültig ist. Die Identität (auch: das "Subjekt") des Zertifikats besagt, für wen oder was das Zertifikat ausgestellt wurde. Für die Identität gibt es vielfältige Syntaxmöglichkeiten, doch normalerweise besteht sie aus einem eindeutigen Namen mit Attributen wie "CN=common name (allgemeiner Name), O=organization (Unternehmen), OU=organizational unit (Organisationseinheit). Der öffentliche Schlüssel ist Bestandteil eines Schlüsselpaars (privater/öffentlicher Schlüssel), das in der Regel für das Public-Key-Kryptosystem RSA erstellt wurde. Im Gegensatz dazu ist der zugehörige private Schlüssel nicht Bestandteil des Zertifikats und nicht zur Anzeige bestimmt.

| **Zertifizierungsstelle.** Ein Paar aus privatem Schlüssel und Zertifikat, das wiederum andere Zertifikate zu Authentifizierungszwecken (z. B. feststellen, ob ein Zertifikat wirklich von demjenigen stammt, der es für sich beansprucht) unterzeichnen kann. Eine Zertifizierungsstelle kann entweder ein Drittunternehmen sein, das Identitätsinformationen prüft und signierte digitale Zertifikate ausstellt, oder es kann sich um eine lokale, nicht öffentliche Stelle handeln. Sobald ein Zertifikat digital signiert wurde, kann es von niemandem mehr unerkannt geändert werden.

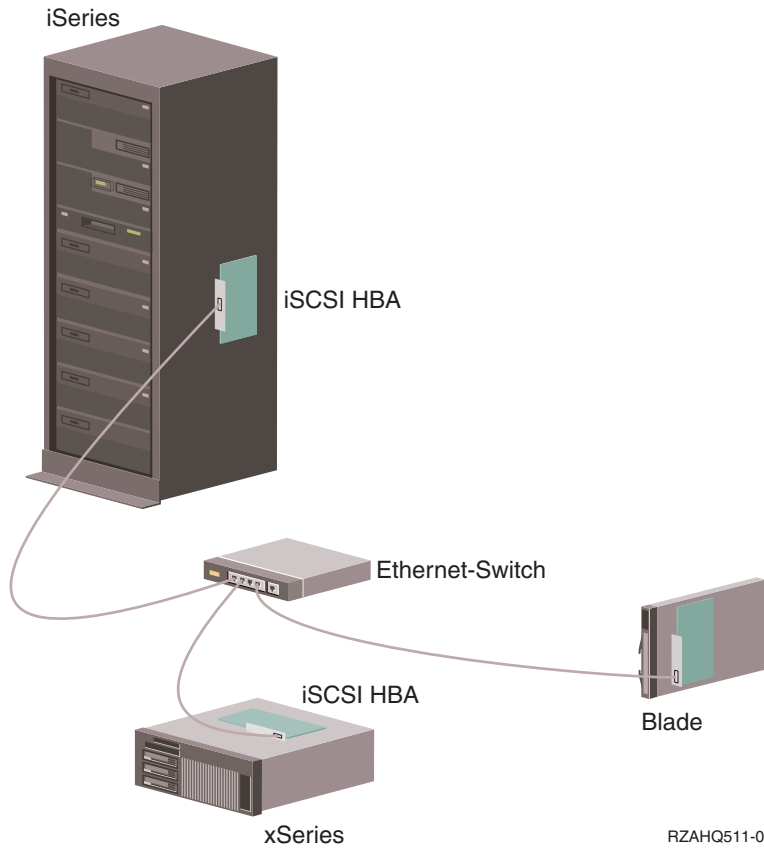
| **Zielknoten.** Ein iSeries-iSCSI-Firmwareobjekt, das die iSCSI-Sitzung und -Verbindung verwaltet.

Hardwarekonzepte

iSeries-Server unterstützen mehrere Hardwarekonfigurationen zur Integration von IBM xSeries- oder BladeCenter-Servern. Die folgende Tabelle erläutert die wesentlichen Unterschiede zwischen einem integrierten xSeries-Server (IXS), einem xSeries-Server, der über einen integrierten xSeries-Adapter (IXA) angeschlossen ist, und einem über iSCSI-angeschlossenen Server.

Vergleich zwischen IXS und xSeries-Servern mit IXA- und iSCSI-HBA-Anschluss.	
 <p>The diagram shows a tall iSeries server rack. Inside the rack, a smaller server unit labeled 'IXS' is installed. The iSeries server is labeled 'iSeries' at the bottom, and the IXS unit is labeled 'IXS' to its right. The reference code 'RZAHQ019-1' is located at the bottom right of the diagram area.</p>	<p>Ein IXS ist ein PC-Server ohne Festplatte, aber mit Prozessor und Speicher, der in einem iSeries-Server installiert ist.</p>
 <p>The diagram shows an iSeries server rack on the left and a separate xSeries server unit on the right. A green line labeled 'HSL' connects the two. The xSeries unit has a smaller server unit labeled 'IXA' attached to its top. The iSeries server is labeled 'iSeries' at the bottom, and the xSeries unit is labeled 'xSeries' below it. The reference code 'RZAHQ020-1' is located at the bottom right of the diagram area.</p>	<p>Ein IXA ist ein HSL-Busadapter (HSL = High-Speed Link), der in einen unterstützten xSeries-Server integriert ist. Der xSeries-Server erscheint als eine Erweiterungseinheit für den iSeries-Server, die über HSL angeschlossen ist.</p>

Vergleich zwischen IXS und xSeries-Servern mit IXA- und iSCSI-HBA-Anschluss.

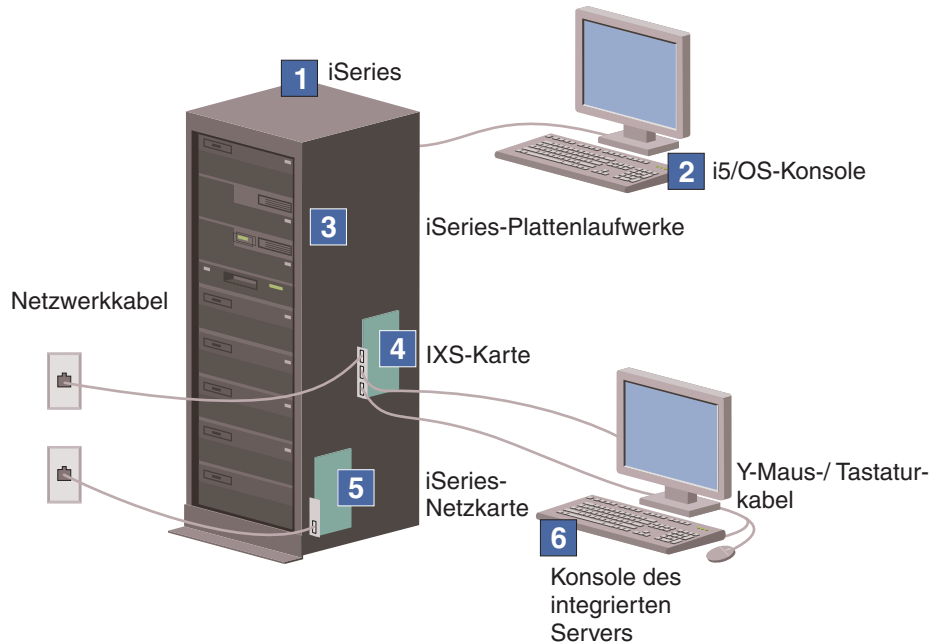


Die iSCSI-Technologie verbindet sowohl xSeries-Server ohne Festplatte als auch IBM BladeCenter-Server mit iSeries-Systemen unter Verwendung kostengünstiger skalierbarer Ethernet-Netzwerke. Im iSeries-Server sowie in jedem teilnehmenden xSeries-Server und jedem teilnehmenden IBM BladeCenter-Server sind iSCSI-Hostbusadapter (HBAs) enthalten.

IXS und Server mit IXA-Anschluss

| Typische IXS-Serverinstallation

| Die folgende Abbildung veranschaulicht eine typische IXS-Installation.



RZAHQ025-0

Abbildung 2. Typische IXS-Installation

1. Sie benötigen einen kompatiblen iSeries-Server. (Informationen zur Kompatibilität finden Sie unter „Hardwarevoraussetzungen“ auf Seite 62.)
2. Die i5/OS-Konsole, von der aus die Verbindung zum iSeries-Server über iSeries Navigator oder die zeichenorientierte Schnittstelle hergestellt wird, ist dargestellt, um die Unterscheidung zwischen dieser Konsole und der Konsole des integrierten Servers zu verdeutlichen.
3. Ein integrierter Server hat kein eigenes Festplattenlaufwerk. i5/OS emuliert Plattenspeicherplatz aus den iSeries-Festplattenlaufwerken für die Verwendung durch den integrierten Server.
4. Die IXS-Karte ist ein Intel-Prozessor mit eigenem Arbeitsspeicher, der auf einer PCI-Platine montiert und in einen iSeries-Erweiterungssteckplatz integriert ist. Physisch gesehen belegt der IXS zwei Steckplätze.
5. Ein normaler iSeries-Server ist mit einer Netzwerkkarte ausgestattet.
6. Eine integrierte Serverkonsole ermöglicht Ihnen das Arbeiten mit dem integrierten Server. Eine integrierte Serverkonsole kann aus einem Monitor, einer Tastatur und einer Maus bestehen, die direkt an die IXS-Karte angeschlossen sind. Weitere Informationen zu diesem und anderen Typen von integrierten Serverkonsolen finden Sie unter „Windows-Konsole“ auf Seite 24.

Anmerkung: Abhängig vom verwendeten IXS-Typ gibt es unterschiedliche Möglichkeiten zur Herstellung der Netzwerkkonnektivität. Bestimmte IXS-Typen können benachbarte PCI-Steckplätze übernehmen, wodurch der IXS eine iSeries-Netzwerkkarte steuern kann. (Weitere Informationen zu den unterstützten Netzwerkkarten befinden sich unter „Hardwarevoraussetzungen“ auf Seite 62.) Auf diese Weise können bis zu drei Netzwerkkarten installiert werden. Andere IXS-Typen verfügen über integrierte Netzwerkcontroller und bieten keine Unterstützung für Netzwerkkarten in benachbarten Steckplätzen.

| Typische Installation eines Servers mit IXA-Anschluss

Integrierte Server mit IXA-Anschluss sind Standardmodelle des xSeries-Servers, die Prozessoren, Hauptspeicher und Erweiterungskarten, jedoch keine Festplatten enthalten. Der gesamte Plattenspeicherplatz befindet sich im iSeries-Server und wird auf dieselbe Weise wie bei IXS-Modellen verwaltet.

Das Installationsverfahren für einen über IXA angeschlossenen integrierten Windows-Server ist quasi mit der Installationsprozedur für einen integrierten IXS-Server identisch. Der Hauptunterschied besteht darin, dass es häufiger neue Releases für xSeries-Server gibt als für integrierte xSeries-Server (IXS) und aktualisierte Funktionen schneller verfügbar sind. Außerdem verfügen über IXA angeschlossene xSeries-Server über eigene Erweiterungssteckplätze, so dass eine weitaus größere Erweiterbarkeit als bei IXS-Modellen gegeben ist.

| Die folgende Abbildung veranschaulicht eine typische Installation eines Servers mit IXA-Anschluss.

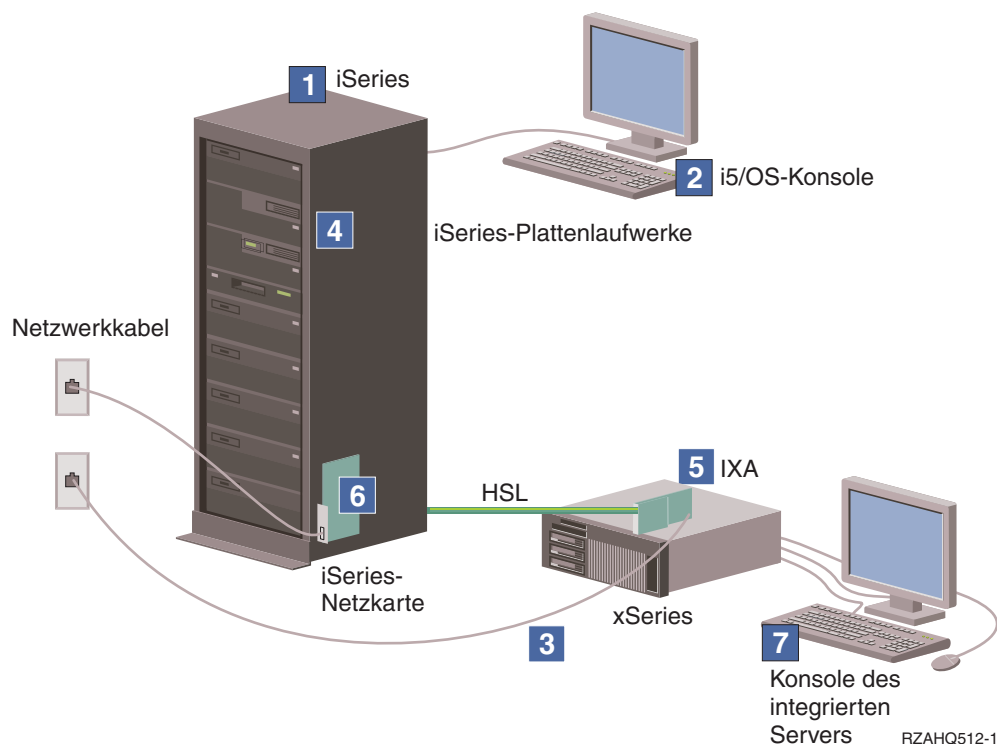


Abbildung 3. Typische Installation eines Servers mit IXA-Anschluss

1. Sie benötigen einen kompatiblen iSeries-Server. (Informationen zur Kompatibilität finden Sie unter „Hardwarevoraussetzungen“ auf Seite 62.)
2. Die i5/OS-Konsole, von der aus die Verbindung zum iSeries-Server über iSeries Navigator oder die zeichenorientierte Schnittstelle hergestellt wird, ist dargestellt, um den Unterschied zwischen dieser Konsole und der Windows-Konsole zu verdeutlichen.
3. Ein normaler xSeries-Server verfügt über mindestens einen integrierten Netzcontroller. Den meisten xSeries-Servern können zwecks Verbesserung der Netzkonnektivität weitere Netzwerkkarten hinzugefügt werden. Informationen über die Kompatibilität der xSeries-Netz Karten finden Sie auf der Website Integrated xSeries solutions.
4. Ein über IXA angeschlossener xSeries-Server hat kein eigenes Festplattenlaufwerk. i5/OS emuliert Plattenspeicherplatz aus den iSeries-Festplattenlaufwerken für die Verwendung durch den integrierten Server.

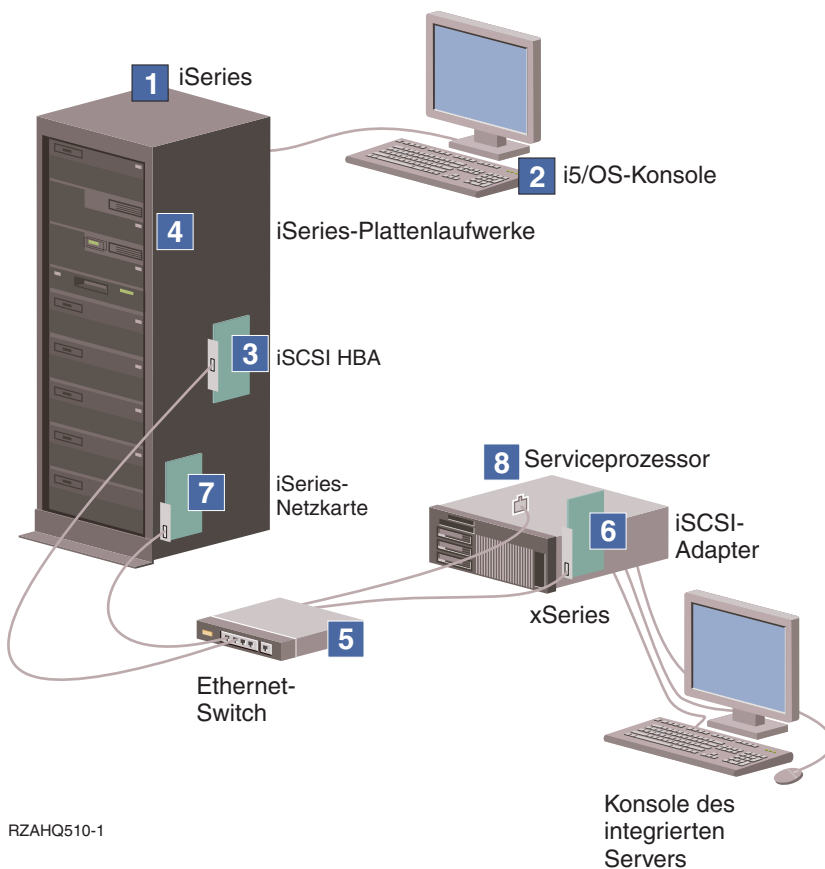
- | 5. Die IXA-Karte wird in einen bestimmten Steckplatz auf dem xSeries-Server integriert und über HSL-Kabel an die iSeries angeschlossen.
- | 6. Ein normaler iSeries-Server ist mit einer Netzwerkkarte ausgestattet.
- | 7. Eine integrierte Serverkonsole ermöglicht Ihnen das Arbeiten mit der über IXA angeschlossenen xSeries. Eine integrierte Serverkonsole kann aus einem Monitor, einer Tastatur und einer Maus bestehen, die direkt an den xSeries-Server angeschlossen sind. Weitere Informationen zu diesem und anderen Typen von integrierten Serverkonsolen finden Sie unter „Windows-Konsole“ auf Seite 24.

| Server mit iSCSI-Anschluss

| **Typische Installation eines über iSCSI angeschlossenen IBM xSeries-Servers oder eines BladeCenter-Servers.**


| Server mit iSCSI-Anschluss sind Standardmodelle des xSeries- oder IBM BladeCenter-Servers, die Prozessoren, Hauptspeicher und Erweiterungskarten, jedoch keine Festplatten enthalten. Der gesamte Plattenspeicherplatz befindet sich im iSeries-Server und wird auf dieselbe Weise wie bei IXS- und IXA-Modellen verwaltet. Für das Installationsverfahren eines über iSCSI angeschlossenen integrierten Windows-Servers muss entsprechende Hardware in der iSeries und den xSeries- oder IBM BladeCenter-Servern installiert und konfiguriert sein. Ebenso wie das IXA-Modell, verfügen auch die über iSCSI-HBA angeschlossenen xSeries-Server über eigene Erweiterungssteckplätze, so dass Erweiterungen installiert werden können, mit denen die Funktionalität des Servers vergrößert werden kann.

| Die folgende Abbildung veranschaulicht eine typische iSCSI-HBA-Installation:



| *Abbildung 4. Typische Installation eines Servers oder eines IBM BladeCenter-Servers mit iSCSI-Anschluss*

1. Sie benötigen eine kompatible iSeries. Weitere Informationen finden Sie unter „Hardwarevoraussetzungen“ auf Seite 62.
2. Die i5/OS-Konsole, von der aus die Verbindung zum iSeries-Server über iSeries Navigator oder die zeichenorientierte Schnittstelle hergestellt wird, ist dargestellt, um dem Unterschied zwischen dieser Konsole und der Windows-Konsole zu verdeutlichen.
3. Je nach physischem Netzwerk stehen Kupfer- oder Glasfaser-iSCSI-HBAs zur Verfügung. Dieser iSCSI-Adapter dient als Zieleinheit und ist über Ethernet-Standardkabel mit einem Ethernet-Netzwerk verbunden.
4. Ein integrierter Server hat kein eigenes Festplattenlaufwerk. i5/OS emuliert Plattenspeicherplatz aus den iSeries-Festplattenlaufwerken für die Verwendung durch den integrierten Server. Der Zugriff auf diese Laufwerke und andere iSeries-Speichereinheiten erfolgt über den iSCSI-HBA.
5. Die iSCSI-HBA-Netzübertragungskabel sind mit einem Standard-Gigabit-Ethernet-Switch verbunden.
6. Es ist ein weiterer iSCSI-HBA im xSeries-Server erforderlich. Dieser Adapter stellt die Verbindung zum iSCSI-HBA für iSeries zur Verfügung. Dieser Adapter kann vom xSeries-Server aus als der Speicheradapter betrachtet werden, auf dem die Platten innerhalb des Netzwerks zu finden sind.
7. Ein normaler iSeries-Server ist mit einer Netzwerkkarte ausgestattet. IBM Director benötigt eine iSeries-LAN-Verbindung, um die fernen xSeries- oder IBM BladeCenter-Server zu erkennen und zu verwalten.
8. Ein Serviceprozessor ermöglicht dem iSeries-Server das Erkennen und Verwalten des fernen Systems. Der Serviceprozessor kann ein RSA II (Remote Supervisor Adapter), ein BMC (Baseboard Management Controller) oder ein Managementmodul eines IBM BladeCenter sein. RSA II, BMC oder Managementmodul sind über ein Ethernet-Netzwerk mit dem iSeries-Server verbunden.

Zusätzliche Informationen zur Hardware finden Sie auf der Website IBM iSeries Integrated xSeries solutions  [.\(www.ibm.com/servers/eserver/series/integratedxseries\)](http://www.ibm.com/servers/eserver/series/integratedxseries)

Server mit iSCSI-Anschluss - Übersicht

Ein iSCSI-Basisnetzwerk besteht aus einem iSCSI-Ziel (ein in einem iSeries-Server installierter iSCSI-HBA) und einem iSCSI-Initiator (ein in einem xSeries- oder IBM BladeCenter-Server installierter iSCSI-HBA). Ziel- und Initiatoreinheit sind über ein Ethernet-LAN miteinander verbunden. Der iSCSI-HBA für iSeries stellt die Speicher- und austauschbaren Datenträgereinheiten für den iSCSI-Initiator zur Verfügung. Abb. 5 zeigt ein iSCSI-Basisnetzwerk.



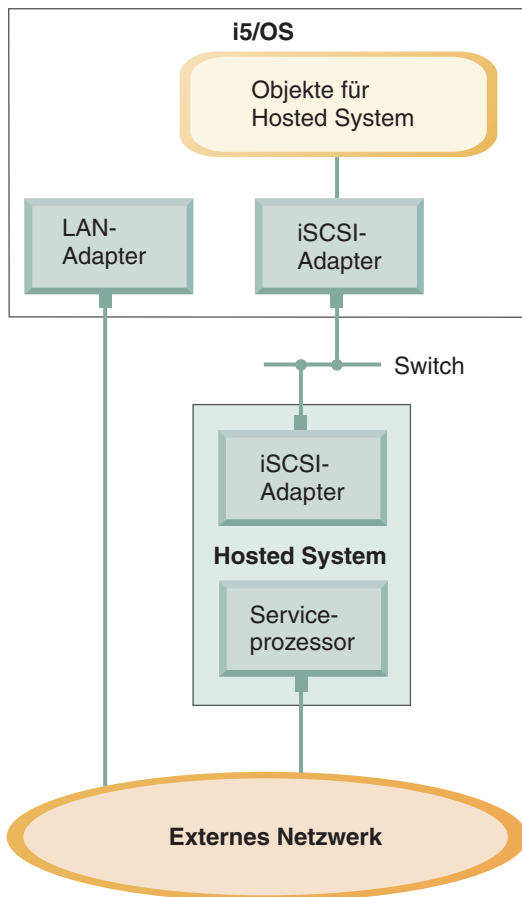
RZAHQ509-0

Abbildung 5. Grundlegende iSCSI-Konzepte

Sowohl das iSCSI-Ziel als auch der Initiator müssen mit Befehlen konfiguriert werden, die auf dem iSeries-Server abgesetzt werden. Das iSCSI-Netzwerk wird ausschließlich für iSCSI-HBA-Datenverkehr benutzt.

Basisunterstützung für Einzelserver

Um einen xSeries- oder IBM BladeCenter-Server via iSCSI an eine iSeries anzuschließen oder zu betreiben, muss sowohl in der iSeries als auch im Hosted System entsprechende Hardware vorhanden sein. Bei der auf jeder Seite erforderlichen Hardware handelt es sich um einen iSCSI-Hostbusadapter (HBA) oder iSCSI-Adapter. Beide Adapter sind über Ethernet-Switch und Ethernet-Standardkabel verbunden. Die einfachste Form der physischen Verbindung zwischen einem Hosted System und einem iSeries-Server wird in Abb. 6 auf Seite 20 dargestellt.



RZAHQ501-1

Abbildung 6. Einzelserver mit iSCSI-Anschluss

Im dem als Hosted System dienenden xSeries- oder IBM BladeCenter-Server ist ein iSCSI-HBA-Initiator installiert. Dieser Adapter verfügt über eine Ethernet-Netzwerkschnittstelle und ist über einen Ethernet-Switch mit dem iSCSI-Ziel-HBA im iSeries-Server verbunden. Das Hosted System ist ein Server ohne Plattenspeicher. Die virtuellen Platten und austauschbaren Datenträgereinheiten werden vom iSCSI-HBA für iSeries betrieben oder bereitgestellt. Die SCSI-Befehle für den Zugriff auf diese Einheiten sind in TCP/IP-Frames gepackt und werden über das Ethernet-Netzwerk vom Hosted System an den iSCSI-HBA für iSeries weitergeleitet. Dieser Übertragungsmodus wird als Internet-SCSI oder iSCSI bezeichnet.

Die über iSCSI angeschlossenen Server werden in i5/OS-Objekten definiert. Weitere Informationen zu diesen Objekten finden Sie unter „Softwarekonzepte“ auf Seite 38.

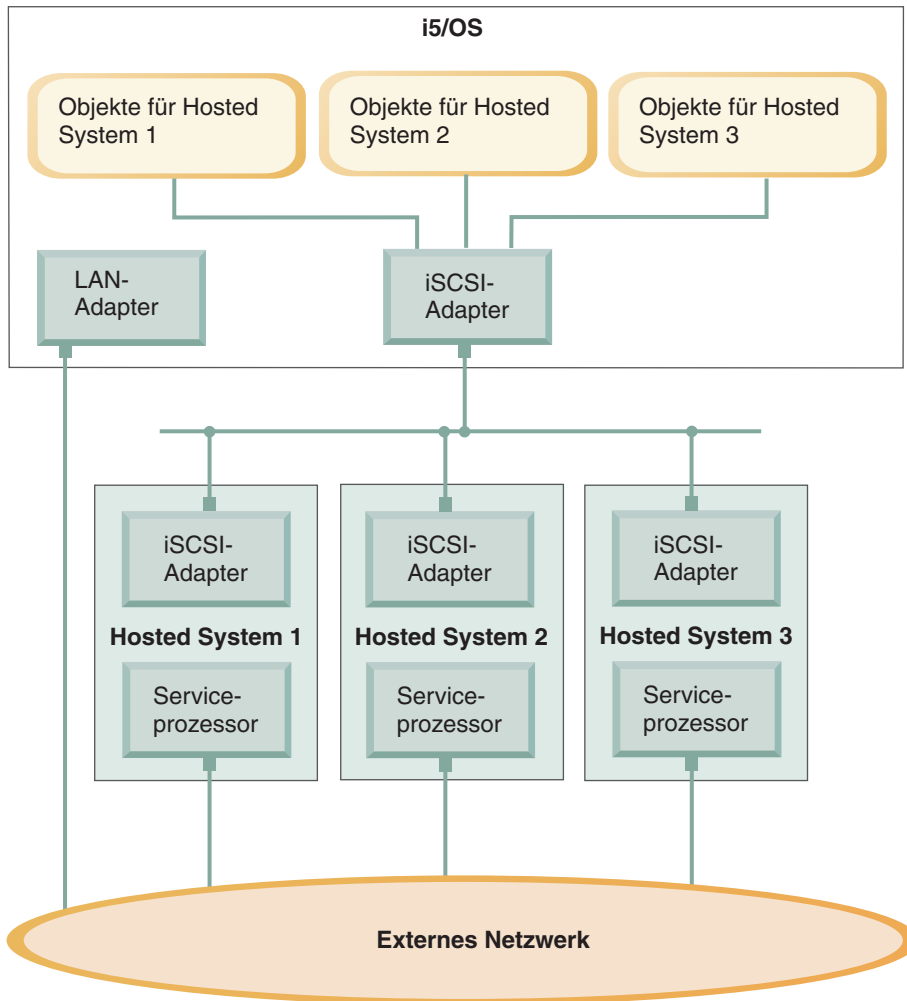
i5/OS kann ferne Systeme lokalisieren und verwalten, indem es über ein Ethernet-Netzwerk Befehle an den Serviceprozessor des fernen Systems sendet. Für diese Funktionen wird IBM Director verwendet, der auf allen Partitionen installiert und aktiv sein muss, die mit den über iSCSI angeschlossenen HBAs verbunden sind. Weitere Informationen finden Sie unter „Fernes Server erkennen und verwalten“ auf Seite 150.

In Abb. 6 sind zwei unterschiedliche Netzwerke dargestellt. Das iSCSI-Netzwerk verwendet einen isolierten Switch. Die Serviceprozessorverbindung verwendet ein externes Netzwerk (gemeinsam genutztes Netzwerk). Es müssen nicht unbedingt zwei unterschiedliche Netzwerke vorhanden sein. Die Serviceprozessorverbindung könnte beispielsweise auch den gleichen isolierten Switch wie das iSCSI-Netzwerk benutzen. Dies ist eine Möglichkeit zum Schutz der Serviceprozessorverbindung. Der i5/OS-LAN-Adapter stünde in diesem Fall jedoch den anderen Anwendungen auf dem externen Netzwerk nicht zur Verfügung.

| Beide Netzwerke sind zu schützen. Weitere Informationen über die Sicherheit von Servern mit iSCSI-Anschluss finden Sie unter „Sicherheitskonzepte“ auf Seite 51.

| **Unterstützung für mehrere Server**

| Ein einziger iSCSI-HBA für iSeries kann Hosting-Service für mehrere xSeries- oder IBM BladeCenter-Server bereitstellen. Dieses Konzept wird in Abb. 7 dargestellt.



RZAHQ502-3

| *Abbildung 7. Mehrere Server mit iSCSI-Anschluss*

| Für jedes Hosted System muss mindestens ein iSCSI-HBA im Server installiert sein. Jeder iSCSI-HBA im Hosted System ist über ein Ethernet-Netzwerk mit dem iSCSI-HBA für iSeries verbunden. Dieses Netzwerk kann ein physisch sicheres oder isoliertes Netzwerk sein, wenn ein physisch sicheres Modell implementiert wird. In i5/OS wird jedes der Hosted oder fernen Systeme durch eine Gruppe von Objekten dargestellt. Eine detaillierte Beschreibung dieser Objekte finden Sie unter „Softwarekonzepte“ auf Seite 38.

| Jedes Hosted System muss über einen installierten Serviceprozessor für die ferne Erkennung und das Energiemanagement verfügen. Mehrere Serviceprozessoren können über ein externes Netzwerk an einen einzigen iSeries-LAN-Adapter angeschlossen werden.

Erweiterte iSCSI-Unterstützung

Ein einziger iSCSI-HBA für iSeries kann mehrere Server oder Hosted Systeme unterstützen. Jedes Hosted System kann außerdem an mehrere iSCSI-HBAs für iSeries angeschlossen werden. Abb. 8 zeigt ein Hosted System, das an mehrere iSCSI-HBAs für iSeries angeschlossen ist.

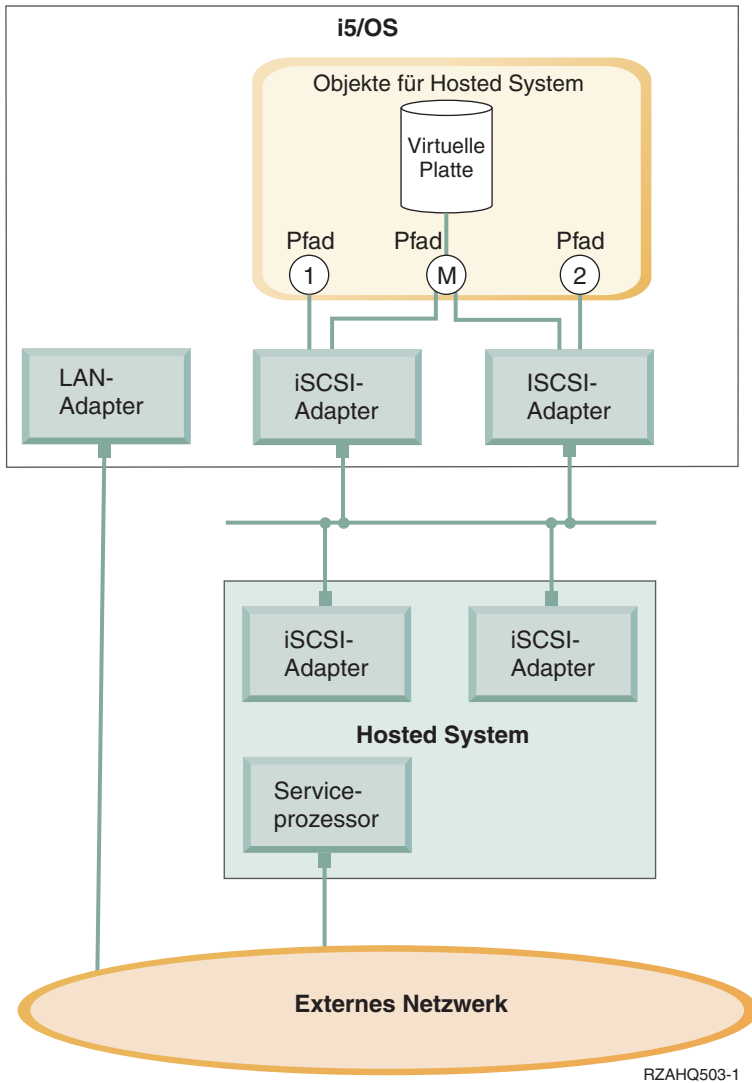


Abbildung 8. Erweiterte Konfiguration

Abb. 8 zeigt mehrere iSCSI-HBAs, die im Hosted System installiert sind.

Pfaddefinition

Wenn ein Hosted System mit einem iSCSI-HBA für iSeries verbunden wird, wird zwischen dem Hosted System und dem iSCSI-HBA für iSeries ein Pfad definiert.

In Abb. 8 sind mehrere unterschiedliche Pfade mit der Bezeichnung 1, 2 und M definiert.

Eine virtuelle Einheit, für die Hosting-Service in einem iSeries-Server bereitgestellt wird, benutzt einen Pfad. Eine konfigurierte virtuelle Platte (z. B. Laufwerk C:), die in i5/OS von einem iSCSI-HBA für iSeries oder NWSH-Adapter betrieben wird, befindet sich hinter diesem NWSH-Adapter.

In Abb. 8 sind die Pfade 1 und 2 jeweils für einen separaten iSCSI-HBA für iSeries definiert. Einheiten, die in Pfad 1 definiert sind, können sich nur hinter dem iSCSI-Adapter befinden, für den der Pfad definiert ist.

l niert ist. Ebenso können sich Einheiten, die in Pfad 2 definiert sind, nur hinter dem iSCSI-Adapter befinden, für den der Pfad definiert ist. Alle Einheiten, die für Pfad 1 oder 2 definiert sind, befinden sich ausschließlich hinter ihrem jeweiligen iSCSI-HBA.

l **Einführung in Multipath-Architektur**

l Ein Hosted System kann über redundante Pfade für den Zugriff auf virtuelle Platten verfügen, die von i5/OS betrieben werden. Bei der umfassendsten Lösung befinden sich redundante Pfade auf beiden Seiten. Der Zugriff auf eine bestimmte virtuelle Platte durch ein Hosted System kann über einen der beiden iSCSI-HBAs erfolgen, die im Hosted System installiert sind; in der iSeries kann die virtuelle Platte mittels eines der beiden iSCSI-HBAs für iSeries gefunden werden. Dies wird als Multipath-Architektur bezeichnet.

l In Abb. 8 auf Seite 22 ist der Mehrfachpfad (Multipath) als M definiert. Der Zugriff auf die virtuellen Platten, die den Mehrfachpfad benutzen, kann über einen der iSCSI-HBAs erfolgen, die im iSeries-Server installiert sind. Ein Mehrfachpfad ist als Gruppe von iSCSI-HBAs für iSeries definiert, die auf Pfad M zugreifen oder diesen benutzen können. Pro Hosted System kann nur eine Mehrfachpfadgruppe definiert werden. Dieser Gruppe können mehrere iSCSI-HBAs für iSeries angehören.

l **Anmerkung:** Austauschbare Datenträgereinheiten können nicht in einer Mehrfachpfadgruppe definiert werden.

l **Dedizierte Bandbreite**

l Gelegentlich sind keine redundanten Pfade erwünscht oder erforderlich, aber für virtuelle Platten, die höhere Leistungswerte erfordern, wird ein dedizierter Pfad benötigt.


l In Abb. 8 auf Seite 22 kann die Konfiguration eines Hosted Systems eine virtuelle Platte definieren, die Pfad 1 oder 2 statt Pfad M benutzt. Auf diese Weise kann die Bandbreite eines iSCSI-Adapters bestimmten virtuellen Platten zugeordnet werden.

l **Booten über iSCSI ohne Plattenspeicher**

l Alle über iSCSI angeschlossenen Standalone- oder IBM BladeCenter-Server sind Systeme ohne Plattenspeicher, die als Booteinheit einen xSeries- oder IBM BladeCenter-iSCSI-HBA benötigen.

l Bevor Sie einen neuen integrierten Windows-Server installieren oder benutzen können, muss sowohl das ferne i5/OS-System als auch der iSCSI-HBA des fernen Servers konfiguriert werden. Weitere Informationen finden Sie unter „Konfiguration des fernen Systems“ auf Seite 45.

l Der iSCSI-HBA muss während des Bootvorgangs der xSeries oder des IBM BladeCenter mit dem mit STRG-Q aufgerufenen Dienstprogramm konfiguriert werden. Es wird empfohlen, diese Konfiguration als Bestandteil der erstmaligen Serverkonfiguration durchzuführen. Im iSCSI-HBA des Hosted Servers muss eine Mindestanzahl von Parametern konfiguriert werden. Diese Parameter müssen mit denen abgeglichen werden, die im Konfigurationsobjekt des fernen Systems enthalten sind. Die Parameter richten sich nach dem ausgewählten Bootmodus.

l Nähere Informationen über die Konfiguration des iSCSI-HBA im Hosted System als iSCSI-Booteinheit finden Sie auf der Webseite [iSCSI install read me first](#) . Weitere Informationen über die Konfiguration der Parameter im Konfigurationsobjekt des fernen Systems finden Sie unter „Konfigurationseigenschaften des fernen Systems ändern“ auf Seite 132.

l **Booteinheit des Hosted Server aktivieren**

l Basierend auf den konfigurierten Parametern fungiert der in einer xSeries oder einem IBM BladeCenter installierte iSCSI-HBA während des Bootvorgangs als Booteinheit.

| Wenn die xSeries nur über einen iSCSI-HBA verfügt, muss dieser als Booteinheit konfiguriert werden.
| Das Booten über iSCSI wird zwar standardmäßig auf allen iSCSI-HBAs aktiviert, aber Sie müssen noch
| weitere Informationen konfigurieren.

| Wenn im xSeries-Server mehrere iSCSI-HBAs installiert sind, muss nur einer dieser Adapter als Boot-
| einheit konfiguriert werden.

| Bei dem iSCSI-HBA des IBM BladeCenter-Servers handelt es sich um einen Adapter mit zwei Ports. Nur
| einer der Ports muss als Booteinheit konfiguriert werden.

| **Bootmodi und -parameter**

| Die iSCSI-Lösung der iSeries unterstützt verschiedene Bootmodi. Je nach ausgewähltem Modus müssen
| unterschiedliche Bootparameter im iSCSI-HBA des Hosted Systems konfiguriert werden.

| Die Konfiguration erfolgt mit Hilfe des mit STRG-Q aufgerufenen Adapterdienstprogramms. Bei der erst-
| maligen Implementierung eines Servers muss eine Booteinheit ausgewählt und konfiguriert werden. Es
| wird empfohlen, die erforderlichen Parameter im Rahmen dieser Erstkonfiguration zu konfigurieren.

| **Integrierter DHCP-Server**

| Der Server mit iSCSI-Anschluss verwendet einen integrierten DHCP-Server, wenn die Konfiguration den
| Standard- oder DHCP-Bootmodus vorsieht. Dieser integrierte DHCP-Server ist kein Universalserver, son-
| dern ausschließlich für die Implementierung von Bootparametern für den iSCSI-HBA des Hosted Servers
| vorgesehen. Der Server wird automatisch mit den Parametern konfiguriert, die in der Konfiguration des
| fernen Systems zur Verfügung gestellt werden, wenn eine NWS (NWS-Beschreibung) angehängt wird.
| Weitere Informationen finden Sie unter „Integrierter DHCP-Server“ auf Seite 149.

Windows-Konsole

Die Interaktion mit dem integrierten Server erfolgt über die Windows-Konsole. Abhängig von den
Konfigurationseinstellungen Ihrer Hard- und Softwareeinheiten können Sie einen Monitor, eine Tastatur
und eine Maus verwenden, die mit Hilfe einer der folgenden Methoden angeschlossen wurden:

| **Direktanschluss von Monitor, Tastatur und Maus**

| Sie können einen Monitor, eine Tastatur und eine Maus verwenden, die direkt an die IXS-Karte,
| einen xSeries-Server mit IXA-Anschluss, einen xSeries- oder einen BladeCenter-Server mit iSCSI-
| Anschluss angeschlossen sind. Diese Einheiten bilden zusammen die Konsole des integrierten Ser-
| vers. Der Benutzer kann über diese Einheiten mit dem integrierten Server genauso interagieren
| wie mit einem herkömmlichen Personal Computer (PC).

| Für Server mit iSCSI-Anschluss sind vor der Installation einige Hardwarekonfigurationen vorzu-
| nehmen. Diese Konfigurationen erfolgen mit Hilfe des direkt angeschlossenen Monitors, der Tas-
| tatur und der Maus.

GUI-Desktopanwendung mit Remotezugriff

| Sie können eine Anwendung wie z. B. Microsoft Terminal Services, Remote Desktop oder die
| Anwendung eines anderen Anbieters verwenden, um die grafische Benutzeroberfläche (GUI) des
| Server-Desktops auf einer fernen Workstation anzuzeigen. Die Mehrzahl der Verwaltungsauf-
| gaben, die normalerweise auf der direkt angeschlossenen Konsole des Servers ausgeführt werden,
| können auch über das ferne Desktop ausgeführt werden. Informationen zur Konfiguration und
| Verwendung eines fernen Desktops für die Serverkonsole finden Sie in der Dokumentation zu
| Microsoft Terminal Services oder in der Dokumentation der benutzten Anwendung eines anderen
| Anbieters.

Virtuelle serielle Konsole

i5/OS bietet die Möglichkeit zum Anschluss einer virtuellen seriellen Konsole für einen IXS des
Typs 4812. Diese Funktion entspricht der i5/OS-Unterstützungsfunktion für virtuelle serielle Kon-

solen, die für logische Partitionen auf iSeries-Systemen zur Verfügung steht. Sie bietet eine im Textmodus arbeitende Konsole für den IXS-Server des Typs 4812 und kann für zahlreiche Verwaltungsaufgaben eingesetzt werden, für die der Zugriff auf ein GUI-Desktop nicht erforderlich ist. Weitere Informationen zum Einrichten einer Sitzung mit der virtuellen seriellen Konsole für einen IXS-Server des Typs 4812 finden Sie unter „Verbindung zur virtuellen seriellen Konsole für IXS Modell 4812 herstellen“ auf Seite 159.

Die virtuelle serielle Konsole wird momentan nur unter Windows Server 2003 unterstützt. Sie kann zum Anzeigen von Serverfehlern oder zum Wiederherstellen der Verbindung zum LAN verwendet werden. Diese Konsolenverbindung kann verwendet werden, bevor TCP/IP auf dem Server konfiguriert wird. Informationen zu den Tasks, die mit Hilfe der virtuellen seriellen Konsole ausgeführt werden können, finden Sie im Dokument Microsoft Emergency Management Services



(www.microsoft.com/whdc/system/platform/server/default.msp). Beachten Sie hierbei Folgendes:

- i5/OS führt die meisten Konfigurationsschritte für die virtuelle serielle Konsole automatisch aus. Aus diesem Grund ist die Ausführung einiger der in der Microsoft-Dokumentation aufgeführten Konfigurationsschritte für die virtuelle serielle Konsole von i5/OS nicht erforderlich.
- Für die iSeries-Implementierung sind keine zusätzlichen Hardwareeinheiten wie z. B. Modems, Konzentratoren oder Kabel erforderlich, die in der Microsoft-Dokumentation aufgeführt sind.

Umleitung der Remote Supervisor Adapter II-Grafikkonsole

Bei xSeries-Servern, die mit einem RSA II ausgestattet sind, bietet der RSA II die vollständige hardwarebasierte Umleitung der Grafikkonsole. Das heißt, dass Sie über ein lokales Desktop auf einen fernen Server zugreifen und diesen steuern können.

Überlegungen

Ein integrierter Windows-Server hat in vielerlei Hinsicht Ähnlichkeit mit einem PC-basierten Windows-Server. Es gibt jedoch einige Unterschiede, die beachtet werden müssen:

- Möglicherweise ist kein Diskettenlaufwerk verfügbar. Dies bedeutet, dass Sie keine Start- oder Notfalldiskette verwenden können. Sie können jedoch den iSeries-Plattenspeicherplatz zur Sicherung Ihrer Dateien oder des gesamten Plattenimages verwenden.
- iSeries-Bandeneinheiten und -Platteneinheiten sind verfügbar.
- Bei der Verwendung des virtuellen Netzwerkbetriebs werden für die TCP/IP-Kommunikation mit dem iSeries-Server oder anderen integrierten Servern keine LAN-Adapter, Kabel, Hubs oder Switches benötigt.
- Die Installation des Betriebssystems Microsoft Windows unterscheidet sich bei der Windows-Umgebung auf der iSeries von der Installation eines herkömmlichen PC-Servers. Sie installieren zunächst IBM i5/OS Integrated Server Support und anschließend Microsoft Windows. Da ein Großteil der Konfigurationsdaten mit dem i5/OS-Befehl INSWNTSVR (Windows-Server installieren) eingegeben wird, werden einige der üblichen Installationsanzeigen für den Windows-Server nicht angezeigt. Der Befehl umfasst auch einige zusätzliche Parameter, die speziell die Integration des Servers mit i5/OS betreffen, wie z. B. "Datum/Uhrzeit synchronisieren".
- Auf der i5/OS-Seite der Serververwaltung wird ein integrierter Windows-Server durch eine NWS-Beschreibung (NSWD) dargestellt. Die Netzwerkschnittstellen werden durch Leitungsbeschreibungen dargestellt. Sie können den Server unter i5/OS durch Ab- bzw. Anhängen der NWS-Beschreibung (NSWD) stoppen oder starten.
- Sie können viele Aufgaben der Benutzeradministration, wie z. B. das Erstellen von Windows-Benutzern, über i5/OS ausführen.
- Da sich die Speicherverwaltung unter i5/OS von der auf einem PC-Server unterscheidet (siehe „i5/OS-Speicherverwaltung“ auf Seite 167), sind bestimmte, für die Speicherverwaltung auf einem PC-Server erforderliche Techniken für integrierte Server überflüssig.


Leistungsverhalten


Die IXS sowie die Server mit IXA- und iSCSI-Anschluss verfügen über eigenen Hauptspeicher und einen oder mehrere Prozessoren, nutzen den iSeries-Festplattenspeicher jedoch gemeinsam in Form von virtuellen (simulierten) Plattenlaufwerken. Die Zuordnung der Plattenlaufwerke zu Windows erfolgt durch Erstellen eines Speicherbereichsobjekts auf der iSeries. Der Hauptunterschied zwischen integrierten Servern und standalone Servern besteht darin, dass standalone Server eher dedizierte Plattenlaufwerke und integrierte Server iSeries-Speicherbereiche als virtuelle Platten benutzen. Neben Virtual Ethernet-Hochgeschwindigkeitsadaptoren enthalten integrierte iSeries-Server außerdem Zusatzeinrichtungen, wie beispielsweise Windows-Treiber für die gemeinsame Nutzung von iSeries-Bandlaufwerken, CD- und DVD-Laufwerken.

Die Nutzung von iSeries-Speicherbereichen (virtuellen Laufwerken) bietet Leistungsvorteile, die in standalone Umgebungen normalerweise nicht ohne erhebliche Investitionen in die Speicherstruktur und Wartungskosten erzielt werden können. Dennoch sind einige Einschränkungen vorhanden, die bei der Planung und Konfiguration integrierter Server zu beachten sind. Die nachfolgenden Informationen beleuchten einige Überlegungen zum Leistungsverhalten.

Unter den folgenden Links finden Sie weitere leistungsrelevante Informationen:

- „iSeries-Speicherbereiche im Vergleich zu dedizierten Festplatten“
- „Lastausgleich des Speicherbereichs“ auf Seite 27
- „Server mit iSCSI-Anschluss - Serverleistung“ auf Seite 28
- „Virtual Ethernet“ auf Seite 29

• IBM iSeries Integrated xSeries solutions 
(www.ibm.com/servers/eserver/series/integratedxseries)

• iSeries Performance Management 
(www.ibm.com/eserver/series/perfmgmt)

• Kapitel 17 im Buch iSeries Performance Capabilities Reference 

iSeries-Speicherbereiche im Vergleich zu dedizierten Festplatten

Die Leistungsmerkmale, die zur Ausführung processor- oder speicherintensiver Verarbeitungsschritte auf einem integrierten Server benötigt werden, entsprechen denen auf einem standalone Server, der dedizierte Plattenlaufwerke verwendet. Da die Plattenlaufwerke des integrierten Servers aus dem iSeries-Speicher zugeordnet werden, hängt die Plattenleistung von der iSeries ab.

Höhere Plattenleistung durch gemeinsam genutzte iSeries-Platten

Bei den meisten standalone Servern sind jedem Server einige wenige Platten zugeordnet. Für Anwendungen mit geringer durchschnittlicher Plattenbelastung ist das Leistungsverhalten auch angemessen. Es kann jedoch Zeiten geben, in denen die Serverleistung durch die Kapazität dieser wenigen dedizierten Platten eingeschränkt wird.

Wenn dieselbe Gruppe von Servern in die iSeries integriert wird, werden die virtuellen Platten über mehr iSeries-Festplatten verteilt. Die gesamte durchschnittliche Plattenbelastung muss nicht größer sein als für eine Servergruppe mit dedizierten Platten. Wenn jedoch ein einzelner Server vorübergehend eine höhere Plattenleistung benötigt, dann steht diese aufgrund der höheren Anzahl von iSeries-Platten zur Verfügung.

Bei Servern mit dedizierten Platten sind die Antwortzeiten relativ konstant. Sie könnten beispielsweise die vorhersehbare Antwortzeit nutzen und die Windows-Leistungsüberwachung so konfigurieren, dass sie Alerts ausgibt, wenn die Plattenantwortzeiten normale Grenzwerte übersteigen, und auf Ausnahmefällen hinweist, die Ihrer Aufmerksamkeit bedürfen.

| Bei einem integrierten Server werden der iSeries-Speicher, die CPU und der Hauptspeicher vom integrierten Server und iSeries-Anwendungen gemeinsam genutzt. Es ist durchaus normal, dass sich die Windows-Plattenantwortzeiten innerhalb eines größeren Bereichs bewegen. Kurzzeitig kann es vorkommen, dass E/A-Operationen mehrerer integrierter Server oder andere iSeries-Operationen um die gleiche Platte "kämpfen". Einige speicherintensive iSeries-Anwendungen (wie SAV und RST) können die Plattenleistung des Windows-Servers eine Zeitlang vermindern. Dies kann die Wahl eines Grenzwerts für kurze Zeiträume erschweren.

| **Beachten Sie bei der Bewertung von Speicherengpässen die gesamte Plattengruppe.**

| Innerhalb von Windows erscheint der iSeries-Speicherbereich als ein einziges Plattenlaufwerk. Wenn die durchschnittliche Warteschlangenlänge der physischen Platte (in der Windows-Leistungsüberwachung) den Wert 2 übersteigt, wird die Serverleistung nicht notwendigerweise von der Platte beeinträchtigt. Vorausgesetzt, die Auslagerung von Speicherseiten wurde ausgeschlossen, weist eine Warteschlangenlänge von 2 oder eine Windows-Plattenauslastung von 100% nur dann auf einen Speicherengpass hin, wenn nur ein einziges physisches Plattenlaufwerk zur Ausführung der Operationen verfügbar ist. Normalerweise arbeiten auf dem iSeries-Server mehrere Platten im Speicherbereichs-ASP parallel. Generell kann man sagen, dass die doppelte Anzahl von Platten im ASP auf einen Plattenengpass hinweisen könnten. Sie müssen möglicherweise auch die durchschnittlichen Warteschlangenlängen aller Server berücksichtigen, die den Speicher-ASP nutzen.

| **Lastausgleich des Speicherbereichs**

| Wenn ein Speicherbereich erstellt wird, werden die Daten in einem benutzerdefinierten Zusatzspeicherpool (ASP) oder einem unabhängigen Zusatzspeicherpool (IASP) über die Platten verteilt. Die Platten innerhalb des Pools können als ungeschützt, mit Paritätsschutz (RAID-5) oder mit Spiegelschutz konfiguriert werden. Ungeschützte Platten bieten keinen Schutz vor Plattenfehlern. Platten mit Paritätsschutz unterhalten Paritätsgruppen, die die Wiederherstellung ermöglichen, wenn der Plattenfehler in einer Paritätsgruppe auftritt (jedoch auf Kosten der Leistung). Die Spiegelungstechnologie bietet einen erheblich besseren Schutz vor Plattenfehlern als der Paritätsschutz. Der integrierte Server nutzt die Vorteile der effizienten iSeries-Speicherarchitektur unabhängig davon, wie ein ASP oder IASP konfiguriert ist.

| Der iSeries-Server verfügt über Funktionen, mit denen die effiziente Verteilung von Daten auf die Platten unterstützt wird. Ein Beispiel für eine solche Funktion ist die Operation STRDSKRGZ (Plattenreorganisation starten), mit der die Speicherbelegung ausgeglichen wird. Eine weitere Funktion ist "Einheiten zu ASPs hinzufügen und Daten ausgleichen", die verfügbar ist, wenn die Festplattenressourcen einem ASP zugewiesen werden. Bei integrierten Servern wird ein Speicherbereich nur auf andere Platten verschoben oder neu ausgeglichen, solange der verknüpfte Server abgehängt ist.

| Die Speicherposition der einem Speicherbereich zugeordneten Daten wird normalerweise automatisch von der iSeries verwaltet. Es besteht keine Notwendigkeit, innerhalb des Betriebssystems Windows einheitenübergreifende Datenträger oder ein Software-RAID der Platten zu konfigurieren. Tatsächlich könnte die Konfiguration dieser Features im Windows-Betriebssystem die effektiven Plattenoperationen verlangsamen. Obwohl der Speicher in kleinen Einheiten über die iSeries-Platten verteilt wird, defragmentieren Sie die zugeordneten Platten unter Windows weiter, um effiziente Datenstrukturen innerhalb des Dateisystems aufrecht zu erhalten.

| Mit Hilfe der Befehle WRKDSKSTS (Mit Plattenstatus arbeiten), WRKNWSSTG (Mit NWS-Speicherbereichen arbeiten) und WRKNWSSTS (Mit NWS-Status arbeiten) können Sie überwachen, wie gut die iSeries die erforderliche Plattenspeicherkapazität des integrierten Servers erfüllt. Hinsichtlich der Leistung muss des Weiteren berücksichtigt werden, dass integrierte Server eigentlich Microsoft Windows-Server sind. Die Windows-Leistungsüberwachung von Microsoft kann wie auf jedem anderen Server angewandt werden. Informationen zur Verwendung der Leistungsüberwachung enthält die Microsoft Windows-Dokumentation.

| **Server mit iSCSI-Anschluss - Serverleistung**

| Für Server mit iSCSI-Anschluss stehen mehrere Konfigurationsoptionen zur Verfügung, die nach Bedarf angepasst werden können, um ein besseres Leistungsverhalten zu erzielen. Für einige Optionen können unterschiedliche Zielplattenkonfigurationen oder Datenträger auf den integrierten Servern erforderlich sein.

| **Windows-Plattenkonfiguration**

| Bei integrierten Servern mit iSCSI-Anschluss sind die virtuellen Plattenlaufwerke für folgende Werte optimiert:

- | • Eine Plattenpartition pro virtuellem Laufwerk.
- | • Speicherbereiche von einem Gigabyte oder mehr.
- | • NTFS-Dateisystem, formatiert mit Clustergrößen von mindestens vier Kilobyte.

| Anhand dieser Richtlinien kann die iSeries den Speicherbereich effizient verwalten und so die Plattenleistung steigern. Diese Richtlinien haben auch Auswirkungen auf IXS und Server mit IXA-Anschluss, jedoch in einem geringeren Ausmaß.

| Wenn Sie einen Plattenspeicher mit dem CL-Befehl CHGNWSSTG (Netzwerkspeicherbereich ändern) vergrößern, müssen Sie gleichzeitig mit dem Windows Server 2003-Befehl DISKPART die Partition unter Windows vergrößern.

| **Anmerkung:** Das Leistungsverhalten wird verbessert, wenn Sie dem Server einen Speicherbereich hinzufügen, statt dem neuen Speicherbereich eine weitere Plattenpartition hinzuzufügen.

| **iSeries-Hauptspeicherpools**

| Bei Servern mit iSCSI-Anschluss werden die Speicheroperationen über einen iSeries-Hauptspeicherpool ausgeführt. Dieser Hauptspeicher fungiert im Wesentlichen als Cachespeicher für die Plattenoperationen, daher kann die Speichergröße Auswirkungen auf die Windows-Festplattenleistung haben. Diese E/A-Operationen führen nicht unmittelbar zu Fehlseitenbedingungen im Basispool. Da der Hauptspeicherpool jedoch gemeinsam mit anderen i5/OS-Anwendungen genutzt wird, können Windows-Festplattenoperationen zu Fehlseitenbedingungen in anderen Anwendungen führen, oder andere Anwendungen können ein Paging von iSCSI-Festplattenoperationen bewirken. In extremen Fällen müssen Sie die Größe der Hauptspeicherpools anpassen oder Anwendungen anderen Hauptspeicherpools zuordnen, um Hauptspeicherprobleme zu vermeiden.

| IXS und Server mit IXA-Anschluss führen keine Festplattenoperationen über einen Basispeicherpool aus. Sie verwenden reservierten Speicherbereich innerhalb des Maschinenpools (Systempool-ID 1). Daher nutzen die Festplattenoperationen keinen Hauptspeicher mit anderen Anwendungen gemeinsam.

| **Konfiguration der iSCSI-Leistung**

| Wenn bei integrierten Servern mit iSCSI-Anschluss eine einzelne Netzwerkstruktur die Kapazitätsgrenze erreicht, können sowohl den xSeries- als auch den iSeries-Servern Kanäle mit zusätzlichen iSCSI-HBAs hinzugefügt werden (vorausgesetzt, das verbindende Netzwerk verfügt über genügend Bandbreite).

| Es gibt verschiedene Möglichkeiten, um den iSCSI- und den Datenaustausch im Netz auf separate Kanäle zu verteilen:

- | • Ordnen Sie SCSI-Operationen einem und Virtual Ethernet-Operationen einem anderen Kanal zu.
- | • Verwenden Sie zwei Speicherziele. Jedes sollte mit einem separaten HBA-Pfad verknüpft sein. Weitere Informationen finden Sie unter „iSCSI-Hostbusadapter verwalten“ auf Seite 143.

- Steuern Sie Anwendungen unter Windows so, dass sie (wenn möglich) beide Laufwerke verwenden, oder ordnen Sie die Laufwerke unterschiedlichen Anwendungen zu, um die Gesamtsumme der Plattenoperationen auf die Laufwerke zu verteilen.
- Konfigurieren Sie die beiden Festplatten in einer dynamischen Windows-Datenträgergruppe, wobei die Daten einheitenübergreifend gespeichert werden. Wenn Anwendungen auf Datenträger zugreifen, werden die Plattenoperationen automatisch auf die Laufwerke innerhalb der Datenträgergruppe verteilt.

Virtual Ethernet

Die Virtual Ethernet-Punkt-zu-Punkt-Verbindung ist die standardmäßige virtuelle Netzwerkverbindung zwischen der iSeries-Hosting-Partition und den einzelnen integrierten Windows-Servern. Die Punkt-zu-Punkt-Verbindung wird hauptsächlich für Verwaltungsoperationen genutzt, die Bestandteil der integrierten Umgebung sind.

Die Kosten der iSeries- und Windows-CPU-Auslastung bei Verwendung einer Punkt-zu-Punkt-Verbindung entsprechen in etwa den Nutzungskosten bei Verwendung eines Hardwarenetzadapters. Bei dieser Verbindung handelt es sich um eine Hochgeschwindigkeitsverbindung, doch die gesamte Bandbreite wird immer gemeinsam mit Platten-, Band- und anderen Operationen auf IXS- und IXA-Adaptoren genutzt. Wenn Sie Internet-SCSI (iSCSI) verwenden, können Sie Virtual Ethernet-Operationen isolieren, indem Sie einen anderen iSCSI-HBA-Kanal verwenden.

Eine Virtual Ethernet-Verbindung zwischen zwei oder mehr integrierten Servern, verwendet die iSeries-CPU, um den Datenverkehr auf die Server aufzuteilen. Dies geschieht auch dann, wenn der iSeries-Server kein Endpunkt des Datenverkehrs ist. Für die meisten Verbindungen ist diese Nutzung nicht von Bedeutung. Wenn Sie jedoch eine anhaltend hohe Netzbelastung über die Virtual Ethernet-Verbindung zwischen den integrierten Servern erwarten, kann es sich für Sie lohnen, die Kosten für die Verwendung des internen Virtual Ethernet-Switch und die Kosten für die Verwendung externer Netzwerkadapter auf den integrierten Servern gegeneinander abzuwägen.

Konzepte für den Netzbetrieb

Hosted Systeme umfassen viele verschiedene Netzverbindungstypen.

Die folgenden Verbindungstypen gelten nur für Systeme mit iSCSI-Anschluss.

- **„Serviceprozessorverbindung“ auf Seite 30**
Diese physische Verbindung erlaubt der i5/OS-Hosting-Partition mit dem Serviceprozessor des Hosted Systems zu kommunizieren.
- **„iSCSI-Netzwerk“ auf Seite 30**
Dieses physische Netzwerk verbindet iSCSI-Adapter in der i5/OS-Hosting-Partition mit iSCSI-Adaptoren im Hosted System.

Alle Typen von integrierten Windows-Servern können über die folgenden Verbindungstypen verfügen.

- **Virtual Ethernet**
Dies ist eine simulierte Ethernet-Verbindung, für die keine zusätzlichen Netzwerkkarten oder -kabel benötigt werden. Es gibt zwei Arten von virtuellem Ethernet.
 - **„Virtual Ethernet-Punkt-zu-Punkt“ auf Seite 33**
Diese Verbindung stellt die allgemeine Kommunikation zwischen dem Hosted System und dem Hosting i5/OS zur Verfügung.
 - **„Virtual Ethernet-Netzwerke“ auf Seite 33**
Diese Netzwerke werden zwischen Hosted Systemen, i5/OS-Partitionen und anderen Partitionen (z. B. Linux) erstellt.
- **„Externe Netzwerke“ auf Seite 38**
Diese herkömmlichen Windows-Netzwerke werden von allen Servern verwendet und über physische Netzwerkkarten erstellt, die vom Hosted System gesteuert werden.

Serviceprozessorverbindung

Anmerkung: Dieser Abschnitt bezieht sich nur auf Systeme mit iSCSI-Anschluss.

Diese physische Verbindung ist erforderlich, damit das Hosted i5/OS mit dem Serviceprozessor des Hosted Systems kommunizieren kann. Die Verbindung kann aus einem einfachen Netz mit Switch oder einem komplexeren Netz mit Routern bestehen. Die Windows-Umgebung auf der iSeries verwendet IBM Director über diese Verbindung, um den Status des Hosted Systems zu verwalten.

An einem Ende der Verbindung befindet sich mindestens ein LAN-Adapter, der von i5/OS gesteuert wird. Der LAN-Adapter kann auch weiterhin für andere Verwendungsmöglichkeiten zur Verfügung stehen. Die IP-Adresse und andere Attribute dieses Adapters werden mit Hilfe standardmäßiger i5/OS-Konfigurationsmethoden gesteuert. Der Adapter wird nicht von der Windows-Umgebung auf der iSeries konfiguriert. Er kann den Serviceprozessor automatisch mit Hilfe von IBM Director und einer oder mehreren i5/OS-TCP-Schnittstellen erkennen, die bereits konfiguriert sind.

Am anderen Ende der Verbindung befindet sich der Serviceprozessor. Dieser verfügt über seinen eigenen Ethernet-Anschluss und TCP/IP-Stack. Der TCP/IP-Stack ist aktiv, solange das Netzkabel des Servers mit einem unter Spannung stehenden Wechselstromausgang verbunden ist; dies gilt auch dann, wenn der Server nicht eingeschaltet ist. Bei bestimmten xSeries-Modellen kann ein einzelner Ethernet-Anschluss von Windows und einem bestimmten Typ von Serviceprozessor, dem so genannten Baseboard Management Controller (BMC), gemeinsam genutzt werden. In diesem Fall stellt ein und derselbe physische Anschluss auf dem Hosted System sowohl die Serviceprozessor- als auch die externe Netzwerkverbindung zur Verfügung.

DHCP-Server für den Serviceprozessor

Für die Einstellung der IP-Adresse des Serviceprozessors kann ein externer DHCP-Server auf dem Netzwerk erforderlich sein, der die Serviceprozessorverbindung bereitstellt. Der DHCP-Server muss aktiv sein, bevor das Netzkabel des Hosted Systems mit einem unter Spannung stehenden Wechselstromausgang verbunden wird. (Dieser DHCP-Server unterscheidet sich von dem DHCP-Server, der auf der i5/OS-Seite des iSCSI-Netzwerks installiert wurde, um das iSCSI-Booten des Hosted Betriebssystems zu unterstützen). Weitere Informationen finden Sie unter „Dynamische IP-Adressierung (DHCP)“ auf Seite 153.

IP-Multicast

Die Windows-Umgebung auf der iSeries bietet zahlreiche Möglichkeiten zur Erkennung des Serviceprozessors. Beachten Sie, dass das Netzwerk für die Möglichkeiten, die den höchsten Automatisierungsgrad bieten, IP-Multicast unterstützen muss. Einige Switches und Netzwerke bieten keine standardmäßige IP-Multicast-Unterstützung. Weitere Informationen finden Sie unter „Erkennungsmethode für Serviceprozessor“ auf Seite 153.

Leistung und größte zu übertragende Einheit (MTU)

Ein Hochgeschwindigkeitsnetz oder eine hoher MTU-Wert sind für die Serviceprozessorverbindung weder erforderlich noch von Vorteil.

Sicherheit

Die Entscheidung, ob Sie für die Bereitstellung der Serviceprozessorverbindung ein isoliertes oder ein gemeinsames genutztes Netzwerk verwenden, kann von der Sicherheitsleistung Ihrer Serviceprozessor-Hardware abhängen. Weitere Informationen finden Sie unter „Serviceprozessor-SSL konfigurieren“ auf Seite 140.

iSCSI-Netzwerk

Dieses physische Netzwerk verbindet Ethernet-iSCSI-Adapter im Hosted i5/OS mit Ethernet-iSCSI-Adaptoren im Hosted System. Es handelt sich hierbei normalerweise um ein einfaches Gigabit-Ethernet-Netz. Über diese Verbindung werden zwei Arten von Datenübertragungen abgewickelt: Speicher- (SCSI) und Virtual Ethernet (LAN).

| An einem Ende der Verbindung befindet sich mindestens ein iSCSI-Adapter, der von i5/OS gesteuert
| wird. Jeder iSCSI-Adapter hat zwei IP-Adressen: eine für SCSI und eine für LAN. Die IP-Adressen und
| anderen Attribute eines Adapters werden in einem i5/OS-Einheitenbeschreibungsjekt konfiguriert, das
| als NWS-Hostadapter bezeichnet wird. Weitere Informationen finden Sie unter „NWS-Hostadapter“ auf
| Seite 45. Für jeden von i5/OS gesteuerten iSCSI-Adapter wird ein eigenes Objekt benötigt. Jeder iSCSI-
| Adapter enthält einen TCP/IP-Stack, der in Hardware implementiert ist, die vom normalen i5/OS-
| TCP/IP-Stack unabhängig ist. Wenn Sie einen NWS-Hostadapter anhängen, verwendet ein von i5/OS
| gesteuerter iSCSI-Adapter die konfigurierten Werte. Wenn Sie andere Werte wünschen, müssen Sie die
| Konfiguration ändern und den NWS-Hostadapter erneut anhängen. Der i5/OS-TCP/IP-Stack erkennt die
| für die iSCSI-Adapter konfigurierten IP-Adressen nicht.

| Am anderen Ende des Netzwerks befindet sich mindestens ein iSCSI-Adapter für das Hosted System. Die
| IP-Adressen und anderen Attribute dieser Adapter werden in einem i5/OS-Objekt konfiguriert, das als
| Konfiguration des fernen Systems bezeichnet wird. Weitere Informationen finden Sie unter „Konfigura-
| tion des fernen Systems“ auf Seite 45. Diese Konfiguration unterscheidet sich an vielen Stellen vom
| i5/OS-Objekt NWS-Hostadapter:

- | • Sie können einen iSCSI-Adapterport in einem Hosted System mit einer oder zwei IP-Adressen konfigu-
| rieren: SCSI oder/und LAN. Innerhalb aller konfigurierten Adapter muss es mindestens eine SCSI- und
| eine LAN-IP-Adresse geben.
- | • Sobald Sie eine IP-Adresse für einen iSCSI-Adapter in einem Hosted System konfigurieren, müssen Sie
| auch die entsprechende MAC-Adresse konfigurieren. Die MAC-Adressen finden Sie auf dem Adapter.
| Achten Sie auf die richtige Konfiguration der MAC-Adressen.
- | • Alle iSCSI-Adapter für ein Hosted System werden in ein und demselben i5/OS-Konfigurationsobjekt
| für das ferne System konfiguriert. Wenn der integrierte Server anschließend angehängt wird, stellt das
| Produkt automatisch sicher, dass die iSCSI-Adapter im Hosted System die Werte in der i5/OS-Konfigu-
| ration des fernen Systems verwenden. Wenn Sie andere Werte wünschen, müssen Sie die Konfiguration
| ändern und den Server erneut anhängen.
- | • Der SCSI-Datenverkehr verwendet den TCP/IP-Stack der iSCSI-Adapterhardware, der LAN-Daten-
| verkehr jedoch den Windows-TCP/IP-Stack. Folglich erkennt der Windows-TCP/IP-Stack die SCSI-IP-
| Adresse nicht sondern nur die LAN-IP-Adresse.

| **Anmerkungen:**

- | 1. In i5/OS-Konfigurationsobjekten werden die Netzschnittstelleninformationen als lokal oder fern
| bezeichnet. Diese Bezeichnungen beziehen sich auf i5/OS. Lokale Schnittstelleninformationen betreffen
| die i5/OS-Seite. Ferne Schnittstelleninformationen betreffen die Seite des Hosted Windows-Systems.
- | 2. Der NWS-Hostadapter und die Konfiguration für das ferne System definieren die IP-Adressinformati-
| onen für die gegenüberliegenden Seiten des iSCSI-Netzwerks. Wenn sie über ein einfaches Wählnetz
| verbunden sind, gelten folgende Regeln:
 - | • Die SCSI-Internetadressen in diesen beiden Objekten, die über einen Switch verbunden sind, müs-
| sen sich im selben Teilnetz befinden. Beispiel: Bei IP-Adressen im Format a.b.x.y und 255.255.255.0
| müssen die Teilnetzmasken a.b.x für beide Objekte denselben Wert haben.
 - | • Die LAN-Internetadressen in diesen beiden Objekten, die über einen Switch verbunden sind, müs-
| sen sich im selben Teilnetz befinden.
 - | • Im NWS-Hostadapter können die Gateway-Elemente beliebige nicht zugeordnete IP-Adressen in
| einem beliebigen Teilnetz sein, wenn sich kein Gateway in Ihrem Netzwerk befindet.
 - | • In der Konfiguration des fernen Systems sollten die Gateway-Elemente leer sein, wenn sich kein
| Gateway in Ihrem Netzwerk befindet.

| **DHCP und DHCP-Weitergabe**

| Für die Übergabe von Boot-Informationen an das Hosted System stehen mehrere Methoden zur Verfü-
| gung. Bei der Standardmethode für die Zustellung von IP- und Speicherinformationen zum Booten von
| Windows wird ein integrierter DHCP(Dynamic Host Configuration Protocol)-Server auf der i5/OS-Seite
| des iSCSI-Netzwerks verwendet. Auch bei Verwendung von DHCP können die IP-Adressen als statisch

| angesehen werden, da der DHCP-Server eine einzelne IP-Adresse einer MAC-Adresse zuordnet. Weitere
| Informationen finden Sie unter „Booten über iSCSI ohne Plattenspeicher“ auf Seite 23.

| Der integrierte DHCP-Server ist so konstruiert, dass er mit allen anderen DHCP-Servern, die sich eventu-
| ell noch auf dem iSCSI-Netzwerk befinden, koexistieren kann.

| Wenn sich auf dem iSCSI-Netzwerk zwischen dem iSeries-Server und dem Hosted System Router befin-
| den und die Übergabe der Boot-Informationen über DHCP erfolgt, muss ein entsprechend konfigurierter
| DHCP-Weitergabeagent (Relay Agent), der auch als BOOTP Relay Agent bezeichnet wird, im Netzwerk
| vorhanden sein.

| **Leistung und größte zu übertragende Einheit (MTU)**

| Für das iSCSI-Netzwerk ist eine hohe Bandbreite und eine niedrige Latenzzeit wünschenswert. Virtual
| Ethernet kann eine MTU in Form eines bis zu 9000 Byte großen 'Jumbo'-Frames nutzen, sofern das Netz-
| werk den höheren MTU-Wert unterstützt. Das Leistungsverhalten des Virtual Ethernet wird dadurch ver-
| bessert.

| **i5/OS-iSCSI-Adapternutzung verwalten**

| In der NWS-Beschreibung konfigurierte Pfade steuern, welcher Speicherdatenverkehr und welcher Virtual
| Ethernet-Datenverkehr (sofern vorhanden) über einen i5/OS-iSCSI-Adapter geleitet wird. Weitere Infor-
| mationen finden Sie unter „iSCSI-HBA-Nutzung verwalten“ auf Seite 144.

| Mehrere Hosted Systeme können einen i5/OS-iSCSI-Adapter gleichzeitig benutzen, wenn mehrere NWS-
| Beschreibungen das gleiche NWS-Hostadapterobjekt verwenden.

| **iSCSI-Adapternutzung des Hosted Systems verwalten**

| Sie können einen iSCSI-Adapter in einem Hosted System mit einer SCSI-IP-Adresse und/oder einer LAN-
| IP-Adresse konfigurieren. Das Vorhandensein einer SCSI-IP-Adresse ermöglicht den Speicherdaten-
| verkehr, das Vorhandensein einer LAN-IP-Adresse ermöglicht den Virtual Ethernet-Datenverkehr. Jeder
| virtuelle Windows-Ethernet-Adapter wird normalerweise automatisch einem physischen iSCSI-Adapter
| zugeordnet. Über die Indexzunge für die erweiterten Eigenschaften eines jeden Virtual Ethernet-Adapters
| kann ein bestimmter physischer iSCSI-Adapter ausgewählt werden. Weitere Informationen finden Sie
| unter „iSCSI-HBA-Zuordnung auf der Windows-Seite des iSCSI-Netzwerks verwalten“ auf Seite 147.

| Die Verwendung des iSCSI-Adapters als universelle externe Netzverbindung wird von IBM nicht unter-
| stützt. Weitere Informationen über externe Netzverbindungen finden Sie unter „Externe Netzwerke“ auf
| Seite 38.

| **Weitere Hinweise**

- | • Das iSCSI-Netzwerk verwendet nur Internet Protocol Version 4.
- | • Das Frameformat ist Ethernet Version 2.
- | • Das iSCSI-Netzwerk unterstützt keine Netzwerkadressumsetzung.

| **Sicherheit**

| Es gibt zahlreiche Möglichkeiten, den Speicherdatenverkehr und den Virtual Ethernet-Datenverkehr zu
| schützen. Weitere Informationen finden Sie unter „Sicherheitskonzepte“ auf Seite 51.

Virtual Ethernet-Punkt-zu-Punkt

i5/OS muss mit seinen integrierten Windows-Servern kommunizieren können. Diese Kommunikation erfolgt über ein Virtual Ethernet-Punkt-zu-Punkt-Netzwerk. Bei der Installation eines integrierten Servers wird ein spezielles virtuelles Netzwerk zwischen dem Server und einer steuernden i5/OS-Partition erstellt. Dieses Netzwerk wird als Punkt-zu-Punkt-Netzwerk (PTP-Netzwerk) bezeichnet, weil es lediglich zwei Endpunkte hat (nämlich den integrierten Server und die iSeries) und weil es außerdem (genauso wie ein Virtual Ethernet-Netzwerk) innerhalb der iSeries emuliert wird und keine zusätzlichen physischen Netzwerkadapter oder -kabel verwendet werden. In i5/OS wird dieses Netzwerk als Ethernet-Leitungsbeschreibung mit dem Wert *VRTETHPTP für die Portnummer konfiguriert.

Wenn Sie den Befehl INSWNTSVR (Windows-Server installieren) ausführen, wird ein Virtual Ethernet-PTP-Netzwerk konfiguriert.

Möglicherweise haben Sie sich bereits gefragt, worin der Unterschied zwischen einer Virtual Ethernet-PTP-Verbindung und einem Virtual Ethernet-Netzwerk besteht. Virtual Ethernet-PTP-Netzwerke werden anders konfiguriert und haben immer nur zwei Endpunkte, nämlich die iSeries und einen integrierten Server. Virtual Ethernet-PTP unterstützt ausschließlich das TCP/IP-Protokoll und verwendet standardmäßig eingeschränkte IP-Adressen in privaten Domänen, so dass die Adressen nicht über Gateways oder Router weitergegeben werden können.

Bei integrierten xSeries-Servern (IXS) und über integrierte xSeries-Adapter (IXA) angeschlossenen xSeries-Servern haben diese Adressen das Format 192.168.xxx.yyy (xxx und yyy können ein bis zwei Ziffern umfassen). Die IP-Adresse für einen IXS, der mit der Hardwareressourcennummer LIN03 definiert ist, lautet beispielsweise 192.168.3.yyy.

Bei iSCSI-Hardware haben diese Adressen das Format 192.168.xxx.yyy, wobei xxx zwischen 100 und 254 liegen kann und in einem eindeutigen Netzwerk der Klasse C resultiert. Im obigen Beispiel wird der i5/OS-Seite des PTP-Netzwerks die IP-Adresse 192.168.100.1 und der Windows-Seite die Adresse 192.168.100.2 zugewiesen. Werden für die gleiche Hardwareressource mehrere Leitungsbeschreibungen definiert, wird der Wert für yyy jeweils erhöht.

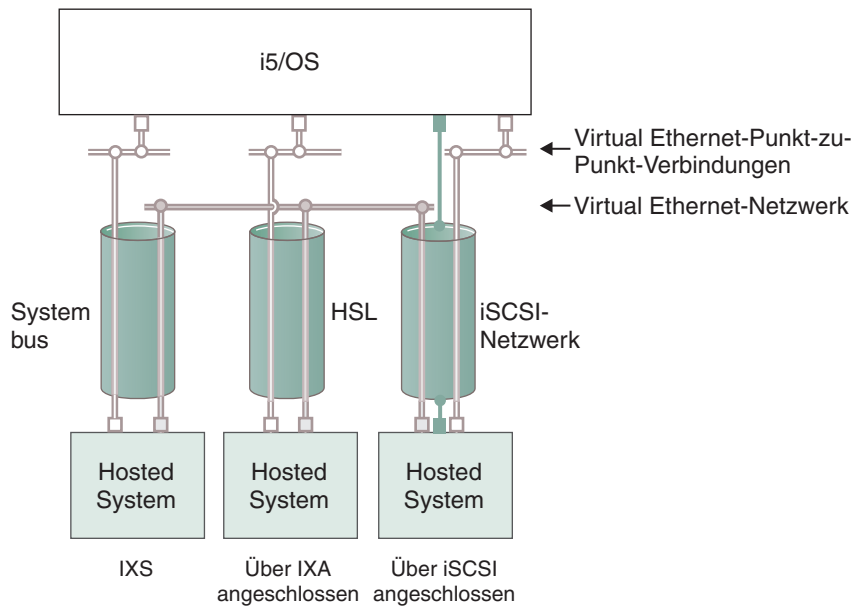
Diese IP-Adressen können mit dem Befehl INSWNTSVR automatisch zugeordnet oder aber manuell konfiguriert werden, um TCP/IP-Adressüberschneidungen mit anderen Hosts auf dem System zu vermeiden.

Virtual Ethernet-Netzwerke

Virtual Ethernet-Netzwerke sind flexibel und können auf viele unterschiedliche Arten konfiguriert werden.

Virtual Ethernet-Netzwerke, die nicht mehr als eine logische Partition enthalten

Die Erstellungsprozedur für Virtual Ethernet-Netzwerke wird unter „Virtual Ethernet-Netzwerke konfigurieren“ auf Seite 121 erläutert.



■ oder □ IP-Adresse auf virtuellem Adapter

■ LAN-IP-Adresse auf iSCSI-Adapter

RZAHQ500-5

Abbildung 9. Systembus, HSL und iSCSI-Netzwerk

IXSs, Systeme mit IXA-Anschluss und Systeme mit iSCSI-HBA-Anschluss können alle an Virtual Ethernet-Netzwerken teilhaben und miteinander kommunizieren.

- Bei IXSs wird der Ethernet-Datenverkehr über iSeries-Systembusse übertragen.
- Bei Systemen mit IXA-Anschluss wird der Virtual Ethernet-Datenverkehr über HSL-Kabel übertragen.
- Bei Hosted Systemen mit iSCSI-Anschluss wird der virtuelle Ethernet-Datenverkehr im Tunnelungsverfahren durch ein physisches iSCSI-Netzwerk übertragen. Virtual Ethernet wird aus verschiedenen Gründen für ein iSCSI-Netzwerk benötigt:
 - Virtual Ethernet kann zusammen mit anderen Virtual Ethernet-Unterstützungsfunktionen in Ihrem iSeries-Server verwendet werden.
 - Virtual Ethernet kann über jeden iSCSI-HBA mehrere separate virtuelle Netzwerke zur Verfügung stellen, selbst wenn Switches im iSCSI-Netzwerk keine IEEE 802.1Q VLANs unterstützen.
 - Wenn IPSec aktiviert ist, wird der Datenverkehr in einem iSCSI-Netzwerk verschlüsselt. Virtual Ethernet kann als leistungsfähiges virtuelles privates Netz (VPN) angesehen werden. Im Gegensatz zu normalen VPNs, die über nur zwei Endpunkte verfügen, kann ein Virtual Ethernet mit IPSec ein vollständiges virtuelles Netzwerk schützen.

Anmerkung: Jede iSCSI-HBA-Schnittstelle kann über zwei IP-Adressen verfügen - eine für Speicher- und eine für LAN-Funktionen, die für die Virtual Ethernet-Übertragung im Tunnelungsverfahren verwendet werden. i5/OS-TCP/IP kann diese IP-Adressen nicht erkennen. Bei iSCSI-HBAs findet die Virtual Ethernet-Übertragung im Tunnelungsverfahren über ein physisches Netzwerk statt, an dessen Endpunkten sich iSCSI-HBAs befinden.

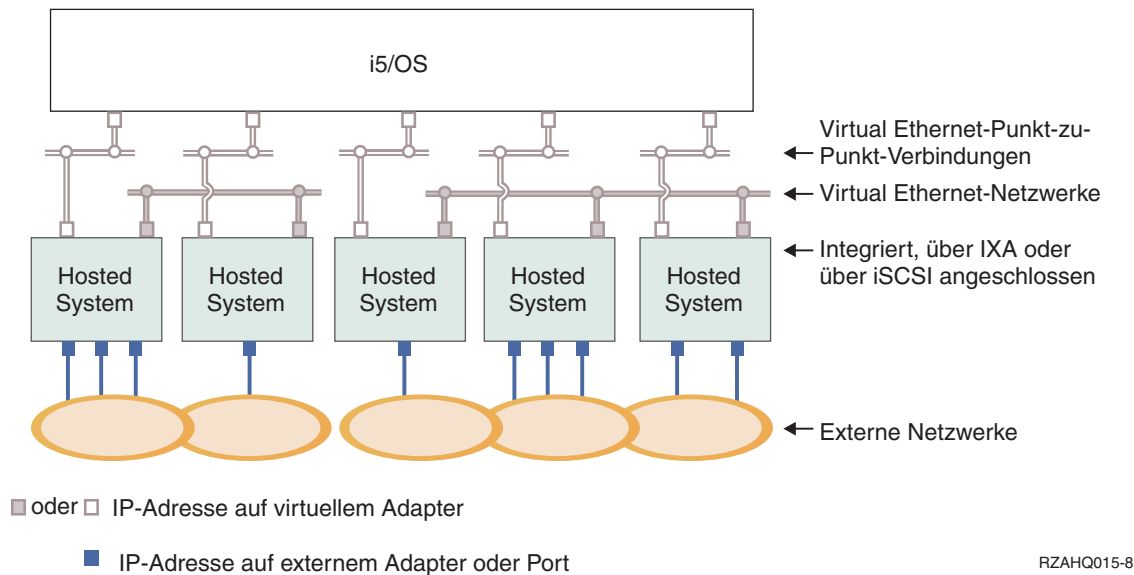
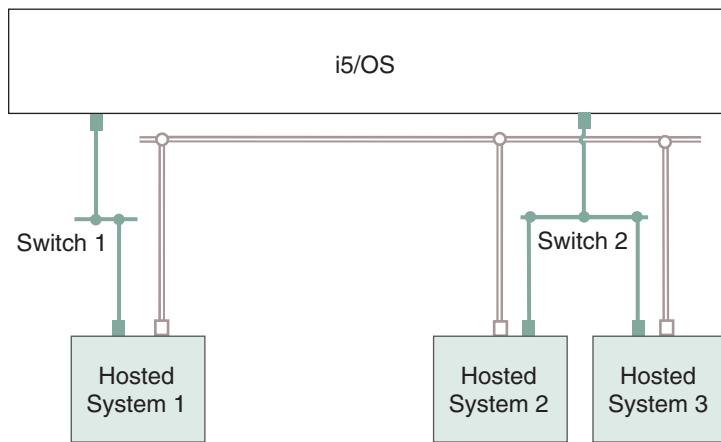


Abbildung 10. Zwei separate Gruppen von integrierten Windows-Servern auf dem gleichen iSeries-Server. Jede Gruppe verfügt über ein eigenes Virtual Ethernet-Netzwerk.

Abb. 10 soll die Funktionsweise von virtuellen Netzwerken in der iSeries veranschaulichen. Es sind fünf separate integrierte Windows-Server dargestellt. Alle Server sind über virtuelle PTP-Ethernet-Netzwerke (in Weiß) mit der gleichen steuernden i5/OS-Partition verbunden. Die blauen Kästchen unter den integrierten Servern stellen physische Netzwerkadapterkarten dar, die den Maschinen den Aufbau externer Netzwerkverbindungen erlauben. Die Ovale, mit denen sie verbunden sind, stehen für externe Netzwerke. Schließlich sind in Grau zwei separate Virtual Ethernet-Netzwerke dargestellt. Jeder integrierte Server kann gleichzeitig bis zu vier Virtual Ethernet-Netzwerken angehören.

Diese Art der Verbindung ist erforderlich, wenn eine Gruppe von integrierten Servern für das Clustering konfiguriert wird.

Wie das virtuelle PTP-Ethernet werden Virtual Ethernet-Netzwerke über Ethernet-Leitungsbeschreibungen konfiguriert. Ein integrierter Server ist mit einem Virtual Ethernet-Netzwerk verbunden, wenn seine i5/OS-Konfiguration (NWS-Beschreibung) einen Wert von *VRTETH0 bis *VRTETH9 für die Portnummer der Ethernet-Leitungsbeschreibung enthält. Integrierte Server, deren NWS-Beschreibungen mit identischen Werten für die Portnummer konfiguriert sind, werden mit dem gleichen Virtual Ethernet-Netzwerk verbunden. Bei der Installation eines neuen integrierten Servers kann der Befehl INSWNTSVR (Windows-Server installieren) die erforderlichen Leitungsbeschreibungen automatisch erstellen und den Beschreibungen IP-Adressen zuordnen. In der Abbildung ist die i5/OS-Seite der Leitungsbeschreibungen nicht dargestellt. Sofern Sie kein Virtual Ethernet verwenden, sollte auf der i5/OS-Seite einer Leitungsbeschreibung, die in einem Virtual Ethernet-Netzwerk verwendet wird, eine TCP/IP-Adresse konfiguriert werden.



- IP-Adresse auf virtuellem Adapter
- LAN-IP-Adresse auf iSCSI-Adapter

RZAHQ513-2

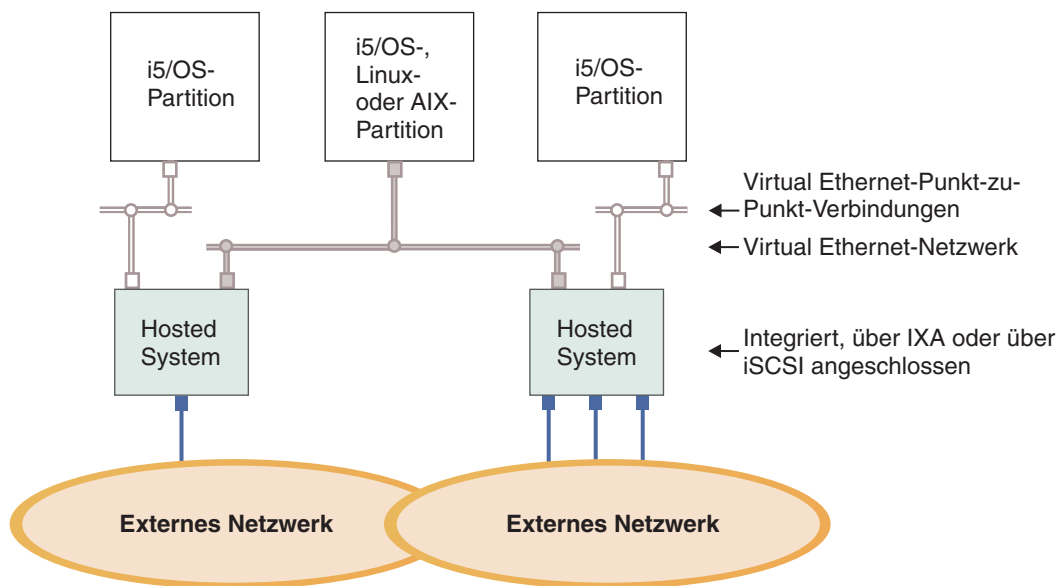
Abbildung 11. Im Tunnelungsverfahren über iSCSI-Netzwerke übertragenes Virtual Ethernet

Virtual Ethernet, das im Tunnelungsverfahren durch iSCSI-Netzwerke übertragen wird, verfügt über spezielle Merkmale, die in Abb. 11 dargestellt sind.

- Hosted System 1 kann mit Hosted System 2 und Hosted System 3 kommunizieren, obwohl separate iSCSI-Netzwerke (separate physische Switches) vorhanden sind.
- An der Virtual Ethernet-Kommunikation zwischen Hosted System 2 und Hosted System 3 ist das iSeries-System beteiligt, obwohl beide Hosted Systeme mit demselben physischen Switch verbunden sind.
- An der Virtual Ethernet-Kommunikation aller Hosted Systeme sind jeweils zwei LAN-IP-Adressen auf dem physischen iSCSI-Netzwerk beteiligt. Die Adressenpaare für Hosted System 2 und Hosted System 3 haben auf der i5/OS-Seite eine IP-Adresse gemeinsam.

| **Virtual Ethernet-Netzwerke, die mehr als eine logische Partition enthalten**

| Die Erstellungsprozedur für Virtual Ethernet-Netzwerke wird unter „Partitionsübergreifende Virtual Ethernet-Netzwerke konfigurieren“ auf Seite 122 erläutert.



■ oder □ IP-Adresse auf virtuellem Adapter

■ IP-Adresse auf externem Adapter oder Port

RZAHQ016-9

| *Abbildung 12. Einfaches, partitionsübergreifendes Virtual Ethernet-Netzwerk*

| In diesem Beispiel wurde die iSeries partitioniert, wobei drei separate virtuelle i5/OS-LPARs auf der iSe-
 | ries erstellt wurden. In der Abbildung sind drei virtuelle Netzwerke dargestellt: zwei virtuelle PTP-Netz-
 | werke (weiß) und ein Virtual Ethernet-Netzwerk (grau). Jeder integrierte Server verfügt über ein Virtual
 | Ethernet-PTP-Netzwerk für die Kommunikation mit seiner steuernden Partition. In diesem Beispiel
 | besteht das Virtual Ethernet-Netzwerk aus drei Teilnehmern, nämlich zwei integrierten Servern, die
 | jeweils durch eine andere i5/OS-Partition gesteuert werden, und einer dritten Partition, auf der i5/OS
 | oder ein anderes Betriebssystem ausgeführt wird. Dies wird als partitionsübergreifendes Ethernet-Netz-
 | werk bezeichnet.

| Auf Servern ohne HMC (Hardware Management Console) bestehen partitionsübergreifende Verbindun-
 | gen zwischen Partitionen, die dieselbe Netzwerknummer verwenden. Integrierte Server sind nur dann
 | verbunden, wenn die zugehörigen i5/OS-Steuerpartitionen ebenfalls verbunden sind. Die Netzwerk-
 | nummern 0-9 sind für integrierte Server relevant. Wenn beispielsweise eine i5/OS-Partition für partitions-
 | übergreifende Verbindungen in den Netzwerken 1 und 5 konfiguriert ist, können integrierte Server, die
 | durch diese Partition gesteuert werden, an der partitionsübergreifenden Kommunikation auf den Ports
 | *VRTETH1 und *VRTETH5 teilnehmen. Die entsprechende Prozedur ist in der Onlinehilfe von iSeries
 | Navigator beschrieben. Eine Übersicht zu diesem Aspekt finden Sie im Abschnitt zu den Konzepten für
 | logische Partitionen.

| Auf Servern mit HMC (Hardware Management Console) bestehen partitionsübergreifende Verbindungen
 | zwischen Partitionen oder integrierten Servern, die dieselbe VLAN-ID verwenden. Die teilnehmenden
 | integrierten Server unterstützen VLAN-IDs nicht direkt. Stattdessen benötigt jeder teilnehmende inte-
 | grierte Server eine Ethernet-Leitungsbeschreibung, die einem virtuellen Adapter, der über eine VLAN-ID
 | verfügt, einen Portwert wie beispielsweise *VRTETH1 zuordnet.

| Den virtuellen Adapter können Sie mit HMC erstellen. Weitere Informationen enthalten die Abschnitte
| zur Partitionierung bei eServer i5 und Konfiguration eines Virtual Ethernet-Adapters für i5/OS im IBM
| Systems Hardware Information Center. Wenn Sie ein partitionsübergreifendes Virtual Ethernet-Netzwerk
| von einem Server ohne HMCs auf einen Server mit einem HMC migrieren, müssen Sie virtuelle Ethernet-
| Adapter zur Verwendung des HMC und zusätzliche Ethernet-Leitungsbeschreibungen erstellen, um die
| erforderlichen Zuordnungen herzustellen. Beachten Sie hierbei, dass Windows-Server innerhalb derselben
| Partition auch kommunizieren können, indem sie dieselbe Virtual Ethernet-Portnummer verwenden.

Externe Netzwerke

| Mit einem integrierten Windows-Server können Sie in derselben Weise an externen Netzwerken teilneh-
| men wie mit einem herkömmlichen PC-Server. Hierfür gibt es verschiedene Möglichkeiten. Auf einem
| über IXA oder iSCSI angeschlossenen integrierten Server sind PCI-Erweiterungssteckplätze verfügbar.
| Daher können Sie jeden beliebigen integrierten Netzwerkadapter verwenden oder wie bei einem PC eine
| Netzwerkadapterkarte installieren. Ein IXS ist ein PC-Server auf einer Karte, die in einem PCI-Steckplatz
| in der iSeries installiert ist. Er verfügt über keine PCI-Erweiterungssteckplätze. Bestimmte IXS-Einheiten
| können auch zur Steuerung des benachbarten iSeries-PCI-Steckplatzes des für die Installation verwendete-
| ten Steckplatzes benutzt werden und auf diese Weise einen iSeries-Netzwerkadapter "übernehmen".
| Außerdem enthalten die IXS-Modelle des Typs 2892 und 4812 einen integrierten Ethernet-Netzwerk-
| adapter.

Unter „Externe Netzwerke“ auf Seite 125 wird beschrieben, wie Netzwerkadapterkarten für den IXS oder
die xSeries installiert und für integrierte Server konfiguriert werden.

Softwarekonzepte

| i5/OS bietet Unterstützung für die Definition, Konfiguration und Verwaltung von integrierten Servern;
| der Hardwaretyp spielt dabei keine Rolle. Die folgenden Diagramme enthalten eine Beschreibung der
| i5/OS-Objekte, die für die diversen Hardwarekonfigurationen verwendet werden.

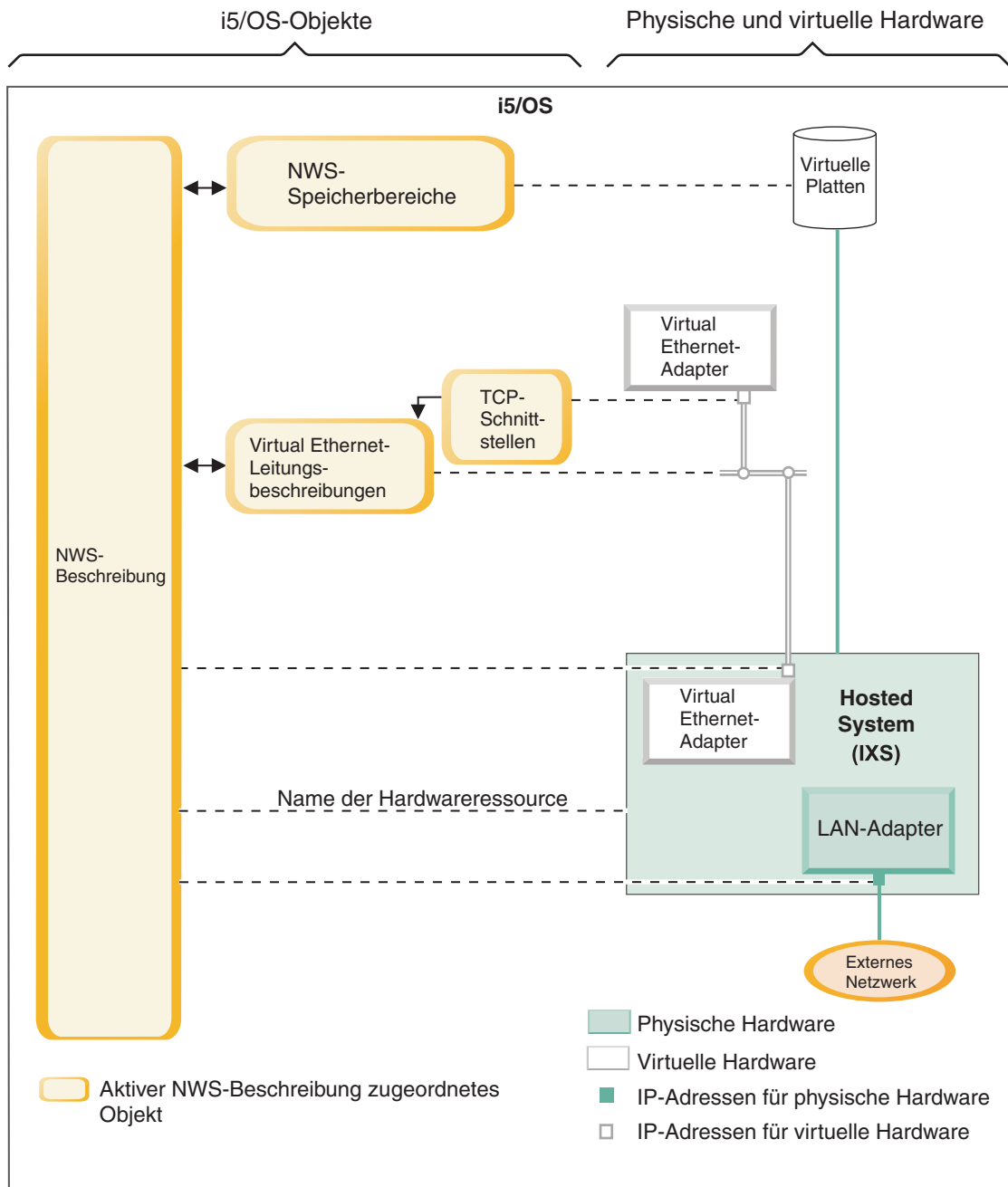
| Unter „Hardwarekonzepte“ auf Seite 14 finden Sie eine Beschreibung der unterstützten Hardware-
| konfigurationen.

| Informationen über die i5/OS-Softwarekonfiguration finden Sie in folgenden Abschnitten:

- | • „Integrierter xSeries-Server (IXS) und über integrierten xSeries-Adapter (IXA) angeschlossene
| xSeries-Server“ auf Seite 39
- | • „xSeries- und IBM BladeCenter-Server mit iSCSI-Anschluss“ auf Seite 43
- | • „Über iSCSI angeschlossene xSeries- und BladeCenter-Server mit Netzsicherheit“ auf Seite 48

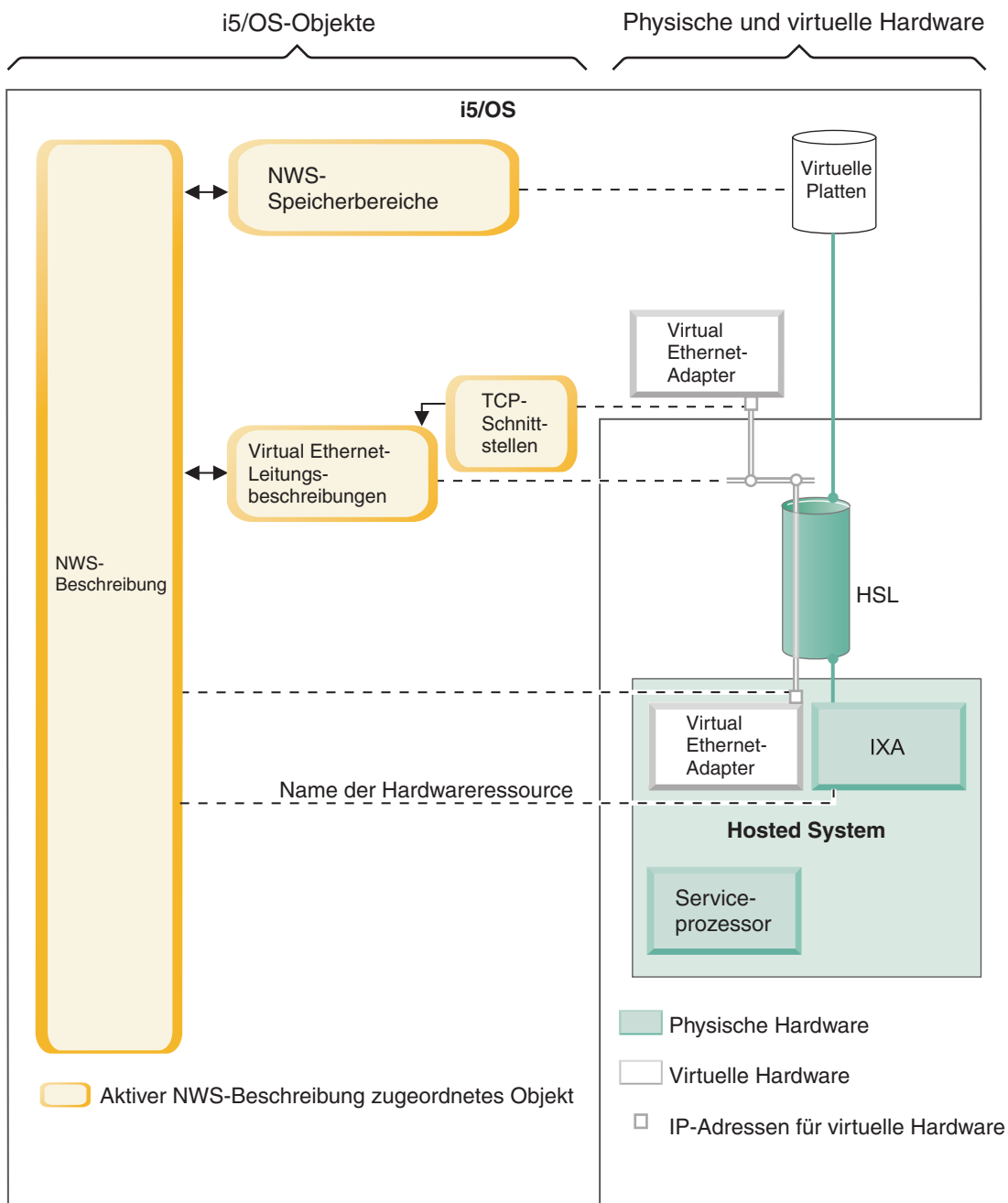
Integrierter xSeries-Server (IXS) und über integrierten xSeries-Adapter (IXA) angeschlossene xSeries-Server

IXS und xSeries-Server mit IXA-Anschluss werden von i5/OS auf ähnliche Weise dargestellt.



RZAHQ508-3

Abbildung 13. IXS-Konfigurationsobjekte in i5/OS



RZAHQ504-2

Abbildung 14. IXA-Konfigurationsobjekte in i5/OS

Abb. 14 zeigt die wichtigsten i5/OS-Objekte sowie die wichtigsten Hardwarekomponenten, die für IXS und xSeries-Server mit IXA-Anschluss verwendet werden.

| Die Objekte in Abb. 13 auf Seite 39 und Abb. 14 auf Seite 40 werden in den folgenden Abschnitten
| beschrieben.

- | • „NWS-Beschreibung“
- | • „Name der Hardwareressource“
- | • „NWS-Speicherbereiche“ auf Seite 42
- | • „Virtual Ethernet-Leitungsbeschreibungen“ auf Seite 42
- | • „TCP/IP-Schnittstellen“ auf Seite 43
- | • „Systembus- und HSL-Datenfluss“ auf Seite 43

| **NWS-Beschreibung**

| Die NWS-Beschreibung (NWSD) in Abb. 13 auf Seite 39 und Abb. 14 auf Seite 40 ist das wichtigste i5/OS-
| Konfigurationsobjekt für alle Arten von integrierten Servern. Das NWSD-Objekt wird verwendet, um alle
| übrigen i5/OS-Objekte miteinander zu verknüpfen, die einen integrierten Server betreffen. Die NWSD
| enthält beispielsweise einen Verweis auf die Server-Hardware, Links zu den virtuellen Plattenlaufwerken
| und Verweise auf die Netzanschlüsse, die vom Server verwendet werden, sowie zahlreiche weitere Ser-
| ver-Attribute. Die NWSD des Servers wird mit Hilfe des i5/OS-Befehls INSWNTSVR (Windows-Server
| installieren) sowie mehreren anderen i5/OS-Objekten erstellt, die vom Server benötigt werden.

| Der i5/OS-Befehl CRTNWSD (NWS-Beschreibung erstellen) enthält eine Beschreibung der in der NWSD
| enthaltenen Werte.

| Bei integrierten Servern wird die Hardware von IXS und xSeries-Servern mit IXA-Anschluss von i5/OS
| gesteuert.

- | • Ein integrierter Server wird durch Anhängen seiner NWSD gestartet. Damit wird der Boot-Vorgang des
| Windows-Betriebssystems eingeleitet.
- | • Ein integrierte Server wird durch Abhängen seiner NWSD abgeschaltet. Damit wird der Systemab-
| schluss des Windows-Betriebssystems eingeleitet.
- | • Bei einem IXS kommuniziert i5/OS direkt mit der IXS-Hardware, um die Tasks zum Starten und Been-
| den auszuführen.
- | • Bei einem xSeries-Server mit IXA-Anschluss kommuniziert i5/OS über einen HSL-Bus (High Speed
| Link) mit dem im xSeries-Server installierten IXA, um die Tasks zum Starten und Beenden einzuleiten.
| Der IXA seinerseits kommuniziert mit dem Serviceprozessor (SP) des xSeries-Systems, um die Tasks
| zum Starten und Beenden auszuführen.

| **Anmerkung:** Da der IXA eine fest verdrahtete Verbindung zum xSeries-Serviceprozessor bereitstellt,
| wird kein i5/OS-Objekt benötigt, um die Merkmale des xSeries-Serviceprozessors zu kon-
| figurieren.

| **Name der Hardwareressource**

| Die Server-Hardware für IXS und xSeries-Server mit IXA-Anschluss wird von i5/OS in Form eines
| Hardwareressourcennamens (z. B. LIN23) dargestellt. Ein Verweis auf den Namen der Hardwareressource
| für einen IXS oder einen xSeries-Server mit IXA-Anschluss wird im NWSD-Objekt gespeichert. Weitere
| Informationen können Sie Abb. 13 auf Seite 39 und Abb. 14 auf Seite 40 entnehmen.

| **Anmerkung:** Da die Hardware eines IXS oder eines xSeries-Servers mit IXA-Anschluss über den
| Hardwareressourcennamen in der NWSD definiert wird, kann die Hardware, auf der ein
| integrierter Server ausgeführt wird, problemlos gewechselt werden. Dies ist von Vorteil,
| wenn die Hardware des IXS oder des xSeries-Servers mit IXA-Anschluss ausfällt. In einem
| solchen Fall kann schnell und einfach auf eine kompatible Ausweichhardware (Hot-Spare-
| Hardware) gewechselt werden, mit der der integrierte Server dann erneut gestartet werden
| kann. Weitere Informationen über die "Hot-Spare-Funktionalität" finden Sie unter „Hot-
| Spare zwischen Server-Hardware“ auf Seite 166.

| **NWS-Speicherbereiche**

| Ein NWS-Speicherbereich (NWSSTG) repräsentiert ein virtuelles Plattenlaufwerk, das vom Server verwendet wird. Weitere Informationen können Sie Abb. 13 auf Seite 39 und Abb. 14 auf Seite 40 entnehmen. Die Größe eines virtuellen Plattenlaufwerks kann zwischen 1 MB und 1000 GB liegen. Je nach Serverkonfiguration können bis zu 64 virtuelle Plattenlaufwerke mit einem Server verlinkt werden, daher kann die Speicherkapazität eines integrierten Servers zwischen einigen Gigabyte und vielen Terabyte liegen. Die virtuellen Plattenlaufwerke werden zunächst als standalone Objekte erstellt und dann durch Angabe der NWSD mit dem jeweiligen integrierten Server verlinkt.

| Jeder Server verfügt über mindestens zwei virtuelle Plattenlaufwerke, die automatisch vom Befehl INSWNTSVR erstellt werden. Benutzerdefinierte virtuelle Plattenlaufwerke sind ebenfalls möglich.

- | • Das Systemlaufwerk (normalerweise C:) enthält das Windows-Server-Betriebssystem (z. B. Windows Server 2003).
- | • Das Installationslaufwerk (normalerweise D:) enthält eine Kopie der Windows-Serverinstallationsmedien sowie den Teil des Codes für den i5/OS Integrated Server Support (Produkt 5722-SS1, Option 29), der auf dem Windows-Server ausgeführt wird. Das Installationslaufwerk wird während des Windows-Installationsprozesses sowie bei jedem Serverstart verwendet, um Konfigurationsdaten von i5/OS an den Server zu übertragen.
- | • Für Serveranwendungen und -daten werden normalerweise weitere benutzerdefinierte Laufwerke verwendet.

| Der tatsächliche Plattenspeicher für die virtuellen Plattenlaufwerke wird aus dem integrierten i5/OS-Dateisystem (IFS) zugeordnet. Die virtuellen Plattenlaufwerke können aus dem Standardsystemplattenpool (auch: Systemzusatzspeicherpool oder System-ASP), aus einem benutzerdefinierten Plattenpool oder aus einem unabhängigen Plattenpool (IASP) zugeordnet werden.

| Weitere Informationen über virtuelle Plattenlaufwerke finden Sie in Kapitel 9, „Speicherverwaltung“, auf Seite 167.

| **Anmerkungen:**

- | 1. Da es sich bei virtuellen Plattenlaufwerken um Objekte im i5/OS-IFS handelt, kann das vollständige Image eines virtuellen Plattenspeichers mit den i5/OS-Befehlen SAV (Sichern) und RST (Zurückspeichern) gesichert werden. Die auf einem virtuellen Plattenlaufwerk enthaltenen Dateien können unter i5/OS individuell gesichert werden. Dies kann auf Dateiebene mit dem Dateisystem QNTC (Network Client) im IFS oder mit Hilfe einer nativen Windows-Sicherungsanwendung erfolgen. Weitere Informationen finden Sie in Kapitel 12, „Integrierte Windows-Server sichern und zurückspeichern“, auf Seite 199.
- | 2. Obwohl Speicherbereiche aus dem IFS zugeordnet werden, werden vom IFS keine Speicheroperationen ausgeführt, solange der integrierte Server angehängt ist. Das bedeutet, dass Operationen wie die Journalfunktion nicht aktiviert werden.

| **Virtual Ethernet-Leitungsbeschreibungen**

| Eine Virtual Ethernet-Leitungsbeschreibung wird für die Konfiguration eines iSeries Virtual Ethernet-Netzwerks verwendet, an dem ein integrierter Server beteiligt ist. Weitere Informationen können Sie Abb. 13 auf Seite 39 und Abb. 14 auf Seite 40 entnehmen. Mittels einer Leitungsbeschreibung wird der integrierte Server so konfiguriert, dass er über das Virtual Ethernet-PTP-Netzwerk mit i5/OS kommuniziert. Ebenfalls mittels einer Leitungsbeschreibung wird der integrierte Server so konfiguriert, dass er über ein partitionsinternes oder ein partitionsübergreifendes Virtual Ethernet-Netzwerk mit anderen integrierten Servern oder logischen Partitionen kommuniziert. Weitere Informationen über Virtual Ethernet-Netzwerke finden Sie unter „Konzepte für den Netzwerkbetrieb“ auf Seite 29.

| **Anmerkung:** Für physische Netzwerkadapter, die ggf. Bestandteil des integrierten Servers sind, werden keine Leitungsbeschreibungen verwendet. Die physischen Adapter werden unter Windows mit Hilfe der normalen Methoden zur Netzwerkadapterkonfiguration konfiguriert.

| **TCP/IP-Schnittstellen**

| Mittels einer TCP/IP-Schnittstelle wird die TCP/IP-Adresse für die i5/OS-Seite des Virtual Ethernet-PTP-Netzwerks konfiguriert. Weitere Informationen können Sie Abb. 13 auf Seite 39 und Abb. 14 auf Seite 40 entnehmen.

| **Anmerkung:** Die TCP/IP-Adresse für die Windows-Seite des Virtual Ethernet-PTP-Netzwerks wird über den Parameter für die TCP/IP-Portkonfiguration (TCPPORTCFG) in der NWSD konfiguriert.

| **Systembus- und HSL-Datenfluss**

| Die Übertragung der SCSI-Plattenlaufwerksdaten und die Virtual Ethernet-Daten zwischen i5/OS und dem integrierten Server erfolgt über den iSeries-Systembus (bei einem IXS) oder eine HSL-Verbindung zwischen einem E/A-Tower und dem iSeries-System (bei einem IXA). Weitere Informationen können Sie Abb. 13 auf Seite 39 und Abb. 14 auf Seite 40 entnehmen. Im Wesentlichen werden die SCSI-Plattenlaufwerks- und Virtual Ethernet-Protokolle in den normalen iSeries-Systembus/HSL-Datenübertragungsprotokollen eingebunden (im Tunnelungsverfahren übertragen).

| **xSeries- und IBM BladeCenter-Server mit iSCSI-Anschluss**

| i5/OS stellt xSeries- und IBM BladeCenter-Server mit iSCSI-Anschluss in ähnlicher Weise dar wie IXS und xSeries-Server mit IXA-Anschluss. Die iSCSI-Technologie macht jedoch zusätzliche i5/OS-Objekte und Konfigurationsdaten erforderlich, die für IXS und xSeries-Server mit IXA-Anschluss nicht erforderlich sind. Da Server mit iSCSI-Anschluss über ein Ethernet-Netzwerk mit dem iSeries-System verbunden sind (und nicht über eine Systembus/HSL-Anschlusseinrichtung, die für IXS und IXA verwendet wird), werden zusätzliche Konfigurationsdaten für die Identifikation und Kommunikation mit dem xSeries- oder IBM BladeCenter-Server im Netzwerk benötigt. Da Server mit iSCSI-Anschluss mit anderen Systemen im Ethernet-Netzwerk koexistieren können, kann außerdem die Sicherheit der Datenübertragung und des Datenflusses zwischen i5/OS und den Servern mit iSCSI-Anschluss von Bedeutung sein. Das folgende Diagramm zeigt, wie Server mit iSCSI-Anschluss von i5/OS dargestellt werden.

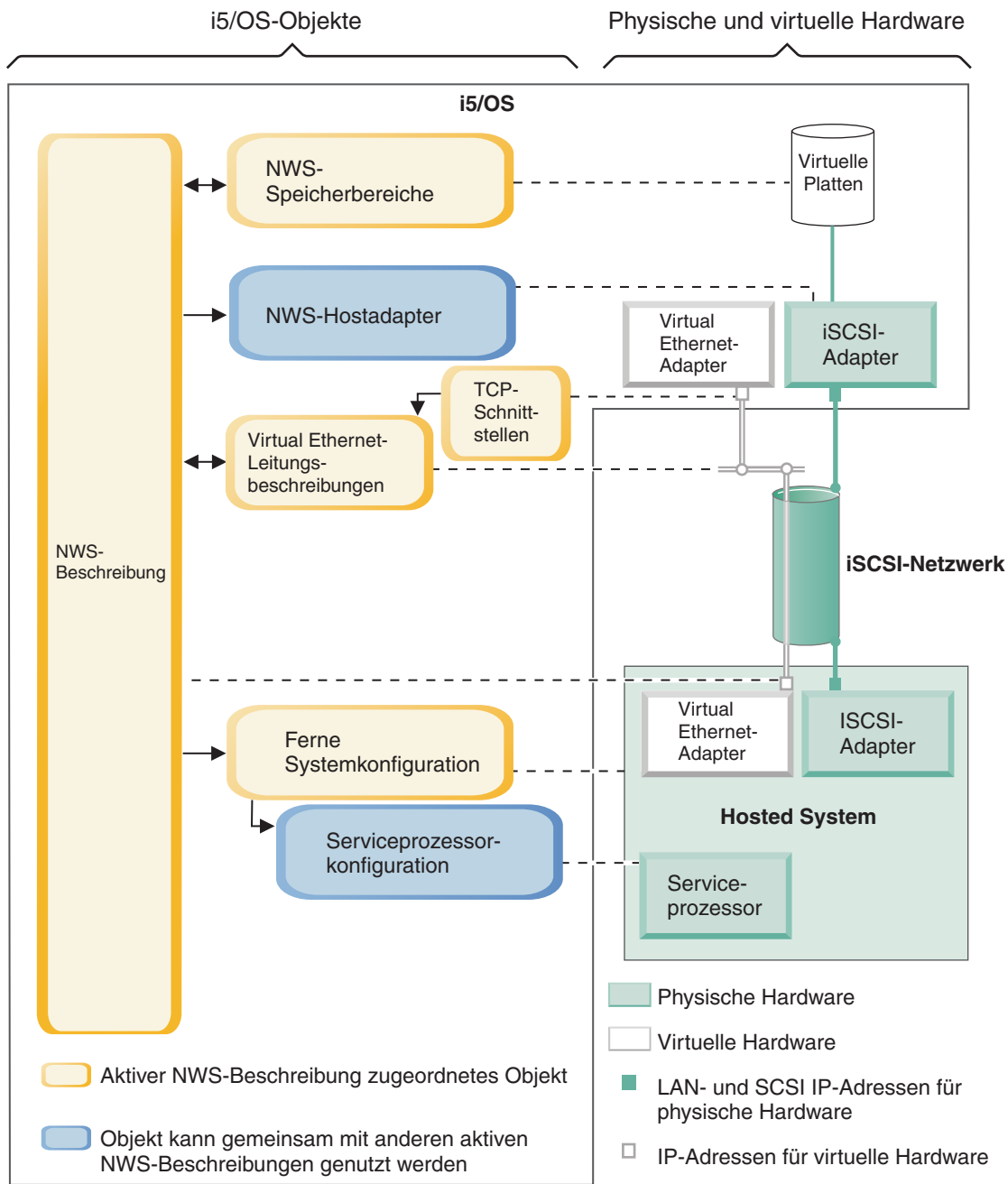


Abbildung 15. iSCSI-Konfigurationsobjekte in i5/OS ohne Netzsicherheit

Abb. 15 zeigt die wichtigsten i5/OS-Objekte sowie die wichtigsten Hardwarekomponenten, die für xSeries- oder IBM BladeCenter-Server mit iSCSI-Anschluss verwendet werden, wenn keine Netzsicherheit verwendet wird.

| Die Objekte in Abb. 15 auf Seite 44 werden in den folgenden Abschnitten beschrieben.

- | • „NWS-Hostadapter“
- | • „Konfiguration des fernen Systems“
- | • „Konfiguration für Serviceprozessor“ auf Seite 46
- | • „NWS-Beschreibung“ auf Seite 46
- | • „NWS-Speicherbereiche“ auf Seite 47
- | • „Datenfluss“ auf Seite 47
- | • „Virtual Ethernet-Leitungsbeschreibungen“ auf Seite 42
- | • „TCP/IP-Schnittstellen“ auf Seite 43

| Informationen über die i5/OS-Objekte, die für xSeries- und IBM BladeCenter-Server mit iSCSI-Anschluss gelten, die Netzsicherheit verwenden, können Sie Abb. 16 auf Seite 48 entnehmen.

| **NWS-Hostadapter**

| Das in Abb. 15 auf Seite 44 dargestellte Einheitenbeschreibungsobjekt für den NWS-Hostadapter (NWSH) ist der iSCSI-Hostbusadapter (HBA), der von der iSeries-Seite der iSCSI-Verbindung verwendet wird:

- | • Er identifiziert den iSeries-Hardwareressourcennamen (z. B. LIN33) für den iSCSI-HBA.
- | • Er definiert, wie Kommunikationsfehler protokolliert werden, sowie entsprechende Wiederherstellungs-
informationen.
- | • Er definiert die Internet-Adressen, Ports u.s.w. für die SCSI- und LAN-Schnittstellen auf dem iSCSI-
HBA.

| Die iSeries kann über mehrere iSCSI-HBAs verfügen, von denen jeder einem NWSH-Objekt zugeordnet ist.

- | • Jede NWSH kann von mehreren integrierten Servern gemeinsam genutzt werden. In Konfigurationen, bei denen die Bandbreite keine Rolle spielt, führt dies zur Kostensenkung.
- | • Jeder integrierte Server kann mehrere NWSHs benutzen. Dadurch sind mehrere SCSI- und Virtual Ethernet-Datenpfade zwischen der iSeries und den xSeries- oder IBM BladeCenter-Systemen möglich, was eine höhere Bandbreite und Verbindungsredundanz bedeutet.

| **Konfiguration des fernen Systems**

| Ein NWS-Konfigurationsobjekt für ein fernes System (NWSCFG Typ RMTSYS) (Abb. 15 auf Seite 44) repräsentiert den über iSCSI angeschlossenen xSeries- oder IBM BladeCenter-Server:

- | • Es identifiziert die Server-Hardware mittels Seriennummer, Typ und Modell.
- | • Es enthält Konfigurationsdaten für die iSCSI-Hostbusadapter (HBAs), die vom xSeries- oder IBM BladeCenter-Server verwendet werden.
- | • Es enthält Werte, die für das Booten des Servers erforderlich sind (z. B. die Angabe, von welchem iSCSI-Adapter gebootet werden soll).
- | • Es enthält einen Verweis auf das NWSCFG-Objekt für den Serviceprozessor (siehe unten), mit dem der xSeries- oder IBM BladeCenter-Server gesteuert wird.
- | • Die Konfiguration des fernen Systems kann wahlweise Werte für den Schutz des Server-Bootvorgangs enthalten.

| Der xSeries- oder IBM BladeCenter-Server kann über mehrere iSCSI-HBAs verfügen. Dadurch sind mehrere SCSI- und Virtual Ethernet-Datenpfade zwischen der iSeries und den xSeries- oder IBM BladeCenter-Systemen möglich, was eine höhere Bandbreite und Verbindungsredundanz bedeutet.

| Das Konfigurationsobjekt für das ferne System eines integrierten Servers wird mit einem Parameter in der NWSD angegeben.

Konfiguration für Serviceprozessor

Ein NWS-Konfigurationsobjekt für einen Serviceprozessor (NWSCFG Typ SRVPRC) (Abb. 15 auf Seite 44) repräsentiert den xSeries-Serviceprozessor oder das IBM BladeCenter-Managementmodul:

- Es identifiziert die Hardware des Serviceprozessors oder des Managementmoduls mittels Seriennummer, Typ und Modell.
- Es definiert, wie der Serviceprozessor oder das Managementmodul auf dem Ethernet-Netzwerk unter Verwendung der Internetadresse oder des Hostnamens lokalisiert wird.
- Das Serviceprozessorobjekt kann wahlweise Werte für den Schutz der Datenübertragung zwischen i5/OS und dem Serviceprozessor enthalten.

Anmerkung: Bei xSeries-Servern mit iSCSI-Anschluss besteht eine Eins-zu-eins-Beziehung zwischen dem Serviceprozessorobjekt und der Konfiguration des fernen Systems, da jeder Serviceprozessor nur einen xSeries-Server steuert. Bei IBM BladeCenter-Servern mit iSCSI-Anschluss kann jedoch eine Eins-zu-viele-Beziehung zwischen dem Serviceprozessorobjekt und der Konfiguration des fernen Systems bestehen, da jedes Managementmodul jeden der IBM BladeCenter-Server steuern kann, die sich im IBM BladeCenter-Gehäuse befinden. Daher nutzen bei IBM BladeCenter-Servern mit iSCSI-Anschluss mehrere Konfigurationen für ferne Systeme dasselbe Serviceprozessorobjekt gemeinsam.

NWS-Beschreibung

Das in Abb. 15 auf Seite 44 dargestellte Objekt für die NWS-Beschreibung (NWSB) entspricht im Wesentlichen dem in Abb. 14 auf Seite 40, bis auf folgende Unterschiede:

- Es enthält einen Verweis auf ein Konfigurationsobjekt für ein fernes System, statt eines iSeries-Hardwareressourcennamens.
- Im Gegensatz zu einem Server mit IXA-Anschluss, der eine IXA-Karte im xSeries-System verwendet, um den gesamten SCSI- und Virtual Ethernet-Datenfluss zu verwalten, können bei einem Server mit iSCSI-Anschluss sowohl die iSeries als auch die xSeries über mehrere iSCSI-Hostbusadapter (HBAs) verfügen. Dadurch sind mehrere SCSI- und Virtual Ethernet-Datenpfade zwischen der iSeries und den xSeries- oder IBM BladeCenter-Systemen möglich, was eine höhere Bandbreite und Verbindungsredundanz bedeutet.
- Sie können einen oder mehrere Speicherpfade definieren. Speicherpfade geben die NWSH-Objekte an, die den iSCSI-HBAs zugeordnet sind, die vom integrierten Server verwendet werden. Sie können angeben, welcher Speicherpfad für den SCSI-Datenfluss der einzelnen virtuellen Plattenlaufwerke verwendet werden soll. Durch das Zuordnen der virtuellen Plattenlaufwerke zu unterschiedlichen Speicherpfaden, können Sie zwecks größerer Bandbreite den gesamten Workload des SCSI-Serverdatenflusses über die iSCSI-HBAs der Speicherpfade verteilen.
- Sie können eine Gruppe mit mehreren Pfaden definieren, die wiederum eine Untergruppe der konfigurierten Speicherpfade bildet. Anschließend können Sie ein virtuelles Plattenlaufwerk dieser Mehrfachpfadgruppe statt einem bestimmten Speicherpfad zuordnen. Dies hat den Vorteil, dass der Workload des SCSI-Datenflusses für dieses virtuelle Plattenlaufwerk automatisch an einen der anderen iSCSI-HBAs in der Mehrfachpfadgruppe weitergeleitet wird, falls der iSCSI-HBA für einen der NWSHs in der Mehrfachpfadgruppe oder die Netzverbindung zum iSCSI-HBA ausfällt. Diese Möglichkeit bietet Verbindungsredundanz und höhere Verfügbarkeit.
- Sie können einen oder mehrere Virtual Ethernet-Pfade definieren. Diese Virtual Ethernet-Pfade geben die NWSH-Objekte an, die vom integrierten Server verwendet werden. Sie können angeben, welcher NWSH für jeden Virtual Ethernet-Port verwendet werden soll, der vom integrierten Server verwendet wird. Durch das Zuordnen unterschiedlicher Virtual Ethernet-Ports zu unterschiedlichen NWSHs, können Sie zwecks größerer Bandbreite den gesamten Workload des Virtual Ethernet-Serverdatenflusses über die iSCSI-HBAs der Virtual Ethernet-Pfade verteilen.
- Ebenso wie bei IXS oder Servern mit IXA-Anschluss wird die Hardware der über iSCSI angeschlossenen xSeries- oder IBM BladeCenter-Server von i5/OS gesteuert.

- Ein Server mit iSCSI-Anschluss wird ebenso gestartet und beendet wie ein IXS oder ein Server mit IXA-Anschluss (siehe Abb. 14 auf Seite 40), nämlich durch An- bzw. Abhängen der NWS für diesen Server.
- Bei einem über iSCSI angeschlossenen xSeries- oder IBM BladeCenter-Server kommuniziert i5/OS über ein Ethernet-Netzwerk mit dem Serviceprozessor (SP) für das xSeries-System oder mit dem IBM BladeCenter-Managementmodul für den IBM BladeCenter-Server, um die Tasks zum Starten und Beenden auszuführen.

Bei der Leistungssteuerung der Server-Hardware besteht der Hauptunterschied zwischen den IXS/IXA-Konfigurationen und der iSCSI-Konfiguration darin, dass die Server-Hardware für IXS oder Server mit IXA-Anschluss vom iSeries-Hardwareressourcenamen identifiziert wird, während sie bei Servern mit iSCSI-Anschluss vom Konfigurationsobjekt für das ferne System identifiziert wird.

Anmerkung: Da der xSeries- oder IBM BladeCenter-Server, auf dem ein Server mit iSCSI-Anschluss ausgeführt wird, einfach über den Konfigurationsnamen für das ferne System in der NWS definiert wird, kann die Hardware, auf der ein integrierter Server mit iSCSI-Anschluss ausgeführt wird, problemlos gewechselt werden. Durch Ändern des Konfigurationsnamens für das ferne System, kann der xSeries- oder IBM BladeCenter-Server, von dem aus eine vorhandene NWS gebootet wird, durch einen Hot-Spare ersetzt werden. Weitere Informationen finden Sie unter „Hot-Spare zwischen Server-Hardware“ auf Seite 166.

NWS-Speicherbereiche

Die in Abb. 15 auf Seite 44 dargestellten NWS-Speicherbereichsobjekte (NWSSTG) sind im Wesentlichen mit denen in Abb. 14 auf Seite 40 identisch, bis auf folgende Unterschiede:

- Wenn das virtuelle Plattenlaufwerk mit der NWS verlinkt wird, muss angegeben werden, welcher der NWS-Speicherpfade für den SCSI-Datenfluss dieses virtuellen Plattenlaufwerks verwendet werden soll.
- Sie können einen bestimmten Speicherpfad oder die Mehrfachpfadgruppe auswählen, oder Sie können den Standard Speicherpfad übernehmen.

Weitere Informationen finden Sie unter „NWS-Speicherbereiche“ auf Seite 42.

Datenfluss

In Abb. 15 auf Seite 44 wird der Datenfluss des SCSI-Plattenlaufwerks und des Virtual Ethernet zwischen i5/OS und dem integrierten Server mit iSCSI-Anschluss über ein Ethernet-Netzwerk geleitet. Im Wesentlichen werden die SCSI-Plattenlaufwerks- und Virtual Ethernet-Protokolle in den normalen Ethernet-Netzwerkprotokollen eingebunden (im Tunnelungsverfahren übertragen).

Über iSCSI angeschlossene xSeries- und BladeCenter-Server mit Netz- sicherheit

Da Server mit iSCSI-Anschluss ein Netzwerk gemeinsam mit anderen Systemen nutzen können, ist es sinnvoll, die Netzverbindungen von iSCSI und dem Serviceprozessor zu schützen. Das folgende Diagramm zeigt die Objekte, die von i5/OS zur Konfiguration der Netzsicherheit für Server mit iSCSI-Anschluss verwendet werden.

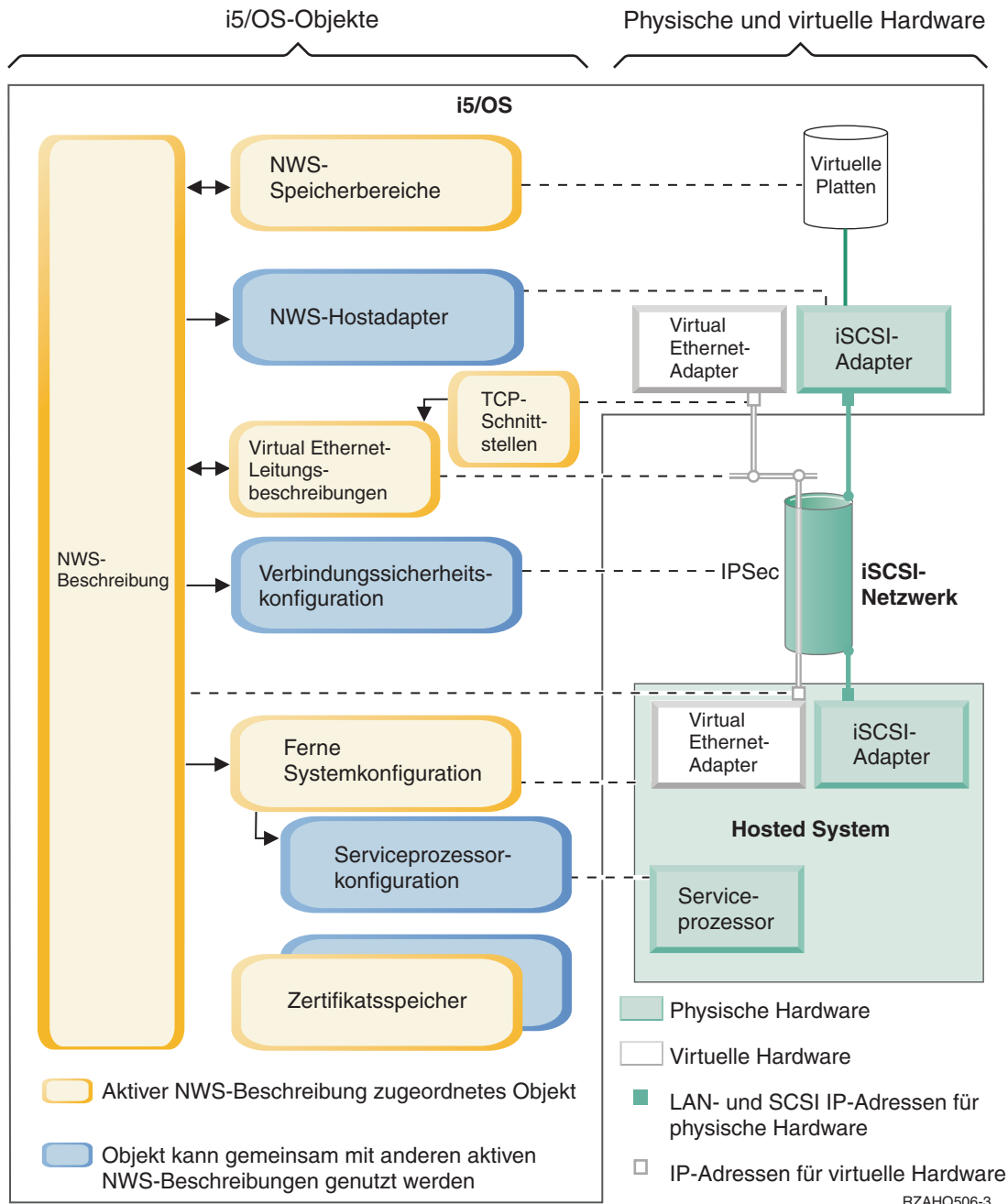


Abbildung 16. iSCSI-Konfigurationsobjekte in i5/OS mit Netzsicherheit

Abb. 16 zeigt die wichtigsten i5/OS-Objekte sowie die wichtigsten Hardwarekomponenten, die für xSeries- oder IBM BladeCenter-Server mit iSCSI-Anschluss verwendet werden, wenn Netzsicherheit verwendet wird.

| Die Objekte in Abb. 16 auf Seite 48 werden in den folgenden Abschnitten beschrieben.

- | • „Konfiguration des fernen Systems“
- | • „Konfiguration für Serviceprozessor“
- | • „Konfiguration für Verbindungssicherheit“
- | • „Zertifikatsspeicher“
- | • „NWS-Beschreibung“ auf Seite 46
- | • „NWS-Speicherbereiche“ auf Seite 47
- | • „Datenfluss“ auf Seite 47
- | • „Virtual Ethernet-Leitungsbeschreibungen“ auf Seite 42
- | • „TCP/IP-Schnittstellen“ auf Seite 43

| **Konfiguration des fernen Systems**

| Das in Abb. 16 auf Seite 48 dargestellte NWS-Konfigurationsobjekt für das ferne System (NWSCFG Typ RMTSYS) entspricht dem in „Konfiguration des fernen Systems“ auf Seite 45 beschriebenen Objekt für Abb. 15 auf Seite 44. Das hier gezeigte Objekt enthält jedoch CHAP-Protokollkonfigurationswerte, mit denen das ferne System beim erstmaligen Speicherzugriff authentifiziert wird.

| **Konfiguration für Serviceprozessor**

| Das in Abb. 16 auf Seite 48 dargestellte NWS-Konfigurationsobjekt für den Serviceprozessor (NWSCFG Typ SRVPRC) entspricht im Wesentlichen dem in „Konfiguration für Serviceprozessor“ auf Seite 46 beschriebenen Objekt für Abb. 15 auf Seite 44, bis auf folgende Unterschiede:

- | • Es enthält einen Benutzernamen und ein Kennwort für den Serviceprozessor, mit denen die Anmeldung beim Serviceprozessor erfolgt.
- | • Es enthält Informationen, die für die Verwaltung eines optionalen SSL-Zertifikats erforderlich sind, mit dem die Kommunikation zwischen i5/OS und dem Serviceprozessor geschützt wird.

| **Konfiguration für Verbindungssicherheit**

| Das in Abb. 16 auf Seite 48 dargestellte NWS-Konfigurationsobjekt für die Verbindungssicherheit (NWSCFG Typ CNNSEC) wird für den Schutz des SCSI- und Virtual Ethernet-Datenflusses zwischen i5/OS und dem xSeries- oder IBM BladeCenter-Server mit iSCSI-Anschluss verwendet.

- | • Es identifiziert eine Reihe von Regeln für die IP-Netzwerk-Sicherheit (IPSec), die für die verschiedenen Speicher- und Virtual Ethernet-Verbindungen gelten.
- | • Sie können entscheiden, welche Datenflüsse geschützt werden sollen und welche nicht. Sie können angeben, dass keine, einige oder alle Speicher- oder Virtual Ethernet-Verbindungen geschützt werden sollen. Sie können beispielsweise angeben, dass nur die Speicherdatenflüsse (SCSI) oder nur eine der Virtual Ethernet-Verbindungen geschützt werden soll(en).
- | • Die zu schützenden Datenflüsse kennzeichnen Sie, indem Sie die entsprechenden Sicherheitsregeln für die NWSD-Parameter für Speicherpfade und Virtual Ethernet-Pfade angeben.
- | • Bei Verwendung von IPSec werden die SCSI- und Virtual Ethernet-Datenflüsse zwischen i5/OS und dem integrierten Server mit iSCSI-Anschluss verschlüsselt, und die normalen Ethernet-Netzwerkprotokolle erhalten eine zusätzliche Kapselungsschicht (Tunnelung).

| **Zertifikatsspeicher**

| Zertifikate werden für den Schutz der Kommunikation zwischen i5/OS und dem Hosted System für zahlreiche Funktionen verwendet. Die Zertifikate sind in den folgenden i5/OS-Zertifikatsspeichern enthalten:

- | • **Der i5/OS-Systemzertifikatsspeicher** Wenn Sie Zertifikate manuell aus einer externen Quelle in den Serviceprozessor des Hosted Systems importieren, werden die entsprechenden Zertifikate der anerkannten Zertifizierungsstelle hier gespeichert. Der Systemzertifikatsspeicher wird von vielen i5/OS-Anwendungen gemeinsam genutzt.

- **Ein Zertifikatsspeicher, der der Serviceprozessorkonfiguration zugeordnet ist.** Dieser Zertifikatsspeicher wird automatisch erstellt. Die enthaltenen Zertifikate werden nur für die Kommunikation mit Hosted Systemen eingesetzt, die die entsprechende Serviceprozessorkonfiguration verwenden. Dieser Zertifikatsspeicher wird gemeinsam genutzt, wenn mehrere Hosted Systeme (z. B. IBM BladeCenter-Blades) ein und dieselbe Serviceprozessorkonfiguration verwenden. Zertifikate werden unter folgenden Bedingungen in diesem Zertifikatsspeicher gespeichert:
 - Wenn Sie in der Serviceprozessorkonfiguration die Option zum Generieren eines Zertifikats wählen.
 - Wenn Sie ein Zertifikat vom Serviceprozessor des Hosted Systems mit der entsprechenden Serviceprozessorkonfiguration synchronisieren.
- **Ein Zertifikatsspeicher, der der NWS-Beschreibung zugeordnet ist.** Dieser Zertifikatsspeicher wird automatisch erstellt und verwaltet. Dieser Speicher ist für Zertifikate vorgesehen, die intern vom i5/OS Integrated Server Support generiert und verwendet werden (z. B. für Zertifikate, die bei der Registrierung von Benutzern auf dem Hosted System verwendet werden). Die Zertifikate in diesem Zertifikatsspeicher werden nur für die Kommunikation mit Hosted Systemen eingesetzt, die die entsprechende NWS-Beschreibung verwenden.

Konzepte für Hochverfügbarkeit

iSeries- und xSeries-Integration und Speichervirtualisierung sind innovative Optionen, mit denen Sie die Zuverlässigkeit und Wiederherstellbarkeit der Windows-Serverumgebung verbessern können. Hosted Systeme können mit Hilfe einer oder mehrere der folgenden Technologien eine höhere Verfügbarkeit bieten.

Hot-Spare-Hardware

Hot-Spare-Hardware bietet eine Möglichkeit, ein schnelles Recovery nach bestimmten Hardwarefehlern durchzuführen. Dies kann die Ausfallzeit des Servers von Stunden oder gar Tagen auf Minuten reduzieren. Bei Hosted Systemen bestehen zwei Möglichkeiten, die Hot-Spare-Hardware zur Minimierung der durch Hardwarefehler verursachten Ausfallzeit einzusetzen:

1. Hosted System-Hardware, einschließlich integrierter xSeries-Server, xSeries-Server, die über einen integrierten xSeries-Adapter angeschlossen sind sowie xSeries- oder IBM BladeCenter-Server, die über einen iSCSI-Hostbusadapter angeschlossen sind, kann durch Hot-Spare-Hardware ersetzt werden. Wenn die Hardware des Hosted Systems ausfällt, können Sie die Plattenimages des Hosted Systems rasch auf kompatible Ersatzhardware umschalten und das Hosted System erneut starten. Weitere Informationen finden Sie unter „Hot-Spare zwischen Server-Hardware“ auf Seite 166.
2. Bei Servern mit iSCSI-Anschluss können die iSeries-iSCSI-Zielhostbusadapter (iSCSI-HBAs) durch Hot-Spare-Hardware ersetzt werden. Wenn der iSCSI-HBA eines Hosted Systems ausfällt, können Sie rasch auf einen Ersatz-iSCSI-HBA umschalten und das Hosted System erneut starten. Weitere Informationen finden Sie unter „Hot-Spare zwischen lokalen iSCSI-Hostadaptern“ auf Seite 143.

iSCSI-Multipath

Ein Hosted System kann redundante iSCSI-Datenpfade für den Zugriff auf virtuelle Platten verwenden, die von i5/OS betrieben werden. Dies wird erzielt, indem eine Gruppe aus mindestens zwei iSCSI-HBAs definiert und anschließend angegeben wird, dass der Zugriff auf eine bestimmte virtuelle Platte über eine Gruppe statt einen einzelnen iSCSI-HBA erfolgen soll. Bei dieser Konfiguration kann der Zugriff auf die Daten auf einer virtuellen Platte über irgendeinen der iSCSI-HBAs in der Gruppe erfolgen.

Ein Vorteil der Konfiguration von Mehrfachpfaden (Multipaths) besteht darin, dass das Hosted System beim Ausfall einer der iSCSI-HBAs in der Gruppe weiterhin ohne Unterbrechung auf die Platten zugreifen kann, die für die Mehrfachpfadgruppe konfiguriert sind, indem es irgendeinen der anderen iSCSI-HBAs in der Gruppe verwendet. Weitere Informationen finden Sie unter „Erweiterte iSCSI-Unterstützung“ auf Seite 22.

| **Microsoft Windows-Clusterdienst (MSCS)**

| Hosted Server können MSCS zur Bereitstellung von echtzeitorientierten Anwendungsübernahmen verwenden, falls es zu Hardware- oder Softwarefehlern des Hosted Systems kommt. Vom Benutzer eingeleitete Übernahmen können einen Server in den Offline-Status versetzen, damit Wartungs- oder Sicherungsaufgaben erfolgen können, während die Anwendung auf dem oder den übrigen Servern im Cluster fortgesetzt wird. Weitere Informationen finden Sie unter „Windows-Clusterdienst“ auf Seite 108.

| **Sicherheitskonzepte**

| Vorgehensweisen zur Implementierung der in diesem Abschnitt beschriebenen Sicherheitskonzepte finden Sie unter „Sicherheit zwischen i5/OS und Hosted Systemen konfigurieren“ auf Seite 138. Es gibt mehrere Arten von Sicherheit.

- | • „Sicherheit für IXS und Systeme mit IXA-Anschluss“
- | • „Sicherheit für Systeme mit iSCSI-Anschluss“

| **Sicherheit für IXS und Systeme mit IXA-Anschluss**

| Speicherdaten und Virtual Ethernet-Daten für IXSs und Systeme mit IXA-Anschluss werden über physisch sichere iSeries-Systembusse und HSL-Kabel übertragen.

| **Sicherheit für Systeme mit iSCSI-Anschluss**

| Die iSCSI-Technologie nutzt die niedrigen Kosten und die Vertrautheit des Ethernet- und IP-Netzbetriebs. Die Flexibilität des Ethernet- und IP-Netzbetriebs ermöglicht Systemen mit iSCSI-Anschluss die gemeinsame Nutzung von Hardware sowie eine größere Reichweite und Bandbreite durch Hinzufügen von Hardware. Diese Vertrautheit und Flexibilität erfordert jedoch auch eine entsprechende Netzsicherheit.

| Jeder der unterschiedlichen Netzwerktypen, die von Systemen mit iSCSI-Anschluss verwendet werden, hat seinen eigenen Sicherheitsaspekt.

| **Verbindungssicherheit für Serviceprozessor**

| Einer oder mehrere der folgenden Mechanismen können Bestandteil der Serviceprozessorsicherheit sein.

- | • Serviceprozessorkennwort
- | • Secure Sockets Layer (SSL)
- | • Netzwerkisolation und physische Sicherheit

| **iSCSI-Netzsicherheit**

| Es gibt zwei Arten von iSCSI-Datenaustausch im Netz.

- | • Einer oder mehrere der folgenden Mechanismen können Bestandteil der Speichersicherheit sein.
 - | – Challenge Handshake Authentication Protocol (CHAP)
 - | – IP-Netzsicherheit (IPSec)
 - | – Firewalls
 - | – Netzwerkisolation, physische Sicherheit und Sicherheitsgateways
- | • Einer oder mehrere der folgenden Mechanismen können Bestandteil der Virtual Ethernet-Sicherheit sein.
 - | – IP-Netzsicherheit (IPSec)
 - | – Firewalls
 - | – Netzwerkisolation, physische Sicherheit und Sicherheitsgateways
 - | – Wenn bei der Benutzerregistrierung oder fernen Befehlsübergabe sensible Daten über das Virtual Ethernet-PTP gesendet werden, verwenden diese Anwendungen außerdem eine SSL-Verbindung zwischen i5/OS und Windows. Weitere Informationen zur Benutzerregistrierung finden Sie unter „Konzepte für Benutzer und Gruppen“ auf Seite 54.

| **Serviceprozessorkennwort**

| Dieses Kennwort wird von i5/OS verwaltet und verwendet, wenn der iSeries-Server einen Datenaustausch mit dem Serviceprozessor des Hosted Systems startet. Der Serviceprozessor überprüft das Kennwort, um sicherzustellen, dass die i5/OS-Konfiguration gültig ist. Neue Serviceprozessoren haben einen Standardnamen und ein Standardkennwort. i5/OS bietet die Möglichkeit, das Kennwort zu ändern.

| **Serviceprozessor-SSL**

| Diese Art von SSL können Sie nur aktivieren, wenn Sie über die entsprechende Serviceprozessorhardware verfügen. SSL verschlüsselt den Datenverkehr über die Serviceprozessorverbindung und stellt sicher, dass der Serviceprozessor gültig ist. Die Authentifizierung basiert auf einem digitalen Zertifikat vom Serviceprozessor, das manuell oder automatisch in i5/OS installiert wird. Dieses Zertifikat unterscheidet sich von den digitalen Zertifikaten, die für die SSL-Verbindung zwischen i5/OS und Windows benutzt werden.

| **SSL-Verbindung zwischen i5/OS und Windows**

| Bestandteil der Windows-Umgebung auf der iSeries sind die Benutzerregistrierung und die ferne Befehlsübergabe, mit der sensible Daten über das Virtual Ethernet-PTP übertragen werden können. Diese Anwendungen bauen automatisch eine SSL-Verbindung auf, um den Austausch sensibler Daten im Netz zu verschlüsseln und sicherzustellen, dass beide am Datenaustausch beteiligten Seiten aufgrund automatisch installierter digitaler Zertifikate authentifiziert sind. Diese Zertifikate unterscheiden sich von den digitalen Zertifikaten, die für Serviceprozessor-SSL benutzt werden. Diese Sicherheitsfunktion wird standardmäßig bereitgestellt und ist nicht konfigurierbar. Dateidaten, Befehlsergebnisse und der Datenverkehr für andere Anwendungen werden von dieser SSL-Verbindung nicht geschützt.

| **Challenge Handshake Authentication Protocol (CHAP)**

| CHAP bietet Schutz vor der Gefahr, dass ein nicht autorisiertes System den iSCSI-Namen eines autorisierten Systems für den Speicherzugriff verwendet. CHAP führt keine Verschlüsselung des Datenaustauschs im Netz durch, sondern entscheidet, welches System auf einen i5/OS-Speicherpfad Zugriff erhält.

| Bestandteil des CHAP ist die Konfiguration eines geheimen Schlüssels, der sowohl i5/OS als auch dem Hosted System bekannt sein muss. Kurze geheime CHAP-Schlüssel können sichtbar gemacht werden, wenn der CHAP-Paketaustausch mit einem LAN-Sniffer aufgezeichnet und offline analysiert wird. Der geheime CHAP-Schlüssel sollte wahlfrei und lang genug sein, damit diese Angriffsmethode chancenlos bleibt. i5/OS kann einen entsprechenden geheimen Schlüssel generieren. Ein Hosted System verwendet denselben geheimen CHAP-Schlüssel für den Zugriff auf sämtliche konfigurierten i5/OS-Speicherpfade.

| CHAP wird zwar nicht standardmäßig aktiviert, wird aber dringend empfohlen.

| **IP-Netzsicherheit (IPSec)**

| IPSec verschlüsselt Speicher- und Virtual Ethernet-Datenverkehr auf dem iSCSI-Netzwerk. Das zugehörige Protokoll Internet Key Exchange (IKE) stellt sicher, dass die kommunizierenden IP-Endpunkte gültig sind.

| Zur Aktivierung von IPSec sind zwei Bedingungen erforderlich:

- | 1. Sowohl die iSeries als auch des Hosted Systems müssen über spezielle iSCSI-HBAs mit Hochgeschwindigkeits-IPSec-Unterstützung verfügen.
- | 2. Sie müssen einen vorab bekannten gemeinsamen Schlüssel konfigurieren. i5/OS kann entsprechende Schlüssel generieren. Wenn die iSeries oder das Hosted System über mehrere iSCSI-HBAs verfügt, können unterschiedliche vorab bekannte gemeinsame Schlüssel unterschiedlichen IP-Adresspaaren zugeordnet werden. Alle weiteren Details von IPSec und IKE werden automatisch ausgeführt. IPSec-Unterstützung in i5/OS-TCP/IP und Windows-TCP/IP sind nicht betroffen.

| IPSec-HBAs stellen eine Filterfunktion zur Verfügung, die die Kommunikation mit nicht konfigurierten IP-Adressen blockiert. IPSec-HBAs führen diese Filterfunktion auch dann aus, wenn die IPSec-Verschlüsselung nicht mittels eines vorab bekannten gemeinsamen Schlüssels aktiviert ist.

| IPSec für Virtual Ethernet wird nicht direkt auf die Virtual Ethernet-Endpunkte angewandt, sondern auf die iSCSI-HBAs, die den Tunnel durch das iSCSI-Netzwerk bilden. Wenn mehrere Windows-Server mit iSCSI-Anschluss über Virtual Ethernet miteinander kommunizieren, sind die IPSec-Konfigurationen der einzelnen Server folglich voneinander unabhängig. Ein Server kann beispielsweise IPSec aktivieren und mit anderen Windows-Servern kommunizieren, die statt IPSec die physische Sicherheit verwenden. Server müssen nicht zwingend denselben vorab bekannten gemeinsamen IPSec-Schlüssel verwenden, um miteinander kommunizieren zu können.

| **Firewalls**

| Zwischen einem gemeinsam genutzten Netzwerk und dem iSeries-Server kann eine Firewall zum Schutz der iSeries vor unerwünschtem Datenaustausch im Netz errichtet werden. Ebenso kann eine Firewall zwischen einem gemeinsam genutzten Netzwerk und einem Hosted System errichtet werden, um das Hosted System vor unerwünschtem Datenaustausch im Netz zu schützen.

| Der Datenverkehr von Systemen mit iSCSI-Anschluss verfügt über die folgenden Attribute, die sich bei der Konfiguration einer Firewall als hilfreich erweisen können:

- | • iSCSI-HBAs haben statische IP-Adressen (es gibt einen DHCP-Bootmodus, aber die verwendeten IP-Adressen sind statisch vorkonfiguriert).
- | • Deterministische und konfigurierbare UDP- und TCP-Ports. Jeder Virtual Ethernet-Adapter auf dem Hosted System verwendet einen anderen UDP-Port für die Übertragung im Tunnelungsverfahren durch das iSCSI-Netzwerk. Virtual Ethernet-Pakete werden folgendermaßen vom übergeordneten hin zum inneren Header eingebunden:
 - | – MAC- und IP-Header für den iSCSI-HBA unter Verwendung von LAN-Adressen (keine SCSI-Adressen).
 - | – UDP-Header. Informationen über die wahlfreie Kontrolle der UDP-Portauswahl finden Sie unter „Firewall konfigurieren“ auf Seite 142.
 - | – MAC- und IP-Header für den Virtual Ethernet-Adapter.

| IPSec-HBAs stellen eine Firewall-ähnliche Funktion zur Verfügung, die die Kommunikation mit nicht konfigurierten IP-Adressen blockiert, selbst wenn IPSec nicht mittels eines vordefinierten bekannten gemeinsamen Schlüssels aktiviert ist.

| **Netzwerkisolation und physische Sicherheit**

| Die Netzwerkisolation minimiert das Risiko eines Datenzugriffs durch nicht berechtigte Einheiten sowie der Datenänderung während die Daten das Netz durchqueren. Ein isoliertes Netzwerk kann mit einem dedizierten Ethernet-Switch oder einem dedizierten virtuellen lokalen Netz (VLAN) auf einem physischen VLAN-Switch/-Netzwerk erstellt werden. Behandeln Sie bei der Konfiguration eines VLAN-Switch einen in Ihrem iSeries-Server installierten iSCSI-HBA als Einheit, die das VLAN nicht erkennt.

| Die physische Sicherheit beinhaltet physische Barrieren, die in einem bestimmten Rahmen (versperrte Gehäuse, Räume, Gebäude, u.s.w.) Zugriffsschutz für Netzeinheiten und -endpunkte bieten.

Konzepte für Benutzer und Gruppen

Einer der Hauptvorteile, die sich bei Verwendung der Windows-Umgebung auf der iSeries ergeben, ist die Benutzeradministrationsfunktion für i5/OS- und Windows-Benutzerprofile. Mit der Benutzeradministrationsfunktion können Administratoren vorhandene Benutzer- und Gruppenprofile von i5/OS in Microsoft Windows registrieren. Die Funktion wird im Folgenden ausführlicher erläutert.

Registrierung

Als Registrierung wird der Prozess bezeichnet, mit dem ein i5/OS-Benutzerprofil oder -Gruppenprofil für die Integrationssoftware registriert wird.

Die Registrierung findet automatisch statt, wenn sie durch ein Ereignis ausgelöst wird. Dies kann beispielsweise die Ausführung des Befehls CHGNWSUSRA zum Registrieren eines Benutzers oder einer Gruppe, die Aktualisierung des Kennworts oder der Benutzerattribute für das i5/OS-Benutzerprofil durch den Windows-Benutzer oder das erneute Starten des integrierten Servers sein. Falls der integrierte Windows-Server aktiv ist, werden die Änderungen sofort vorgenommen. Ist der integrierte Server zu diesem Zeitpunkt abgehängt, werden die Änderungen beim nächsten Starten des Servers ausgeführt.

Windows-Domänen und lokale Server

Die Registrierung kann entweder für eine Windows-Domäne oder für einen lokalen Server erfolgen. Eine Windows-Domäne besteht aus einer Reihe von Ressourcen (Anwendungen, Computer, Drucker), die miteinander vernetzt sind. Ein Benutzer hat in der Domäne einen einzigen Account und muss sich nur an der Domäne anmelden, um auf alle Ressourcen zugreifen zu können. Ein integrierter Server kann ein Mitgliedsserver einer Windows-Domäne sein und i5/OS-Benutzeraccounts in die Windows-Domäne integrieren.

Im Gegensatz dazu wird ein integrierter Server, auf dem i5/OS-Benutzer registriert werden und der nicht zu einer Domäne gehört, als **lokaler Server** bezeichnet. In diesem Fall werden die Benutzeraccounts nur auf diesem integrierten Server erstellt.

Anmerkung: Beim Windows-Netzwerkbetrieb können Gruppen von lokalen Servern in Windows-Arbeitsgruppen flexibel zusammengefasst werden. Wenn Sie beispielsweise die Position "Netzwerkumgebung" öffnen und auf "Arbeitsgruppencomputer anzeigen" klicken, wird eine Liste der Computer angezeigt, die zur gleichen Arbeitsgruppe gehören.

i5/OS-Gruppen in Microsoft Windows

Bei der Installation eines integrierten Servers werden in Microsoft Windows zwei Gruppen von Benutzern erstellt.

- **AS400_Users** Jeder i5/OS-Benutzer wird bei seiner ersten Registrierung in der Windows-Umgebung in die Gruppe "AS400_Benutzer" gestellt. Sie können einen Benutzer in der Windows-Umgebung aus dieser Gruppe entfernen. Bei der nächsten Aktualisierung, die durch den iSeries-Server vorgenommen wird, wird der Benutzer jedoch ersetzt. Anhand dieser Gruppe kann gut geprüft werden, welche i5/OS-Benutzerprofile in der Windows-Umgebung registriert sind.
- **AS400_Permanent_Users** Benutzer in dieser Gruppe können durch den iSeries-Server nicht aus der Windows-Umgebung entfernt werden. Diese Gruppe dient dazu, das versehentliche Löschen von Windows-Benutzern durch Aktionen zu verhindern, die unter i5/OS ausgeführt werden. Selbst wenn das Benutzerprofil aus i5/OS gelöscht wird, ist der Benutzer in der Windows-Umgebung weiterhin vorhanden. Die Zugehörigkeit zu dieser Gruppe wird - anders als die zur Gruppe "AS400_Benutzer" - über die Windows-Umgebung gesteuert. Wenn Sie einen Benutzer aus dieser Gruppe löschen, wird er bei einer i5/OS-Aktualisierung nicht ersetzt.

i5/OS-Benutzerprofilattribut LCLPWDMGT verwenden

Für die Verwaltung von Kennwörtern für Benutzerprofile gibt es zwei Methoden.

- **Herkömmlicher Benutzer:** Sie können auswählen, dass i5/OS-Kennwörter und Windows-Kennwörter identisch sein sollen. Die Verwendung von identischen Kennwörtern in i5/OS und Windows legen Sie fest, indem Sie den Attributwert für das i5/OS-Benutzerprofil auf LCLPWDMGT(*YES) setzen. Bei Verwendung von LCLPWDMGT(*YES) verwalten registrierte Windows-Benutzer ihre eigenen Kennwörter unter i5/OS. Das Attribut LCLPWDMGT wird mit dem i5/OS-Befehl CRTUSRPRF (Benutzerprofil erstellen) oder CHGUSRPRF (Benutzerprofil ändern) angegeben.
- **Windows-Benutzer:** Sie können auswählen, dass die Kennwörter von registrierten Windows-Profilen unter Windows verwaltet werden sollen. Durch die Angabe von LCLPWDMGT(*NO) wird das Kennwort für das i5/OS-Benutzerprofil auf *NONE gesetzt. Bei dieser Einstellung können registrierte Windows-Benutzer ihr Kennwort in Windows verwalten, ohne dass i5/OS das Kennwort überschreibt.

Weitere Informationen enthält der Abschnitt „Arten von Benutzerkonfigurationen“ auf Seite 56.

Enterprise Identity Mapping (EIM) unter i5/OS verwenden

| Die EIM-Unterstützung von i5/OS kann auf zwei unterschiedlichen Wegen genutzt werden. Mit Hilfe
| von Funktionen in der Windows-EIM-Registrierungsdatenbank können Sie eine EIM-Zuordnung automa-
| tisch erstellen. Durch das Definieren von EIM-Zuordnungen kann i5/OS die Windows-Einzelanmeldung
| unter Verwendung einer Authentifizierungsmethode wie beispielsweise Kerberos unterstützen. Das auto-
| matische Erstellen und Löschen von EIM-Quellenzuordnungen für Windows erfolgt, wenn bei Verwen-
| dung der i5/OS-Befehle CRTUSRPRF, CHGUSRPRF oder DLTUSRPRF (Benutzerprofil erstellen, ändern
| bzw. löschen) für den Parameter EIMASSOC die Werte *TARGET, *TGTSRC oder *ALL angegeben wer-
| den.

Sie können EIM-Zuordnungen im Windows-EIM-Register aber auch manuell definieren. Wenn unter i5/OS eine EIM-Zielzuordnung und unter Windows eine EIM-Quellenzuordnung für ein i5/OS-Benutzerprofil definiert wird, kann das registrierte i5/OS-Benutzerprofil in Windows mit einem abweichenden Benutzerprofilnamen definiert werden.

| **Anmerkung:** SBMNWSCMD, QNTC und Sicherungsvorgänge auf Dateiebene funktionieren nur mit
| Kerberos-EIM-Zuordnungen. i5/OS-Benutzerprofile, die verschiedenen Windows-
| Benutzernamen zugeordnet sind, die eine Windows-EIM-Registrierungsdatenbank verwen-
| den, werden nicht erkannt. Diese Operationen versuchen nach wie vor entsprechende
| Namen zu verwenden.

Weitere Informationen finden Sie unter „EIM (Enterprise Identity Mapping)“ auf Seite 191.

Vorhandene Windows-Benutzerprofile registrieren

Sie können auch einen Benutzer registrieren, der bereits in der Windows-Umgebung vorhanden ist. Das Kennwort des Benutzers muss unter i5/OS mit dem Kennwort des bereits vorhandenen Windows-Benutzers (oder der Gruppe) identisch sein. Weitere Informationen enthält der Abschnitt „Überlegungen zu Kennwörtern“ auf Seite 59.

Schablonen für die Benutzerregistrierung

Die einem Benutzer während der Registrierung zugewiesenen Berechtigungen und Eigenschaften können mit Hilfe von Schablonen für die Benutzerregistrierung angepasst werden. Weitere Informationen enthält der Abschnitt „Schablonen für die Benutzerregistrierung“ auf Seite 58.

Wird bei der Registrierung keine Schablone verwendet, erhalten Benutzer die folgenden Standardeinstellungen:

- Benutzer werden Mitglied der Gruppe "AS400_Benutzer" sowie entweder der Gruppe "Benutzer" auf einem lokalen integrierten Windows-Server oder der Gruppe "Domänenbenutzer" in einer Windows-Domäne.
- i5/OS überwacht das Kennwort, das Ablaufdatum des Kennworts, die Beschreibung und den Aktivierungsstatus aus i5/OS für den Benutzer.

i5/OS-Gruppen registrieren

| Bisher war nur die Rede von der Registrierung einzelner i5/OS-Benutzerprofile in der Windows-Umgebung. Es besteht aber auch die Möglichkeit, ganze i5/OS-Gruppen zu registrieren. Wenn Sie anschließend Benutzer zu den i5/OS-Gruppen hinzufügen, die in der Windows-Umgebung registriert wurden, werden diese Benutzer automatisch auch in der Windows-Umgebung erstellt und registriert.

Registrierung in mehreren Domänen vornehmen

Benutzer und Gruppen können in mehreren Domänen registriert werden, dies ist im Allgemeinen jedoch nicht erforderlich. In den meisten Windows-Umgebungen bestehen "Trust Relationships" (Vertrauensbeziehungen) zwischen den einzelnen Domänen. Es reicht in solchen Fällen aus, den Benutzer in einer Domäne zu registrieren, da er aufgrund der "Trust Relationships" automatisch Zugriff auf die anderen Domänen erhält. Weitere Informationen zu "Trust Relationships" enthält die Windows-Dokumentation.

Registrierungsdaten sichern und zurückspeichern

Nachdem Sie die Benutzer- und Gruppenregistrierungen definiert haben, müssen Sie die Registrierungsdefinitionen sichern. Zum Sichern der Registrierungsdaten können Sie die Optionen 21 oder 23 des Menüs GO SAVE, den Befehl SAVSECDTA (Sicherungsdaten speichern) oder die API QSRSAVO verwenden. Das Zurückspeichern der Benutzerprofile erfolgt mit dem Befehl RSTUSRPRF (Benutzerprofile zurückspeichern) unter Verwendung der Werte USRPRF(*ALL) oder SECDTA(*PWDGRP).

Parameter PRPDMNUSR verwenden

Wenn mehrere Server Mitgliedserver derselben Domäne sind, können Sie verhindern, dass auf jedem Mitgliedserver eine doppelte Registrierung für die Domäne erfolgt. Verwenden Sie hierzu den Parameter PRPDMNUSR (Domänenbenutzer weitergeben) in dem Befehl CHGNWD (NWS-Beschreibung ändern) oder CRTNWS (NWS-Beschreibung erstellen). Weitere Informationen finden Sie unter „Benutzer QAS400NT“ auf Seite 193.

Arten von Benutzerkonfigurationen

Integrierte Windows-Benutzer lassen sich in drei Grundarten unterteilen:

- **Herkömmlicher Benutzer (Kennwortverwaltung durch i5/OS)**
Benutzer werden standardmäßig mit dieser Art definiert. Ein solcher Benutzer arbeitet sowohl unter Windows als auch unter i5/OS. Das i5/OS-Kennwort und das Windows-Kennwort werden synchronisiert. Bei jedem Neustart des integrierten Windows-Servers wird das Kennwort des Benutzers auf das i5/OS-Kennwort zurückgesetzt. Kennwortänderungen können nur unter i5/OS erfolgen. Diese Benutzerart wird für die Ausführung von Sicherungen auf Dateiebene und von fernen Windows-Befehlen empfohlen. Um einen Windows-Benutzer auf diese Konfiguration zu setzen, wird das Benutzerprofilattribut LCLPWDMGT unter Verwendung des Befehls WRKUSRPRF (Mit Benutzerprofil arbeiten) auf den Wert *YES gesetzt.

- **Benutzer mit Windows-Kennwortverwaltung**

Ein solcher Benutzer führt die meisten Aufgaben unter Windows aus und meldet sich nur selten oder auch gar nicht bei i5/OS an. Wenn sich der Benutzer bei i5/OS anmeldet, muss er eine Authentifizierungsmethode wie beispielsweise Kerberos verwenden, um auf i5/OS zugreifen zu können. Dieser Aspekt wird im nächsten Abschnitt (Windows-Benutzer mit konfiguriertem Enterprise Identity Mapping (EIM)) erläutert.

Wenn für einen i5/OS-Benutzer das Benutzerprofilattribut LCLPWDMGT(*NO) definiert wird, wird das Kennwort für das i5/OS-Benutzerprofil auf *NONE gesetzt. Das Kennwort für die i5/OS-Registrierung wird gesichert, bis die Windows-Registrierung erfolgreich ausgeführt wurde. Nachdem der i5/OS-Benutzer für Windows registriert wurde, kann der Windows-Benutzer sein Kennwort unter Windows ändern und verwalten, ohne dass i5/OS das Kennwort überschreibt. Die bei dieser Methode entstehende Umgebung ist sicherer, da weniger Kennwörter verwaltet werden müssen. Angaben zur Erstellung eines Benutzers dieser Art können Sie unter „Benutzerprofilattribut LCLPWDMGT ändern“ auf Seite 190 nachlesen.

- **Windows-Benutzer mit automatisch konfigurierten EIM-Zuordnungen**

Bei Angabe des Wertes *TGT, TGTSRC oder *ALL für das Benutzerprofilattribut EIMASSOC kann der integrierte Server automatisch EIM-Quellenzuordnungen für Windows definieren. Die Verwendung der automatischen Definitionen für die Zuordnungen vereinfacht die Konfiguration von EIM. Angaben zur Erstellung eines Benutzers dieser Art können Sie unter „EIM (Enterprise Identity Mapping)“ auf Seite 191 nachlesen.

- **Windows-Benutzer mit manuell konfigurierten EIM-Zuordnungen**

Der Benutzer kann auswählen, dass EIM-Quellenzuordnungen für Windows manuell definiert werden sollen. Mit dieser Methode kann für das i5/OS-Benutzerprofil, das registriert werden soll, ein abweichender Name für das Windows-Benutzerprofil festgelegt werden. Der Benutzer muss eine i5/OS-Zielzuordnung für das i5/OS-Benutzerprofil und auch eine Windows-Quellenzuordnung für die gleiche EIM-Kennung manuell definieren.

Table 1. Arten von Benutzerkonfigurationen

Benutzerart	Verfügbare Funktion	Benutzerprofildefinition
Herkömmlich	<ul style="list-style-type: none"> • Volle Funktionalität von i5/OS und Windows • Einfache Konfiguration • Kennwortänderung erfolgt unter i5/OS • Benutzer-ID und Kennwort von i5/OS und Windows sind identisch • Empfohlen für Systemadministratoren, für Benutzer mit häufiger Verwendung von i5/OS oder für Systeme, die Benutzerprofile mit i5/OS sichern und wiederherstellen 	LCLPWDMGT(*YES) und keine definierte EIM-Quellenzuordnung für Windows
Benutzer mit Windows-Kennwortverwaltung	<ul style="list-style-type: none"> • Kennwortänderung kann unter Windows erfolgen. • Einfache Konfiguration • Windows-Kennwortverwaltung macht diese Konfiguration sicherer, da das i5/OS-Kennwort *NONE lautet. • i5/OS-Anmeldung erfordert eine Authentifizierungsmethode wie die von iSeries Navigator unterstützte i5/OS-Anmeldung mit Kerberos 	LCLPWDMGT(*NO)

Tabella 1. Arten von Benutzerkonfigurationen (Forts.)

Benutzerart	Verfügbare Funktion	Benutzerprofildefinition
Windows-Benutzer mit automatisch konfigurierten EIM-Zuordnungen	Automatische Erstellung von Windows-Quellenzuordnungen vereinfacht die Installation und Konfiguration von Anwendungen mit Kerberos-Unterstützung	Beispiel: EIMASSOC(*CHG *TARGET *ADD *CRTEIMID)
Windows-Benutzer mit manuell konfigurierten EIM-Zuordnungen	Benutzer kann EIM-Zuordnungen für registrierte i5/OS-Benutzerprofile abweichend von den Benutzerprofilen in Windows definieren.	Mit iSeries Navigator müssen EIM-Zielzuordnungen für i5/OS und Quellenzuordnungen für Windows manuell definiert werden

Schablonen für die Benutzerregistrierung

Eine Schablone für die Benutzerregistrierung ist ein Tool, mit dessen Hilfe i5/OS-Benutzer effizienter für die Windows-Umgebung registriert werden können. Statt viele neue Benutzer mit identischen Einstellungen manuell zu konfigurieren, können Sie Benutzer mit einer Schablone für die Benutzerregistrierung automatisch konfigurieren. Jede Schablone entspricht einem Windows-Benutzerprofil, das die Benutzerberechtigungen, wie z. B. Gruppenzugehörigkeit, Verzeichnispfade und Container für Organisationseinheiten definiert.

Bei der Registrierung von Benutzern und Gruppen aus i5/OS in der Windows-Umgebung kann eine Benutzerschablone angegeben werden, auf der die neuen Windows-Benutzer basieren sollen. Beispiel: Sie können eine Benutzerschablone mit dem Namen USRTEMP erstellen, die Mitglied der Windows-Servergruppen NTG1 und NTG2 ist. Unter i5/OS verfügen Sie über die Gruppe MGMT, die inklusive ihrer Mitglieder auf dem Windows-Server registriert werden soll. Bei der Registrierung geben Sie USRTEMP als Benutzerschablone an. Daraufhin werden automatisch alle Mitglieder der Gruppe MGMT den Gruppen NTG1 und NTG2 hinzugefügt.

Benutzerschablonen ersparen Ihnen die Einrichtung von Gruppenzugehörigkeiten für einzelne Benutzer. Darüber hinaus gewährleisten sie die Konsistenz der Attribute von registrierten Benutzern.

Benutzerschablonen können zu jeder Windows-Gruppe hinzugefügt werden, und zwar unabhängig davon, ob diese Gruppe über i5/OS registriert wurde oder nicht. Es können auch Benutzer mit einer Schablone registriert werden, die einer Gruppe angehören, die nicht über i5/OS registriert wurde. In diesem Fall werden die Benutzer jedoch zudem Mitglied der nicht registrierten Gruppe. i5/OS erkennt ausschließlich die Gruppen, die von i5/OS registriert wurden. Benutzer können daher nur mit Hilfe des Programms "Benutzer-Manager" unter Windows aus der Gruppe entfernt werden.

Wenn Sie eine Schablone zum Definieren der Registrierungsdaten eines neuen Benutzers verwenden und für die Schablone ein Ordner oder ein Verzeichnis mit **Pfad** oder **Verbinden mit** definiert ist, verfügt der neu erstellte Windows-Benutzer über dieselben Definitionen. Die Ordnerdefinitionen ermöglichen dem Benutzeradministrator, die Vorteile der Ordnerumleitung zu nutzen und die Anmeldung am Terminaldienst zu verwalten.


Wenn Sie eine Schablone zum Definieren der Registrierungsdaten eines neuen Benutzers verwenden und es sich bei der Schablone um ein Benutzerobjekt in einem Container für Organisationseinheiten des Windows Active Directory handelt, befindet sich das neu erstellte Windows-Benutzerobjekt im gleichen Container für Organisationseinheiten. Eine Organisationseinheit stellt eine Methode dar, um Benutzern die Möglichkeit zur Verwaltung und Steuerung von Ressourcen zu geben.

Es besteht die Möglichkeit, vorhandene Benutzerschablonen zu ändern. Die Änderungen wirken sich jedoch nur auf die Benutzer aus, die nach der Bearbeitung der Schablone registriert werden.

Schablonen werden nur bei der Erstellung eines in der Windows-Umgebung neu registrierten Benutzers verwendet. Dient die Registrierung zur Synchronisation eines vorhandenen Windows-Benutzers mit einem i5/OS-Gegenstück, ignoriert Windows die Schablone.

Eine ausführliche Beschreibung der Prozedur können Sie unter „Benutzerschablonen erstellen“ auf Seite 189 nachlesen.

Überlegungen zu Kennwörtern

1. Vergewissern Sie sich, dass das i5/OS-QRETSVRSEC-System auf 1 gesetzt ist. Sie können dazu den Befehl WRKSYSVAL (Mit Systemwerten arbeiten) verwenden. Wenn Sie das nicht tun, können Sie erst dann Benutzer bei Ihrem integrierten Windows-Server registrieren, wenn sich diese bei i5/OS anmelden.
Anmerkung: Dieser Systemwert ist ebenfalls für die Unterstützung des integrierten iSCSI-Servers erforderlich.
2. Es sollten nur i5/OS-Kennwörter verwendet werden, die den unter Windows zulässigen Zeichen und Kennwortlängen entsprechen, wenn der Benutzer registriert werden soll. Die Kennwortstufe in i5/OS kann so festgelegt werden, dass Benutzerprofilkennwörter mit einer Länge von 1-10 Zeichen oder mit einer Länge von 1-128 Zeichen zulässig sind. Eine i5/OS-Kennwortstufenänderung des Systemwertes QPWDLVL erfordert ein IPL.
3. Die i5/OS-Kennwortstufe 0 oder 1 unterstützt Kennwörter mit 1-10 Zeichen und begrenzt den Zeichensatz. Auf Stufe 0 oder 1 konvertiert i5/OS die Kennwörter für Windows in Kleinbuchstaben.
4. Die i5/OS-Kennwortstufen 2 oder 3 unterstützen Kennwörter mit 1-128 Zeichen sowie zusätzliche Zeichen, u. a. Groß- und Kleinschreibung. Auf Stufe 2 oder 3 von i5/OS bleibt die Groß-/Kleinschreibung von Kennwörtern für Windows erhalten.
5. Wenn die i5/OS-Kennwörter registrierter Benutzer ablaufen, laufen ebenfalls deren Kennwörter für Windows ab. Kennwörter können zwar unter Windows geändert werden, müssen in jedem Fall jedoch unter i5/OS ebenfalls geändert werden. Wird zuerst das i5/OS-Kennwort geändert, wird das Windows-Kennwort automatisch aktualisiert.
6. Lautet der i5/OS-Systemwert QSECURITY 10, benötigen die vorhandenen Windows-Benutzer kein Kennwort für die Anmeldung. Bei allen anderen Stufen des i5/OS-Systemwerts QSECURITY muss das Benutzerobjekt zur Anmeldung über ein Kennwort verfügen. Weitere Informationen zu Sicherheitsstufen finden Sie in der iSeries Security Reference. 
7. Bei Verwendung einer anderen Sprache als Englisch kann die Verwendung von anderen als invarianten Zeichen in Benutzerprofilen und Kennwörtern zu unvorhersehbaren Ergebnissen führen. Weitere Informationen zu den Zeichen im invarianten Zeichensatz finden Sie im Thema zur Globalisierung. Diese Aussage gilt nur, wenn der Systemwert QPWDLVL mit 0 oder 1 definiert ist. Wurde der Systemwert QPWDLVL auf 2 oder 3 gesetzt, können invariante Zeichen problemlos verwendet werden.

Kapitel 5. Windows-Umgebung auf der iSeries installieren und konfigurieren

Zur Einrichtung der Windows-Umgebung auf der iSeries müssen Hardware und zwei unterschiedliche Softwarekomponenten installiert werden: IBM i5/OS Integrated Server Support und das Betriebssystem Windows 2000 Server oder Windows Server 2003 von Microsoft.


So installieren und konfigurieren Sie die Windows-Umgebung auf der iSeries:


1. Prüfen Sie die Angaben auf der Website IBM iSeries Integrated xSeries solutions  (www.ibm.com/servers/eserver/series/integratedxseries). Vergewissern Sie sich, dass Sie die aktuellen Neuerungen und Informationen kennen.
2. Prüfen Sie, ob die jeweilige Site neueste Nachrichten und Informationen über die zu installierende Hardware enthält.
 - IXA install read me first 
(www.ibm.com/servers/eserver/series/integratedxseries/ixareadme)
 - iSCSI install read me first 
(www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme)
 - IXS install read me first 
(www.ibm.com/servers/eserver/series/integratedxseries/ixsreadme)
3. Prüfen Sie, ob Sie die richtige Hardware und Software verwenden.
 - a. „Hardwarevoraussetzungen“ auf Seite 62.
 - b. „Softwarevoraussetzungen“ auf Seite 64.
4. Installieren Sie ggfs. die Hardware für IXS oder Server mit IXA-Anschluss. Weitere Informationen finden Sie unter iSeries-Features installieren. Wählen Sie das Modell Ihres iSeries-Servers. Wählen Sie **PCI-Adapter** für einen IXS und **Integrated xSeries Adapter** für einen IXA aus. Wenn Sie einen iSCSI-HBA installieren, finden Sie die entsprechenden Installationsanweisungen in Schritt 6b.
5. Installieren Sie IBM iSeries Integrated Server Support.
 - a. „Installation von integrierten Windows-Servern vorbereiten“ auf Seite 64
 - b. „IBM i5/OS Integrated Server Support installieren“ auf Seite 69
6. Installieren Sie Microsoft Windows 2000 Server oder Windows Server 2003 auf dem integrierten Server.
 - a. „Installation des Windows-Servers planen“ auf Seite 70
 - b. „Windows 2000 Server oder Windows Server 2003 installieren“ auf Seite 98
7. Nachdem Sie die Installation abgeschlossen haben, konfigurieren Sie den integrierten Windows-Server.
 - a. „Codekorrekturen“ auf Seite 117. Diese Codekorrekturen beheben alle Fehler im Lizenzprogramm, die seit seiner Freigabe festgestellt wurden.
 - b. Kapitel 6, „Virtual Ethernet- und externe Netzwerke verwalten“, auf Seite 121
 - c. „Integrierten Windows-Server für automatisches Anhängen mit TCP/IP einstellen“ auf Seite 117

Hardwarevoraussetzungen

Zur Ausführung von integrierten Windows-Servern benötigen Sie die folgende Hardware:

1. Einen der folgenden integrierten xSeries-Server (IXSs), integrierten xSeries-Adapter (IXAs) oder iSCSI-HBAs.

Beschreibung	Feature-Code	Typ-Modell
Integrierter xSeries-Server (2,0 GHz)	4811 48124813	4812-001
Integrierter xSeries-Server (2,0 GHz)	4710	2892-002
Integrierter xSeries-Server (2,0 GHz)	4810	2892-002
Integrierter xSeries-Server (1,6 GHz)	2792	2892-001
Integrierter xSeries-Server (1,6 GHz)	2892	2892-001
Integrierter xSeries-Server (1,0 GHz)	2799	2890-003
Integrierter xSeries-Server (1,0 GHz)	2899	2890-003
Integrierter xSeries-Server (850 MHz)	2791	2890-002
Integrierter xSeries-Server (850 MHz)	2891	2890-002
Integrierter xSeries-Server (700 MHz)	2790	2890-001
Integrierter xSeries-Server (700 MHz)	2890	2890-001
Integrierter xSeries-Adapter, Modell 100	0092 ^{2,3}	2689-001
Integrierter xSeries-Adapter, Modell 200	0092 ^{2,4}	2689-002
Anmerkungen:		
1. Der IXA erfordert einen xSeries-Server. Für den xSeries-Server gelten möglicherweise zusätzliche Voraussetzungen. Weitere Informationen hierzu finden Sie auf der Website Integrated xSeries solutions (www.ibm.com/servers/eserver/series/integratedxseries)  .		
2. Die Hardware wird über das Buchungssystem als Maschinentyp 1519-100 bestellt.		
3. Die Hardware wird über das Buchungssystem als Maschinentyp 1519-200 bestellt.		

Anmerkung: Wenn Sie über integrierte Server-Hardware verfügen, die nicht in der obigen Tabelle aufgeführt ist, können Sie die Spezifikationen auf der Website IBM Integrated xSeries solutions  nachlesen.

Informationen zur Installation der Hardware finden Sie im Abschnitt „iSeries-Features installieren“. Eine Beschreibung von IXSs, IXAs und iSCSI-HBAs enthält der Abschnitt „Hardwarekonzepte“ auf Seite 14.

2. Einen iSeries-Server mit ausreichend freiem Plattenspeicherplatz, inklusive 100 MB für den Code der Software IBM i5/OS Integrated Server Support und 2047 MB zur Verwendung durch das Windows-Systemlaufwerk oder den NWS-Speicherbereich.

3. Für IXS-Systeme mindestens einen zugelassenen LAN-Port oder PCI-Adapter:

Beschreibung	Feature-Code	Unterstützt durch IXS-Hardwaretyp 4812	Unterstützt durch IXS-Hardwaretyp 2892	Unterstützt durch IXS-Hardwaretyp 2890
iSeries 1000/100/10 Mbit/s Ethernet-Adapter (Kupfer-UTP)	5701		X	
iSeries Gigabit-Ethernet-Adapter (1000 Mbit/s) (Glasfaser)	5700		X	
iSeries Gigabit-Ethernet-Adapter (1000/100/10 Mbit/s) (Kupfer-UTP)	2760			X
iSeries Gigabit-Ethernet-Adapter (1000 Mbit/s) (Glasfaser)	2743			X
iSeries 2892 Ethernet-Port (10/100 Mbit/s)	2892		X	
IBM iSeries Ethernet-Adapter (10/100 Mbit/s)	2838			X
Token-Ring-PCI-Adapter für hohe Geschwindigkeiten (100/16/4 Mbit/s)	2744		X	X
iSeries 4812 Ethernet-Port (1000/100/10 Mbit/s)	4812	X		

4. Einen SVGA-kompatiblen Monitor, eine Maus und eine Tastatur. Ein IXS ist nur mit einem einzigen Tastatur-/Mausport ausgestattet. Daher benötigen Sie außerdem ein Y-Kabel für Tastatur/Maus, um beides gleichzeitig anschließen zu können. Wenn Sie mehrere integrierte Server verwenden und nur jeweils einen verwalten wollen, ist es unter Umständen sinnvoll, einen Satz von E/A-Hardware für die integrierten Server gemeinsam zu verwenden und bei Bedarf umzuschalten.

5. Mindestens 128 MB Arbeitsspeicher (RAM) oder mindestens 256 MB Arbeitsspeicher, wenn Sie Windows 2003 Server verwenden. Dieser Arbeitsspeicher ist im integrierten Server installiert und muss separat bestellt werden.

6. Ein PC mit Microsoft Windows und iSeries Access (beinhaltet iSeries Navigator).

Anmerkung: iSeries Navigator wird für die meisten Konfigurationstasks für die Windows-Umgebung auf der iSeries bevorzugt.

Angaben zu weiteren Hardwarevoraussetzungen finden Sie in den folgenden Abschnitten:

- „Maschinenpoolvoraussetzungen“ auf Seite 66
- „Konzepte für den Netzwerkbetrieb“ auf Seite 29

Softwarevoraussetzungen

Sie benötigen die folgende Software:

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

So überprüfen Sie den Release-Level:

- a. Geben Sie in der i5/OS-Befehlszeile den Befehl Go LICPGM ein, und drücken Sie die Eingabetaste.
- b. Geben Sie im Feld "Auswahl" eine 10 ein, um die installierten Produkte anzuzeigen.
- c. Suchen Sie nach dem Produkt 5722SS1. Das daneben angezeigte Release ist die installierte Version. (In einigen Releases muss zuerst F11 gedrückt werden, bevor die Versionsnummer erscheint.)

2. IBM i5/OS Integrated Server Support (5722-SS1 Option 29) V5R4. Weitere Informationen finden Sie unter „IBM i5/OS Integrated Server Support installieren“ auf Seite 69.


3. IBM iSeries Navigator, der zum Lieferumfang von IBM iSeries Access for Windows (5722-XE1) gehört.

Anmerkungen:

- a. Wenn Sie iSeries Navigator auf einem Windows-PC installieren möchten, führen Sie eine vollständige oder eine angepasste Installation durch, und wählen Sie die wahlfreie Komponente "Verwaltung integrierter Server" aus.
- b. iSeries Navigator wird für die meisten Konfigurationstasks für die Windows-Umgebung auf der iSeries bevorzugt.

4. TCP/IP Connectivity Utilities für i5/OS V5R4 (5722-TC1).

5. Für IXS und Server mit IXA-Anschluss wird Microsoft Windows 2000 Server oder Windows Server 2003 benötigt. Für Server mit iSCSI-Anschluss wird Windows Server 2003 benötigt.

6. Alle erforderlichen Service-Packs für Microsoft Windows. Aktuelle Informationen zu den verfügbaren Service-Packs, die von IBM mit der i5/OS-Unterstützung für integrierte Server getestet wurden, finden Sie im Abschnitt über Anwendungen auf der Website IBM Integrated xSeries solutions .

Für iSCSI-Server benötigen Sie außerdem die folgende Software:

1. IBM Director 5.10

Anmerkung: IBM Director ist eine kostenfreie Option der Virtualization Engine (5733-VE2), für die zusätzliche Softwarevoraussetzungen gelten. Weitere Informationen finden Sie im Abschnitt über die Installation von IBM Director unter i5/OS im IBM Systems Software Information Center.

2. IBM i5/OS Digital Certificate Manager (5722-SS1 Option 34) V5R4

3. IBM HTTP Server für iSeries (5722-DG1)

Weitere Informationen zu der Software, die für die Installation erforderlich ist, enthält das Handbuch iSeries Softwareinstallation. 

Installation von integrierten Windows-Servern vorbereiten

Mit Hilfe einiger vorbereitender Maßnahmen können Sie eine problemlose Installation sicherstellen.

1. Prüfen Sie, ob Sie über die erforderliche Berechtigung für die Installation verfügen. Sie benötigen die Sonderberechtigungen *IOSYSCFG, *ALLOBJ und *JOBCTL für i5/OS. Zur Ausführung von Schritt 8 in dieser Prüfliste ist die Sonderberechtigung *SECADM erforderlich. Informationen zu Sonder-

berechtigungen finden Sie in der iSeries Security Reference. 

2. Prüfen Sie die Angaben unter „Maschinenpoolvoraussetzungen“ auf Seite 66.
3. Vergewissern Sie sich, dass die Zeitsynchronisation richtig konfiguriert ist. Weitere Informationen enthält der Abschnitt „Zeitsynchronisation“ auf Seite 67.

4. „i5/OS-TCP/IP für integrierte Windows-Server“ auf Seite 67.
5. Legen Sie fest, wie viele integrierte Windows-Server und Teilnetze für Ihre Anforderungen benötigt werden.

Bei der Installation eines Servers mit iSCSI-Anschluss benötigt jeder iSCSI-HBA für iSeries zwei feste IP-Adressen und jedes Hosted xSeries-System oder IBM BladeCenter mindestens zwei IP-Adressen für iSCSI. Weitere Informationen zu den Voraussetzungen für IP-Adressen finden Sie unter „Konzepte für den Netzwerkbetrieb“ auf Seite 29.

Wenn Ihr Unternehmen feste IP-Adressen verwendet (Unternehmen, die DHCP verwenden, können den integrierten Windows-Server so konfigurieren, dass eine IP-Adresse wie bei einem PC-Standardserver automatisch zugeordnet wird), besorgen Sie sich die TCP/IP-Adressen bei Ihrem Netzwerkadministrator. Dazu gehören:

- IP-Adressen für alle externen TCP/IP-Ports
- Teilnetzmaske
- Domänenname oder Arbeitsgruppenname
- IP-Adresse für den DNS-Server (falls vorhanden)
- IP-Adresse des Standardgateways für das LAN (falls vorhanden)

Wenn Sie TCP/IP auf Ihrer iSeries ausführen, wurden die letzten beiden Elemente in der vorstehenden Liste bereits für das System zur Verfügung gestellt. Geben Sie für diese Parameter *SYS an, während Sie den Befehl INSWNTSVR (Windows-Server installieren) ausführen.

6. Legen Sie fest, ob Sie iSeries Access für Windows benutzen wollen, wodurch der Einsatz von iSeries Navigator und Open Database Connectivity (ODBC) als Windows-Dienst ermöglicht wird. Weitere Informationen enthält das Thema zur Gegenüberstellung von iSeries NetServer und iSeries Access for Windows im Information Center.
7. Aktivieren Sie NetServer und richten Sie ein Gastbenutzerprofil ein, damit Sie Serviceaufgaben für den integrierten Server ausführen können. Weitere Informationen finden Sie unter „iSeries NetServer aktivieren“ auf Seite 68 und „Gastbenutzerprofil für iSeries NetServer erstellen“ auf Seite 68.
8. Es besteht die Möglichkeit, bei der Installation auf eine physische CD-ROM zu verzichten, um beispielsweise im Fall einer erneuten Serverinstallation Verzögerungen und Kosten für die Lieferung der CD-ROM an einen fernen Standort zu vermeiden, oder ein Microsoft Service-Pack oder Hotfix direkt in die Installationsquelle herunterzuladen, um einen Virusbefall zu verhindern (MS Knowledge Base, Artikel 828930). Speichern Sie das Image der Installations-CD, und geben Sie bei der Installation im Feld Windows-Quellenverzeichnis den Pfad zu diesem Image an. Weitere Informationen enthält das Redbook Microsoft Windows Server 2003 Integration with iSeries, SG24-6959





Anmerkung:

Für den Inhalt der Installations-CD können Lizenzen der entsprechenden Autoren und Distributoren erforderlich sein. Für die Einhaltung der mit diesen Lizenzen verbundenen Auflagen ist der Kunde zuständig. Durch das Anbieten dieser Funktion übernimmt IBM keine Verantwortung für die Einhaltung oder Durchsetzung der für die CD geltenden Lizenzvereinbarungen.

9. Die Installation kann durch Verwendung einer Konfigurationsdatei angepasst werden. Damit können die Standardwerte in der Scriptdatei (unattend.txt) für die nicht überwachte Installation von Windows geändert werden. Weitere Informationen hierzu finden Sie in Kapitel 15, „Konfigurationsdateien für NWS-Beschreibung (NWSB)“, auf Seite 261.
10. Wenn der Server auf einem externen xSeries-Server mit einem integrierten xSeries-Adapter installiert werden soll, helfen Ihnen die folgenden Links:

- IXA install read me first 
- iSeries-Features installieren

11. Wenn der Server auf einem integrierten xSeries-Server installiert werden soll, lesen Sie die Informationen unter IXS install read me first .
12. Wenn der Server auf einem externen xSeries- oder IBM BladeCenter-Server mit einem iSCSI-HBA installiert werden soll, müssen Sie den xSeries oder IBM BladeCenter-Server vorbereiten. Weitere Informationen finden Sie in iSCSI install read me first .
13. Wenn der Server auf einem externen xSeries- oder IBM BladeCenter-Server mit einem iSCSI-HBA installiert werden soll, vergewissern Sie sich, dass der i5/OS-Systemwert QRETSVRSEC auf 1 gesetzt ist. Sie können dazu den Befehl WRKSYSVAL (Mit Systemwerten arbeiten) verwenden.
14. Wenn Sie auf Ihrem iSeries-Server logische Partitionen verwenden, müssen Sie beachten, dass IBM i5/OS Integrated xSeries Server Support nur auf der logischen Partition installiert werden muss, die zum Anhängen des Servers verwendet werden soll. Das Lizenzprogramm muss nicht auf allen logischen Partitionen installiert werden. Auf einer logischen Partition können beispielsweise i5/OS Integrated xSeries Server Support und mindestens ein integrierter Windows-Server installiert sein, während auf einer anderen logischen Partition weder i5/OS Integrated xSeries Server Support noch ein integrierter Server installiert ist.
15. Wenn Sie einen Windows-Server unter i5/OS installieren, wird ein NWSD-Objekt erstellt, das Konfigurationsdaten wie z. B. die Version von Windows und die zu verwendende Hardware-ressource enthält. Allerdings kann nur jeweils eine NWSD angehängt (ausgeführt) werden.

Maschinenpoolvoraussetzungen

Der Maschinenhauptspeicherpool wird für Maschinen- und Betriebssystemprogramme mit einer intensiven gemeinsamen Benutzung verwendet. Der Maschinenhauptspeicherpool stellt den Hauptspeicher für die Jobs zur Verfügung, die vom System ausgeführt werden müssen, jedoch nicht Ihre Aufmerksamkeit erfordern. Wird für die Größe dieser Speicherpools ein zu geringer Wert angegeben, beeinträchtigt dies die Systemleistung. Für QMCHPOOL muss ein Wert von mindestens 256 KB angegeben werden. Die Größe für diesen Hauptspeicherpool wird im Systemwert für die Größe des Maschinenhauptspeicherpools (QMCHPOOL) angegeben. In diesem Hauptspeicherpool werden keine Benutzerjobs ausgeführt.

- Die Hardware aller unterstützten integrierten IXS und Server mit IXA-Anschluss benötigt einen Hauptspeicher von mindestens 856 KB. Weitere Informationen über die Voraussetzungen für Server mit iSCSI-Anschluss finden Sie in iSCSI install read me first .

Die Größe des Maschinenpools kann mit Hilfe des Befehls WKRSYSSTS (Mit Systemstatus arbeiten) angezeigt und geändert werden. Der erste Speicherpool in der Anzeige WKRSYSSTS ist der Maschinenpool.

Der Systemwert QPFRADJ kann geändert werden, damit das System die Größen der Systempools automatisch anpasst. Da ein stark ausgelastetes System durch die automatische Leistungsanpassung verlangsamt werden kann, ist es möglicherweise sinnvoll, dessen Einsatz in folgenden Zeiträumen einzuschränken:

- In den ersten Tagen nach der Installation.
- Etwa eine Stunde vor und nach dem Zeitraum, in dem die Systembelastung vom Tagesbetrieb (vor allem interaktive Prozesse) zum Nachtbetrieb (vor allem Stapelverarbeitung) umgestellt wird (und umgekehrt).

Zeitsynchronisation

So synchronisieren Sie die Uhrzeit zwischen i5/OS und der Windows-Umgebung:

1. Wählen Sie *YES für das Synchronisieren von Datum und Uhrzeit im Befehl INSWNTSVR (Windows-Server installieren) oder im Befehl CHGNWSD (NWS-Beschreibung ändern) aus. Durch Auswahl von *YES wird die Uhrzeit zwischen i5/OS und dem integrierten Windows-Server alle 30 Minuten synchronisiert. Bei Auswahl von *NO wird die Uhrzeit nur beim Starten des Servers synchronisiert.
2. Vergewissern Sie sich, dass Uhrzeit, Datum und Zeitzone der iSeries korrekt definiert sind. Sobald diese Werte festgelegt wurden, aktualisieren sie sich selbst automatisch alle sechs Monate bei der Umstellung auf Sommer- bzw. Winterzeit. Der Systemwert QTIMZON macht die manuelle Änderung des Systemwerts QUTCOFFSET überflüssig, die zwei Mal jährlich vorgenommen werden müsste.
3. Klicken Sie in der Windows-Konsole auf **Systemsteuerung** → **Datum und Uhrzeit**, wählen Sie die Indexzunge **Zeitzone** aus, und wählen Sie in der Dropdown-Liste Ihre Zeitzone aus.
4. Wählen Sie das Markierungsfeld **Uhr automatisch auf Sommer-/Winterzeit umstellen** aus. Klicken Sie anschließend auf OK.

Haben Sie Probleme mit der Zeitsynchronisation, dann prüfen Sie, ob der i5/OS-Systemwert für LOCALE ordnungsgemäß festgelegt ist.

| **Anmerkung:** Für aktive Windows-Domänenserver und Domänenmitgliedsserver muss für die Zeit-
| synchronisation *NO angegeben werden. Da das Windows Active Directory über eine
| eigene Funktion zur Zeitsynchronisation verfügt, würde die Angabe von *YES zu einem
| Konflikt führen.

i5/OS-TCP/IP für integrierte Windows-Server

Bei der Installation der Windows-Umgebung für die iSeries besteht die Möglichkeit, für die Konfiguration des integrierten Servers die Werte zu verwenden, die in der TCP/IP-Konfiguration von i5/OS als Standardwerte angegeben wurden. Wenn diese Möglichkeit genutzt werden soll, TCP/IP aber noch nicht konfiguriert wurde, muss die TCP/IP-Konfiguration vor der Installation von IBM i5/OS Integrated Server Support erfolgen. Außerdem muss die Gateway-Adresse zu i5/OS hinzugefügt werden. Weitere Informationen zu TCP/IP finden Sie unter TCP/IP.

Wenn auf Ihrem System iSeries Navigator installiert ist, können Sie dieses Programm zur Konfiguration der benötigten TCP/IP-Verbindungen verwenden. Die Onlinehilfefunktion von iSeries Navigator enthält Anweisungen zur Konfiguration von TCP/IP. Wenn auf Ihrem System iSeries Navigator nicht installiert ist, führen Sie die folgenden Arbeitsschritte aus:

1. Geben Sie an der i5/OS-Konsole den Befehl CFGTCP ein, und drücken Sie die Eingabetaste. Das Menü TCP/IP konfigurieren wird angezeigt.
2. Geben Sie Auswahl 12 TCP/IP-Domäneninformationen ändern ein, und drücken Sie die Eingabetaste. Die Anzeige TCP/IP-Domäne ändern (CHGTCPDMN) erscheint.
3. Geben Sie den Namen der lokalen Domäne an, den Sie im „Installationsarbeitsblatt für i5/OS-Parameter“ auf Seite 73 notiert haben.
4. Geben Sie im Feld Domain-Name-Server bis zu drei IP-Adressen aus der Advisorfunktion für die Installation des Windows-Servers oder aus dem „Installationsarbeitsblatt für i5/OS-Parameter“ auf Seite 73 an, und drücken Sie dann die Eingabetaste.

So fügen Sie die IP-Adresse Ihres Gateways zu i5/OS hinzu:

5. Wählen Sie im Menü TCP/IP konfigurieren Auswahl 2 Mit TCP/IP-Leitwegen arbeiten aus. Die Anzeige Mit TCP/IP-Leitwegen arbeiten wird aufgerufen.
6. Geben Sie eine 1 im Feld "Auswahl" ein, um einen TCP/IP-Leitweg hinzuzufügen. Die Anzeige TCP/IP-Leitweg hinzufügen wird aufgerufen.
7. Füllen Sie die entsprechenden Felder mit den Informationen für die Gateway-Adresse aus.

iSeries Access für Windows auf integrierten Windows-Servern

IBM iSeries Access für Windows ermöglicht es Ihnen, einen Personal Computer (PC) über ein lokales Netz (LAN), eine Twinaxialverbindung oder eine ferne Verbindung an einen iSeries-Server anzuschließen. Dieses Programm umfasst sämtliche Funktionen, die es Desktop-Benutzern ermöglichen, i5/OS-Ressourcen genauso einfach wie die lokalen PC-Funktionen zu nutzen. Mit iSeries Access können Benutzer und Anwendungsprogrammierer Informationen, Anwendungen und Ressourcen für das gesamte Unternehmen schnell verarbeiten.

ODBC (Open Database Connectivity) kann als Windows-Dienst eingerichtet und ausgeführt werden. Hierzu müssen Sie auf dem integrierten Server iSeries Access für Windows installieren. Auf diese Weise erhalten Sie die Möglichkeit, Serveranwendungen zu schreiben, die den ODBC-Einheitentreiber aufrufen, um auf DB2 für iSeries zuzugreifen.

Um ODBC so zu konfigurieren, dass dieses Produkt als Windows-Dienst gestartet wird, müssen Sie nach der Installation von iSeries Access den Befehl CWBCFG mit der Option /s ausführen.

Für Einzelbenutzer, die bei Windows angemeldet sind, werden alle anderen Funktionen von iSeries Access vollständig unterstützt.

Zusätzliche Informationsquelle:

- Gegenüberstellung von iSeries Access für Windows und iSeries NetServer.

iSeries NetServer aktivieren

iSeries NetServer ermöglicht Windows-Clients die Herstellung von TCP/IP-Verbindungen zu gemeinsam benutzten Verzeichnispfaden bzw. gemeinsam benutzten Ausgabewarteschlangen unter i5/OS. Zur Installation von Service-Packs müssen Sie mit einem Windows-Account angemeldet sein, der einem iSeries-Benutzerprofil entspricht und das gleiche Kennwort verwendet, oder für Sie muss ein NetServer-Gastbenutzerprofil konfiguriert sein.

Soll iSeries NetServer nur zum Ausführen von Service-Tasks verwendet werden, kann die Konfiguration ohne iSeries Navigator erfolgen. In diesem Fall kann die Schnellstartmethode verwendet werden, die im Abschnitt zum „Konfigurieren des iSeries-Servers für NetServer“ erläutert wird. Wenn Sie das gesamte Leistungsspektrum von iSeries NetServer nutzen möchten, ist iSeries Navigator erforderlich. Um dieses Produkt zu verwenden, müssen Sie iSeries Access auf einem PC konfigurieren, der für Verwaltungszwecke benutzt wird (siehe „iSeries Access für Windows auf integrierten Windows-Servern“). Sobald Sie eine der beiden Versionen konfiguriert haben, müssen Sie ein Gastbenutzerprofil einrichten. Weitere Informationen finden Sie unter „Gastbenutzerprofil für iSeries NetServer erstellen“.

Gastbenutzerprofil für iSeries NetServer erstellen

Damit Codekorrekturen und Systemupgrades für die Windows-Umgebung auf der iSeries angewendet werden können, müssen Sie mit einem Windows-Account und einem iSeries-Benutzerprofil mit dem gleichen Kennwort angemeldet sein, oder Sie müssen ein Gastbenutzerprofil für iSeries NetServer konfigurieren. Dazu müssen Sie über die Sonderberechtigung *SECADM verfügen.


Wenn iSeries auf Ihrem System installiert ist, können Sie ein Gastbenutzerprofil für iSeries NetServer ohne Sonderberechtigungen und Kennwort über die grafische Benutzeroberfläche einrichten.

Wenn Sie nicht mit iSeries Navigator arbeiten, müssen Sie die folgenden Arbeitsschritte ausführen, um ein Gastbenutzerprofil für iSeries NetServer einzurichten:

1. Erstellen Sie unter i5/OS ein Benutzerprofil ohne Sonderberechtigungen und ohne Kennwort. Geben Sie dazu folgenden Befehl ein:

```
CTUSRPRF USRPRF(Benutzername) PASSWORD(*NONE) SPCAUT(*NONE)
```

Anmerkung:

Weitere Informationen zu Benutzerprofilen finden Sie in der iSeries Security Reference. 

2. Geben Sie den folgenden Befehl ein, wobei *Benutzername* der Name des erstellten Benutzerprofils ist:
CALL QZLSCHSG PARM(*Benutzername* X'00000000')
3. Geben Sie den folgenden Befehl ein, um iSeries NetServer zu stoppen:
ENDTCPSVR SERVER(*NETSVR)
4. Geben Sie den folgenden Befehl ein, um iSeries NetServer erneut zu starten:
STRTCPSVR
SERVER(*NETSVR)

Jetzt können Sie wieder zum Abschnitt „iSeries NetServer aktivieren“ auf Seite 68 oder „Installation von integrierten Windows-Servern vorbereiten“ auf Seite 64 zurückkehren.

IBM i5/OS Integrated Server Support installieren

So installieren Sie IBM i5/OS Integrated Server Support auf der iSeries:

1. Bei einem Upgrade des Lizenzprogramms IBM iSeries Integration für Windows-Server von V5R2 oder V5R3 verwenden Sie die Anweisungen im Abschnitt „Upgrade des Lizenzprogramms IBM iSeries Integration für Windows-Server durchführen“ auf Seite 105. Führen Sie die Schritte unter „Upgrade vorbereiten“ aus, und kehren Sie dann hierher zurück.
2. Legen Sie die i5/OS-CD mit dem Programm 5722-SS1, Option 29 ein.
3. Geben Sie G0 LICPGM ein, und drücken Sie die Eingabetaste.
4. Wählen Sie im Menü Mit Lizenzprogrammen arbeiten die Auswahl 11 aus, und drücken Sie die Eingabetaste.
5. Blättern Sie in der Liste der Lizenzprogramme bis zur Beschreibung Integrated Server Support vor.
6. Geben Sie eine 1 im Feld Option neben der Beschreibung ein.
7. Drücken Sie die Eingabetaste.
8. Geben Sie den Namen der Installationseinheit ein, in die die i5/OS-CD eingelegt wurde.
9. Drücken Sie die Eingabetaste. Das System installiert daraufhin die Integrationssoftware.
10. Nachdem IBM i5/OS Integrated Server Support installiert wurde, installieren Sie das neueste kumulative PTF-Paket (vorläufige Programmkorrekturen) von IBM. Beachten Sie hierbei, dass während der Installation von PTFs keine Benutzer auf der iSeries arbeiten dürfen. Verwendet das System logische Partitionen, laden Sie die PTFs auf die sekundären Partitionen, auf denen i5/OS Integrated Server Support installiert wird, und geben Sie an, dass die PTFs mit Verzögerung angewendet werden sollen. Laden Sie danach die PTFs auf die primäre Partition. Weitere Informationen finden Sie unter Vorläufige Programmkorrekturen (PTFs) auf einem System mit logischen Partitionen installieren.
11. So installieren Sie die neueste vorläufige Programmkorrektur (PTF):
 - a. Geben Sie in der i5/OS-Befehlszeile den Befehl G0 PTF ein, und drücken Sie die Eingabetaste.
 - b. Geben Sie zum Installieren des PTF-Pakets Auswahl 8 ein, und drücken Sie die Eingabetaste.
 - c. Geben Sie im Feld Einheit den Namen der optischen Einheit ein.
 - d. Verwenden Sie die Standardeinstellung *YES für Automatisches IPL, es sei denn, das System benutzt logische Partitionen. Drücken Sie die Eingabetaste, um alle PTFs zu installieren. Das System wird automatisch heruntergefahren und erneut gestartet, es sei denn, Sie haben die Einstellung in *NO geändert.

Weitere Informationen zu PTFs finden Sie im Abschnitt zu den Fixes in den **iSeries-Basisoperationen**.

12. Bei einem Upgrade des Lizenzprogramms IBM iSeries Integration für Windows-Server von V5R2 oder V5R3 verwenden Sie die Anweisungen im Abschnitt „Upgrade des Lizenzprogramms IBM iSeries Integration für Windows-Server durchführen“ auf Seite 105. Führen Sie die unter „Nach dem i5/OS-Upgrade“ beschriebenen Schritte aus, und kehren Sie dann hierher zurück.
13. Wenn Sie einen Upgrade von i5/OS Integrated Server Support von einem früheren Release vornehmen, müssen Sie einen Upgrade der vorhandenen integrierten Windows-Server auf den neuen Level vornehmen. Entsprechende Anweisungen finden Sie unter „Upgrade von IBM i5/OS Integrated Server Support auf der Seite des integrierten Servers durchführen“ auf Seite 107.

Installation des Windows-Servers planen

Sie sollten den ersten integrierten Windows-Server im Netzwerk als Domänencontroller konfigurieren und einen wohl überlegten Namen für diesen festlegen. (Beachten Sie, dass zum Ändern des Namens eines Controllers zuerst dessen Aufgabenbereich geändert werden muss.) Auf den Domänencontrollern befindet sich die Master-Sicherheitsdatenbank. Jeder Domänencontroller ist in der Lage, Änderungen vorzunehmen, die dann auf allen anderen Domänencontrollern repliziert werden.

Wenn Sie einen Server mit iSCSI-Anschluss installieren, sollten Sie außerdem die Anweisungen im Abschnitt „Installation der iSCSI-Hardware planen“ beachten.

Bevor Sie Windows 2000 Server oder Windows Server 2003 installieren können, müssen Sie den Befehl ausführen und sichern, der durch die „Advisorfunktion für die Installation des Windows-Servers“ generiert wird. Alternativ können Sie aber auch das „Installationsarbeitsblatt für i5/OS-Parameter“ auf Seite 73 ausfüllen.

Fahren Sie mit dem Abschnitt „Windows 2000 Server oder Windows Server 2003 installieren“ auf Seite 98 fort.

Installation der iSCSI-Hardware planen

Konfigurieren Sie Ihre iSCSI-Hardware, bevor Sie mit der Installation des Windows-Servers beginnen.

- „Bootmodus für Hosted System planen“
- „Konfiguration des Serviceprozessors und des fernen Systems erstellen“ auf Seite 71
- „Serviceprozessorverbindung planen“ auf Seite 72
- „Erkennungsmethode für Serviceprozessor auf dem iSeries-Server konfigurieren“ auf Seite 72

Bootmodus für Hosted System planen

Der Bootmodus legt fest, wie die für das Booten von Windows erforderlichen IP- und Speicherinformationen für einen iSCSI-HBA im Hosted System übergeben werden.

Dynamisch über DHCP an das fernes System übergeben

Dies ist der Standardmodus. Ein DHCP-Server auf dem iSeries-Server stellt Konfigurationsdaten automatisch über die konfigurierten NWSH-Adapter zur Verfügung. Weitere Informationen finden Sie unter „Booten über iSCSI ohne Plattenspeicher“ auf Seite 23.

- Mehrere NWSDs können zu unterschiedlichen Zeiten das Hosted System benutzen.
- Dieser Modus kann auf Netzen mit Switches oder Routern verwendet werden, die über ein DHCP-Relay angeschlossen sind.
- Wenn IPsec aktiviert ist, kann der DHCP-Datenverkehr zwischen den iSCSI-HBAs weitergeleitet werden.

Manuell auf dem fernen System konfiguriert

- Nur eine NWSD kann das Hosted System benutzen.
- Diese Einstellung ist für Netzwerke ohne DHCP-Weitergabe möglich.
- Wenn IPsec zwischen den iSCSI-HBAs aktiviert ist, wird der DHCP-Datenverkehr auf dem iSCSI-Netzwerk blockiert.

Konfiguration des Serviceprozessors und des fernen Systems erstellen

Bevor Sie den Server installieren, können Sie optional eine Konfiguration für einen Serviceprozessor und ein fernes System erstellen, so dass deren Namen als Parameter für den Befehl INSWNTSVR (Windows-Server installieren) zur Verfügung gestellt werden. Dies kann vor der Definition der Hardware für das Hosted System erfolgen, und ist optional, da INSWNTSVR diese Objekte generieren kann, wenn dieselben Informationen als Parameter bereitgestellt werden. Wenn eine der nachfolgenden Bedingungen zutrifft, wird empfohlen, die Konfiguration des Serviceprozessors und des fernen Systems vor Ausführung des Befehls INSWNTSVR zu erstellen.

- Sie haben noch nie zuvor einen Server mit iSCSI-Anschluss installiert und wünschen eine ausführliche Anleitung.
- Sie bevorzugen den Einsatz grafischer Oberflächen.
- Zu einem späteren Zeitpunkt haben Sie nur erschwerten Zugang zur Seriennummer des fernen Systems und des iSCSI-HBA.

So erstellen Sie die Konfiguration des Serviceprozessors und des fernen Systems:

1. Wenn Sie bisher noch keine Serviceprozessorkonfiguration für den neuen Server erstellt haben, tun Sie dies jetzt. Dieses Objekt können Sie zu einem späteren Zeitpunkt wieder ändern.
 - a. Erweitern Sie .
 - b. Erweitern Sie **iSCSI-Verbindungen**.
 - c. Klicken Sie mit der rechten Maustaste auf **Serviceprozessoren**.
 - d. Wählen Sie **Neue Konfiguration für Serviceprozessor** aus.
 - e. Auf der Indexzunge **Allgemein**:
 - Geben Sie den **Namen** und die **Beschreibung** ein.
 - Geben Sie die **Seriennummer** des Gehäuses ein, um den Serviceprozessor im Netzwerk zu kennzeichnen. Sie Seriennummer finden Sie auf dem Systemgehäuse.
 - Wählen Sie die **Objektberechtigung** aus.
 - f. Geben Sie auf der Indexzunge **Sicherheit** die Option **Kein Zertifikat verwenden (physische Sicherheit erforderlich)** an.
 - g. Klicken Sie auf **OK**.
2. Wenn Sie bisher noch keine Konfiguration für ein fernes System erstellt haben, tun Sie dies jetzt.
 - a. Erweitern Sie .
 - b. Erweitern Sie **iSCSI-Verbindungen**.
 - c. Klicken Sie mit der rechten Maustaste auf **Ferne Systeme**.
 - d. Wählen Sie **Neue Konfiguration für fernes System** aus.
 - e. Auf der Indexzunge **Allgemein**:
 - Geben Sie den **Namen** und die **Beschreibung** ein.
 - Wählen Sie für **Konfiguration für Serviceprozessor** die vorhandene oder neue Serviceprozessorkonfiguration aus Schritt 1 aus.
 - Geben Sie die **Identifikation des fernen Systems** an.

Anmerkung: Zur Angabe dieser ID für ein IBM BladeCenter-Blade, wählen Sie die Option **Folgende Werte verwenden** aus, und geben Sie die Seriennummer des IBM BladeCenter-Blades an. Übernehmen Sie für andere Server die ausgewählte Option **Gehäuseidentifikation verwenden**.
 - Wählen Sie die **Objektberechtigung** aus.
 - f. Führen Sie in der Indexzunge **Netzwerkschnittstellen** die folgenden Schritte für jeden iSCSI-HBA aus, der im Hosted System verwendet werden soll.
 - 1) Klicken Sie auf **Hinzufügen...**

- 2) Geben Sie in der Anzeige **Eigenschaften der Netzwerkschnittstelle** mindestens eine **Adresse des lokalen Adapters (MAC)** an, die Sie einem Aufkleber auf dem iSCSI-HBA entnehmen können. Um festzustellen, ob eine Adresse für die **Ferne SCSI-Schnittstelle** und die **Ferne LAN-Schnittstelle** angegeben werden muss, folgen Sie den Anweisungen unter „iSCSI-Netzwerk“ auf Seite 30. Wenn Sie sich nicht sicher sind, geben Sie für beide Schnittstellen eine Adresse an. Jede Adresse besteht aus 12 Hexadezimalzeichen.

- Die Adresse für die **Ferne SCSI-Schnittstelle** finden Sie unter ‘iSCSI’ auf dem Aufkleber.
- Die Adresse für die **Ferne LAN-Schnittstelle** finden Sie unter ‘TOE’ auf dem Aufkleber.

Anmerkung: Für iSCSI-HBAs mit zwei Ports enthält der Aufkleber vier Adressen. Jeder Port hat eine iSCSI- und eine TOE-Adresse.

- 3) Geben Sie für jede angegebene (MAC)-Adapteradresse auch eine für Ihr iSCSI-Netzwerk geeignete **Internetadresse** und eine **Teilnetzmaske** an. Lassen Sie das Feld **Gateway** leer, wenn Ihr iSCSI-Netzwerk nicht über Gateways verfügt.

- 4) Klicken Sie in der Anzeige **Eigenschaften der Netzwerkschnittstelle** auf **OK**.

g. Auf der Indexzunge **Bootparameter:**

- Konfigurieren Sie einen Bootmodus. Weitere Informationen finden Sie unter „Bootmodus für Hosted System planen“ auf Seite 70. In den meisten Fällen werden Sie die Standardoption **Dynamisch über DHCP an das ferne System übergeben** übernehmen. Weitere Informationen finden Sie unter „Booten über iSCSI ohne Plattenspeicher“ auf Seite 23. Ignorieren Sie das Markierungsfeld **Mehrere iSCSI-Schnittstellen im fernen System**.

h. Auf der Indexzunge **CHAP-Authentifizierung:**

- Wählen Sie **CHAP nicht verwenden** aus. Weitere Informationen finden Sie unter „Sicherheit für Systeme mit iSCSI-Anschluss“ auf Seite 51.

- i. Wenn Sie weitere Informationen für dieses Objekt konfigurieren möchten, tun Sie dies jetzt.

- j. Klicken Sie auf **OK**.

Serviceprozessorverbindung planen

Wenn Sie eine neue Serviceprozessorkonfiguration für den neuen Server erstellt haben, müssen Sie festlegen welche Methoden von Ihrem Serviceprozessor für jeden der im Folgenden genannten Punkte unterstützt werden, und welche unterstützten Methoden Sie verwenden möchten.

- Konfigurationsmethode
- Statische oder dynamische IP-Adressierung
- Erkennungsmethode
- Sicherheitsmethode

Diese Informationen werden in den nächsten Schritten benötigt, wenn Sie die Hardware vorbereiten und die Serviceprozessorkonfiguration ändern. Um zu entscheiden, welche Methoden Sie verwenden möchten, lesen Sie „Serviceprozessorverbindung“ auf Seite 30 und „Erkennungskonfiguration für Serviceprozessor“ auf Seite 151, aber führen Sie die Konfigurationsschritte noch nicht aus.

Erkennungsmethode für Serviceprozessor auf dem iSeries-Server konfigurieren

Konfigurieren Sie eine Erkennungsmethode für den Serviceprozessor. Überspringen Sie an dieser Stelle alle Schritte, die auf dem Hosted System ausgeführt werden müssen, da diese Schritte zu einem späteren Zeitpunkt im Rahmen der Hardwarevorbereitung ausgeführt werden. Weitere Informationen finden Sie unter „Erkennungsmethode für Serviceprozessor“ auf Seite 153.

NWS-Beschreibungen

NWS-Beschreibungen (NWSDs) stellen einen integrierten Windows-Server auf der iSeries dar. Der Befehl INSWNTSVR (Windows-Server installieren) erstellt automatisch eine NWSd für jeden installierten integrierten Server. Die NWSd hat im Allgemeinen den gleichen Namen wie der Server. Wenn für die NWSd eine Aktion durchgeführt wird, gilt diese auch für den Server. So wird beispielsweise der Server beim Anhängen der NWSd gestartet und beim Abhängen der NWSd beendet.

Installationsarbeitsblatt für i5/OS-Parameter

Führen Sie vor der Installation von Windows 2000 Server oder Windows Server 2003 entweder die Advisorfunktion für die Installation des Windows-Servers aus, oder füllen Sie dieses Installationsarbeitsblatt aus.

Dieses Arbeitsblatt erleichtert Ihnen die Installation und Konfiguration Ihres Systems.

Feld	Beschreibung und Anweisungen	Wert
NWSd (NWS-Beschreibung)	<p>Definiert die Betriebsmerkmale und DFV-Verbindungen des Netzwerkservers, der den integrierten Windows-Server steuert. Weitere Informationen finden Sie unter „NWS-Beschreibungen“.</p> <p>Es sollte ein leicht zu merkender Name verwendet werden. Der Name kann bis zu acht Zeichen lang sein. Verwenden Sie nur die Zeichen A-Z und 0-9 für den Namen, wobei das erste Zeichen ein Buchstabe sein muss. Der Name der NWS-Beschreibung ist gleichzeitig der Computernamen und der TCP/IP-Hostname des integrierten Servers.</p>	
INSTYPE (Installationstyp)	<p>Gibt die Art der durchzuführenden Installation an. Wählen Sie eine der folgenden Möglichkeiten aus:</p> <p>*FULL</p> <p>Dieser Installationstyp ist erforderlich, wenn auf einem internen integrierten xSeries(R)-Server (IXS) installiert wird. Sie ist optional, wenn auf einem externen xSeries-Server installiert wird, der über einen integrierten xSeries-Adapter (IXA) oder iSCSI-HBA angeschlossen ist.</p> <p>*BASIC</p> <p>Dieser Installationstyp ist optional, wenn auf einem externen xSeries-Server installiert wird, der über einen IXA oder iSCSI-HBA angeschlossen ist. Bei dieser Option wird der erste Teil des Installationsprozesses über den i5/OS-Befehl INSWNTSVR (Windows-Server installieren) gesteuert. Anschließend wird die Installation durch den xSeries-Installationsprozess unter Verwendung der ServerGuide-CD beendet.</p>	

Feld	Beschreibung und Anweisungen	Wert
RSRCNAME (Ressourcenname)	<p>Gibt die Hardware des Windows-Servers an.</p> <p>Geben Sie für xSeries- und IBM BladeCenter-Server mit iSCSI-Anschluss den Ressourcenamen *ISCSI an.</p> <p>Geben Sie sowohl für IXS als auch für xSeries-Server mit IXA-Anschluss den Ressourcenamen des Dateiserver-IOA an. Der Name kann durch Eingabe von DSPHDWRSC *CMN in der i5/OS-Befehlszeile ermittelt werden. Der Ressourcenname erscheint als LINxx, wobei xx eine Zahl ist.</p> <p>„Tipp: Ressourcenamen bei mehreren integrierten Servern suchen“ auf Seite 97</p>	
TCPPORTCFG (TCP/IP-Portkonfiguration)	<p>Geben Sie die Windows TCP/IP-Konfigurationswerte an, die für jeden lokal gesteuerten Adapterport spezifisch sind. Andernfalls überspringen Sie diesen Schritt und verwenden den Standardwert *NONE.</p> <p>Anmerkung: Nur Adapter, die direkt von der iSeries betrieben und logisch vom IXS gesteuert werden, können mit dem Parameter TCPPORTCFG konfiguriert werden. LAN-Adapter mit IXA- oder iSCSI-HBA-Anschluss und vom xSeries-Server betrieben werden, können mit diesem Parameter nicht konfiguriert werden.</p>	<ul style="list-style-type: none"> • Port 1 <ul style="list-style-type: none"> – IP-Adresse – Teilnetzmaske – Gateway (optional) • Port 2 <ul style="list-style-type: none"> – IP-Adresse – Teilnetzmaske – Gateway (optional) • Port 3 <ul style="list-style-type: none"> – IP-Adresse – Teilnetzmaske – Gateway (optional) • Port 4 <ul style="list-style-type: none"> – IP-Adresse – Teilnetzmaske – Gateway (optional)

Feld	Beschreibung und Anweisungen	Wert
VRTETHPORT (Virtual Ethernet-Port)	<p>Gibt die TCP/IP-Konfiguration der Virtual Ethernet-Netzwerke an, die vom Dateiserver verwendet werden.</p> <p>Für die Installation des Windows-Clusterdienstes ist ein entsprechender Virtual Ethernet-Port erforderlich.</p> <p>*NONE: Gibt an, dass keine Konfiguration für einen Virtual Ethernet-Port vorhanden ist.</p> <p>Element 1: Port</p> <ul style="list-style-type: none"> *VRTETHx: Der Virtual Ethernet-Port <i>x</i> des Netzwerkservers wird konfiguriert, wobei <i>x</i> für einen Wert zwischen 0 und 9 steht. <p>Element 2: Windows-Internetadresse Die Windows-Internetadresse für den Port im Format "nnn.nnn.nnn.nnn" (hierbei steht "nnn" jeweils für eine Dezimalzahl zwischen 0 und 255).</p> <p>Element 3: Windows-Teilnetzmaske Die Teilnetzmaske für die Windows-Internetadresse im Format "nnn.nnn.nnn.nnn" (hierbei steht "nnn" jeweils für eine Dezimalzahl zwischen 0 und 255).</p> <p>Element 4: Zugeordneter Port Der Ressourcenname, der den Port beschreibt, mit dem eine Verbindung zwischen einem Windows-Netzwerkserver und dem Netzwerk aufgebaut wird.</p> <ul style="list-style-type: none"> *NONE: Der Leitung ist kein Ressourcenname für den zugeordneten Port zugeordnet. Ressourcenname: Der Ressourcenname. 	<ul style="list-style-type: none"> • Virtueller Port 1 <ul style="list-style-type: none"> – *VRTETHx – IP-Adresse – Teilnetzmaske – Zugeordneter Port (optional) • Virtueller Port 2 <ul style="list-style-type: none"> – *VRTETHx – IP-Adresse – Teilnetzmaske – Zugeordneter Port (optional) • Virtueller Port 3 <ul style="list-style-type: none"> – *VRTETHx – IP-Adresse – Teilnetzmaske – Zugeordneter Port (optional) • Virtueller Port 4 <ul style="list-style-type: none"> – *VRTETHx – IP-Adresse – Teilnetzmaske – Zugeordneter Port (optional)
TCPDMNNAME (Name der lokalen TCP/IP-Domäne)	Gibt den Namen der lokalen TCP/IP-Domäne an, der dem integrierten Server zugeordnet ist. Bei Angabe von *SYS wird der Wert verwendet, der auch vom i5/OS-System verwendet wird.	
TPCNAMSVR (TCP/IP-Namensserversystem)	Gibt die Internetadresse des vom integrierten Server verwendeten Namensservers an. Sie können bis zu drei Internetadressen angeben. Bei Angabe von *SYS wird der Wert verwendet, der auch von i5/OS verwendet wird.	
TOWRKGRP (Zu Arbeitsgruppe)	Gibt den Namen der Windows-Serverarbeitsgruppe an, zu der der Server gehört.	
TODMN (Zu Domäne)	Gibt den Namen der Windows-Domäne an, zu der der Server gehört.	

Feld	Beschreibung und Anweisungen	Wert
MSGQ (Servernachrichtenwarteschlange und Bibliothek)	<p>Geben Sie den Namen der Nachrichtenwarteschlange und den Namen der Bibliothek an, in die sie gestellt werden soll. Wenn die Nachrichtenwarteschlange noch nicht vorhanden ist, wird sie vom Befehl INSWNTSVR (Windows NT-Server installieren) erstellt. An die Nachrichtenwarteschlange werden alle Ereignisprotokolle und Fehler im Zusammenhang mit diesem Server gesendet. Ein Name und eine Bibliothek für die Nachrichtenwarteschlange (MSGQ) sollten angegeben werden. Sie können auch *JOBLOG angeben, wenn nicht schwer wiegende Fehler an das Jobprotokoll der Benutzeradministrationsüberwachung und schwer wiegende Fehler an QSYSOPR gesendet werden sollen. Bei Angabe von *NONE werden nicht schwer wiegende Fehler nicht an i5/OS gesendet, und schwer wiegende Fehler werden an QSYSOPR gesendet.</p>	<p>Warteschlange: Bibliothek:</p>
EVTLOG (Ereignisprotokollverarbeitung)	<p>Gibt an, ob i5/OS Ereignisprotokollnachrichten vom integrierten Server empfängt. Als Auswahlmöglichkeiten stehen *ALL, *SYS, *SEC, *APP oder *NONE zur Verfügung.</p> <p>*ALL i5/OS empfängt alle Ereignisprotokollnachrichten.</p> <p>*NONE Es werden keine Ereignisprotokollnachrichten empfangen.</p> <p>*SYS i5/OS empfängt Nachrichten des Systemereignisprotokolls.</p> <p>*SEC i5/OS empfängt alle Ereignisprotokollnachrichten.</p> <p>*APP i5/OS empfängt Nachrichten des Anwendungsereignisprotokolls.</p> <p>Anmerkung: Wenn der integrierte Server sein Sicherheitsprotokoll an die iSeries senden soll (Angabe von *ALL oder *SEC), müssen Sie darauf achten, für die Nachrichtenwarteschlange die korrekte Sicherheitseinstellung zu konfigurieren.</p>	

Feld	Beschreibung und Anweisungen	Wert
ASP SVRSTGSIZE SVRSTGASP STGASPDEV (Installationsquelle, Systemlaufwerk- größen und Zusatz- speicherpool)	<p>Geben Sie die Größe der NWS-Speicherbereiche für das Installationsquellenlaufwerk und das Systemlaufwerk sowie mit einem Wert zwischen 1 und 255 den Zusatzspeicherpool (ASP) an, in dem sich diese befinden sollen. Anstelle der ASP-Nummern 33 bis 255 kann ein ASP-Einheitename angegeben werden, wenn der Speicherbereich in einem unabhängigen Zusatzspeicherpool erstellt werden soll. Falls ein Name verwendet wird, muss im Feld für die ASP-Nummer jedoch der Standardwert 1 oder der Platzhalterwert *N beibehalten werden.</p> <p>Das Installationsquellenlaufwerk (Laufwerk D) muss groß genug sein, um den Inhalt des Verzeichnisses I386 auf dem Installations-CD-Image für den Windows-Server und den Code von IBM i5/OS Integrated Server Support speichern zu können.</p> <p>Das Systemlaufwerk (Laufwerk C) muss groß genug sein, um das Betriebssystem für den Windows-Server zu speichern. Die Wert liegt je nach Ressourcenzkapazität bei 1.024 bis 1.024.000 MB. Beachten Sie folgende Faktoren:</p> <ul style="list-style-type: none"> • Vorhandene Version des Windows-Servers (die Betriebssystemvoraussetzungen sind in der entsprechenden Microsoft-Dokumentation angegeben) • Primäre Nutzung (Druck-/Dateiserver) und Anzahl der Terminal-Server-Benutzer • Freier Plattenplatz auf dem Systemlaufwerk • Anwendungsressourcenvoraussetzungen • Notwendigkeit einer Speicherauszugsdatei beim Systemabsturz • Auf dem Server installierter Speicher <p>i5/OS erstellt und verbindet das Laufwerk abhängig von der Größe als FAT-32 oder NTFS-NWS-Speicherbereich.</p> <p>Weitere Informationen zu diesen Laufwerken finden Sie unter „Vordefinierte Plattenlaufwerke für integrierte Windows-Server“ auf Seite 171.</p>	Installationsquellenlaufwerk: Größe: ASP: ASPDEV: Systemlaufwerk: Größe: ASP: ASPDEV:

Feld	Beschreibung und Anweisungen	Wert
(Fortsetzung)	<p>Anmerkungen:</p> <ol style="list-style-type: none"> 1. Mit dem Befehl INSWNTSVR wird die Systemplattengröße automatisch auf die Mindestgröße festgelegt, die sich z.T. nach Faktoren wie der Windows-Version und dem installierten Speicher richtet. 2. Wenn Sie die Größe der einzelnen Laufwerke festlegen, sollten Sie auch zukünftige Erfordernisse (neue Anwendungen oder Upgrades für den Windows-Server) berücksichtigen. Wenn Sie *CALC für SVRSTGSIZE angeben, müssen Sie beachten, dass i5/OS die Mindestplattengröße zuordnet, die für die Installation von Windows erforderlich ist. Wenn Sie zusätzlichen Speicherbereich für Anwendungen oder Daten benötigen, sollten Sie die Laufwerksgröße besser manuell angeben. 3. Die Unterstützung unabhängiger ASPs (33-255) wird von iSeries Navigator bereitgestellt. Weitere Informationen zur Verwendung unabhängiger ASPs finden Sie im Abschnitt über Unabhängige Plattenpools. Sowohl im Information Center als auch in iSeries Navigator werden ASPs als Plattenpools bezeichnet. Zur Benutzung eines unabhängigen ASPs muss die ASP-Einheit vor Ausführung des Befehls INSWNTSVR verfügbar sein. 	

Feld	Beschreibung und Anweisungen	Wert
LICMODE (Lizenzmodus)	<p>Legt den Lizenzmodus für die Installation des Microsoft Windows-Servers fest.</p> <p>Element 1 Lizenzart:</p> <p>*PERSEAT Gibt an, dass für jeden Computer, der auf den Server zugreift, eine Clientlizenz erworben wurde.</p> <p>*PERSERVER Gibt an, dass die Clientlizenzen für den Server erworben wurden, um eine bestimmte Anzahl gleichzeitig bestehender Verbindungen zum Server zu ermöglichen.</p> <p>Element 2 Clientlizenzen:</p> <p>*NONE Gibt an, dass keine Clientlizenzen installiert sind. *NONE muss angegeben werden, wenn *PERSEAT angegeben wurde.</p> <p>Anzahl der Clientlizenzen: Gibt die Anzahl der Clientlizenzen an, die für den zu installierenden Server erworben wurden.</p> <p>Element 3 Windows-Terminaldienste:</p> <p>*TSENABLE Installiert für Windows 2000 die Windows-Terminaldienste und die Lizenzierung für die Terminaldienste.</p> <p>*PERDEVICE *PERDEVICE installiert und konfiguriert die Terminaldienste von Windows 2003 so, dass für jede angeschlossene Einheit eine gültige Zugriffslizenz für den Windows-Terminal-Server erforderlich ist. Wenn der Client über eine Zugriffslizenz für den Terminal-Server verfügt, kann er auf mehrere Terminal-Server zugreifen.</p> <p>*PERUSER Installiert und konfiguriert den Terminal-Server von Windows 2003 so, dass für jeden aktiven Benutzer eine Zugriffslizenz für den Terminal-Server bereitgestellt wird.</p> <p>*NONE Es sind keine Terminal-Server-Desktop-Lizenzen für diesen Server vorhanden.</p>	<p>Lizenzart:</p> <p>Clientlizenzen:</p> <p>Terminaldienste:</p>

Feld	Beschreibung und Anweisungen	Wert
PRPDMNUSR (Domänenbenutzer weitergeben)	<p>Gibt an, ob über diesen Server Benutzer an die Windows-Domäne oder das Active Directory weitergegeben und mit diesen synchronisiert werden sollen.</p> <p>*YES Benutzeraktualisierungen über diesen Server an die Windows-Domäne oder das Active Directory senden.</p> <p>*NO Keine Benutzeraktualisierungen über diesen Server an die Windows-Domäne oder das Active Directory senden.</p>	
SHUTDTIMO (Zeitlimit bei Systemabschluss)	<p>Dieser Wert bestimmt, wie lange i5/OS wartet, damit Programme beendet werden können, bevor der integrierte Server beendet wird. Die Verzögerung kann zwischen 2 und 45 Minuten betragen. Wenn Sie keinen Wert angeben, wird der Wert auf 15 Minuten festgelegt.</p>	Zeitlimit bei Systemabschluss:
RSTDEVRSC (Eingeschränkte Einheitenressourcen)	<p>Schränkt die Benutzung von iSeries-Bandeinheiten und optischen Einheiten durch den integrierten Server ein.</p> <p>*NONE Der integrierte Server kann Bandeinheiten oder optische Einheiten uneingeschränkt benutzen.</p> <p>*ALL Der integrierte Server kann keine Bandeinheiten oder optischen Einheiten benutzen.</p> <p>*ALLTAPE Schränkt die Verwendung aller Bandressourcen durch den integrierten Server ein.</p> <p>*ALLOPT Schränkt die Verwendung aller optischen Ressourcen durch den integrierten Server ein.</p> <p>Eingeschränkte Einheit Geben Sie bis zu zehn Einheitenressourcen an, die vom integrierten Server nicht benutzt werden sollen.</p>	
Zeitzone	<p>(Optional) Zeichnet die Zeitzone der iSeries für die Verwendung bei der Installation des Windows-Servers auf. Weitere Informationen enthält der Abschnitt „Zeitsynchronisation“ auf Seite 67.</p>	

Feld	Beschreibung und Anweisungen	Wert
VRTPTPPOINT (Virtual Ethernet-Punkt-zu-Punkt)	<p>Zwischen i5/OS und dem Windows-Server besteht ein lokales Netzwerk (siehe „Konzepte für den Netzwerkbetrieb“ auf Seite 29). Sowohl die i5/OS-Seite als auch die Windows-Serverseite dieses LANs besitzen IP-Adressen und Teilnetzmasken.</p> <p>Anmerkung: In der Standardeinstellung konfiguriert der Befehl INSWNTSVR diese Adressen automatisch. Die Adressen haben das Format 192.168.xx.yy. Wenn Sie Adressen der Klasse C verwenden, werden ggf. doppelte IP-Adressen generiert.</p> <p>Um potenzielle Konflikte zu vermeiden, können Sie IP-Adressen festlegen, die auf Ihrem System in jedem Fall eindeutig sind. Die Adressen werden im Format a.b.x.y angegeben, wobei a.b.x für beide Seiten der Virtual Ethernet-Punkt-zu-Punkt-Verbindung den identischen Wert aufweist. Außerdem muss sichergestellt werden, dass sie unter i5/OS ein eigenes Teilnetz belegt. Verwenden Sie den Parameter "Virtual Ethernet-PTP-Port" unter den zusätzlichen Parametern des Befehls INSWNTSVR.</p> <p>Die Teilnetzmaske ist immer 255.255.255.0.</p>	<p>i5/OS-seitige IP-Adresse:</p> <p>Windows-Serverseitige IP-Adresse:</p>
CFGFILE (Konfigurationsdatei)	<p>Während der Installation wird eine angepasste NWS-Beschreibung (NWSB) erstellt und angegeben (siehe Kapitel 15, „Konfigurationsdateien für NWS-Beschreibung (NWSB)“, auf Seite 261).</p> <p>Der Standardwert ist *NONE. Um eine selbst erstellte Konfigurationsdatei anzugeben, müssen Sie den Namen der Datei und der Bibliothek am Speicherort ersetzen (*LIBL, *CURLIB oder Name der Bibliothek).</p>	

| Installationsarbeitsblatt für weitere Internet-SCSI (iSCSI)-Parameter

Feld	Beschreibung und Anweisungen	Wert
ACTTMR (Aktivierungszeitgeber)	Gibt an, wie lange (in Sekunden) das System auf die Herstellung der Verbindung mit dem Serviceprozessor des fernen Systems und das Einschalten des fernen Servers wartet. Der Standardwert ist 120. Geben Sie einen Wert zwischen 30 und 1800 Sekunden an.	Aktivierungszeitgeber:

Feld	Beschreibung und Anweisungen	Wert
CMNMSGQ (DFV-Nachrichtenwarteschlange)	<p>Gibt den Namen einer Nachrichtenwarteschlange für den Empfang von Nachrichten zum Verbindungsstatus an.</p> <p>Qualifikationsmerkmal 1:</p> <ul style="list-style-type: none"> • *SYSOPR Nachrichten werden in die Nachrichtenwarteschlange für Systembediener gestellt. • Name Geben Sie den Namen der Nachrichtenwarteschlange für den Empfang von Nachrichten zu Verbindungsstatus an. <p>Qualifikationsmerkmal 2:</p> <ul style="list-style-type: none"> • *LIBL Alle Bibliotheken in der Bibliotheksliste des Jobs werden durchsucht, bis die erste Übereinstimmung gefunden wird. • *CURLIB Die aktuelle Bibliothek für den Job wird durchsucht. Wenn keine Bibliothek als aktuelle Bibliothek für den Job angegeben ist, wird die Bibliothek QGPL verwendet. • Bibliotheksname Geben Sie den Namen der zu verwendenden Bibliothek an. 	<p>Nachrichtenwarteschlange: Bibliothek:</p>
STGPTH (Speicherpfad)	<p>Gibt den Speicherpfad an, der von den Speicherbereichen verwendet werden kann. Diese Informationen bestehen aus der Beschreibung des NWS-Hostadapters (NWSH).</p> <p>Anmerkung: Nach der Installation des Servers können Sie weitere Speicherpfade hinzufügen.</p> <p>Name Geben Sie den Namen einer vorhandenen Beschreibung des NWS-Hostadapters (NWSH) an.</p>	<p>NWSH-Name:</p>

Feld	Beschreibung und Anweisungen	Wert
VRTETHPTH (Virtual Ethernet-Pfad)	<p>Gibt die Virtual Ethernet-Pfade an, die von den Ethernet-Leitungsbeschreibungen verwendet werden können. Diese Informationen bestehen aus zwei Teilen: dem Virtual Ethernet-Port und der Beschreibung des NWS-Hostadapters (NWSH). Für diesen Parameter können bis zu fünf Werte eingegeben werden. Sie müssen mindestens einen Virtual Ethernet-Pfad eingeben, der von der Leitungsbeschreibung *VRTETHPTP verwendet werden soll.</p> <p>Anmerkung: Nach der Installation des Servers können Sie weitere Virtual Ethernet-Pfade hinzufügen.</p> <p>Element 1: Port</p> <p>*VRTETHPTP</p> <p>Der Virtual Ethernet-Punkt-zu-Punkt-Port des Netzwerkservers wird konfiguriert.</p> <p>*VRTETHx Der Virtual Ethernet-Port x des Netzwerkservers wird konfiguriert, wobei x für einen Wert zwischen 0 und 9 steht.</p> <p>Element 2: NWS-Hostadapter</p> <p>Name Geben Sie den Namen einer vorhandenen Beschreibung des NWS-Hostadapters (NWSH) an. Der Name des NWSH muss nicht für jeden Parameter VRTETHPTH dieser NWSD eindeutig sein.</p>	Virtual Ethernet-Pfad: Port: NWSH:
SHUTDPORT (TCP-Port für Systemabschluss)	<p>Gibt den TCP-Port für den Systemabschluss an.</p> <p>Anmerkung: Es handelt sich hierbei um einen wichtigen Parameter, der sich als nützlich erweisen kann, wenn das iSCSI-Netzwerk eine Firewall hat.</p> <p>8700 TCP-Portnummer 8700 verwenden.</p> <p>Ganzzahl</p> <p>Gibt die Nummer des Ports an, der für den Systemabschluss verwendet werden soll. Gültige Werte liegen zwischen 1024 und 65.535.</p>	
VRTETHCTLP (Virtual Ethernet-Steuerport)	<p>Gibt den TCP-Port an, der für die Virtual Ethernet-Steuerung verwendet werden soll.</p> <p>Anmerkung: Es handelt sich hierbei um einen wichtigen Parameter, der sich als nützlich erweisen kann, wenn das iSCSI-Netzwerk eine Firewall hat.</p> <p>8800 TCP-Portnummer 8800 verwenden.</p> <p>Ganzzahl</p> <p>Gibt die Nummer des Ports an, der für die Virtual Ethernet-Steuerung verwendet werden soll. Gültige Werte liegen zwischen 1024 und 65.535.</p>	

Feld	Beschreibung und Anweisungen	Wert
RMTNWSCFG (NWSCFG des fernen Systems)	<p>Gibt die NetzwerksERVERKONFIGURATION des fernen Systems an, die für diesen Server verwendet werden soll.</p> <p>Anmerkung: Es kann wünschenswert oder gar erforderlich sein, die Konfiguration des fernen Systems vor Ausführung des Befehls INSWNTSVR zu erstellen. Weitere Informationen finden Sie unter „Konfiguration des Serviceprozessors und des fernen Systems erstellen“ auf Seite 71.</p> <p>*DFT Der Standardname für die NWS-Konfiguration des fernen Systems 'nwsdnameRM' wird verwendet, wobei nwsdname der Name der NWS-Beschreibung ist.</p> <p>Name Geben Sie den Namen einer vorhandenen NWS-Konfiguration des fernen Systems an.</p>	
SPNWSCFG (NWSCFG des Serviceprozessors)	<p>Gibt die NetzwerksERVERKONFIGURATION des Serviceprozessors an, die für diesen Server verwendet werden soll.</p> <p>Anmerkung: Es kann wünschenswert oder gar erforderlich sein, die Serviceprozessorkonfiguration vor Ausführung des Befehls INSWNTSVR zu erstellen. Weitere Informationen finden Sie unter „Konfiguration des Serviceprozessors und des fernen Systems erstellen“ auf Seite 71.</p> <p>*DFT Der vom System generierte Standardname für die Serviceprozessor-NWSCFG 'nwsdnameSP' wird verwendet, wobei nwsdname der Name der NWS-Beschreibung ist.</p> <p>Name Geben Sie den Namen einer vorhandenen Serviceprozessor-NWSCFG an.</p>	
C>NNNWSCFG (NWSCFG der Verbindungssicherheit)	<p>Gibt die NWSCFG der Verbindungssicherheit an, die für diesen Server verwendet werden soll.</p> <p>*DFT Der vom System generierte Standardname für die Verbindungssicherheits-NWSCFG 'nwsdnameCN' wird verwendet, wobei nwsdname der Name der NWS-Beschreibung ist.</p> <p>Name Geben Sie den Namen einer vorhandenen Verbindungssicherheits-NWSCFG an.</p>	

Feld	Beschreibung und Anweisungen	Wert
DFTSECRULE (IP-Standardsicherheitsregel)	<p>Gibt die IP-Standardsicherheitsregel (IPSec-Regel) an, die zwischen dem Hosting und dem fernen System verwendet werden soll.</p> <p>Anmerkung: Für diesen Parameter kann kein Wert angegeben werden, wenn im Parameter C>NNNWSCFG eine vorhandene Verbindungssicherheitskonfiguration angegeben wurde.</p> <p>*NONE Es sind keine IP-Sicherheitsregeln konfiguriert.</p> <p>*GEN Das System erstellt automatisch einen vorab bekannten wahlfreien gemeinsamen Schlüssel.</p> <p>Vorab bekannter gemeinsamer Schlüssel Geben Sie den vorab bekannten gemeinsamen Schlüssel an. Es handelt sich hierbei um eine nicht triviale Zeichenfolge von maximal 32 Zeichen.</p>	
IPSECRULE (IP-Sicherheitsregel)	<p>Geben Sie den in der vorhandenen Verbindungssicherheits-NWSCNF definierten Wert für den Parameter IPSECRULE an, der als anfängliche Einstellung für die IP-Netzsicherheit zwischen dem Hosting und dem fernen System verwendet werden soll.</p> <p>*DFTSECRULE Verwenden Sie den für die IP-Standardsicherheitsregel (Parameter DFTSECRULE) angegebenen Wert.</p> <p>*NONE Die ferne Schnittstelle verwendet keine Sicherheitsregel.</p> <p>1-16 Die ferne Schnittstelle verwendet die angegebene Sicherheitsregel.</p>	

Feld	Beschreibung und Anweisungen	Wert
INZSP (Service- prozessor initialisieren)	<p>Gibt an, wie der Serviceprozessor des fernen Systems geschützt wird.</p> <p>Anmerkung: *SYNC kann nicht angegeben werden, wenn die Serviceprozessorkonfiguration bereits vorhanden ist. *MANUAL, *AUTO und *NONE werden nur verwendet, wenn noch keine Serviceprozessor-konfiguration vorhanden ist.</p> <p>*MANUAL Dies ist die sicherste Methode. Sie müssen den Benutzernamen, das Kennwort und das Zertifikat für den Serviceprozessor manuell konfigurieren. Zertifikatmanagement ist erforderlich. Diese Methode ist geeignet, um Ihr Serviceprozessorkennwort zu schützen, wenn Sie die Verbindung zum Serviceprozessor über ein öffentliches Netz herstellen.</p> <p>*AUTO Es müssen keine Parameter auf dem Serviceprozessor des fernen Systems manuell konfiguriert werden. Der Serviceprozessor des fernen Systems generiert das Zertifikat automatisch. Einmal initialisiert, ist die Verbindung sicher. Diese Option sollte gewählt werden, wenn Sie die Verbindung zum Serviceprozessor über ein Netzwerk herstellen, das physisch sicher oder durch eine Firewall geschützt ist.</p> <p>*SYNC Diese NWS-Konfiguration synchronisiert den Benutzer, das Kennwort und das selbst signierte Zertifikat mit dem Serviceprozessor.</p> <p>*NONE Es gibt keine Sicherheit für das Serviceprozessorkennwort. Verwenden Sie diese Option nur, wenn Sie die Verbindung zum Serviceprozessor über ein physisch sicheres Netzwerk herstellen.</p>	
ENBUNICAST (Unicast aktivieren)	<p>Unicast ist eine Übertragungsmethode, bei der Pakete direkt an den angegebenen Serviceprozessornamen (Parameter SPNAME) oder die angegebene Serviceprozessordresse (Parameter SPINTNETA) gesendet werden. Die Systemidentifikation für die Gehäuseidentifikation (Parameter EID) wird automatisch abgerufen, wenn *AUTO angegeben und von der Systemhardware unterstützt wird.</p> <p>Anmerkung: Für diesen Parameter kann kein Wert angegeben werden, wenn im Parameter SPNWSCFG eine vorhandene Serviceprozessorkonfiguration angegeben wurde.</p> <p>*NO Unicast inaktivieren.</p> <p>*YES Unicast aktivieren.</p>	

Feld	Beschreibung und Anweisungen	Wert
EID (Gehäuse-identifikation)	<p>Gibt Seriennummer, Typ und Modell des Gehäuses an, das den Serviceprozessor enthält. Diese Angaben sind erforderlich, damit das ferne System auf dem Netzwerk lokalisiert werden kann, wenn ENBUNICAST(*NO) abgegeben wird. Sie finden diese Angaben auf dem Systemaufkleber.</p> <p>Anmerkung: Für diesen Parameter kann kein Wert angegeben werden, wenn im Parameter SPNWSCFG eine vorhandene Serviceprozessorkonfiguration angegeben wurde.</p> <p>*AUTO Die ID wird bei Angabe von ENBUNICAST(*YES) automatisch abgerufen.</p> <p>Element 1: Seriennummer Geben Sie die Seriennummer des fernen Systems an. Verwenden Sie nur alphanumerische Zeichen ohne Bindestriche.</p> <p>Element 2: Hersteller, Typ und Modell Geben Sie den Maschinentyp und das Modell des fernen Systems im Format ttttmmm an, wobei tttt der Maschinentyp und mmm die Modellnummer ist.</p>	
SPNAME (Serviceprozessornamen)	<p>Gibt den Hostnamen für den Serviceprozessor des fernen Systems an.</p> <p>Anmerkung: Für diesen Parameter kann kein Wert angegeben werden, wenn im Parameter SPNWSCFG eine vorhandene Serviceprozessorkonfiguration angegeben wurde.</p> <p>*SPINTNETA Das ferne System wird durch den Wert für den Parameter SPINTNETA (Serviceprozessordresse) identifiziert.</p> <p>Hostname: Geben Sie den Hostnamen für den Serviceprozessor des fernen Systems an.</p>	
SPINTNETA (Serviceprozessordresse)	<p>Geben Sie die Internetadresse für den Serviceprozessor des fernen Systems an. Internetadressen werden im Dezimalformat nnn.nnn.nnn.nnn angegeben, wobei nnn eine Dezimalzahl zwischen 0 und 255 ist.</p> <p>Anmerkung: Für diesen Parameter kann kein Wert angegeben werden, wenn im Parameter SPNWSCFG eine vorhandene Serviceprozessorkonfiguration angegeben wurde.</p> <p>Internetadresse: Geben Sie die Internetadresse des Serviceprozessors an.</p>	

Feld	Beschreibung und Anweisungen	Wert
SPAUT (SP-Authentifizierung)	<p>Gibt den Benutzernamen und das Kennwort des Serviceprozessors an.</p> <p>Anmerkung: Für diesen Parameter kann kein Wert angegeben werden, wenn im Parameter SPNWSCFG eine vorhandene Serviceprozessorkonfiguration angegeben wurde.</p> <p>*DFT Für den Benutzernamen und das Kennwort des Serviceprozessors werden die Standardwerte verwendet.</p> <p>Element 1: Benutzername Geben Sie den Benutzernamen für den Serviceprozessor des fernen Systems an.</p> <p>Element 2: Benutzerkennwort Geben Sie das Kennwort für den Serviceprozessor des fernen Systems an. Das Kennwort muss mindestens fünf Zeichen umfassen und mindestens ein alphabetisches Zeichen und ein numerisches oder Symbolzeichen enthalten.</p>	<p>Name:</p> <p>Kennwort:</p>

Feld	Beschreibung und Anweisungen	Wert
SPCERTID (SP-Zertifikats-ID)	<p>Die SP-Zertifikats-ID ist eins von drei möglichen Feldern, die das Zertifikat des Serviceprozessors identifizieren. Dieser Parameter wird angegeben, um weitere Überprüfungsmöglichkeiten für die Echtheit des Zertifikats bereitzustellen. Der Inhalt des ausgewählten Felds muss exakt mit dem Wert übereinstimmen, der eingegeben wurde, als das Zertifikat generiert oder bei der Zertifizierungsstelle angefordert wurde.</p> <p>Anmerkung: Für diesen Parameter kann kein Wert angegeben werden, wenn im Parameter SPNWSCFG eine vorhandene Serviceprozessorkonfiguration angegeben wurde.</p> <p>Einzelwerte:</p> <p>*NONE Es ist kein Serviceprozessorzertifikat konfiguriert.</p> <p>Element 1: Komponente</p> <p>*COMMONNAME Wählt den allgemeinen Namen des Zertifikats aus, der angegeben wurde, als das Zertifikat generiert oder bei einer Zertifizierungsstelle angefordert wurde. Das entsprechende Feld auf dem RSA II ist "ASM-Domänenname", mit dessen Hilfe ein selbst signiertes Zertifikat oder eine Anforderung zum Signieren eines Zertifikats generiert wird.</p> <p>*EMAIL Wählt die E-Mail-Adresse des Zertifikats aus, die angegeben wurde, als das Zertifikat generiert oder bei einer Zertifizierungsstelle angefordert wurde. Das entsprechende Feld auf dem RSA II ist E-Mail-Adresse, mit dessen Hilfe ein selbst signiertes Zertifikat oder eine Anforderung zum Signieren eines Zertifikats generiert wird.</p> <p>*ORGUNIT Wählt die Organisationseinheit des Zertifikats aus, die angegeben wurde, als das Zertifikat generiert oder bei einer Zertifizierungsstelle angefordert wurde. Das entsprechende Feld auf dem RSA II ist Organisationseinheit, mit dessen Hilfe ein selbst signiertes Zertifikat oder eine Anforderung zum Signieren eines Zertifikats generiert wird.</p> <p>Element 2: Vergleichswert</p> <p>Vergleichswert Geben Sie den Komponentenvergleichswert des Zertifikats an. Geben Sie maximal 255 in Hochkommas eingeschlossene Textzeichen an.</p>	<p>Komponente:</p> <p>Vergleichswert:</p>

Feld	Beschreibung und Anweisungen	Wert
RMTSYSID (ID des fernen Systems)	<p>Gibt Seriennummer, Typ und Modell des fernen Systems an. Mit Hilfe dieser Angaben wird das ferne System auf dem Netzwerk lokalisiert. Sie finden diese Angaben auf dem Aufkleber des fernen Systems.</p> <p>Anmerkung: Für diesen Parameter kann kein Wert angegeben werden, wenn im Parameter RMTNWSCFG eine vorhandene Konfiguration eines fernen Systems angegeben wurde.</p> <p>Einzelwerte:</p> <p>*EID Die Gehäuseidentifikation des Serviceprozessors wird verwendet.</p> <p>Element 1: Seriennummer</p> <p>Seriennummer Geben Sie die Seriennummer des fernen Systems an.</p> <p>Element 2: Hersteller, Typ und Modell</p> <p>Typ-Modell Geben Sie den Maschinentyp und das Modell des fernen Systems im Format ttttmmm an, wobei tttt der Maschinentyp und mmm die Modellnummer ist.</p>	<p>Seriennummer:</p> <p>Hersteller, Typ und Modell:</p>
DELIVERY (Übergabemethode)	<p>Gibt an, wie die für die Konfiguration des fernen Systems erforderlichen Parameter zugestellt werden.</p> <p>Anmerkung: Für diesen Parameter kann kein Wert angegeben werden, wenn im Parameter RMTNWSCFG eine vorhandene Konfiguration eines fernen Systems angegeben wurde.</p> <p>*DYNAMIC Die Parameter werden dynamisch über DHCP an das ferne System übergeben.</p> <p>*MANUAL Die Parameter werden mit den BIOS-Dienstprogrammen (System-BIOS oder Adapter-BIOS - STRG-Q) manuell auf dem fernen System konfiguriert.</p>	

Feld	Beschreibung und Anweisungen	Wert
CHAPAUT (CHAP-Authentifizierung)	<p>Gibt das Challenge Handshake Authentication Protocol (CHAP-Protokoll) für das iSCSI-Ziel des Hostsystems an, um den Initiator-Knoten des fernen Systems zu authentifizieren.</p> <p>Anmerkung: Für diesen Parameter kann kein Wert angegeben werden, wenn im Parameter RMTNWS CFG eine vorhandene Konfiguration eines fernen Systems angegeben wurde.</p> <p>Einzelwerte:</p> <p>*NONE Die CHAP-Authentifizierung ist nicht aktiviert.</p> <p>Element 1: CHAP-Name Geben Sie den CHAP-Namen an.</p> <p>Element 2: Geheimer CHAP-Schlüssel Geben Sie den geheimen Schlüssel für das CHAP-Protokoll an. Verwenden Sie einen maximal 24 Zeichen umfassenden Wert.</p>	<p>CHAP-Name:</p> <p>Geheimer CHAP-Schlüssel:</p>
BOOTDEVID (Boot-einheiten-ID)	<p>Gibt die PCI-Funktionsadresse (Bus/Einheit/Funktion) auf dem iSCSI-Adapter im fernen System an, von der aus gebootet wird. Der Zugriff auf diese Informationen kann mit den BIOS-Dienstprogrammen (System-BIOS oder Adapter-BIOS - STRG-Q) erfolgen.</p> <p>Anmerkung: Für diesen Parameter kann kein Wert angegeben werden, wenn im Parameter RMTNWS CFG eine vorhandene Konfiguration eines fernen Systems angegeben wurde.</p> <p>Einzelwerte:</p> <p>*SINGLE Auf dem fernen System wird der einzelne iSCSI-Adapter verwendet. Anmerkung: Bei fernen Systemen mit mehreren iSCSI-Adaptoren muss angegeben werden, welcher Adapter für den Bootvorgang verwendet werden soll.</p> <p>Element 1: Busnummer Geben Sie die Busnummer des iSCSI-Adapters auf dem fernen System an, mit dem gebootet wird.</p> <p>Element 2: Einheitennummer Geben Sie die Einheitennummer des SCSI-Adapters auf dem fernen System an, mit der gebootet wird.</p> <p>Element 3: Funktion Funktionsnummer Geben Sie die Funktionsnummer des iSCSI-Adapters auf dem fernen System an, mit der gebootet wird.</p>	<p>Busnummer:</p> <p>Einheit:</p> <p>Funktion:</p>

Feld	Beschreibung und Anweisungen	Wert
DYNBOOTOPT (Dynamische Bootoptionen)	<p>Dies ist eine erweiterte Funktion.</p> <p>Mit diesem Parameter wird der interne DHCP-Server konfiguriert, der Bestandteil der Firmware für den iSCSI-Zielhostbusadapter ist und für die Bereitstellung der Parameter für IP-Adresse und Booten ohne Platten Speicher für den fernen iSCSI-Initiator erforderlich ist.</p> <p>Anmerkung: Für diesen Parameter kann kein Wert angegeben werden, wenn im Parameter RMTNWSCFG eine vorhandene Konfiguration eines fernen Systems angegeben wurde.</p> <p>Element 1:</p> <p>Lieferanten-ID Client und Server sind für eine feststehende Lieferanten-ID vorkonfiguriert. Netzadministratoren können Clients so konfigurieren, dass sie ihre eigenen Werte zur Übertragung von Hardware-, Betriebssystem- und anderen Informationen definieren. Für diese Funktion wird DHCP-Option 60 verwendet, die im IETF RFC 2132 beschrieben wird.</p> <p>*DFT Die standardmäßige Lieferanten-ID wird verwendet.</p> <p>Lieferanten-ID Die Lieferanten-ID des iSCSI-Adapters auf dem fernen System wird verwendet.</p> <p>Element 2:</p> <p>Alternative Client-ID Wird von Clients zur Übergabe ihrer eindeutigen Kennung an den Server verwendet. Alle Client-IDs, die auf dem effektiven DHCP-Netzwerk verwendet werden, mit dem die Clients verbunden sind (d. h. das lokale Teilnetz und alle fernen Teilnetze, die über DHCP-Weitergabe erreichbar sind), müssen eindeutig sein. Lieferanten und Systemadministratoren sind für die Auswahl von Client-IDs verantwortlich, die die Bedingung der Eindeutigkeit erfüllen. Für diese Funktion wird DHCP-Option 61 verwendet, die im IETF RFC 2132 beschrieben wird.</p> <p>*ADPT Die Standard-Client-ID ist die Adapteradresse des iSCSI-Adapters des fernen Systems. Mit diesem Wert wird das ferne System identifiziert.</p> <p>Client-ID Geben Sie die Client-ID des iSCSI-Adapters auf dem fernen System an, mit dem gebootet wird.</p>	Lieferanten-ID: Alternative Client-ID:

Feld	Beschreibung und Anweisungen	Wert
RMTIFC (Ferne Schnittstellen)	<p>Gibt die Schnittstelle des fernen Systems an. Die Schnittstellen des fernen Systems werden anhand dieser Informationen identifiziert und konfiguriert. Jeder Adapterport verfügt über zwei Funktionen für die Unterstützung einer SCSI- und einer LAN-Schnittstelle.</p> <p>Anmerkung: Für diesen Parameter kann kein Wert angegeben werden, wenn im Parameter RMTNWS CFG eine vorhandene Konfiguration eines fernen Systems angegeben wurde.</p> <p>Element 1: SCSI-Schnittstelle</p> <p>Element 1: Adapteradresse Geben Sie die aus 12 Hexadezimalzeichen bestehende Adapteradresse für die SCSI-Schnittstelle des fernen Systems an.</p> <p>Element 2: Internetadresse Internetadresse für die SCSI-Schnittstelle des fernen Systems.</p> <p>Element 3: Teilnetzmaske Teilnetzmaske für die SCSI-Schnittstelle des fernen Systems.</p> <p>Element 4: Gatewayadresse Gatewayadresse für die SCSI-Schnittstelle des fernen Systems.</p> <p>Element 5: Qualifizierter iSCSI-Name</p> <p>*GEN</p> <p>Das System erstellt den qualifizierten iSCSI-Namen automatisch.</p> <p>iqn-Name</p> <p>Qualifizierter iSCSI-Name für die SCSI-Schnittstelle des fernen Systems.</p>	<p>SCSI-Schnittstelle</p> <ul style="list-style-type: none"> • Adapteradresse: • Internetadresse: • Teilnetzmaske: • Gatewayadresse (optional): • Qualifizierter iSCSI-Name:
RMTIFC (Ferne Schnittstellen) (Forts.)	<p>Element 2: LAN.Schnittstelle</p> <p>Element 1: Adapteradresse</p> <p>12-stellige hexadezimale Adapteradresse für die LAN- oder TCP Offload Engine (TOE)-Schnittstelle des fernen Systems.</p> <p>Element 2: Internetadresse</p> <p>für die LAN-Schnittstelle des fernen Systems.</p> <p>Element 3: Teilnetzmaske</p> <p>für die LAN-Schnittstelle des fernen Systems.</p> <p>Element 4: Gatewayadresse</p> <p>für die LAN-Schnittstelle des fernen Systems.</p>	<p>LAN-Schnittstelle</p> <ul style="list-style-type: none"> • Adapteradresse: • Internetadresse: • Teilnetzmaske: • Gatewayadresse (optional):

Informationen zum Windows-Clusterdienst

Anmerkungen:

1. Füllen Sie dieses Arbeitsblatt nur dann aus, wenn Sie einen integrierten Server installieren, der an einem Cluster beteiligt ist, und wenn Ihr Hardwaremodell den Windows-Clusterdienst unterstützt. (Integrierte Netfinity-Server unterstützen den Windows-Clusterdienst nicht.)
2. Netzwerkadapter werden in i5/OS als Ports bezeichnet.

Element	Beschreibung und Anweisungen	Wert
Clustername	<p>Gibt den Namen des Clusters an. Administratoren verwenden diesen Namen für Verbindungen zum Cluster. Der Clustername darf nicht mit dem Domännennamen, den Namen der Computer und den Namen anderer Cluster innerhalb der Domäne übereinstimmen.</p> <p>Der Clustername wird zudem zum Erstellen des NWS-Speicherbereichs verwendet, der als Quorum-Ressource des Windows-Clusters dient.</p> <p>*NONE: Keinen Windows-Cluster bilden oder zu einem Windows-Cluster hinzufügen.</p> <p>Clustername: Gibt den Namen des Clusters an.</p>	

Element	Beschreibung und Anweisungen	Wert
Cluster- konfiguration: (Elemente 1 - 4)	<p>Gibt die Parameter an, die zum Konfigurieren eines neuen Windows-Clusters erforderlich sind.</p> <p>Anmerkungen: Dieser Parameter wird verwendet, um die i5/OS-Clusterkonfiguration zu überprüfen. Der Clusterdienst wird mit Hilfe der Konfigurationsassistenten von Microsoft installiert.</p> <p>Dieser Parameter ist nur dann erforderlich, wenn ein neuer Windows-Cluster mit dem Parameter CLU (Clustername) erstellt wird.</p> <p>Element 1: Clusterdomänenname Gibt die Domäne an, zu der der Cluster gehört. Wenn der Cluster bereits vorhanden ist, wird er verbunden, andernfalls wird er gebildet. Beim Bilden eines Clusters muss der Parameter CLUCFG (Clusterkonfiguration) angegeben werden.</p> <p>Clusterdomänenname: Gibt beim Bilden eines neuen Clusters den Namen der Domäne an, der der Cluster angehört.</p> <p>Element 2: Quorum-Ressourcengröße Gibt in Megabyte die Größe des Speicherbereichs an, der als Windows-Quorum-Ressource verwendet wird.</p> <p>*CALC Gibt an, dass für die Größe der Standardwert anhand des Parameters für die Windows-Serverversion (WNTVER) berechnet werden soll.</p> <p>Quorum-Größe Gibt die Größe der Windows-Quorum-Ressource in Megabyte an. Die Größe muss zwischen 550 und 1.024.000 Megabyte liegen.</p> <p>Element 3: Quorum-Ressourcen-ASP Gibt den Zusatzspeicherpool für den Speicherbereich an, der als Windows-Quorum-Ressource verwendet werden soll. Geben Sie einen der folgenden Werte an:</p> <p>1: Der Speicherbereich wird im Zusatzspeicherpool 1, dem System-ASP, erstellt.</p> <p>Quorum-ASP: Gibt einen Wert zwischen 2 und 255 als ASP-ID an. Gültige Werte sind von der Anzahl der auf dem System definierten ASPs abhängig.</p> <p>Element 4: Quorum-ASP-Einheit Gibt den Einheitennamen des unabhängigen Zusatzspeicherpools für den Speicherbereich an, der als Windows-Quorum-Ressource verwendet werden soll. Anmerkung: Sie können entweder einen Wert für den Quorum-Ressourcen-ASP oder einen Wert für die Quorum-ASP-Einheit angeben, jedoch nicht für beides.</p>	Clusterdomänenname: Quorum-Ressourcengröße: Quorum-Ressourcen-ASP: Quorum-ASP-Einheit:

Element	Beschreibung und Anweisungen	Wert
Cluster-konfiguration: (Elemente 5-7)	<p>Element 5: Cluster-Verbindungsport Gibt den Verbindungsport an, der für die Clusterdienst-Kommunikation verwendet wird.</p> <p>*VRTETHx: Der Virtual Ethernet-Port x des Netzwerkserver wird konfiguriert, wobei x für einen Wert zwischen 0 und 9 steht.</p> <p>Anmerkung: Der Virtual Ethernet-Port muss so konfiguriert werden, dass er mit diesem Wert übereinstimmt.</p> <p>Element 6: Cluster-Internet-Adresse Gibt die Internet-Adresse des Clusters an.</p> <p>IP-Adresse: Gibt die Internet-Adresse des Clusters im Format xxx.yyy.zzz.nnn an, wobei xxx, yyy, zzz und nnn Dezimalzahlen zwischen 0 und 255 darstellen.</p> <p>Anmerkung: Die ausgewählte Internet-Adresse muss in allen NWS-Objekten und der TCP/IP-Konfiguration von i5/OS eindeutig sein.</p> <p>Element 7: Clusterteilnetzmaske</p> <p>Teilnetzmaske: Gibt die Teilnetzmaske des Clusters im Format nnn.nnn.nnn.nnn an, wobei nnn eine Dezimalzahl zwischen 0 und 255 darstellt.</p>	<p>Verbindungsport:</p> <p>Cluster-Internet-Adresse:</p> <p>Clusterteilnetzmaske:</p>

Vergleich der Dateisysteme FAT, FAT32 und NTFS

Bei Windows 2000 Server und Windows Server 2003 können Sie zwischen den Dateisystemen NTFS und FAT32 wählen. IBM i5/OS Integrated Server Support installiert die Systemlaufwerke mit einem geeigneten Dateisystem. Dieses ist abhängig von der Kapazität der Hardwareressourcen, der verwendeten Windows-Version und dem gewünschten Verwendungszweck. Der Installationsbefehl konvertiert FAT32-Laufwerke in NTFS, sofern nicht CVTNTFS(*NO) angegeben wird.

Anmerkung:

Laufwerk D darf **nicht** in NTFS konvertiert werden. Es muss als FAT-Laufwerk bestehen bleiben.

Laufwerk C kann konvertiert werden. Die folgende Tabelle enthält einige Vergleiche, die Ihnen bei der Entscheidung helfen können:

FAT	FAT32	NTFS
Datenträger von Diskettengröße bis 4 GB	Datenträger von 512 MB bis 2 Terabyte	Datenträger von 10 MB bis 2 TB
Maximale Dateigröße 2 GB	Maximale Dateigröße 4 GB	Dateigröße durch Datenträgergröße begrenzt
Keine Unterstützung für Windows 2000 oder Windows Server 2003 Active Directory	Keine Unterstützung für Windows 2000 oder Windows Server 2003 Active Directory	Für Verwendung von Windows 2000 oder Windows Server 2003 Active Directory oder gemeinsam genutzte Clusterlaufwerke erforderlich
Ermöglicht den Zugriff auf Dateien der Festplatte im PC-DOS-Modus	Ermöglicht den Zugriff auf Dateien der Festplatte im PC-DOS-Modus	Kein Zugriff im PC-DOS-Modus auf Dateien der Festplatte

FAT	FAT32	NTFS
Ermöglicht die Anpassung des Servers mit NWSD-Konfigurationsdateien	Ermöglicht die Anpassung des Servers mit NWSD-Konfigurationsdateien	Keine Verwendung von NWSD-Konfigurationsdateien möglich
Ermöglicht die Verwendung des NWSD-Speicherauszugstools (QFPDMPLS), um Dateien von der Platte abzurufen	Ermöglicht die Verwendung des NWSD-Speicherauszugstools (QFPDMPLS), um Dateien von der Platte abzurufen	Keine Verwendung des Speicherauszugstools zum Abrufen von Dateien von der Platte möglich

Tipp: Ressourcennamen bei mehreren integrierten Servern suchen

Auf Ihrer iSeries können mehrere integrierte Server desselben Typs installiert sein. In diesem Fall kann es schwierig werden, sie in der Anzeige DFV-Ressourcen anzeigen voneinander zu unterscheiden.

So stellen Sie fest, auf welchen integrierten Server ein Ressourcename verweist:

1. Wenn Sie die Anzeige DFV-Ressourcen anzeigen noch nicht aufgerufen haben, müssen Sie DSPHDWRSC *CMN eingeben und die Eingabetaste drücken.
2. Geben Sie im Feld Auswahl links neben dem Ressourcennamen eine 7 für einen FSI0P ein. Die Anzeige Ressourcendetails anzeigen wird aufgerufen. Für Server mit iSCSI-Anschluss lokalisieren Sie den NWS-Hostadapter. Diese Ressource wird beim Erstellen eines NWSH-Objekts verwendet. Der Name des NWSH-Objekts wird bei der Installation der NWSD verwendet.
3. Beachten Sie die Kartenposition unter der Überschrift Physische Position.
4. Prüfen Sie die Etiketten auf den Steckplätzen der iSeries. Ein Steckplatz sollte mit der gleichen Zahl oder Kombination aus Buchstaben und Zahlen beschriftet sein, die im Feld Kartenposition angezeigt wird. Dieser Steckplatz enthält die Hardware des integrierten xSeries-Servers, auf die der Ressourcename verweist.

Bitte fahren Sie nun wieder mit dem „Installationsarbeitsblatt für i5/OS-Parameter“ auf Seite 73 fort.

Unterstützte Sprachversionen

Die folgenden Sprachen werden im Parameter für die Sprachversion (LNGVER) des Befehls INSWNTSVR (Windows-Server installieren) unterstützt:

LNGVER	Landessprache
*PRIMARY	Verwendet die Sprachversion der Primärsprache, die auf der iSeries installiert ist
2911	Slowenisch
2922	Portugiesisch
2923	Holländisch
2924	Englisch (Groß-/Kleinschreibung)
2925	Finnisch
2926	Dänisch
2928	Französisch
2929	Deutsch
2931	Spanisch
2932	Italienisch
2933	Norwegisch
2937	Schwedisch
2938	Englisch (Großschreibung DBCS)

LNGVER	Landessprache
2939	Deutsch (MNCS)
2940	Französisch (MNCS)
2942	Italienisch (MNCS)
2950	Englisch (Großschreibung)
2962	Japanisch DBCS
2963	Holländisch (MNCS)
2966	Belgisches Französisch
2975	Tschechisch
2976	Ungarisch
2978	Polnisch
2979	Russisch
2980	Brasilianisches Portugiesisch
2981	Kanadisches Französisch (MNCS)
2984	Englisch (Groß-/Kleinschreibung DBCS)
2986	Koreanisch DBCS
2987	Traditionelles Chinesisch
2989	Vereinfachtes Chinesisch
2994	Slowakisch
2996	Portugiesisch MNCS


IBM i5/OS Integrated Server Support unterstützt die mehrsprachige Benutzeroberfläche von Windows.

Windows 2000 Server oder Windows Server 2003 installieren

Zur Durchführung der Installation benötigen Sie Folgendes:




- CD mit der Software für Windows 2000 Server oder Windows Server 2003 (oder ein Image der CD).
- Windows-Lizenzschlüssel (auf der Rückseite des Transportbehälters für die Installations-CD oder im Zertifikatsdokument).
- Ausgefülltes und gedrucktes „Installationsarbeitsblatt für i5/OS-Parameter“ auf Seite 73 oder die Befehlszeichenfolge, die durch die Advisorfunktion für die Installation generiert wurde.

Anmerkung: Die Microsoft Dokumentation enthält Anweisungen, die besagen, dass die Plattenspiegelung inaktiviert und die unterbrechungsfreie Stromversorgung (USV) getrennt werden soll, bevor die Installation oder der Upgrade des Windows-Servers erfolgt. Dies betrifft allerdings nicht die Plattenspiegelung oder die unterbrechungsfreie Stromversorgung Ihrer iSeries.

Anmerkung: Wenn Ihr integrierter xSeries-Server, ein integrierter xSeries-Adapter oder ein iSCSI-HBA im Abschnitt „Hardwarevoraussetzungen“ auf Seite 62 nicht aufgeführt ist, können Sie die Installationsanweisungen auf der Website IBM Integrated xSeries solutions nachlesen. 

Führen Sie die folgenden Schritte aus:

1. Bereiten Sie die Hardware des integrierten xSeries-Servers vor. Weitere Informationen finden Sie unter den folgenden Links.

- | • IXA install read me first 
| (www.ibm.com/servers/eserver/series/integratedxseries/ixareadme)
 - | • iSCSI install read me first 
| (www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme)
 - | • IXS install read me first 
| (www.ibm.com/servers/eserver/series/integratedxseries/ixsreadme)
- | 2. Wenn Sie einen Server mit iSCSI-Anschluss installieren, beachten Sie den Abschnitt „iSCSI-Hardware für Windows-Installation vorbereiten“
 - | 3. „Installation über die i5/OS-Konsole starten“ auf Seite 100.
 - | 4. „Installation über die Konsole des integrierten Windows-Servers fortsetzen“ auf Seite 103.
 - | 5. „Serverinstallation abschließen“ auf Seite 104.

Wenn während der Installation Fehlermeldungen ausgegeben werden, finden Sie im Abschnitt „Fehlermeldungen während der Installation beantworten“ auf Seite 116 weitere Informationen.

| **iSCSI-Hardware für Windows-Installation vorbereiten**

| Für Server mit iSCSI-Anschluss müssen nach der Vorbereitung der Hardware weitere Konfigurationsschritte erfolgen.

- | • „Serviceprozessorsicherheit initialisieren“
- | • „NWS-Hostadapter erstellen und starten“

| **Serviceprozessorsicherheit initialisieren**

| Wenn Sie eine neue Serviceprozessorkonfiguration für einen neuen Serviceprozessor erstellt haben, sollten Sie die Sicherheitseinstellungen ändern und statt der Standardwerte für den Benutzernamen und das Kennwort des Serviceprozessors neue Werte eingeben.

| Wählen Sie aus der folgenden Liste die Prozedur aus, die der Sicherheitsmethode entspricht, die Sie verwenden möchten.

- | • Verwenden Sie für ein Serviceprozessorkennwort ohne SSL die unter „Serviceprozessorkennwort“ auf Seite 142 beschriebene Prozedur.
- | • Verwenden Sie für ein Serviceprozessorkennwort mit SSL die unter „Serviceprozessor-SSL konfigurieren“ auf Seite 140 beschriebene Prozedur.

| **NWS-Hostadapter erstellen und starten**

| Bevor Windows auf einem Server mit iSCSI-Anschluss installiert werden kann, muss ein iSCSI-Ziel-HBA im iSeries-Server konfiguriert werden. Diese Konfiguration wird als NWS-Hostadaptereinheit (NWSH) bezeichnet.

| Eine NWSH-Einheit kann von mehreren aktiven Servern benutzt werden. Wenn Ihr neuer Server eine vorhandene NWSH-Einheit benutzen soll, verifizieren Sie, dass diese gestartet ist.

| So erstellen und starten (anhängen) Sie eine neue NWSH-Einheit:

- | 1. Identifizieren Sie die NWSH-Hardwareressource folgendermaßen mit iSeries Navigator:
 - | a. Erweitern Sie **Konfiguration und Service** —> **Hardware** —> **Datenübertragung**.
 - | b. Notieren Sie den Ressourcennamen für alle Ressourcen mit der Beschreibung "NWS-Hostadapter".
 - | c. Wenn Sie einen CL-Befehl verwenden möchten, geben Sie WRKHDWRSC TYPE(*CMN) ein.
- | 2. Erstellen Sie eine NWSH-Einheit. Weitere Informationen finden Sie unter „NWS-Hostadapterobjekt erstellen“ auf Seite 127.
- | 3. Starten Sie die NWSH-Einheit. Weitere Informationen finden Sie unter „NWS-Hostadapter starten“ auf Seite 129.

Installation über die i5/OS-Konsole starten

Zum Installieren von Windows 2000 Server oder Windows Server 2003 auf der iSeries benötigen Sie die Sonderberechtigungen *IOSYSCFG, *ALLOBJ und *JOBCTL. Außerdem müssen Sie den Lizenzschlüssel für den Windows-Server zur Hand haben. In den meisten Fällen ist er auf der Rückseite des Transportbehälters für die Installations-CD aufgedruckt.

1. Wenn Sie eine Installation der Art *FULL ausführen, legen Sie die Installations-CD in das optische Laufwerk des iSeries-Servers ein (falls kein Image der Installations-CD verwendet werden soll).
Wenn Sie eine Installation der Art *BASIC ausführen, legen Sie die ServerGuide-CD in das CD-ROM-Laufwerk des angeschlossenen xSeries-Servers ein.

2. Starten Sie die Installation mit einer der folgenden Methoden:

- Wenn der Befehl INSWNTSVR (Windows-Server installieren) verfügbar ist, der von der Advisorfunktion für die Installation des Windows-Servers generiert wurde:
 - a. Geben Sie call QCMD in der i5/OS-Befehlszeile ein, um eine Befehlseingabeaufforderung zu starten, und wählen Sie F11=Vollbild aus.
 - b. Fügen Sie den von der Advisorfunktion für die Installation des Windows-Servers generierten Befehl INSWNTSVR in die i5/OS-Befehlszeile ein, und drücken Sie die Eingabetaste, um den Befehl auszuführen.
 - c. Die Installation wird jetzt gestartet. Sie kann bis zu einer Stunde dauern. Möglicherweise werden Sie im Verlauf zur Eingabe weiterer Informationen aufgefordert. Bitte fahren Sie anschließend mit dem Abschnitt „Installation über die Konsole des integrierten Windows-Servers fortsetzen“ auf Seite 103 fort.
- Sie können die Installation auf starten, indem Sie in die i5/OS-Befehlszeile den Befehl INSWNTSVR eingeben und zum Aufruf des Befehls F4 drücken. Geben Sie die Werte aus dem „Installationsarbeitsblatt für i5/OS-Parameter“ auf Seite 73 in den folgenden Feldern ein:

3. Geben Sie im Feld "NWS-Beschreibung" (siehe „NWS-Beschreibungen“ auf Seite 73) den Servernamen aus dem „Installationsarbeitsblatt für i5/OS-Parameter“ auf Seite 73 ein, und drücken Sie die Eingabetaste.
4. Geben Sie im Feld Installationsart den Wert ein (*FULL oder *BASIC), den Sie im „Installationsarbeitsblatt für i5/OS-Parameter“ auf Seite 73 angegeben haben.
5. Geben Sie im Feld Ressourcenname denselben Wert wie im „Installationsarbeitsblatt für i5/OS-Parameter“ auf Seite 73 ein.
6. Wählen Sie die Windows-Serverversion aus, die Sie installieren möchten, und drücken Sie die Eingabetaste.

Anmerkung: Für Server mit iSCSI-Anschluss ist Windows Server 2003 erforderlich.

7. Soll der Server von einem gespeicherten Image anstelle der physischen CD installiert werden, geben Sie den Pfad für dieses Image im Feld Windows-Quellenverzeichnis an.
8. Verwenden Sie im Feld Installationsauswahl die Standardeinstellung *INSTALL.
9. Wenn bei der Installation die TCP/IP-Eigenschaften aller auf der iSeries installierten Netzwerkadapter konfiguriert werden sollen, die durch den neuen integrierten Server gesteuert werden, geben Sie die Werte für die Windows-TCP/IP-Konfiguration aus dem „Installationsarbeitsblatt für i5/OS-Parameter“ auf Seite 73 an. Andernfalls überspringen Sie diesen Schritt und verwenden den Standardwert *NONE.
10. Zur Installation und Konfiguration eines Virtual Ethernet-Ports geben Sie die Werte für die Windows-TCP/IP-Konfiguration aus dem Feld für den Virtual Ethernet-Port im „Installationsarbeitsblatt für i5/OS-Parameter“ auf Seite 73 an.
11. Geben Sie die Werte aus dem „Installationsarbeitsblatt für i5/OS-Parameter“ auf Seite 73 in den folgenden Feldern ein:
 - Name der lokalen TCP/IP-Domäne
 - TCP/IP-Namensserversystem

- | • Servernachrichtwarteschlange
 - | • Bibliothek
- | 12. Geben Sie im Feld Ereignisprotokoll an, welche Ereignisprotokollnachrichten i5/OS vom Server empfangen soll.
 - | 13. Geben Sie in den Feldern für die Serverspeicherbereiche die Werte aus dem „Installationsarbeitsblatt für i5/OS-Parameter“ auf Seite 73 ein:
 - | • Geben Sie Werte in den Feldern für die Größe der Installationsquelle und der Systemgröße ein, oder wählen Sie den Standardwert *CALC aus, damit das System die Mindestgröße errechnet.
 - | • Soll für das Installationsquellenlaufwerk und das Systemlaufwerk jeweils ein unterschiedlicher Zusatzspeicherpool (ASP) gewählt werden, geben Sie den Pool im entsprechenden Element der Felder Speicherbereichs-ASP oder ASP-Einheit SVR-Speicherbereich an.
 - | • Bei Systemlaufwerken bis 32 GB können Sie im Feld "In NTFS umsetzen" den Wert *NO angeben, um die Formatierung des Systemlaufwerks des integrierten Servers als FAT-Dateisystem (FAT32=File Allocation Table) beizubehalten. Soll das Systemlaufwerk während der Installation in das NTFS-Dateisystem (NTFS=New Technology File System) konvertiert werden, geben Sie den Wert *YES an. Informationen, die Ihnen bei dieser Entscheidung helfen können, finden Sie unter „Vergleich der Dateisysteme FAT, FAT32 und NTFS“ auf Seite 96. Mit dem Befehl INSWNTSVR werden Systemlaufwerke, die größer 32 GB sind, automatisch in NTFS umgesetzt (sofern erforderlich).
 - | 14. **Optional:** Geben Sie entweder eine Windows-Arbeitsgruppe oder -Domäne für die entsprechenden Parameter Zu Arbeitsgruppe oder Zu Domäne an.
 - | 15. **Optional:** Geben Sie im Feld Vollständiger Name den Namen des Benutzers an, der die Windows-Serverlizenz besitzt, die installiert wird.
 - | 16. **Optional:** Geben Sie im Feld Organisation den Namen der Organisation an, die die Windows-Serverlizenz besitzt, die installiert wird.
 - | 17. Geben Sie im Feld Sprachversion den Wert *PRIMARY an, damit IBM i5/OS Integrated Server Support die Primärsprache verwendet. Stellen Sie sicher, dass das Lizenzprogramm für die Integration und der Windows-Server dieselbe Sprache verwenden, um zu verhindern, dass Probleme mit vordefinierten Namen auftreten, die nicht registriert werden können. Weitere Informationen zu den von diesem Befehl unterstützten Sprachen finden Sie unter „Unterstützte Sprachversionen“ auf Seite 97.
 - | 18. Geben Sie im Feld Datum und Uhrzeit synchronisieren den Wert *YES an, damit i5/OS Datum und Uhrzeit alle 30 Minuten mit dem integrierten Server synchronisiert. Soll i5/OS Datum und Uhrzeit nur dann mit dem integrierten Server synchronisieren, wenn er angehängt wird, geben Sie den Wert *NO ein.
 - | 19. Geben Sie im Feld Domänenbenutzer weitergeben an, ob über diesen Server Benutzer an die Windows-Domäne oder das Active Directory weitergegeben und mit diesen synchronisiert werden sollen.
 - | 20. Geben Sie im Feld Windows-Lizenzberechtigung den von Microsoft gelieferten CD-Schlüssel einschließlich Gedankenstrich an. In den meisten Fällen ist der CD-Schlüssel auf der Rückseite des Transportbehälters für die Windows-Installations-CD aufgedruckt.
 - | 21. Geben Sie im Feld Lizenzart die Art der erworbenen Windows-Serverlizenz an.
 - | 22. Wenn Sie im Feld Lizenzart den Wert *PERSERVER angegeben haben, müssen Sie im Feld Clientlizenzen die Anzahl der erworbenen Clientlizenzen eingeben.
 - | 23. Geben Sie im Feld Terminalservices die zu installierenden Terminalserviceoptionen an.
 - | 24. Geben Sie im Feld Eingeschränkte Einheitenressourcen den Wert aus dem „Installationsarbeitsblatt für i5/OS-Parameter“ auf Seite 73 ein.
 - | 25. Geben Sie im Feld Zeitlimit bei Systemabschluss für den integrierten Server das Zeitlimit für den Systemabschluss in Minuten an. Dieser Wert wird verwendet, um die Zeit zu begrenzen, die dem Betriebssystem des integrierten Servers für den Systemabschluss zur Verfügung steht, bevor der Server abgehängt wird.

26. Wenn Sie einen Server mit IXA-Anschluss oder einen IXS-Server installieren, fahren Sie mit Schritt 34 auf Seite 103 fort, und geben Sie die zusätzlichen Parameter an. Wenn Sie einen Server mit iSCSI-Anschluss installieren, geben Sie die Werte für die iSCSI-Parameter aus dem „Installationsarbeitsblatt für i5/OS-Parameter“ auf Seite 73 in die folgenden Felder ein:
- Aktivierungszeitgeber
 - DFV-Nachrichtenwarteschlange
27. Geben Sie im Feld Speicherpfad den Namen des NWS-Hostadapters an, der für die iSCSI-Speicherübertragung verwendet werden soll. Weitere Informationen finden Sie unter „NWS-Hostadapter“ auf Seite 45.
28. Geben Sie im Feld Virtual Ethernet-Pfad den Namen eines oder mehrerer NWS-Hostadapter ein, die für die iSCSI-LAN-Übertragung verwendet werden sollen.
- Geben Sie mindestens einen Wert für den Port *VRTETHPTP und alle weiteren Ports an, die weiter oben im Feld Virtual Ethernet-Port angegeben wurden.
29. **Optional:** Geben Sie den TCP-Port für Systemabschluss und den Virtual Ethernet-Steuerport an.
30. Geben Sie für die folgenden Felder einen vorhandenen Namen für die NWS-Konfiguration ein, oder wählen Sie die Standardwerte aus.
- NWSCFG des fernen Systems
 - NWSCFG des Serviceprozessors
 - NWSCFG der Verbindungssicherheit
- Drücken Sie die Eingabetaste.
31. Geben Sie die zu verwendende IP-Sicherheitsregel (IPSec) ein:
- Für eine vorhandene NWSCFG der Verbindungssicherheit:
 - a. Geben Sie die konfigurierte Sicherheitsregel im Feld IP-Sicherheitsregel an.
 - b. Drücken Sie die Eingabetaste.
 - Für eine standardmäßige NWSCFG der Verbindungssicherheit:
 - a. Geben Sie die gewünschte IP-Standardsicherheitsregel (IPSec) im gleichnamigen Feld an.
 - b. Drücken Sie die Eingabetaste.
32. Geben Sie nach Aufforderung Daten zur Serviceprozessorkonfiguration aus dem „Installationsarbeitsblatt für i5/OS-Parameter“ auf Seite 73 in diesen Feldern ein, wenn Sie den Standardwert für NWSCFG-Name für Serviceprozessor verwenden:
- Geben Sie im Feld Serviceprozessor initialisieren Folgendes ein:
 - a. Wenn für die Initialisierung des Serviceprozessors ein anderer Wert als *NONE gilt, geben Sie einen Komponenten- und Vergleichswert im Feld für die SP-Zertifikats-ID ein.
 - Wählen Sie die gewünschte Unicast-Option im Feld "Unicast aktivieren" aus:
 - a. Wenn Sie Unicast nicht verwenden, geben Sie mindestens einen Wert für die Gehäuseidentifikation ein, und geben Sie einen Wert für die Seriennummer sowie (optional) Hersteller und Modell an.
 - b. Wenn Sie Unicast verwenden, geben Sie einen Wert für den Serviceprozessornamen an, oder geben Sie eine IP-Adresse im SP-Internetadressfeld ein.
 - Wenn Sie den Standardwert für "NWSCFG-Name für fernes System" verwenden, und für die Initialisierung des Serviceprozessors ein anderer Wert als *NONE gilt, geben Sie die SP-Authentifizierungswerte für den Benutzernamen und das Benutzerkennwort an.
33. Geben Sie nach Aufforderung Daten zur Konfiguration des fernen Systems aus dem „Installationsarbeitsblatt für i5/OS-Parameter“ auf Seite 73 in diesen Feldern ein, wenn Sie den Standardwert für NWSCFG-Name für fernes System verwenden:
- Geben Sie im Feld ID des fernen Systems einen der folgenden Werte ein an:
 - a. Verwenden Sie die Seriennummer aus dem Feld für die Gehäuseidentifikation der Serviceprozessor-NWSCFG.

- | b. Geben Sie einen Wert für die Seriennummer sowie (optional) Hersteller und Modell im Feld
- | für die ID des fernen Systems an.
- | • Geben Sie im Feld Übergabemethode die Methode ein, mit der das ferne System konfiguriert wird.
- | • Geben Sie im Feld CHAP-Authentifizierung die CHAP-Werte (CHAP = Challenge Handshake
- | Authentication Protocol) ein, die für die Authentifizierung des fernen Systems verwendet werden.
- | • Geben Sie im Feld Booteinheiten-ID den iSCSI-Adapter an, mit dem das ferne System gebootet
- | wird. Verwenden Sie den Standardwert *SINGLE, wenn das ferne System nur über eine iSCSI-
- | Booteinheit verfügt.
- | • Wenn Sie *DYNAMIC als Übergabemethode verwenden, können Sie wahlweise alle weiteren Opti-
- | onen im Feld Dynamische Bootoptionen angeben.
- | • Geben Sie im Feld Ferne Schnittstelle Werte für die im fernen System verwendete Schnittstelle
- | ein.
- | a. Geben Sie im Feld SCSI-Schnittstelle Werte für die SCSI-Funktion ein. Dazu gehören:
- | 1) Die SCSI-Adapteradresse
- | 2) Die SCSI-Internetadresse
- | 3) Die SCSI-Teilnetzmaske
- | 4) **Optional:** Geben Sie die SCSI-Gatewayadresse ein
- | 5) Geben Sie den qualifizierten iSCSI-Name ein, oder erlauben Sie dem System durch Eingabe
- | von *GEN, die Adresse automatisch zu generieren.
- | b. Geben Sie im Feld LAN-Schnittstelle Werte für die LAN-Funktion ein. Dazu gehören:
- | 1) Die LAN (TOE)-Adapteradresse
- | 2) Die LAN-Internetadresse
- | 3) Die LAN-Teilnetzmaske
- | 4) **Optional:** Geben Sie die LAN-Gatewayadresse ein

34. Bei Angabe von zusätzlichen Parametern können Sie Folgendes ausführen:

- Einen von der Standardeinstellung abweichenden Tastaturtyp auf dem integrierten Server installieren. (Gültige Tastaturbelegungs-IDs befinden sich in der Datei TXTSETUP.SIF im Verzeichnis I386 der Installationsquelle für den Windows-Server.)
- Ihre eigenen IP-Adressen für das Virtual Ethernet-PTP verwenden.
- Eine NWSD-Konfigurationsdatei verwenden. Weitere Informationen hierzu finden Sie in Kapitel 15, „Konfigurationsdateien für NWS-Beschreibung (NWSD)“, auf Seite 261.
- Eine neue oder vorhandene Windows-Clusterkonfiguration definieren.

Geben Sie alle weiteren noch benötigten Informationen ein, und drücken Sie die Eingabetaste.

Der integrierte Windows-Server wird jetzt installiert. Die zweite Phase des Installationsprozesses ist im Abschnitt „Installation über die Konsole des integrierten Windows-Servers fortsetzen“ beschrieben. Der Prozess dauert etwa eine Stunde, abhängig von der vorhandenen Hardwarekonfiguration.

Installation über die Konsole des integrierten Windows-Servers fortsetzen

Wenn die i5/OS-Phase der Installation beendet ist, wird der integrierte Server gestartet. Damit beginnt die Windows-Server-Phase der Installation. Diese Installationsphase ist einfach durchzuführen, wenn Sie die im Abschnitt „Installation von integrierten Windows-Servern vorbereiten“ auf Seite 64 beschriebenen Schritte ausgeführt und die Installationsattribute im Befehl INSWNTSVR (Windows-Server installieren) angegeben haben.

So schließen Sie die Installation des Windows-Servers ohne die ServerGuide-CD ab:

1. Klicken Sie im Schritt **Lizenzvereinbarung** (im Fenster für den Setup des Windows-Servers) auf das Optionsfeld **Vereinbarung akzeptieren**. Klicken Sie dann auf **Weiter**.

2. Wenn Fehlermeldungen angezeigt werden, klicken Sie auf **OK**. Das Installationsprogramm lässt Ihnen Zeit, um die Fehler zu korrigieren oder die erforderlichen Informationen zur Verfügung zu stellen. Beispiele dieser Fehlermeldungen und Informationen zu deren Beantwortung finden Sie unter „Fehlermeldungen während der Installation beantworten“ auf Seite 116.
3. Geben Sie das Kennwort im Fenster **Computernamen und Administratorkennwort** ein.
4. Führen Sie in der Anzeige **Datum und Uhrzeiteinstellungen** folgende Schritte aus:
 - a. Bestätigen Sie, dass die i5/OS-Zeitzone richtig ist und mit dem Systemwert für die Zeitzone übereinstimmt, der in der Advisorfunktion für die Installation des Windows-Servers angegeben wurde. Entsprechende Angaben finden Sie unter „Zeitsynchronisation“ auf Seite 67.
 - b. Befindet sich das System in einem Gebiet mit Sommerzeitumstellung, lassen Sie das Markierungsfeld **Uhr automatisch auf Sommer-/Winterzeit umstellen** aktiviert.
Ist keine Umstellung auf die Sommerzeit erforderlich, inaktivieren Sie das Markierungsfeld "Uhr automatisch auf Sommer-/Winterzeit umstellen".
5. Klicken Sie im Fenster für die Fertigstellung des Windows-Installationsassistenten auf **Fertig stellen**.
6. Klicken Sie im Fenster für den **Windows-Setup** auf die Schaltfläche **Jetzt neu starten**, oder warten Sie 15 Sekunden, bis der Server automatisch neu startet.

Anmerkung:

Wird der integrierte Windows-Server als Domänencontroller installiert, sollte das Active Directory zu diesem Zeitpunkt mit dem Befehl DCPRMO installiert werden. Weitere Informationen zur Installation des Active Directory finden Sie in der Dokumentation von Microsoft.


So schließen Sie die Installation des Windows-Servers bei Verwendung der ServerGuide-CD ab:

- Legen Sie die ServerGuide-CD in das lokale optische Laufwerk des über HSL angeschlossenen Servers ein (dies ist der über IXA angeschlossene xSeries-Server).
- Geben Sie **G** als Antwort auf die Nachricht NTA100C "(C G) Die ServerGuide CD-ROM in die optische Einheit &2 einlegen." ein.
- Befolgen Sie die Anweisungen des ServerGuide-Assistenten zur Ausführung des Installationsprozesses.

Weitere Informationen enthält der Abschnitt „Serverinstallation abschließen“.

Serverinstallation abschließen

Einige abschließende Schritte nach der Installation von Windows 2000 Server oder Windows Server 2003 unter i5/OS gewährleisten, dass der Server korrekt installiert wurde und betriebsbereit ist.

1. Es empfiehlt sich, das neueste unterstützte Service-Pack von Microsoft zu installieren. Eine Liste der neuesten unterstützten Service-Packs finden Sie auf der Seite mit den Microsoft Service-Packs. Diese Seite erreichen Sie über die Seite mit den Serviceinformationen der Website IBM Integrated xSeries solutions. 
2. Wenn der integrierte Windows-Server nach dem Starten von TCP/IP automatisch angehängt werden soll, lesen Sie die Informationen unter „Integrierten Windows-Server für automatisches Anhängen mit TCP/IP einstellen“ auf Seite 117.
3. Wenn der Systemwert QRETSVRSEC noch nicht für die Installation eines Servers mit iSCSI-Anschluss aktiviert wurde, ändern Sie den Wert unter i5/OS, um sicherzustellen, dass i5/OS Kennwörter speichert (dies vermeidet Verzögerungen bei der Benutzeranmeldung):
 - Geben Sie in der i5/OS-Befehlszeile den folgenden Befehl ein:
WRKSYSVAL SYSVAL(QRETSVRSEC)
 - Geben Sie zum Ändern des Werts eine 2 im Feld Auswahl ein, und drücken Sie die Eingabetaste.
 - Ändern Sie den Wert für Server-Sicherheitsdaten sichern in 1.
4. Soll der Server einen anderen als den NWSD-Namen erhalten (z. B. einen Namen mit mehr als acht Zeichen), können Sie den Systemnamen an der Windows-Konsole ändern. Weitere Informationen finden Sie in der Windows-Dokumentation.

5. Für Anwendungen und Daten können Sie zusätzliche Plattenlaufwerke erstellen, statt sie auf dem Systemlaufwerk zu speichern. Weitere Informationen finden Sie unter „Plattenlaufwerke zu integrierten Windows-Servern hinzufügen“ auf Seite 172.
6. Sie können zusätzliche Virtual Ethernet-LANs für Ihren Server definieren, so dass er Verbindungen zu anderen Servern in derselben oder anderen Partitionen herstellen kann. Weitere Informationen finden Sie in Kapitel 6, „Virtual Ethernet- und externe Netzwerke verwalten“, auf Seite 121.
7. Sie können einige Ihrer i5/OS-Benutzer beim Windows-Server oder der Windows-Domäne registrieren. Weitere Informationen finden Sie in Kapitel 11, „Benutzer des integrierten Windows-Servers unter i5/OS verwalten“, auf Seite 187.
8. Sie können verhindern, dass für das optische Laufwerk der Laufwerkbuchstabe beim Anhängen eines benutzereigenen Speicherbereichs an den Server geändert wird. Ordnen Sie dem optischen Laufwerk des integrierten Servers mit der **Datenträgerverwaltung** einen Laufwerkbuchstaben zu. (Sie könnten beispielsweise Laufwerk X festlegen.)
9. Sie können die Server durch Erstellen einer eigenen NWSD-Konfigurationsdatei anpassen. Weitere Informationen hierzu finden Sie in Kapitel 15, „Konfigurationsdateien für NWS-Beschreibung (NWSD)“, auf Seite 261.
10. Wenn Sie Windows-Clustering wünschen, finden Sie weitere Informationen unter „Windows-Clusterdienst“ auf Seite 108.
11. Wenn der Server mit Windows Server 2003 installiert wurde und das Active Directory installiert ist (weil beispielsweise der Server ein Domänencontroller ist), lesen Sie die Informationen im Abschnitt „Kerberos für Windows Server 2003 Active Directory Server aktivieren“ auf Seite 115.
12. Bei Verwendung des IXS-Hardwaretyps 2892-002 oder 4812-001 mit Microsoft Windows 2000 Server müssen Sie spezielle Bildschirmeinheitentreiber installieren, um den ATI Radeon-Video-Chip auf dem IXS 2892-002 bzw. 4812-001 nutzen zu können. Weitere Informationen finden Sie unter „ATI Radeon 7000M-Bildschirmeinheitentreiber für Windows 2000 auf dem integrierten xSeries-Server 2892-002 oder 4812-001 installieren“ auf Seite 115.
13. Bei Verwendung des IXS-Hardwaretyps 2892-002 oder 4812-001 mit Microsoft Windows Server 2003 müssen die Einstellungen für die Hardwarebeschleunigung angepasst werden, um eine optimale Systemleistung zu erzielen. Weitere Informationen finden Sie unter „Hardwarebeschleunigung für Windows Server 2003 auf dem integrierten xSeries-Server 2892-002 oder 4812-001 anpassen“ auf Seite 116.


Achtung: Wenn Sie planen, eine Firewall mit dem integrierten Server zu benutzen, muss sichergestellt werden, dass die Internet-Adressen für das Virtual Ethernet-PTP nicht an einen SOCKS-Server (SOCKS = Software Common Knowledge IR System) weitergeleitet werden, der als Firewall dient. Andernfalls kommt es zu Verbindungsfehlern. Weitere Informationen zum Einrichten einer Firewall finden Sie im Thema zu Firewall: Einführung.

Für Server mit iSCSI-Anschluss können Sie außerdem die folgenden Schritte ausführen:

1. Sie können Ihren Server für die Verwendung zusätzlicher iSCSI-HBAs konfigurieren, um damit das Leistungsverhalten oder die Verfügbarkeit verbessern. Weitere Informationen finden Sie unter „iSCSI-HBA-Nutzung verwalten“ auf Seite 144.
2. Wenn Ihr iSCSI-Netzwerk große Rahmengrößen unterstützt, können Sie möglicherweise das Leistungsverhalten des Virtual Ethernet verbessern. Weitere Informationen finden Sie unter „Überlegungen zur größten zu übertragenden Einheit (MTU)“ auf Seite 147.


Upgrade des Lizenzprogramms IBM iSeries Integration für Windows-Server durchführen

Wenn Sie einen Upgrade von i5/OS und IBM iSeries Integration für Windows-Server auf V5R4 ausführen, benötigen Sie die CD mit dem Produkt 5722-SS1. Ist auch die Installation neuer Hardware für den

integrierten xSeries-Server geplant, müssen Sie zuerst diese neue Software installieren. Befolgen Sie die Anweisungen zur Upgradeprozedur im Handbuch iSeries Softwareinstallation.  Führen Sie zusätzlich die folgenden Arbeitsschritte durch:

Upgrade vorbereiten:

1. Vergewissern Sie sich, dass Sie die neuesten Codekorrekturen (Fixes) auf allen vorhandenen integrierten Windows-Servern und unter i5/OS installiert haben. Weitere Informationen finden Sie unter „Codekorrekturen“ auf Seite 117.
2. Vergewissern Sie sich, dass eine Systemdatensicherung verfügbar ist, die den gesamten Speicher enthält, der den integrierten Servern zugeordnet ist.
3. Als Vorsichtsmaßnahme sollten Sie die zugeordneten Ressourcen für die Hardware notieren:
 - a. Geben Sie in der i5/OS-Befehlszeile den Befehl `WRKCFGSTS *NWS` ein, und drücken Sie die Eingabetaste.
 - b. Geben Sie eine 8 in der Spalte "Auswahl" neben der NWS-Beschreibung (NWSD) ein. Die Anzeige "Mit NWS-Beschreibung arbeiten" erscheint.
 - c. Geben Sie eine 5 in der Spalte "Auswahl" neben der NWS-Beschreibung (NWSD) ein.
 - d. Blättern Sie bis zum Feld Ressourcename vor, und notieren Sie den Wert für diesen Netzwerkserver (z. B. LIN05).
 - e. Drücken Sie F12 zweimal, um diesen Befehl zu verlassen.
 - f. Geben Sie in der i5/OS-Befehlszeile den Befehl `WRKHDWRSC TYPE(*CMN)` ein, und drücken Sie die Eingabetaste.
 - g. Geben Sie eine 7 (Ressourcendetail anzeigen) in der Spalte "Auswahl" neben dem Ressourcennamen ein, den Sie in Schritt 3 d ermittelt haben. In der Spalte "Typ" befindet sich die CCIN-Nummer für die Hardware des integrierten xSeries-Servers. Die Beschreibung sollte FSIOP (File Server IOP) oder E/A-Adapter für Dateiserver lauten.
 - h. Sind mehrere integrierte xSeries-Server desselben Typs auf der iSeries installiert, können Sie die richtige Einheit möglicherweise anhand der Kartenposition feststellen:
 - 1) Suchen Sie die Kartenposition unter der Überschrift Physische Position.
 - 2) Prüfen Sie die Etiketten auf den Steckplätzen der iSeries. Ein Steckplatz sollte mit der gleichen Zahl oder Kombination aus Buchstaben und Zahlen beschriftet sein, die im Feld Kartenposition angezeigt wird. Dieser Steckplatz enthält den integrierten xSeries-Server, auf den der Ressourcename verweist.
 - i. Notieren Sie die Informationen, die in den Feldern Typ-Modell und Seriennummer erscheinen.
 - j. Drücken Sie F12 zweimal, um den Befehl zu verlassen.
4. Hängen Sie alle integrierten Server ab. Weitere Informationen hierzu finden Sie in „Integrierten Server starten und stoppen“ auf Seite 157.

Fahren Sie zum Installieren der neuen Version von i5/OS auf der iSeries mit der im Handbuch iSeries Softwareinstallation beschriebenen Prozedur fort. 

Führen Sie nach dem Upgrade von i5/OS folgende zusätzliche Schritte aus:

1. Starten Sie den integrierten Server (siehe „Integrierten Server starten und stoppen“ auf Seite 157), und vergewissern Sie sich, dass er den gleichen Ressourcennamen hat:
 - a. Geben Sie in der i5/OS-Befehlszeile den Befehl `WRKHDWRSC TYPE(*CMN)` ein, und drücken Sie die Eingabetaste.
 - b. Geben Sie eine 7 (Ressourcendetail anzeigen) in der Spalte "Auswahl" neben dem Ressourcennamen ein, der im Schritt 3d ermittelt wurde. Vergewissern Sie sich, dass die Informationen, die in den Feldern Typ-Modell und Seriennummer erscheinen, mit den für diese Ressource notierten Angaben übereinstimmen.

- c. Stimmen diese Felder nicht mit den Aufzeichnungen überein, führen Sie folgende Schritte aus:
 - 1) Drücken Sie F12, um zur vorherigen Anzeige zurückzukehren.
 - 2) Verwenden Sie Auswahl 7, um die Ressourcendetails für andere Ressourcennamen in der Liste anzuzeigen, bis Sie den Eintrag gefunden haben, dessen Typ-Modell und Seriennummer mit den Aufzeichnungen übereinstimmen. Notieren Sie den Ressourcennamen, den i5/OS jetzt der Hardware dieses integrierten xSeries-Servers zuordnet. Drücken Sie F12, um diesen Befehl zu verlassen.
 - 3) Geben Sie in der i5/OS-Befehlszeile den Befehl WRKNWSD ein, und drücken Sie die Eingabetaste. Die Anzeige "Mit NWS-Beschreibung arbeiten" erscheint.
 - 4) Geben Sie eine 2 (Ändern) in der Spalte "Auswahl" neben der NWS-Beschreibung (NWSD) ein und drücken Sie die Eingabetaste. Die Anzeige "NWS-Beschreibung ändern" erscheint.
 - 5) Ändern Sie den Ressourcennamen in den korrekten Ressourcennamen für diesen Netzwerkserver.
2. Installieren Sie IBM i5/OS Integrated Server Support auf den vorhandenen integrierten Servern. Entsprechende Anweisungen finden Sie unter „IBM i5/OS Integrated Server Support installieren“ auf Seite 69.

Upgrade von IBM i5/OS Integrated Server Support auf der Seite des integrierten Servers durchführen

IBM i5/OS Integrated Server Support ist die Software, die die Verbindung zwischen der iSeries und den integrierten Windows-Servern herstellt. Sie ist mit einer Art Übersetzungsprogramm vergleichbar. Die eine Hälfte des Programms wird auf der iSeries ausgeführt und dient zur Übersetzung der Windows-Sprache in die i5/OS-Sprache. Die andere Hälfte wird auf den integrierten Servern ausgeführt, um dort den Code von der i5/OS-Sprache in die Windows-Sprache zu übersetzen .

Neue Versionen von IBM i5/OS Integrated Server Support werden unter i5/OS installiert. Anschließend muss die Komponente des Lizenzprogramms für den integrierten Server auf den integrierten Server kopiert und dort installiert werden.

Für das Lizenzprogramm auf den vorhandenen integrierten Windows-Servern muss ein Upgrade ausgeführt werden, wenn Sie Folgendes installieren:

- Eine neue Version von IBM i5/OS Integrated Server Support.
- Eine neue Version des Windows-Servers von Microsoft.

Neue Version von IBM i5/OS Integrated Server Support

Wenn Sie eine neue Version von IBM i5/OS Integrated Server Support installieren, müssen Sie für alle vorhandenen integrierten Server einen Upgrade auf diesen Level durchführen. Sind mehrere integrierte Server vorhanden, können Sie den Upgrade für diese Server auch im Fernzugriff über i5/OS ausführen.

Bei dieser Prozedur ist es erforderlich, dass Ihre Benutzer-ID und Ihr Kennwort auf den integrierten Windows-Servern und unter i5/OS identisch sind.

So führen Sie einen Upgrade für einen integrierten Server durch:

1. Beenden Sie alle laufenden Anwendungen.
2. Vergewissern Sie sich, dass keine Benutzer am integrierten Server angemeldet sind.
Achtung: Nach Abschluss der Installation wird der integrierte Server automatisch erneut gestartet, daher besteht die Gefahr eines Datenverlustes, wenn die Schritte 1 und 2 übersprungen werden.
3. Klicken Sie im Menü **Start** auf **Programme, IBM iSeries, Integration for Windows Server** und dann auf **Software-Level**.

Anmerkung:

Wenn ein neuer Level des Lizenzprogramms für die Installation zur Verfügung steht und sich ein Administrator am integrierten Server anmeldet, wird die Komponente "Software-Level" automatisch gestartet.

4. Wenn Sie einen Upgrade von V5R3 oder später ausführen, wählen Sie Option für das **Synchronisieren** aus. Wählen Sie andernfalls die Option für die **Releaseinstallation von der iSeries** aus.
5. Befolgen Sie die Anweisungen in der Benutzeroberfläche, um die Installation auszuführen.
6. **Tipp:** Sichern Sie anschließend die vordefinierten Installations- und Systemlaufwerke für diesen Server. Informationen zur Sicherung dieser Laufwerke finden Sie unter „Vordefinierte Plattenlaufwerke für integrierte Windows-Server sichern“ auf Seite 201. Da es sicherer ist, alle Speicherbereiche für den Server zum gleichen Zeitpunkt zu sichern, sollten Sie auch den zugeordneten, vom Benutzer erstellten Speicher sichern (eine entsprechende Beschreibung enthält der Abschnitt „Benutzerdefinierte Plattenlaufwerke für einen integrierten Windows-Server sichern“ auf Seite 202).

Neue Version von Windows-Server

Anweisungen für den Upgrade der Server von Windows NT 4.0 auf Windows 2000 können Sie unter dem Thema zum Upgrade des Servers von Windows NT 4.0 auf Windows 2000 Server im iSeries Information Center für V5R3 nachlesen.

Hardware des integrierten xSeries-Servers von 285x oder 661x auf 2890 migrieren

IPCS- oder INS-Server (Typ 2850 und 6617) müssen erneut auf neuerer Hardware installiert oder auf die IXS-Hardware 2890 migriert werden, bevor V5R4 installiert werden kann. Weitere Informationen finden Sie unter dem Thema zur Migration der Hardware des Integrated xSeries Servers von 285x oder 661x auf 2890 im iSeries Information Center für V5R3.

Migration auf Server mit iSCSI-Anschluss durchführen

- Die Migration auf einen Server mit iSCSI-Anschluss wird nicht unterstützt. Für alle Server mit iSCSI-Anschluss ist eine Neuinstallation erforderlich.

Windows-Clusterdienst

Der Windows-Clusterdienst verbindet einzelne Server, damit diese gemeinsame Aufgaben ausführen können. Für den Fall, dass einer der Server ausfällt, wird seine Arbeitsbelastung durch einen als Funktionsübernahme bezeichneten Prozess automatisch auf einen anderen Server versetzt, um einen kontinuierlichen Dienst zu gewährleisten. Neben der Funktionsübernahme setzen manche Formen des Clustering auch den Lastausgleich ein, der die Verteilung der datenverarbeitungsbezogenen Arbeitsbelastung auf ein Netzwerk verbundener Computer ermöglicht.

Windows 2000 Advanced Server unterstützt einen Cluster mit zwei Knoten, während Windows Server 2003 Enterprise Edition Cluster mit acht Knoten unterstützt. Rechenzentrumsversionen von Windows werden nicht unterstützt.


Die Unterstützung des Windows-Clusterservice steht nur auf integrierten Windows-Servern zur Verfügung, auf denen entweder Windows 2000 Advanced Server oder Windows Server 2003 Enterprise Edition ausgeführt wird.

Anmerkungen:

1. Die Windows-Netzwerkserverknoten müssen sich für das Clustering in einer einzigen iSeries-Partition befinden.
2. xSeries-Systeme mit iSCSI-Anschluss können nicht gemeinsam mit Servern in Gruppen zusammengefasst werden, die über IXS/IXA angeschlossen sind.

Die traditionelle Windows-Lösung für Server-Cluster setzt zwar eine gemeinsam benutzte physische SCSI- oder Fibre Channel-Einheit voraus, der integrierte Windows-Server verwendet jedoch einen virtuellen Fibre Channel-Bus, um die virtuellen Platteneinheiten zwischen den Knoten eines Clusters freizugeben.

Darüber hinaus ermöglicht die neue Unterstützung von Virtual Ethernet höchste Leistungen sowie eine sichere Kommunikation für die interne Knoten-zu-Knoten-Kommunikation zwischen gruppierten Knoten.

Detaillierte Prüflisten für die Planung und Erstellung eines Server-Clusters sind in der Online-Hilfe von Microsoft zu Server-Clustern verfügbar. Es wird empfohlen, diese Listen vor der Installation und Konfiguration eines Windows-Cluster-Servers zu lesen. Weitere Informationen, einschließlich einer schrittweisen Anleitung für die Installation des Clusterdienstes, finden Sie auf der Microsoft-Website. 

Weitere Informationen zur Unterstützung des Windows-Clusterdienstes finden Sie in den folgenden Themen:


„Windows-Clusterdienst installieren“

Hier erfahren Sie, wie Sie den Windows-Clusterdienst auf einem integrierten Windows-Server installieren und konfigurieren.

„Windows-Clusterdienst auf einem vorhandenen Server installieren“ auf Seite 110

Hier erfahren Sie, wie Sie Cluster auf einem integrierten Windows-Server erstellen.

| **Clusterunterstützung auf einem Server mit iSCSI-Anschluss**

- | Informationen über die iSeries-Unterstützung für Microsoft Cluster Service (MSCS) auf einem Server mit iSCSI-Anschluss finden Sie unter MSCS on an iSCSI attached server  auf der Website Integrated xSeries solutions (www.ibm.com/servers/eserver/series/integratedxseries/windows/iscsiclusters.html).

Windows-Clusterdienst installieren

Lesen Sie vor der Installation des Clusterdienstes alle Prüflisten von Microsoft für die Installation von Server-Clustern. Sie vermeiden so zukünftige Probleme bei der Planung und Installation.

Anmerkung: Während der Installation des Clusterdienstes auf dem ersten Knoten müssen alle anderen Knoten, die zum Cluster gehören, vor dem Starten von Windows abgehängt werden.

Alle Verweise in den Clusterdaten des Servers auf gemeinsam benutzte SCSI- oder Fibre Channel-Einheiten beziehen sich auf die virtuelle Fibre Channel-Implementierung, die für den Zugriff auf die gemeinsam benutzten NWS-Speicherbereiche verwendet wird.

Die folgenden Abschnitte beschreiben die Installation und Ausführung des Windows-Clusterdienstes:

1. Windows-Clusterdienst auf dem integrierten xSeries-Server installieren
 - „Windows-Clusterdienst auf einem neuen integrierten Windows-Server installieren“
 - „Windows-Clusterdienst auf einem vorhandenen Server installieren“ auf Seite 110
2. „Windows-Clusterdienst unter Windows installieren“ auf Seite 112

Windows-Clusterdienst auf einem neuen integrierten Windows-Server installieren

Die Installation und Konfiguration des Windows-Clusterdienstes ist während der ersten Konfiguration eines integrierten Servers am einfachsten. Verwenden Sie hierzu den Befehl INSWNTSVR (Windows-Server installieren) mit den folgenden Parametern, um die Konfigurationsdaten für den Cluster anzugeben:

- Parameter CLU (Clustername)
- Parameter CLUCFG (Clusterkonfiguration)

Weitere Informationen zur Installation des integrierten Servers finden Sie unter „Windows 2000 Server oder Windows Server 2003 installieren“ auf Seite 98.

Nachdem Sie den Befehl INSWNTSVR ausgeführt haben (und die Installation des integrierten Windows-Servers abgeschlossen ist), müssen Sie vor der Installation des Windows-Clusterdienstes auf der Windows-Seite einige zusätzliche Konfigurationsschritte über die Konsole des integrierten Servers ausführen. Weitere Informationen finden Sie unter „Windows für die Installation des Windows-Clusterdienstes vorbereiten“ auf Seite 111.

Clustername:

Der Parameter CLU (Clustername) gibt den Namen des Clusters an. Dieser wird von Administratoren verwendet, um eine Verbindung zum Cluster herzustellen. Er steht für die Gruppe der unabhängigen Netzwerkknoten, die als ein System zusammenarbeiten. Der für den Cluster eingegebene Name wird zudem als Name des erstellten NWS-Speicherbereichs verwendet, der als Quorum-Ressource für den Cluster dient.

Clusterkonfiguration:

Der Parameter CLUCFG (Clusterkonfiguration) wird zur Definition des Clusters sowie zur Konfiguration des NWS-Speicherbereichs verwendet, der die Quorum-Ressource darstellt. Darüber hinaus kann mit diesen Informationen überprüft werden, dass alle sekundären Knoten über die erforderliche i5/OS-Konfiguration verfügen, um virtuelle Clusterverbindungen für die gemeinsam benutzten Speichereinheiten und den Virtual Ethernet-Port zu erstellen, der für die private,interne Clusterverbindung verwendet wird. Der Wert *CLU für die Clusterkonfiguration ruft die Clusterkonfiguration aus der vorhandenen Quorum-Ressource (NWS-Speicherbereich), die im Parameter CLU angegeben wurde, ab.

Anmerkung:

Der Clusterverbindungsport erfordert die Konfiguration eines entsprechenden Virtual Ethernet-Ports. Weitere Informationen zur Konfiguration eines Virtual Ethernet-Ports finden Sie unter „Virtual Ethernet-Netzwerke konfigurieren“ auf Seite 121.

Windows-Clusterdienst auf einem vorhandenen Server installieren

Sie können den Windows-Clusterdienst auf einem vorhandenen Server mit Windows 2000 Advanced Server oder Windows Server 2003 Enterprise Edition installieren, der auf einer unterstützten Dateiserverressource mit V5R2 (oder höher) der Software für die Integration für Windows-Server ausgeführt wird.

Vergewissern Sie sich, dass der Level des Integrated Server Support mit i5/OS synchronisiert ist. Entsprechende Anweisungen finden Sie unter „Upgrade von IBM i5/OS Integrated Server Support auf der Seite des integrierten Servers durchführen“ auf Seite 107. Auf diese Weise wird die Verfügbarkeit aller Serverfunktionen gewährleistet, die zur Installation des Windows-Clusterdienstes benötigt werden.

Die Installation des Windows-Clusterdienstes auf einem vorhandenen Server umfasst die folgenden Schritte:

- Speicherbereich erstellen (Quorum-Ressource)
- Virtual Ethernet-Verbindungsport konfigurieren
- Quorum-Ressourcenlaufwerk mit der NWS-Beschreibung verbinden

Nach Abschluss der obigen Schritte und vor Installation des Windows-Clusterdienstes auf der Seite des integrierten Windows-Servers müssen einige zusätzliche Konfigurationsschritte an der Konsole des integrierten Windows-Servers ausgeführt werden. Weitere Informationen finden Sie unter „Windows für die Installation des Windows-Clusterdienstes vorbereiten“ auf Seite 111.

Speicherbereich erstellen (Quorum-Ressource):

Erstellen Sie zunächst einen Speicherbereich, der als Quorum-Ressource verwendet wird. Verwenden Sie hierzu den CL-Befehl CRTNWSSTG (NWS-Speicherbereich erstellen), und geben Sie das Sonderformat *NTFSQR an.

Der Name des NWS-Speicherbereichs muss mit dem Namen des Clusters übereinstimmen, den Sie erstellen. Die empfohlene Größe beträgt mindestens 550 MB. Sie werden von dem Befehl aufgefordert, die folgenden Clusterdaten einzugeben:

- Clusterdomänenname
- Virtual Ethernet-Verbindungsport
- IP-Adresse für den Windows-Cluster
- Teilnetzmaske für den Windows-Cluster

Virtual Ethernet-Verbindungsport konfigurieren:

Als Nächstes müssen Sie den Virtual Ethernet-Verbindungsport konfigurieren, der für die private Clusterkommunikation verwendet werden soll. Entsprechende Anweisungen finden Sie unter „Virtual Ethernet-Netzwerke konfigurieren“ auf Seite 121. Der verwendete Virtual Ethernet-Verbindungsport muss mit dem Verbindungsport übereinstimmen, der mit dem NWS-Speicherbereich der Quorum-Ressource angegeben wurde.

Quorum-Ressourcenlaufwerk mit der NWS-Beschreibung verbinden:

Verbinden Sie den Speicherbereich der Quorum-Ressource mit dem Netzwerkserver, indem Sie den Befehl ADDNWSSTGL (NWS-Speicherbereichsverbindung hinzufügen) mit ACCESS(*SHRUPD), DYNAMIC(*YES) und DRVSEQNBR(*QR) ausführen.

Anmerkung:

Während der Installation des Clusterdienstes auf dem ersten Knoten müssen alle anderen Knoten vor dem Start des integrierten Servers abgehängt werden. Zu diesem Zeitpunkt können zusätzliche gemeinsam benutzte Speichereinheiten erstellt und verbunden werden. Alle gemeinsam benutzten Speicherbereiche müssen *NTFS entsprechen und mit ACCESS(*SHRUPD) verbunden worden sein.

Windows für die Installation des Windows-Clusterdienstes vorbereiten

Nach der Installation des integrierten Servers müssen Sie den Server für die Installation des Windows-Clusterdienstes vorbereiten.

Die Vorbereitung von Windows für die Installation des Windows-Clusterdienstes umfasst die folgenden Schritte:

1. Quorum-Ressource formatieren.
2. Privaten Netzwerkadapter konfigurieren.

Nach Abschluss dieser Schritte ist Windows für die Installation des Windows-Clusterdienstes vorbereitet. Weitere Informationen finden Sie unter „Windows-Clusterdienst unter Windows installieren“ auf Seite 112.

Quorum-Ressource formatieren:

Der erste Schritt zur Vorbereitung von Windows auf die Installation des Windows-Clusters ist die Formatierung der Quorum-Ressource als NTFS. Die Quorum-Ressource muss nicht nur für die Installation des Windows-Clusterdienstes formatiert werden. Dies ist zudem der erste Schritt bei der Installation des ersten Knotens eines Clusters. Weitere Informationen finden Sie unter „Plattenlaufwerke für integrierten Server formatieren“ auf Seite 175.

- | Bei IXS oder Servern mit IXA-Anschluss wird die Quorum-Ressource als unformatiertes Plattenlaufwerk
- | angezeigt, normalerweise mit dem logischen Laufwerkbuchstaben E. Die Position der Quorum-Ressource
- | lautet Bus Nummer 1, Ziel-ID 0 und LUN 0.

Formatieren Sie den Datenträger, und benennen Sie ihn genauso wie den Cluster (entspricht dem Namen des NWS-Speicherbereichs der Quorum-Ressource). Darüber hinaus sollten Sie zu diesem Zeitpunkt alle anderen gemeinsam benutzten Speicherbereiche formatieren. Es wird empfohlen, dem Laufwerk der Quorum-Ressource und den anderen gemeinsam benutzten Speichereinheiten einen festen Laufwerkbuchstaben zuzuordnen.

Anmerkung:

Der Laufwerkbuchstabe, der den Speicherbereichen auf dem gemeinsam benutzten Speicherbus zugeordnet ist, muss auf allen Knoten des Clusters gleich sein.

Privaten Netzwerkadapter konfigurieren:

Konfigurieren Sie anschließend den privaten Netzwerkadapter, der vom Windows-Clusterdienst verwendet wird. Führen Sie hierzu die folgenden Schritte auf dem ersten Knoten im Cluster durch:

1. Klicken Sie in der Konsole des integrierten Windows-Servers mit der rechten Maustaste auf **Netzwerkumgebung**, und wählen Sie die Option **Eigenschaften** aus.
2. Klicken Sie auf das Symbol **LAN-Verbindung 2**.

Anmerkung:

Welche Netzwerkadapter privat und welche öffentlich sind, hängt von der Konfiguration des Servers ab. Hier wird von folgenden Voraussetzungen ausgegangen:

- Der erste Netzwerkadapter (Verbindung im lokalen Netzwerk) ist über einen physischen LAN-Adapter unter dem integrierten Windows-Server mit dem öffentlichen Netzwerk verbunden.
- Der zweite Netzwerkadapter (Verbindung im lokalen Netzwerk 2) ist der Virtual Ethernet-Adapter, der als Verbindungspunkt für die Clusterkonfiguration konfiguriert wurde und als privates Clusternetzwerk verwendet werden soll.
- Der dritte Netzwerkadapter (Verbindung im lokalen Netzwerk 3) ist die Punkt-zu-Punkt-Verbindung des Virtual Ethernet zu i5/OS und sollte nicht für das Clustering aktiviert werden.

Die Anzahl und Reihenfolge der Netzwerkadapter weicht je nach physischer und virtueller Konfiguration des Servers und Netzwerks ggf. hiervon ab.

3. Klicken Sie auf **Status**, um das Fenster für den **Status der LAN-Verbindung 2** anzuzeigen, in dem der Verbindungsstatus sowie die Verbindungsgeschwindigkeit zu sehen sind.
4. Klicken Sie im Fenster für den **Status der LAN-Verbindung 2** auf **Eigenschaften**.
5. Stellen Sie im Dialogfenster **Eigenschaften** sicher, dass das Feld **Verbinden über** das IBM iSeries Virtual Ethernet x enthält. Hierbei steht x für den *VRTETHx, den Sie als Verbindungspunkt der Clusterkonfiguration angegeben haben.
6. Klicken Sie auf **Schließen**, und klicken Sie dann erneut auf **Schließen**.

Sie sollten die Symbole für die lokalen Netzwerke zur Verdeutlichung umbenennen. Sie können beispielsweise den Namen für die Verbindung im lokalen Netzwerk 2 in "Private Clusterverbindung" ändern.

Windows-Clusterdienst unter Windows installieren

Die Installation des Windows-Clusterdienstes hängt von der Windows-Version ab, die während der Installation der Windows-Umgebung auf der iSeries installiert wurde. In den meisten Fällen finden Sie in der Dokumentation von Microsoft eine Anleitung für die Installation des Windows-Clusterdienstes. Diese Informationen zeigen spezifische Schritte auf, die bei der Installation des Windows-Clusterdienstes auf einem integrierten Windows-Server erforderlich sind.

- „Windows-Clusterdienst unter Windows 2000 Server installieren“ auf Seite 113
- „Windows-Clusterdienst unter Windows Server 2003 installieren“ auf Seite 113

Anmerkung: Vergewissern Sie sich, dass der Windows-Clusterdienst zunächst auf einem Server installiert und ausgeführt wird, bevor Sie Windows auf einem anderen Server im Cluster starten. Wenn Sie das Betriebssystem auf mehreren Servern starten, bevor der Windows-Clusterdienst auf einem Server ausgeführt wird, kann der Clusterspeicher beschädigt werden. Nach der Konfiguration des ersten Servers können Sie die verbleibenden Server gleichzeitig installieren.

Windows-Clusterdienst unter Windows 2000 Server installieren: Verwenden Sie für die Installation des Windows-Clusterdienstes den Assistenten für die Konfiguration des Clusterdienstes. Im Assistenten geben Sie alle Anfangsdaten für die Clusterkonfiguration ein.

Die Installation des Windows-Clusterdienstes umfasst die folgenden Schritte:

1. Assistenten für die Konfiguration des Clusterdienstes starten.
2. Clusterdienst mit Hilfe des Assistenten konfigurieren.

Assistenten für die Konfiguration des Clusterdienstes starten

So starten Sie den Assistenten für die Konfiguration des Clusterdienstes:

1. Klicken Sie im Windows-Menü **Start** auf **Einstellungen** und **Systemsteuerung**.
2. Doppelklicken Sie im Fenster **Systemsteuerung** auf **Software**.
3. Klicken Sie im Fenster **Software** auf **Windows-Komponenten hinzufügen/entfernen**.
4. Wählen Sie im Dialogfenster **Assistent für Windows-Komponenten** die Option **Clusterdienst** aus, und klicken Sie auf **Weiter**.

Windows-Clusterdienst konfigurieren

Nachdem Sie den Assistenten für die Konfiguration des Clusterdienstes gestartet haben, führt dieser Sie durch die Installation des Windows-Clusterdienstes. Sie geben im Assistenten alle Anfangsdaten für die Clusterkonfiguration ein, die zum Erstellen des Clusters benötigt werden.

Wenn Sie aufgefordert werden, die Quorum-Ressource einzugeben, müssen Sie das formatierte und benannte Laufwerk auswählen. Zumeist handelt es sich bei einer Neuinstallation um das Laufwerk E:, der Datenträger-Manager kann dem Laufwerk jedoch auch einen anderen Buchstaben zugeordnet haben.

Netzwerkverbindungen erfordern spezielle Aufmerksamkeit:

Anmerkung:

Die Reihenfolge, in der die Netzwerkdaten vom Assistenten für die Konfiguration des Clusterdienstes angezeigt werden, kann hiervon abweichen.

- Inaktivieren Sie das Markierungsfeld **Dieses Netzwerk für die Verwendung im Cluster aktivieren** für das IBM iSeries Virtual Ethernet-Punkt-zu-Punkt (zumeist LAN-Verbindung 3).
- Wählen Sie die Option **Nur interne Clusterkommunikation** für das IBM iSeries Virtual Ethernet x aus. Hierbei steht x für den *VRTETHx, den Sie am Verbindungsport für die Clusterkonfiguration angegeben haben (zumeist LAN-Verbindung 2).
- Konfigurieren Sie die verbleibenden Netzwerkverbindungen je nach Bedarf.

Geben Sie den Adapter für das IBM iSeries Virtual Ethernet x (zumeist LAN-Verbindung 2) als primäres Netzwerk für die interne Clusterkommunikation an.

Windows-Clusterdienst unter Windows Server 2003 installieren: Verwenden Sie zur Installation des Clusterdienstes unter Windows Server 2003 und zum Hinzufügen eines Knotens zu einem bestehenden Cluster die Clusterverwaltung. Sowohl die Installation des Clusterdienstes als auch das Hinzufügen zu einem bestehenden Cluster setzen voraus, dass Sie die Clusterverwaltung öffnen. Sie öffnen die **Clusterverwaltung**, indem Sie im Windows-Menü **Start** die Optionen **Alle Programme**, **Verwaltung** und **Clusterverwaltung** auswählen.

So installieren und konfigurieren Sie den Windows-Clusterdienst:

1. Öffnen Sie die **Clusterverwaltung**.
2. Wählen Sie in dem eingeblendeten Dialogfenster **Verbindung mit Cluster öffnen** unter **Vorgang** die Option **Neues Cluster erstellen** aus.
3. Klicken Sie auf **OK**, um den Assistenten für neue Server-Cluster anzuzeigen, der Sie durch die Installation des Clusterdienstes für den ersten Knoten führt.
4. Klicken Sie auf **Weiter**.
5. Geben Sie die **Domäne** (Standardwert) und den **Clusternamen** ein.
6. Geben Sie den **Computernamen** ein (Standardwert).
7. Geben Sie die **IP-Adresse** für die Clusterverwaltung ein.
8. Geben Sie den **Benutzernamen des Clusterdienstaccounts**, das **Kennwort** und die **Domäne** ein.
9. Überprüfen Sie die **vorgeschlagene Clusterkonfiguration**.


Knoten zu bestehendem Cluster hinzufügen

So fügen Sie einen Knoten zu einem bestehenden Cluster hinzu:

1. Öffnen Sie die **Clusterverwaltung**.
2. Wählen Sie im Dialogfenster **Verbindung mit Cluster öffnen** unter **Aktion** die Option **Knoten dem Cluster hinzufügen** aus.
3. Geben Sie anschließend unter **Cluster- oder Servername** den Namen eines bestehenden Clusters ein, wählen Sie einen Namen in der Liste aus, oder klicken Sie auf **Durchsuchen**, um verfügbare Cluster zu suchen.
4. Klicken Sie auf **OK**, um den Assistenten für das Hinzufügen eines Server-Clusters anzuzeigen.
5. Wählen Sie den Namen mindestens eines Computers aus, der dem Cluster hinzugefügt werden soll, und klicken Sie anschließend auf **Hinzufügen**.
6. Geben Sie das Kennwort des Domänenaccounts für den Clusterdienst ein.
7. Nach der Installation des Clusterdienstes können Sie mit der Clusterverwaltung den soeben erstellten Cluster suchen und auswählen.
8. Erweitern Sie **Clusterkonfiguration, Netzwerkschnittstellen**. Auf diese Weise wird im rechten Fenster eine Liste aller **LAN-Verbindungen** geöffnet.
9. Geben Sie den Netzwerknamen (LAN-Verbindung x) für das IBM iSeries Virtual Ethernet x ein. Hierbei steht x für das *VRTETHx, das am Verbindungspunkt für die Clusterkonfiguration angegeben wurde. Sie müssen dieses Netzwerk später angeben. Merken Sie sich daher dessen Namen.
10. Geben Sie den Netzwerknamen (LAN-Verbindung x) für das IBM iSeries Virtual Ethernet-Punkt-zu-Punkt an. Sie müssen dieses Netzwerk später angeben. Merken Sie sich daher dessen Namen.
11. Erweitern Sie im Fenster **Clusterverwaltung** die Optionen **Clusterkonfiguration** und **Netzwerke**.
12. Klicken Sie mit der rechten Maustaste auf den Netzwerknamen (LAN-Verbindung x) für das IBM iSeries Virtual Ethernet x, und wählen Sie die Option **Eigenschaften** aus.
13. Wählen Sie für dieses Netzwerk die Option **Nur interne Clusterkommunikation** aus.
14. Klicken Sie mit der rechten Maustaste auf den Netzwerknamen (LAN-Verbindung x) für das IBM iSeries Virtual Ethernet-Punkt-zu-Punkt, und wählen Sie die Option **Eigenschaften** aus.
15. Inaktivieren Sie für dieses Netzwerk das Markierungsfeld **Dieses Netzwerk für die Verwendung im Cluster aktivieren**.

Konfigurieren Sie die verbleibenden Netzwerkverbindungen je nach Bedarf.

Kerberos für Windows Server 2003 Active Directory Server aktivieren

QNTC, SBMNWSCMD und die Sicherung auf Dateiebene können Kerberos für die Authentifizierung bei Windows Active Directory Domänenmitgliedsservern benutzen. Um Kerberos benutzen zu können, müssen Sie ggf. ein Update für Windows Server 2003 auf den Microsoft Active Directory Controller-Servern installieren. Dieses Update ist in Service-Pack 1 oder Microsoft Hotfix KB833708 verfügbar. Weitere Informationen einschließlich Informationen über die Installation des Service-Packs oder Hotfixes finden Sie auf der Microsoft-Website. 

Nach der Installation des Hotfixes oder Service-Packs 1 müssen Sie auch das Windows Server 2003-Registry aktualisieren. Führen Sie die folgenden Schritte aus:

1. Klicken Sie auf **Start>Ausführen**
2. Geben Sie regedit im Markierungsfeld **Öffnen** ein.
3. Klicken Sie auf **OK**.
4. Wählen Sie den Registry-Unterschlüssel **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc** aus.
5. Klicken Sie mit der rechten Maustaste auf **Kdc**.
6. Wählen Sie **Neu** aus.
7. Klicken Sie auf **DWORD Value**.
8. Geben Sie KdcUseRequestedEtypesForTickets als neuen Wert ein.
9. Klicken Sie mit der rechten Maustaste auf **KdcUseRequestedEtypesForTickets**.
10. Wählen Sie **Modifizieren** aus.
11. Setzen Sie den Registry-Wert **KdcUseRequestedEtypesForTickets** auf 1.
12. Klicken Sie nochmals auf **OK**.
13. Beenden Sie den Registrierungseditor.
14. Um die Änderung zu aktivieren, starten Sie den Service für die Schlüsselverteilung (Key Distribution Center) erneut, oder führen Sie einen Warmstart des Servers durch.

ATI Radeon 7000M-Bildschirmeinheitentreiber für Windows 2000 auf dem integrierten xSeries-Server 2892-002 oder 4812-001 installieren

Die integrierten xSeries-Server 2892-002 und 4812-001 enthalten einen ATI Radeon 7000M-Video-Chip. Die erforderlichen Treiber sind auf der Verteilungs-CD von Microsoft Windows 2000 Server nicht enthalten. Sie müssen den ATI-Bildschirmtreiber auf dem integrierten Windows-Server installieren, um das Funktionsspektrum des ATI-Video-Chips optimal nutzen zu können.

Auf den Systemen muss DirectX 8.1 (oder höher) installiert sein, bevor die ATI-Bildschirmtreiber installiert werden können.

So installieren Sie den ATI-Bildschirmtreiber für Windows 2000:

1. Installieren Sie DirectX Version 8.1 oder höher. Mit Windows 2000 wird Version 7.0 von DirectX ausgeliefert. Für die ATI-Bildschirmtreiber ist jedoch Version 8.1 oder höher von DirectX erforderlich und muss vor der Installation der ATI-Bildschirmtreiber installiert werden. Microsoft unterhält eine Website mit Informationen und Downloads für DirectX. Die Adresse lautet:
<http://www.microsoft.com/directx>.
2. Installieren Sie den ATI-Bildschirmtreiber:
 - a. Schließen Sie alle Programme.
 - b. Klicken Sie auf die Schaltfläche **Start**, und wählen Sie die Option **Ausführen** aus.
 - c. Klicken Sie auf die Schaltfläche **Durchsuchen**.
 - d. Suchen Sie nach dem Verzeichnis %SystemDrive%\WSV, in dem sich die Datei atidrvr.exe befindet.
 - e. Wählen Sie die Datei atidrvr.exe aus, und klicken Sie auf "OK", um das Programm auszuführen.

- f. Befolgen Sie die angezeigten Installationsanweisungen.
3. Optional können Sie die Indexzungen für den Advanced ATI Control Panel installieren.
 - a. Schließen Sie alle Programme.
 - b. Klicken Sie auf die Schaltfläche **Start**, und wählen Sie die Option **Ausführen** aus.
 - c. Klicken Sie auf die Schaltfläche **Durchsuchen**.
 - d. Suchen Sie nach dem Verzeichnis %SystemDrive%\WSV, in dem sich die Datei aticp.exe befindet.
 - e. Wählen Sie die Datei aticp.exe aus, und klicken Sie auf "OK", um das Programm auszuführen.
 - f. Befolgen Sie die angezeigten Installationsanweisungen.

Hardwarebeschleunigung für Windows Server 2003 auf dem integrierten xSeries-Server 2892-002 oder 4812-001 anpassen

Wenn Sie Windows Server 2003 auf einer IXS-Einheit vom Typ 2892-002 oder 4812-001 installieren, sind einige zusätzliche Konfigurationsschritte erforderlich, um eine optimale Systemleistung im Videobereich zu erzielen. Führen Sie zur Anpassung der Systemleistung die folgenden Schritte aus:

1. Klicken Sie im Windows-Menü **Start** auf **Einstellungen** -> **Systemsteuerung** -> **Anzeige**.
2. Klicken Sie in der Anzeige **Anzeigeneigenschaften** auf die Registerkarte **Einstellungen**.
3. Klicken Sie auf **Erweitert**.
4. Klicken Sie auf die Registerkarte **Problembehandlung**.
5. Passen Sie die Einstellung des Schiebereglers **Hardwarebeschleunigung** an.
6. Klicken Sie auf **Übernehmen**.
7. Klicken Sie auf **OK**.
8. Klicken Sie nochmals auf **OK**, um die Änderung zu übernehmen.

Fehlernachrichten während der Installation beantworten

Während der Installationsphase des integrierten Windows-Servers werden fehlende Informationen markiert, die während der i5/OS-Phase der Installation nicht bereitgestellt wurden. Diese fehlenden Informationen können dann noch eingegeben werden. Dieser Abschnitt enthält Beispiele dieser Fehlernachrichten und die entsprechenden Maßnahmen.

Fehler (Server installieren)

Wenn Sie in den Feldern In Arbeitsgruppe oder In Domäne der i5/OS-Anzeige Windows-Server installieren keinen Wert angegeben haben, wird die folgende Fehlernachricht angezeigt:

Fehler (Server installieren)

Es fehlt ein Setup-Parameter, den Ihr Systemadministrator oder Computerhersteller angegeben hat, oder der Parameter ist ungültig. Geben Sie die erforderlichen Informationen jetzt ein.

Sobald diese Informationen verfügbar sind, wird die unbeaufsichtigte Installation fortgesetzt.

Teilen Sie dem Systemadministrator oder Computerhersteller mit, dass der Parameter "JoinWorkgroup" fehlt oder ungültig ist.

Klicken Sie auf **OK**.

Das Installationsprogramm zeigt daraufhin eine Eingabeaufforderung an, damit Sie den Computer einer Arbeitsgruppe oder Domäne hinzufügen können.

Integrierten Windows-Server für automatisches Anhängen mit TCP/IP einstellen

Sie können den integrierten Server so konfigurieren, dass er beim Starten von TCP/IP automatisch angehängt wird. Verwenden allerdings mehrere integrierte Server eine einzige Dateiserverressource, sollte nur einer von ihnen für den automatischen Start konfiguriert werden. Es kann jeweils nur ein Netzwerkserver die Dateiserverressource benutzen. Werden mehrere TCP/IP-Schnittstellen für den automatischen Start von Netzwerkservern konfiguriert, die dieselbe Ressource gemeinsam benutzen, kann dies zu unvorhersehbaren Ergebnissen führen.

So können Sie einen integrierten Server automatisch beim Starten von TCP/IP anhängen:

1. Geben Sie in der i5/OS-Befehlszeile den Befehl CFGTCP (TCP/IP konfigurieren) ein.
2. Geben Sie Auswahl 1 Mit TCP/IP-Schnittstellen arbeiten ein, und drücken Sie die Eingabetaste.
3. Geben Sie eine 2 (Ändern) im Feld "Auswahl" neben der Schnittstelle für die Leitungsbeschreibung des Virtual Ethernet-Punkt-zu-Punkt für den Server ein, und drücken Sie die Eingabetaste.

Anmerkung:

Die Leitungsbeschreibung für das Virtual Ethernet-Punkt-zu-Punkt besteht aus dem Namen der NWS-Beschreibung (NWS) gefolgt von 'PP' für das Virtual Ethernet-PTP-LAN. Ist beispielsweise der NWS-Name MYSVR, lautet die Leitungsbeschreibung für das Virtual Ethernet-PTP-LAN MYSVRPP.

4. Ändern Sie den Parameterwert für Autostart in *YES, und drücken Sie die Eingabetaste. Der integrierte Server wird beim Starten von TCP/IP automatisch angehängt.

Anmerkung:

Ab V5R1 kann TCP/IP beim IPL automatisch vom System gestartet werden, indem die IPL-Attribute des Systems geändert werden. Eine Startprozedur ist dafür nicht mehr erforderlich. Alle TCP-Schnittstellen, bei denen im Parameter für automatisches Starten *YES eingestellt wurde, werden beim IPL gemeinsam mit TCP/IP gestartet.

Anmerkung:

Beachten Sie, dass eine IP-Adresse, die an der integrierten Konsole für das Virtual Ethernet-PTP eingegeben wurde, den Wert in der NWS-Beschreibung für den TCPPORTCFG-Parameter des Ports *VRTETHPTP überschreibt. Operationen wie SBMNWSCMD verwenden jedoch weiterhin den Wert in der NWS-Beschreibung, um den Server zu suchen. Beide Werte sollten daher übereinstimmen.

Codekorrekturen

Die Codekorrekturen für IBM iSeries Integrated Server Support bieten Ihnen schon vor der Freigabe des nächsten Software-Releases den neuesten Code mit den aktuellsten Korrekturen. Diese Komponenten dienen zur Aktualisierung des iSeries Integrated Server Support-Codes, der die Ausführung des Microsoft Windows-Servers auf dem integrierten Server ermöglicht, und sind unabhängig von den Service-Packs für die eigentliche Windows-Software, die über Microsoft bezogen werden müssen.

Weitere Informationen können Sie unter „Arten von Codekorrekturen“ auf Seite 118 nachlesen.

Der Prozess, bei dem die Codekorrekturen auf den integrierten Servern installiert werden, wird als Synchronisation bezeichnet. Wenn Sie einen integrierten Server synchronisieren, stellt die Integrationssoftware sicher, dass die Integrationssoftware auf dem integrierten Server denselben Service-Pack- und Release-Level wie die i5/OS-Integrationssoftware aufweist. Der Code-Level auf der Windows-Seite ist vom Code-Level auf der i5/OS-Seite abhängig.

Wenn Sie einen integrierten Server unter Verwendung der Integrationssoftware synchronisieren, gibt es vier potenzielle Aktionen, die hierdurch implizit stattfinden können:

1. Falls für i5/OS ein Upgrade auf ein neues Release durchgeführt wurde (z. B. von V5R3 auf V5R4), ersetzt die Software für das neue Release diejenige für das alte Release.
2. Wurde ein neues Service-Pack für IBM iSeries Integrated Server Support unter i5/OS installiert, wird es auf den integrierten Server kopiert.
3. Wenn ein Service-Pack für IBM iSeries Integrated Server Support aus i5/OS entfernt wurde, wird es auch vom integrierten Server entfernt und durch den Code ersetzt, der gegenwärtig in i5/OS vorhanden ist.
4. Weisen der Code für die i5/OS-Integration und der Code für den integrierten Server denselben Level auf, kann die Synchronisationsoperation trotzdem stattfinden. Auf diese Weise können gelöschte oder beschädigte Dateien auf dem integrierten Server wiederhergestellt werden.

In allen Fällen wird der integrierte Server auf den Level der Software gebracht, der in i5/OS vorliegt.



Für die Ausführung einer Synchronisation gibt es drei unterschiedliche Methoden:

- „Level der Integrationssoftware über die Konsole des integrierten Windows-Servers synchronisieren“ auf Seite 119.
- „Level der Integrationssoftware mit iSeries Navigator synchronisieren“ auf Seite 119.
- „Level der Integrationssoftware mit einem fernen Befehl synchronisieren“ auf Seite 119.

Falls bei der Synchronisation Probleme auftreten, finden Sie unter „Snap-in-Programm von IBM iSeries Integrated Server Support“ auf Seite 235 weitere Informationen.

Arten von Codekorrekturen

Es gibt vier Arten von Codekorrekturen:

1. Codekorrekturen, die für den Code der i5/OS-Integration angewendet und als **reguläre vorläufige Programmkorrekturen (PTFs)** bezeichnet werden:
 - Um diese Korrekturen anzuwenden, müssen Sie sie lediglich unter i5/OS installieren.
 - Diese Codekorrekturen sind über die IBM Unterstützungsfunktion oder im Internet unter der Adresse <http://www.ibm.com/servers/eserver/series/integratedxseries> erhältlich (Wählen Sie den Link für die Serviceinformationen in der Navigationsleiste auf der linken Seite aus.) 
2. Codekorrekturen, die auf die Laufwerke des integrierten Servers kopiert, auf dem integrierten Server ausgeführt und als **Service-Pack-PTFs** bezeichnet werden:
 - Das Lizenzprogramm IBM iSeries Integrated Server Support verfügt über eine Komponente für den integrierten Server, die von der i5/OS-Seite aus kopiert wird. Wenn Sie ein kumulatives PTF-Paket für i5/OS anwenden, kann in diesem Paket ein Service-Pack für Integrated Server Support enthalten sein, das auf dem integrierten Server angewendet werden kann. Dies führen Sie aus, indem Sie den integrierten Server synchronisieren.
 - Diese Codekorrekturen sind auch über die IBM Unterstützungsfunktion oder online unter der Adresse <http://www.ibm.com/servers/eserver/series/integratedxseries/> erhältlich (Wählen Sie den Link für die Serviceinformationen in der Navigationsleiste auf der linken Seite aus.) 
3. Codekorrekturen, die auf dem Microsoft Windows-Server selbst angewendet und als **Service-Packs** bezeichnet werden:
 - Diese Korrekturen werden von Microsoft zur Verfügung gestellt. Sie können sie auf der entsprechenden Website für die Windows-Aktualisierung herunterladen.
 - Wenden Sie keine Microsoft-Codekorrekturen an, die Codeelemente des Windows-Servers ändern könnten, die von IBM iSeries Integrated Server Support verwendet werden. Laden Sie beispielsweise keine Treiber für SCSI-Speichereinheiten oder LAN-Einheitentreiber von der Site für die Windows-Aktualisierung herunter.
 - Andere Bereiche sind im Allgemeinen sicher. So können Sie z. B. USB-Einheitentreiber von der Site für die Windows-Aktualisierung auf eigene Verantwortung herunterladen.

- | 4. Hotfixes, die auf dem Microsoft Windows-Server selbst unter Verwendung von Windows Update angewendet werden.

Level der Integrationssoftware über die Konsole des integrierten Windows-Servers synchronisieren

Um den Software-Level mit Hilfe des Snap-in-Programms von iSeries Integrated Server Support zu synchronisieren, müssen Sie über Windows-Systemadministratorberechtigungen verfügen. Bevor Sie mit der Installation beginnen, beenden Sie alle laufenden Anwendungen und vergewissern Sie sich, dass keine Benutzer am integrierten Server angemeldet sind. Sollte dies nicht geschehen, besteht das Risiko eines Datenverlustes, da der integrierte Server nach Beenden der Installation möglicherweise erneut gestartet werden muss.

1. Klicken Sie auf **Start -> Programme -> IBM iSeries -> IBM iSeries Integrated Server Support**.
2. Klicken Sie auf den Namen des integrierten Servers und dann auf **Software-Level**.
3. Der Software-Level der i5/OS-Integrationssoftware und der Windows-Integrationssoftware wird angezeigt. Klicken Sie auf **Synchronisieren**, um die Windows-Integrationssoftware auf denselben Level wie die i5/OS-Integrationssoftware zu bringen.
4. Wenn die Installation erfolgreich ausgeführt wird, wird eine Bestätigungsnachricht ausgegeben.

Anmerkung: Falls Sie sich als Administrator an der Konsole des integrierten Windows-Servers anmelden und die Software-Level nicht übereinstimmen, werden Sie automatisch zur Synchronisation der Software aufgefordert.

Level der Integrationssoftware mit iSeries Navigator synchronisieren

- | 1. Klicken Sie im iSeries Navigator auf **-> Server**.
- 2. Klicken Sie mit der rechten Maustaste auf den integrierten Server, den Sie synchronisieren wollen, und wählen Sie die Option **iSeries Integration Software synchronisieren** aus. (Falls der i5/OS-Server, auf den Sie zugreifen, kein Server der Version V5R3 oder später ist, wird eine Liste mit früheren Optionen ausgegeben. Sie können dann lediglich einzelne Service-Packs installieren und deinstallieren oder eine Releaseaktualisierung ausführen.)
- 3. Klicken Sie auf **Synchronisieren**, um die Aktion zu bestätigen.
- 4. Daraufhin wird die Nachricht ausgegeben, dass die Synchronisation läuft. Anschließend wird eine Beendigungsnachricht angezeigt, die angibt, dass ein Warmstart ausgeführt werden muss. Sie können an dieser Stelle nicht auswählen, ob der Warmstart sofort oder zu einem späteren Zeitpunkt ausgeführt werden soll.

So können Sie ermitteln, welcher Software-Level unter i5/OS und auf dem integrierten Server installiert ist:

- | 1. Klicken Sie im iSeries Navigator auf **-> Server**.
- 2. Klicken Sie mit der rechten Maustaste auf den integrierten Server, dessen Level Sie überprüfen wollen, und wählen Sie die Option **Eigenschaften** aus.
- 3. Klicken Sie auf die Indexzunge **Software**. Dort werden die Software-Level angezeigt.

Level der Integrationssoftware mit einem fernen Befehl synchronisieren

Wenn Sie den Befehl `lvlsync` an der Eingabeaufforderung der Konsole des integrierten Servers eingeben, wird der integrierte Server synchronisiert. Hauptnutzen dieses Befehlszeilenprogramms ist die Tatsache, dass Sie einen integrierten Server synchronisieren können, indem Sie einen Befehl im Fernzugriff übergeben. Dieses Leistungsmerkmal ist beispielsweise dann praktisch, wenn Sie ein CL-Programm schreiben wollen, das Ihre integrierten Server in regelmäßigen Abständen synchronisiert. Mehr über Befehle, die im Fernzugriff übergeben werden, erfahren Sie im Abschnitt „Befehle für den integrierten Windows-Server im Fernzugriff ausführen“ auf Seite 161.

Mit der folgenden einfachen Prozedur kann ein integrierter Server im Fernzugriff synchronisiert werden, indem der Befehl `lvlsync` über die `i5/OS`-Konsole fern übergeben wird:

1. Geben Sie in der zeichenorientierten Schnittstelle von `i5/OS` den Befehl `SBMNWSCMD` ein, und drücken Sie **F4**.
2. Geben Sie im Feld **Befehl** den Wert `lvlsync` ein, und drücken Sie die **Tabulatortaste**.
3. Geben Sie den Namen der NWS-Beschreibung für den integrierten Server im Feld **Server** ein, und drücken Sie die Eingabetaste.

Früher konnten zusammen mit dem Programm "`lvlsync`" optionale Parameter angegeben werden. Diese Parameter sind nicht mehr gültig. Werden sie dennoch angegeben, haben sie allerdings keine Auswirkungen auf die Funktionalität des Befehls.

Das Programm "`lvlsync`" gibt die folgenden Fehlercodes zurück:

lvlsync-Fehlercodes

Fehlercode	Fehler
0	Keine Fehler
01	Administratorberechtigung zum Ausführen von <code>lvlsync</code> erforderlich
02	Release-Level auf dem integrierten Windows-Server ist höher als unter <code>i5/OS</code>
03	Service-Pack-Level auf dem integrierten Server ist höher als unter <code>i5/OS</code>
04	Release kann unter <code>i5/OS</code> nicht installiert werden - Dateien mit sprachabhängigen Anweisungen sind unter <code>i5/OS</code> nicht vorhanden
05	Syntax nicht gültig
06	Kein Zugriff auf Service-Pack-Informationen unter <code>i5/OS</code>
07	Netzlaufwerk kann nicht zugeordnet werden
08	Kein Zugriff auf Service-Pack-Informationen in der Registrierung
09	Datei " <code>qvnacfg.txt</code> " kann nicht geöffnet werden
10	Kein Service-Pack unter <code>i5/OS</code> installiert
11	NWSD nicht gefunden
13	NWSD nicht aktiv
20	Kein Service-Pack unter <code>i5/OS</code> verfügbar
21	Anwendung <code>InstallShield</code> kann nicht gestartet werden
31	Unerwarteter Fehler beim Start von <code>lvlsync</code>
44	Unerwarteter Fehler während der Durchführung von <code>lvlsync</code>

Anmerkung:

Bei der Fehlernachricht `NTA0218` handelt es sich um eine Diagnosenachricht (`*DIAG`), die ausgegeben wird, wenn Syntax, Berechtigung und `NWSD` nicht gefunden wurden.

Kapitel 6. Virtual Ethernet- und externe Netzwerke verwalten

Der folgende Abschnitt enthält Prozeduren, die Ihnen die Erstellung und das Verständnis der Virtual Ethernet- und externen Netzwerke erleichtern, die unter „Konzepte für den Netzwerkbetrieb“ auf Seite 29 beschrieben sind.

- „IP-Adresse, Gateway und MTU-Werte konfigurieren“
- „Virtual Ethernet-Netzwerke konfigurieren“
- „Partitionsübergreifende Virtual Ethernet-Netzwerke konfigurieren“ auf Seite 122
- „Virtual Ethernet-Punkt-zu-Punkt-Netzwerke anzeigen und ändern“ auf Seite 123
- „Externe Netzwerke“ auf Seite 125
- „Netzwerkadapter entfernen“ auf Seite 126

IP-Adresse, Gateway und MTU-Werte konfigurieren

Die Werte für IP-Adresse, Gateway und MTU (größte zu übertragende Einheit) für virtuelle und physische Netzwerkadapter im Hosted System werden unter dem Windows-Betriebssystem verwaltet. Eine Ausnahme davon gilt in folgenden Fällen.

- Die IP-Adresse und die Teilnetzmaske für eine neue Virtual Ethernet-Leitungsbeschreibung können wahlweise vom i5/OS-Befehl INSWNTSVR (Windows-Server installieren) zugeordnet werden. Nachdem der Server installiert wurde, können diese Werte nur unter dem Windows-Betriebssystem geändert werden.
- IP-Adresse und Teilnetzmaske können zugeordnet werden, wenn eine Virtual Ethernet-Leitung einem vorhandenen Server hinzugefügt wird. Nachdem die Leitungsbeschreibung hinzugefügt wurde, können diese Werte nur unter dem Windows-Betriebssystem geändert werden.
- Änderungen der Virtual Ethernet PTP-IP-Adressen sollten sowohl unter dem Windows-Betriebssystem als auch unter i5/OS konfiguriert werden. Weitere Informationen finden Sie unter „IP-Adressenkonflikte bei Virtual Ethernet-Punkt-zu-Punkt“ auf Seite 251.
- IP-Adresse und Gateway für die Windows-Seite eines iSCSI-Netzwerks werden immer unter der Konfiguration des fernen i5/OS-Systems konfiguriert und geändert. Weitere Informationen finden Sie unter „Konfigurationseigenschaften des fernen Systems ändern“ auf Seite 132.
- Die Werte für IP-Adresse, Teilnetzmaske, Gateway und MTU für externe IXS-LAN-Adapter können wahlweise mit dem i5/OS-Befehl INSWNTSVR (Windows-Server installieren) festgelegt werden. Nachdem der Server installiert wurde, können diese Werte nur unter dem Windows-Betriebssystem geändert werden.

Virtual Ethernet-Netzwerke konfigurieren

Dieser Abschnitt beschreibt, wie Sie ein Virtual Ethernet-Netzwerk zwischen integrierten Servern konfigurieren. (Bitte beachten Sie, dass Sie bei einer Neuinstallation des integrierten Servers die Virtual Ethernet-Netzwerke auch vom Installationsbefehl INSWNTSVR konfigurieren lassen können.) Informationen zur Ausdehnung von Virtual Ethernet-Netzwerken auf weitere logische iSeries-Partitionen finden Sie in „Partitionsübergreifende Virtual Ethernet-Netzwerke konfigurieren“ auf Seite 122. Die Prozedur besteht aus den folgenden Hauptschritten:

1. Konfigurieren Sie einen Virtual Ethernet-Port und eine Virtual Ethernet-Leitungsbeschreibung für den integrierten Server. Mit iSeries Navigator:
 - a. Erweitern Sie —>**Server**.
 - b. Klicken Sie mit der rechten Maustaste auf den integrierten Server, und wählen Sie die Option **Eigenschaften** aus.
 - c. Klicken Sie auf der Anzeige mit den Eigenschaften auf die Indexzunge **Virtual Ethernet**.

- d. Klicken Sie auf die Schaltfläche **Hinzufügen...**, um einen neuen Virtual Ethernet-Port hinzuzufügen.
 - e. Geben Sie auf der Anzeige mit den Eigenschaften für Virtual Ethernet die Werte für den neuen Virtual Ethernet-Port an:
 - 1) Wählen Sie die Nummer des Virtual Ethernet-Ports aus.
 - 2) Geben Sie die IP-Adresse ein, die der integrierte Server verwenden soll.
 - 3) Geben Sie die Teilnetzmaske ein, die der integrierte Server verwenden soll.
 - 4) Übernehmen Sie den Standardnamen der Leitungsbeschreibung oder ändern Sie ihn. Der Standardname entspricht dem NWS-Name gefolgt von einem v und der Portnummer. Wird beispielsweise Port 3 einer NWS mit dem Namen Mynwsd hinzugefügt, dann lautet der Standardname der Leitungsbeschreibung Mynwsdv3.
 - 5) Übernehmen Sie den Wert **Keiner** für den zugeordneten Port.
 - 6) Übernehmen Sie den Standardwert **8996** für die maximale Rahmengröße.
 - 7) Wenn es sich bei dem Server um einen Server mit iSCSI-Anschluss handelt, wählen Sie den NWS-Hostadapter entsprechend zu dem iSCSI-HBA aus, den i5/OS für die Verbindung zum Hosted System in dieser Virtual Ethernet-Konfiguration verwenden soll.
 - 8) Klicken Sie auf **OK**, um den neuen Port zur Indexzeile **Virtual Ethernet** auf der Anzeige mit den Servereigenschaften hinzuzufügen.
 - f. Klicken Sie auf der Anzeige mit den Servereigenschaften auf die Indexzeile **OK**, um die Änderungen zu speichern. Dadurch wird die NWS aktualisiert und eine Leitungsbeschreibung für den neuen Virtual Ethernet-Port erstellt.
 - g. Wenn dieser integrierte Server mit mehreren Virtual Ethernet-Netzwerken verbunden werden soll, wiederholen Sie die obigen Schritte, und erstellen Sie für jedes Netzwerk einen Virtual Ethernet-Port und eine Leitungsbeschreibung. Verwenden Sie hierbei unterschiedliche Virtual Ethernet-Portnummern.
2. Wiederholen Sie die Prozedur für alle integrierten Server, die mit dem Netzwerk verbunden werden sollen. Geben Sie hierbei für jeden Server den gleichen Virtual Ethernet-Port an.
 3. Starten Sie die integrierten Server erneut. Daraufhin wird automatisch ein Einheits-treiber für den Virtual Ethernet-Adapter installiert und auf die Windows-TCP/IP-Adresse gesetzt, die Sie für ihn in der NWS angegeben haben. Eine über die Konsole des integrierten Servers eingegebene IP-Adresse überschreibt allerdings die Werte, die in der NWS-Beschreibung eingestellt sind.
 4. Testen Sie, ob das Virtual Ethernet-Netzwerk funktioniert, indem Sie beispielsweise an einem Server ein Pingsignal an die IP-Adressen absetzen, die Sie für die anderen Server angegeben haben.

Partitionsübergreifende Virtual Ethernet-Netzwerke konfigurieren

Partitionsübergreifende Netzwerke mit Hardware Management Console

Wenn ein integrierter Server mit anderen logischen Partitionen oder mit integrierten Servern, die durch andere i5/OS-Partitionen gesteuert werden, kommunizieren soll, müssen Sie mindestens ein partitionsübergreifendes Netzwerk konfigurieren. Die Konfiguration von partitionsübergreifenden Netzwerken auf iSeries-Systemen mit HMC (Hardware Management Console) weicht von der Konfiguration solcher Netzwerke auf anderen Systemen ab. Auf einem iSeries-System mit HMC bestehen partitionsübergreifende Verbindungen zwischen Partitionen oder integrierten Servern, die dieselbe VLAN-ID verwenden. Die teilnehmenden integrierten Server unterstützen VLAN-IDs nicht direkt. Stattdessen benötigt jeder teilnehmende integrierte Server eine Ethernet-Leitungsbeschreibung, die einem virtuellen Adapter, der über ein VLAN-ID verfügt, einen Virtual Ethernet-Portwert zuordnet. Die Konfigurationsprozedur besteht aus den folgenden Schritten:

1. Erstellen Sie mit HMC (Hardware Management Console) für alle Partitionen und für alle integrierten Server, die am partitionsübergreifenden Netzwerk beteiligt sein sollen, je einen Virtual Ethernet-Adapter. Weitere Informationen finden Sie in den Abschnitten zur Partitionierung bei eServer i5 und Konfiguration partitionsinterner Virtual Ethernet-Netzwerke. Geben Sie für jeden virtuellen Adapter, der

einen integrierten Server oder eine i5/OS-Partition mit dem partitionsübergreifenden Netzwerk verbindet, eine konsistente VLAN-ID für den Port an, und nehmen Sie außerdem die Auswahl der Option für den **IEEE 802.1Q-kompatiblen Adapter** zurück.

2. Konfigurieren Sie einen Virtual Ethernet-Port und eine Leitungsbeschreibung wie in Schritt 1 auf Seite 121 unter „Virtual Ethernet-Netzwerke konfigurieren“ auf Seite 121 beschrieben, falls dies für den betreffenden Port (0 bis 9) noch nicht erfolgt ist. Wählen Sie einen Portnamen (Cmnxx) für die entsprechende 268C-Ressource aus.
3. Fahren Sie mit Schritt 2 unter „Virtual Ethernet-Netzwerke konfigurieren“ auf Seite 121 (für alle i5/OS-Partitionen, die einen teilnehmenden integrierten Server steuern) und mit Schritt 3 unter „Virtual Ethernet-Netzwerke konfigurieren“ auf Seite 121 fort.
4. Damit eine Partition vollständig teilnehmen kann, müssen Sie das/die Protokoll(e) innerhalb der Partition entsprechend konfigurieren. Erstellen Sie in jeder i5/OS-Partition eine Ethernet-Leitungsbeschreibung für die entsprechende dedizierte 268C-Portressource. Konfigurieren Sie in jeder Partition, die an der TCP/IP-Übertragung beteiligt ist, eine geeignete, eindeutige IP-Adresse.
5. Testen Sie, ob das partitionsübergreifende Netzwerk funktioniert, indem Sie beispielsweise ein Pingsignal zwischen den verbundenen integrierten Servern und Partitionen absetzen.

Partitionsübergreifende Netzwerke ohne Hardware Management Console

Auf iSeries-Servern ohne HMC bestehen partitionsübergreifende Verbindungen zwischen Partitionen, die dieselbe Netzwerknummer verwenden. Integrierte Server sind nur dann verbunden, wenn die zugehörigen i5/OS-Steuerpartitionen ebenfalls verbunden sind. Die Netzwerknummern 0-9 sind für integrierte Server relevant. Wenn beispielsweise eine i5/OS-Partition für partitionsübergreifende Verbindungen in den Netzwerken 1 und 5 konfiguriert ist, können integrierte Server, die durch diese Partition gesteuert werden, an der partitionsübergreifenden Kommunikation auf den Virtual Ethernet-Ports 1 und 5 teilnehmen. Der Konfigurationsvorgang besteht aus den folgenden Schritten:

1. Konfigurieren Sie die Netzwerknummer, mit der jede Partition verbunden werden soll. Entsprechende Anweisungen finden Sie im Abschnitt zu den Logical Konzepten für logische Partitionen und in der Onlinehilfe von iSeries Navigator. Bitte denken Sie daran, dass integrierte Server nur dann verbunden sind, wenn ihre jeweiligen steuernden i5/OS-Partitionen verbunden sind.
2. Konfigurieren Sie einen Virtual Ethernet-Port und eine Leitungsbeschreibung, falls dies für den gewünschten Port (0 bis 9) noch nicht erfolgt ist. Siehe Schritt 1 in „Virtual Ethernet-Netzwerke konfigurieren“ auf Seite 121. Übernehmen Sie den Wert **Keiner** für den zugeordneten Portnamen.
3. Fahren Sie mit Schritt 2 unter „Virtual Ethernet-Netzwerke konfigurieren“ auf Seite 121 (für alle i5/OS-Partitionen, die einen teilnehmenden integrierten Server steuern) und mit Schritt 3 unter „Virtual Ethernet-Netzwerke konfigurieren“ auf Seite 121 fort.
4. Damit eine Partition vollständig teilnehmen kann, müssen Sie das/die Protokoll(e) innerhalb der Partition entsprechend konfigurieren. Verwenden Sie in jeder i5/OS-Partition, die teilnehmen soll, den Befehl `WRKHDWRSC *CMN`, um den Namen des entsprechenden Ports mit dem Hardwaretyp 268C zu ermitteln, der automatisch erstellt wurde. Siehe Schritt 1 in „Virtual Ethernet-Netzwerke konfigurieren“ auf Seite 121. Erstellen Sie anschließend eine Ethernet-Leitungsbeschreibung für die 268C-Portressource. Konfigurieren Sie in jeder Partition, die an der TCP/IP-Übertragung beteiligt ist, eine geeignete, eindeutige IP-Adresse.
5. Testen Sie, ob das partitionsübergreifende Netzwerk funktioniert, indem Sie beispielsweise ein Pingsignal zwischen den verbundenen integrierten Servern und Partitionen absetzen.

Virtual Ethernet-Punkt-zu-Punkt-Netzwerke anzeigen und ändern

Jeder integrierte Server verfügt über eine virtuelle Punkt-zu-Punkt-Ethernet-Netzwerkverbindung zur iSeries, die der iSeries die Steuerung des integrierten Servers ermöglicht. Im Folgenden erfahren Sie, wie Sie diese Verbindungen - trotz ihrer automatischen Konfiguration während der Installation - anzeigen oder ändern können.

Punkt-zu-Punkt-Ethernet-Verbindungen in i5/OS anzeigen

Punkt-zu-Punkt-Ethernet-Verbindungen bestehen in i5/OS aus einer Leitungsbeschreibung und einem Eintrag in der NWSD des integrierten Servers.

1. Um die Leitungsbeschreibung anzuzeigen, setzen Sie den Befehl WRKCFGSTS *NWS in der zeichenorientierten Schnittstelle von i5/OS ab.
2. Suchen Sie nach der Eintragsfolge für den gewünschten integrierten Server. Einer der Einträge in der Spalte "Leitungsbeschreibung" hat denselben Namen wie die NWSD und endet mit den Zeichen PP. Geben Sie links neben diesem Eintrag eine 8 ein, und drücken Sie die Eingabetaste.
3. Sie befinden sich jetzt im Menü "Mit Leitungsbeschreibungen arbeiten". Geben Sie links neben der Leitungsbeschreibung eine 5 ein, und drücken Sie die Eingabetaste, um ihre Informationen anzuzeigen.
4. Drücken Sie die Taste **F3** so oft, bis Sie zum Basismenü zurückgekehrt sind.
5. Setzen Sie nun den Befehl CFGTCP ab, und wählen Sie Auswahl 1, **Mit TCP/IP-Schnittstelle arbeiten**, aus.
6. Einer der Einträge in der Spalte "Leitungsbeschreibung" sollte denselben Namen wie die NWSD haben und mit den Zeichen PP enden.
7. Die Auswahl 5 zeigt die Informationen zur TCP/IP-Schnittstelle an. Mit der Auswahl 9 oder 10 können Sie die Schnittstelle aktivieren bzw. inaktivieren. Notieren Sie die Internet-Adresse. Sie wird später benötigt.
8. Sehen Sie sich nun den Eintrag in der NWSD des integrierten Servers an. Setzen Sie den Befehl WRKNWSD ab. Suchen Sie nach der NWSD des integrierten Servers, und geben Sie eine 5 ein, um sie anzuzeigen. Drücken Sie die Eingabetaste, um in den Attributen der NWSD zu blättern.
9. Eine der Anzeigen heißt **Zugeordnete Leitungen**. Sie zeigt die Portnummer *VRTETHPTP und den Namen der Leitungsbeschreibung an, die vom Netzwerk verwendet wird.
10. Wenn Sie sich wieder im Menü **Mit NWS-Beschreibungen arbeiten** befinden, können Sie diese Informationen mit der Auswahl 2 ändern.

Punkt-zu-Punkt-Ethernet-Verbindungen über die Konsole des integrierten Windows-Servers anzeigen

1. Klicken Sie in der Konsole des integrierten Servers auf **Start** → **Einstellungen** → **Systemsteuerung**. Wählen Sie anschließend die Option **Netzwerk- und DFÜ-Verbindungen** aus.
2. Eines der Symbole heißt **Virtual Ethernet-Punkt-zu-Punkt**. Doppelklicken Sie auf dieses Symbol.
3. Klicken Sie im aufgerufenen Dialogfenster auf **Eigenschaften**.
4. Doppelklicken Sie im nächsten Dialogfenster auf **Internetprotokoll (TCP/IP)**.
5. In diesem letzten Dialogfenster sollte nun die IP-Adresse angezeigt sein, die der Virtual Ethernet-Punkt-zu-Punkt-Verbindung auf der Seite des integrierten Servers zugeordnet ist. Es sollte sich hierbei um die IP-Adresse von i5/OS handeln, die um 1 erhöht wurde und somit ein gerader Wert anstelle eines ungeraden Wertes ist.
6. Schließen Sie alle geöffneten Fenster, klicken Sie auf **Start** → **Ausführen**, und geben Sie den Befehl `cmd` ein. Drücken Sie die Eingabetaste. Dies startet eine Instanz der Windows-Eingabeaufforderung.
7. Geben Sie an der angezeigten Eingabeaufforderung "C:\>" den Befehl "ping" gefolgt von der i5/OS-IP-Adresse an, die Sie im vorherigen Schritt ermittelt haben (Beispiel: `ping 192.168.3.1`). Bei einer erfolgreichen Ausführung gibt der Befehl die Nachricht Antwort von ... zurück. Der Befehl "ping" sendet ein Datenpaket an eine bestimmte Internet-Adresse und misst die Zeit, die für das Senden benötigt wird.
8. (Optional) Kehren Sie zur zeichenorientierten Schnittstelle von i5/OS zurück, und geben Sie den Befehl `call qcmd` ein. (Dies vergrößert den Darstellungsbereich, damit Sie die Ergebnisse der Befehle sehen können.) Verwenden Sie den entsprechenden i5/OS-Befehl, um ein Pingsignal an den integrierten Server abzusetzen (Beispiel: `ping '192.168.3.2'`). Wenn dieser Befehl erfolgreich ausgeführt wird, verfügen Sie über ein einwandfrei funktionierendes Virtual Ethernet-Punkt-zu-Punkt-Netzwerk.

Externe Netzwerke

Sie können eine neue Netzwerkkartenkarte in einem freien PCI-Steckplatz installieren. In diesem Fall muss der neue Adapter auf dem integrierten Windows-Server konfiguriert werden.

Anweisungen zur Installation einer neuen Netzwerkkartenkarte finden Sie in den Informationen zur Installation von iSeries-Features. Wählen Sie das gewünschte iSeries-Modell, und lesen Sie die Informationen zur **Installation von PCI-Karten und integrierten xSeries-Adapterkarten**.

Anweisungen zur Installation eines neuen Netzwerkadapters finden Sie unter „Einheitentreiber für Netzwerkadapter installieren und Adressinformationen des Adapters zum integrierten Windows-Server hinzufügen“.

Anweisungen zur Erstellung einer Virtual Ethernet-Verbindung finden Sie unter „Virtual Ethernet-Netzwerke konfigurieren“ auf Seite 121.

Um einen Netzwerkkarten zu entfernen, verwenden Sie die Informationen im Abschnitt „Netzwerkadapter entfernen“ auf Seite 126.

Einheitentreiber für Netzwerkadapter installieren und Adressinformationen des Adapters zum integrierten Windows-Server hinzufügen

Mit den Informationen in diesem Abschnitt können Sie Adaptertreiber installieren und Adapteradressinformationen für die neuen Adapter auf dem integrierten Windows-Server hinzufügen.


Die Adapter und Einheitentreiber unter Windows 2000 Server und Windows Server 2003 unterstützen die so genannte "Plug-n-Play"-Fähigkeit. Führen Sie nach der physischen Installation der Adapter einen Neustart des integrierten Servers durch, indem Sie diesen anhängen. Die Adapter sind nun verfügbar. Beachten Sie bitte, dass für jeden Adapter (jede Verbindung) die entsprechende IP-Adresse konfiguriert werden muss.

Wenn Sie einen Upgrade des integrierten xSeries-Servers von Windows NT 4.0 auf Windows 2000 Server durchführen, müssen Sie den alten Adapter entfernen, bevor der neue Adapter installiert wird. Entsprechende Anweisungen finden Sie unter „Netzwerkadapter entfernen“ auf Seite 126.

Windows 2000 Server oder Windows Server 2003 erkennt den neuen Adapter. So konfigurieren Sie die IP-Adresse für einen Adapter:

1. Klicken Sie mit der rechten Maustaste auf **Netzwerkumgebung**, und klicken Sie anschließend im Pull-down-Menü auf **Eigenschaften**.
2. Doppelklicken Sie auf den richtigen Adapter (LAN-Verbindung), um die IP-Adresse zu konfigurieren.
3. Klicken Sie auf die Schaltfläche **Eigenschaften**.
4. Wählen Sie **Internetprotokoll (TCP/IP)** aus, und klicken Sie anschließend auf die Schaltfläche **Eigenschaften**.
5. Aktivieren Sie das Optionsfeld **Folgende IP-Adresse verwenden**, wenn es noch nicht aktiviert ist.
6. Geben Sie im Feld **IP-Adresse** die IP-Adresse ein.
7. Geben Sie im Feld **Teilnetzmaske** die Teilnetzmaske an.
8. Geben Sie im Feld **Standardgateway** die Adresse des Standardgateways an.
9. Klicken Sie auf **OK** -> **OK** -> **Schließen**, um die Einstellung der IP-Adresse zu beenden.

Anmerkung:

Wenn Sie von Windows darauf hingewiesen werden, dass die IP-Adresse bereits für einen anderen Adapter konfiguriert ist und Sie keinen Adapter finden können, der diese Adresse verwendet, hat Windows vermutlich eine vorherige Hardwareumgebung erkannt, die diese Adresse verwendet hat. Weitere Informationen zum Anzeigen eines LAN-Adapters aus einer früheren Hardwareumgebung, so dass die IP-Adresse freigegeben werden kann, enthält der Artikel Q241257 Device Manager Does Not Display Devices Not Currently Present in Windows 2000  in der Microsoft Knowledge Base.

Netzwerkadapter entfernen

- | Bevor Sie eine Netzwerkadapterkarte aus einem integrierten Windows-Server entfernen, müssen Sie diese in Windows deinstallieren.

- | So deinstallieren Sie Netzwerkadapter von einem integrierten Server:
 - | 1. Klicken Sie auf **Start, Einstellungen und Systemsteuerung**.
 - | 2. Starten Sie den **Hardware-Assistenten**, und klicken Sie in der ersten Anzeige auf **Weiter**.
 - | 3. Klicken Sie auf **Gerät deinstallieren bzw. entfernen**.
 - | 4. Klicken Sie in der Anzeige zum **Auswählen einer Aufgabe zum Entfernen** auf **Weiter**, um die Standardeinstellung (Gerät deinstallieren) zu verwenden.
 - | 5. Wählen Sie die Einheit, die deinstalliert werden soll, in der Liste aus (z. B. IBM PCI Token-Ring-Adapter).
 - | 6. Klicken Sie auf **Ja**, um das Entfernen des Adapters zu bestätigen.
 - | 7. Da Windows 2000 Server und Windows Server 2003 "Plug-and-Play"-Betriebssysteme sind, muss der Adapter entweder physisch aus i5/OS entfernt oder inaktiviert werden, bevor der Server erneut gestartet wird. Wenn der Adapter beim Starten des integrierten Servers noch immer vorhanden ist, stellt das Betriebssystem ihn als neue Hardware fest und installiert den Einheits-treiber erneut. So können Sie den Adapter inaktivieren, ohne ihn zu entfernen:
 - | a. Wählen Sie in der **Systemsteuerung** den Eintrag **Netzwerk- und DFÜ-Verbindungen** aus.
 - | b. Wählen Sie den LAN-Adapter aus.
 - | c. Klicken Sie mit der rechten Maustaste, und wählen Sie **Deaktivieren** aus.
 - | 8. Starten Sie den Server erneut, um diese Prozedur abzuschließen.

Kapitel 7. Verbindungen der Server mit iSCSI-Anschluss verwalten

Die folgenden Abschnitte führen Sie durch einige allgemeine und im täglichen Betrieb anfallende Aufgaben, die auf integrierten Servern mit iSCSI-HBA ausgeführt werden.

- „Mit iSCSI-Konfigurationsobjekten arbeiten“
- „Sicherheit zwischen i5/OS und Hosted Systemen konfigurieren“ auf Seite 138
- „iSCSI-Hostbusadapter verwalten“ auf Seite 143
- „Fernen Server erkennen und verwalten“ auf Seite 150

Mit iSCSI-Konfigurationsobjekten arbeiten

i5/OS-Objekte werden verwendet, um iSCSI-HBAs für iSeries, den fernen xSeries oder das IBM Blade-Center-System, den Serviceprozessor des fernen Systems und die Sicherheitsattribute des iSCSI-Netzes zu konfigurieren und zu verwalten. Weitere Informationen enthalten die folgenden Abschnitte.

- „NWS-Hostadapter verwalten“
- „Konfigurationen von Netzwerkservern ferner Systeme verwalten“ auf Seite 130
- „Netzwerkserverkonfigurationen des Serviceprozessors verwalten“ auf Seite 133
- „Netzwerkserverkonfigurationen für Verbindungssicherheit verwalten“ auf Seite 135

NWS-Hostadapter verwalten

NWSH-Objekte werden verwendet, um den iSCSI-Hostbusadapter (iSCSI-HBA) zu konfigurieren, der als Ziel für iSeries dient. Ein NWSH-Objekt muss gestartet (angehängt) sein, damit ein integrierter Server den entsprechenden iSCSI.HBA für den Speichervorgang oder für Virtual Ethernet-Datenflüsse verwendet. Wenn ein NWSH-Objekt gestoppt (abgehängt) wird, steht der entsprechende iSCSI-HBA den integrierten Servern nicht mehr zur Verfügung, die Speicher- oder Virtual Ethernet-Pfade für dessen Verwendung definiert haben. Weitere Informationen finden Sie unter „NWS-Hostadapter“ auf Seite 45.

Die folgenden Tasks können bei NWSH-Objekten ausgeführt werden:

- „NWS-Hostadapterobjekt erstellen“
- „Ein NWS-Hostadapterobjekt auf der Basis eines anderen erstellen“ auf Seite 128
- „Eigenschaften des NWS-Hostadapters anzeigen“ auf Seite 128
- „Eigenschaften des NWS-Hostadapters ändern“ auf Seite 129
- „NWS-Hostadapter starten“ auf Seite 129
- „NWS-Hostadapter stoppen“ auf Seite 129
- „NWS-Hostadapter löschen“ auf Seite 130

NWS-Hostadapterobjekt erstellen

Für jeden iSeries-Ziel-iSCSI-HBA (iSCSI-HBA) muss ein NWS-Hostadapterobjekt erstellt werden.

Gehen Sie wie folgt vor, um mit iSeries Navigator einen NWS-Hostadapter zu erstellen:

1. Erweitern Sie **Verwaltung integrierter Server**.
2. Erweitern Sie **iSCSI-Verbindungen**.
3. Klicken Sie mit der rechten Maustaste auf **Lokale Hostadapter**.
4. Wählen Sie **Neue NWS-Hostadapter** aus.
5. Auf der Indexzunge **Allgemein**:
 - Geben Sie für die NWSH-Einheit **Name** und **Beschreibung** ein.

- | • Wählen Sie **Hardwareressource** aus.
- | • Wählen Sie **Objektberechtigung** aus.
- | 6. Auf der Indexzunge **Lokale Schnittstellen** geben Sie die Informationen ein, mit denen SCSI- und LAN-Schnittstellen für den iSCSI-HBA definiert werden.
- | 7. Klicken Sie auf **OK**.

| **Anmerkung:** Der NWS-Hostadapter und die ferne Systemkonfiguration definieren die IP-Adressinformationen für die gegenüberliegenden Seiten des iSCSI-Netzwerks. Wenn sie über ein einfaches Wählnetz verbunden sind, gelten folgende Regeln:

- | • Die SCSI-Internetadressen in diesen beiden Objekten, die über einen Switch verbunden sind, müssen sich im selben Teilnetz befinden. Beispiel: Bei Teilnetzmasken mit den IP-Adressen im Format a.b.x.y und 255.255.255.0 muss a.b.x in beiden Objekten den gleichen Wert haben.
- | • Die LAN-Internetadressen in diesen beiden Objekten, die über einen Switch verbunden sind, müssen sich im selben Teilnetz befinden.
- | • Im NWS-Hostadapter können die Gateway-Elemente beliebige IP-Adressen in einem beliebigen Teilnetz sein, wenn sich kein Gateway in Ihrem Netzwerk befindet.
- | • In der fernen Systemkonfiguration sollten die Gateway-Elemente leer sein, wenn sich kein Gateway in Ihrem Netzwerk befindet.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter CRTDEVNWSH oder WRKDEVD.

| **Ein NWS-Hostadapterobjekt auf der Basis eines anderen erstellen**

| Sie können ein bestehendes NWS-Hostadapterobjekt kopieren, um ein neues zu erstellen. Dies spart Zeit, wenn einige der neuen NWSH-Attribute den existierenden NWSH-Attributen ähneln oder gleichen.

| Gehen Sie wie folgt vor, um einen NWS-Hostadapter auf der Basis eines bestehenden Adapters mit iSeries Navigator zu erstellen:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Lokale Hostadapter** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf einen lokalen Hostadapter in der Liste.
- | 5. Wählen Sie **Neu basierend auf...** aus.
- | 6. Geben Sie für die neue NWSH-Einheit einen **Namen** ein.
- | 7. Geben Sie alle anderen Attribute an, die sich von denen des kopierten NWSH unterscheiden.
- | 8. Klicken Sie auf **OK**.

| Wenn Sie einen CL-Befehl verwenden möchten, finden Sie weitere Informationen unter WRKDEVD.

| **Eigenschaften des NWS-Hostadapters anzeigen**

| Ein NWSH-Objekt enthält die Konfigurationsdaten für einen iSeries-Ziel-iSCSI-HBA (iSCSI-HBA).

| Gehen Sie wie folgt vor, um mit iSeries Navigator die Attribute eines NWS-Hostadapters anzuzeigen:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Lokale Hostadapter** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf einen lokalen Hostadapter in der Liste.
- | 5. Wählen Sie **Eigenschaften** aus.
- | 6. Klicken Sie auf die Indexzungen der Eigenschaften, die Sie anzeigen wollen.
- | 7. Klicken Sie auf **Abbrechen**, um die Anzeige zu schließen.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter DSPDEVD oder WRK-
| DEVD.

| **Eigenschaften des NWS-Hostadapters ändern**

| Ein NWSH-Objekt enthält die Konfigurationsdaten für einen iSeries-Ziel-iSCSI-HBA (iSCSI-HBA).

| Gehen Sie wie folgt vor, um mit iSeries Navigator die Attribute eines NWS-Hostadapters zu ändern:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Lokale Hostadapter** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf einen lokalen Hostadapter in der Liste.
- | 5. Wählen Sie **Eigenschaften** aus.
- | 6. Klicken Sie auf die Indexzungen der Eigenschaften, die Sie ändern wollen.
- | 7. Klicken Sie auf **OK**, um die Änderungen zu speichern.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter CHGDEVNWSH oder
| WRKDEVD.

| **NWS-Hostadapter starten**

| Um einen integrierten Server als iSeries-Ziel-iSCSI-HBA (iSCSI-HBA) für Speicherung oder Virtual Ether-
| net-Datenfluss zu verwenden, muss der entsprechende NWS-Hostadapter (NWSH) gestartet (angehängt)
| sein.

| Gehen Sie wie folgt vor, um mit iSeries Navigator einen NWS-Hostadapter zu starten:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Lokale Hostadapter** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf einen lokalen Hostadapter in der Liste.
- | 5. Wählen Sie **Starten** aus.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter VRYCFG oder WRK-
| CFGSTS.

| **NWS-Hostadapter stoppen**

| Wenn ein NWSH-Objekt gestoppt (abgehängt) wird, steht der entsprechende iSeries-iSCSI-Ziel-HBA (iSC-
| SI-HBA) den integrierten Servern nicht mehr zur Verfügung, die Speicher- oder Virtual Ethernet-Pfade für
| dessen Verwendung definiert haben.

| Das Stoppen eines NWS-Hostadapters, der von aktiven Servern verwendet wird, kann zu Systemfehlern
| bei diesen Servern führen, wenn auf kritische Speicherressourcen nicht zugegriffen werden kann, weil der
| iSCSI-HBA nicht mehr zur Verfügung steht, der dem NWS-Hostadapter entspricht. Normalerweise sollten
| integrierte Server, die den NWSH verwenden, erst dann abgeschaltet werden, nachdem der NWSH
| gestoppt wurde. Weitere Informationen finden Sie unter „Integrierten Windows-Server mit iSeries Navi-
| gator starten und stoppen“ auf Seite 157.

| Gehen Sie wie folgt vor, um mit iSeries Navigator einen NWS-Hostadapter zu stoppen:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Lokale Hostadapter** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf einen lokalen Hostadapter in der Liste.
- | 5. Wählen Sie **Stoppen** aus.
- | 6. Klicken Sie auf der Bestätigungsanzeige auf **Stoppen**.

| 7. Wenn die aktiven Server gerade den NWSH verwenden, wird eine Warnung angezeigt. Klicken Sie auf **Weiter**.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter VRYCFG oder WRK-CFGSTS.

| **NWS-Hostadapter löschen**

| Gehen Sie wie folgt vor, um mit iSeries Navigator einen NWS-Hostadapter zu löschen:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Lokale Hostadapter** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf einen lokalen Hostadapter in der Liste.
- | 5. Wählen Sie **Löschen** aus.
- | 6. Klicken Sie in der Bestätigungsanzeige auf **Löschen**.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter DLTDEVD oder WRK-DEVD.

| **Konfigurationen von Netzwerkservern ferner Systeme verwalten**

| Die Objekte für NWS-Konfiguration des fernen Systems (NWSCFG-Subtyp RMTSYS) werden verwendet, um die Attribute eines an iSCSI angeschlossenen fernen xSeries- oder IBM BladeCenter-Servers zu konfigurieren. Mit der Konfiguration des fernen Systems wird die spezifische xSeries- oder IBM BladeCenter-Hardware identifiziert, auf der der integrierte Server ausgeführt wird. Sie definiert auch, wie das ferne System bootet und mit dem iSeries-System kommuniziert. Weitere Informationen finden Sie unter „Konfiguration des fernen Systems“ auf Seite 45.

| Die folgenden Tasks können bei Konfigurationsobjekten für ferne Systeme ausgeführt werden:

- | • „Konfigurationsobjekt für ein fernes System erstellen“
- | • „Konfigurationsobjekt des fernen Systems auf der Basis eines anderen erstellen“ auf Seite 131
- | • „Konfigurationseigenschaften des fernen Systems anzeigen“ auf Seite 131
- | • „Konfigurationseigenschaften des fernen Systems ändern“ auf Seite 132
- | • „Status des fernen Systems anzeigen“ auf Seite 132
- | • „Konfigurationsobjekt für ein fernes System löschen“ auf Seite 132

| **Konfigurationsobjekt für ein fernes System erstellen**

| Ein Konfigurationsobjekt für Netzwerkserver ferner Systeme (NWSCFG-Subtyp RMTSYS) muss für jeden xSeries- oder IBM BladeCenter-Server erstellt werden, auf dem ein an iSCSI angeschlossener integrierter Server ausgeführt werden soll.

| Gehen Sie wie folgt vor, um mit iSeries Navigator ein fernes System zu konfigurieren:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Klicken Sie mit der rechten Maustaste auf **Ferne Systeme**.
- | 4. Wählen Sie **Neue Konfiguration für fernes System**.
- | 5. Auf der Indexzunge **Allgemein**:
 - | • Geben Sie **Name** und **Beschreibung** ein.
 - | • Wählen Sie **Serviceprozessorkonfiguration** aus.
 - | • Geben Sie die **Identität des fernen Systems** an.
 - | • Wählen Sie **Objektberechtigung** aus.

- | 6. Geben Sie auf der Indexzunge **Netzwerkschnittstelle** Informationen ein, um die SCSI- und LAN-Schnittstellenattribute für das ferne System zu definieren.
- | 7. Geben Sie, falls gewünscht, Werte in den Indexzungen **Bootparameter** und **CHAP-Authentifizierung** ein.
- | 8. Klicken Sie auf **OK**.

| **Anmerkung:** Der NWS-Hostadapter und die ferne Systemkonfiguration definieren die IP-Adressinformationen für die gegenüberliegenden Seiten des iSCSI-Netzwerks. Wenn sie über ein einfaches Wählnetz verbunden sind, gelten folgende Regeln:

- | • Die SCSI-Internetadressen in diesen beiden Objekten, die über einen Switch verbunden sind, müssen sich im selben Teilnetz befinden. Beispiel: Bei Teilnetzmasken mit den IP-Adressen im Format a.b.x.y und 255.255.255.0 muss a.b.x in beiden Objekten den gleichen Wert haben.
- | • Die LAN-Internetadressen in diesen beiden Objekten, die über einen Switch verbunden sind, müssen sich im selben Teilnetz befinden.
- | • Im NWS-Hostadapter können die Gateway-Elemente beliebige IP-Adressen in einem beliebigen Teilnetz sein, wenn sich kein Gateway in Ihrem Netzwerk befindet.
- | • In der fernen Systemkonfiguration sollten die Gateway-Elemente leer sein, wenn sich kein Gateway in Ihrem Netzwerk befindet.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter CRTNWSCFG oder WRKNWSCFG.

| **Konfigurationsobjekt des fernen Systems auf der Basis eines anderen erstellen**

| Sie können ein Objekt einer bestehenden NWS-Konfiguration des fernen Systems (NWSCFG-Subtyp RMTSYS) kopieren, wenn Sie ein neues Objekt erstellen. Dies spart Zeit, wenn einige der neuen Attribute für die Konfiguration des fernen Systems den existierenden Attributen ähneln oder gleichen.

| Gehen Sie wie folgt vor, um mit iSeries Navigator ein fernes System auf der Basis eines bestehenden Systems zu erstellen:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Ferne Systeme** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf eine Konfiguration des fernen Systems in der Liste.
- | 5. Wählen Sie **Neu basierend auf...** aus.
- | 6. Geben Sie den **Namen** für die neue Konfiguration des fernen Systems ein.
- | 7. Geben Sie alle anderen Attribute an, die sich von den Attributen der kopierten Konfiguration unterscheiden sollen.
- | 8. Klicken Sie auf **OK**.

| **Anmerkung:** Für diese Task gibt es keinen äquivalenten CL-Befehl.

| **Konfigurationseigenschaften des fernen Systems anzeigen**

| Ein Konfigurationsobjekt für Netzwerkserver ferner Systeme (NWSCFG-Subtyp RMTSYS) enthält Konfigurationsdaten für einen IBM xSeries- oder BladeCenter-Server, auf dem ein an iSCSI angeschlossener integrierter Server ausgeführt werden soll.

| Gehen Sie wie folgt vor, um mit iSeries Navigator die Konfigurationsattribute eines fernen Systems anzuzeigen:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Ferne Systeme** aus.

- | 4. Klicken Sie mit der rechten Maustaste auf die Konfiguration eines fernen Systems in der Liste.
- | 5. Wählen Sie **Eigenschaften** aus.
- | 6. Klicken Sie auf die Indexungen der Eigenschaften, die Sie anzeigen wollen.
- | 7. Klicken Sie auf **OK**, um die Anzeige zu schließen.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter DSPNWSCFG oder WRKNWSCFG.

| **Konfigurationseigenschaften des fernen Systems ändern**

| Ein Konfigurationsobjekt für Netzwerkserver ferner Systeme (NWSCFG-Subtyp RMTSYS) enthält Konfigurationsdaten für einen xSeries- oder IBM BladeCenter-Server, auf dem ein an iSCSI angeschlossener integrierter Server ausgeführt werden soll.

| Gehen Sie wie folgt vor, um mit iSeries Navigator die Konfigurationsattribute eines fernen Systems zu ändern:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Ferne Systeme** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf die Konfiguration eines fernen Systems in der Liste.
- | 5. Wählen Sie **Eigenschaften** aus.
- | 6. Klicken Sie auf die Indexungen der Eigenschaften, die Sie ändern wollen.
- | 7. Klicken Sie auf **OK**, um die Änderungen zu speichern.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter CHGNWSCFG oder WRKNWSCFG.

| **Status des fernen Systems anzeigen**

| Sie können den Hardwarestatus von xSeries- oder IBM BladeCenter-Servern anzeigen. So können Sie z. B. feststellen, ob die Hardware von einem an iSCSI angeschlossenen integrierten Server verwendet werden kann.

| Gehen Sie wie folgt vor, um mit iSeries Navigator den Status eines fernen Systems anzuzeigen:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Ferne Systeme** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf die Konfiguration eines fernen Systems in der Liste.
- | 5. Wählen Sie **Status** aus.
- | 6. Der Hardwarestatus des fernen Systems wird angezeigt.
- | 7. Klicken Sie auf **Abbrechen**, um die Anzeige zu schließen.

| Wenn Sie einen CL-Befehl verwenden möchten, finden Sie weitere Informationen unter WRKNWSCFG.

| **Konfigurationsobjekt für ein fernes System löschen**

| Gehen Sie wie folgt vor, um mit iSeries Navigator die Konfiguration eines fernen Systems zu löschen:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Ferne Systeme** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf die Konfiguration eines fernen Systems in der Liste.
- | 5. Wählen Sie **Löschen** aus.
- | 6. Klicken Sie in der Bestätigungsanzeige auf **Löschen**.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter DLTNWSCFG oder WRKNWSCFG.

| **Netzwerkserverkonfigurationen des Serviceprozessors verwalten**

| Die Objekte der Netzwerkserverkonfigurationen von Serviceprozessoren (NWSCFG-Subtyp 1SRVPRC) werden verwendet, um die Attribute eines an iSCSI angeschlossenen fernen xSeries- oder IBM BladeCenter-Servers zu konfigurieren. Die Serviceprozessorkonfiguration definiert die Attribute, mit denen der Serviceprozessor festgestellt und zu ihm oder dem Managementmodul im Netz Verbindung hergestellt wird. Die NWS-Konfigurationsobjekte des fernen Systems enthalten einen Verweis auf das entsprechende Konfigurationsobjekt des Serviceprozessors. Es wird verwendet, um die Hardware des fernen Systems zu steuern. Weitere Informationen finden Sie unter „Konfiguration für Serviceprozessor“ auf Seite 46.

| **Anmerkung:** Nicht für jeden IBM BladeCenter-Server in einem BladeCenter-Chassis ist eine eigene Serviceprozessorkonfiguration erforderlich. Für das IBM BladeCenter-Chassis ist eine Serviceprozessorkonfiguration ausreichend.

| Die folgenden Tasks können bei Konfigurationsobjekten von Serviceprozessoren ausgeführt werden:

- | • „Konfigurationsobjekt für einen Serviceprozessor erstellen“
- | • „Konfigurationsobjekt des Serviceprozessors auf der Basis eines anderen erstellen“ auf Seite 134
- | • „Konfigurationseigenschaften des Serviceprozessors anzeigen“ auf Seite 134
- | • „Konfigurationseigenschaften des Serviceprozessors ändern“ auf Seite 134
- | • „Serviceprozessor initialisieren“ auf Seite 135
- | • „Konfigurationsobjekt für einen Serviceprozessor löschen“ auf Seite 135

| **Konfigurationsobjekt für einen Serviceprozessor erstellen**

| Ein Konfigurationsobjekt für Netzserver ferner Systeme (NWSCFG-Subtyp SRVPRC) muss für den Serviceprozessor oder das Managementmodul auf jedem xSeries- oder IBM BladeCenter-Server erstellt werden, auf dem ein an iSCSI angeschlossener integrierter Server ausgeführt werden soll.

| **Anmerkung:** Nicht für jedes Blade im IBM BladeCenter-Chassis eine Serviceprozessorkonfiguration erforderlich. Für das BladeCenter-Chassis genügt eine Serviceprozessorkonfiguration.

| Gehen Sie wie folgt vor, um mit iSeries Navigator eine Serviceprozessorkonfiguration zu erstellen:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Klicken Sie mit der rechten Maustaste auf **Serviceprozessoren**.
- | 4. Wählen Sie **Neue Serviceprozessorkonfiguration** aus.
- | 5. Auf der Indexzunge **Allgemein**:
 - | • Geben Sie **Name** und **Beschreibung** ein.
 - | • Geben Sie entweder **Hostname**, **Internetadresse** oder **Seriennummer** ein, um den Serviceprozessor im Netz zu identifizieren.
 - | • Wählen Sie **Objektberechtigung** aus.
- | 6. Definieren Sie auf der Indexzunge **Sicherheit** den Typ der Sicherheit, der bei der Verbindung des Serviceprozessors verwendet werden soll.
- | 7. Klicken Sie auf **OK**.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter CRTNWSCFG oder WRKNWSCFG.

| **Konfigurationsobjekt des Serviceprozessors auf der Basis eines anderen erstellen**

| Sie können ein Objekt einer bestehenden NWS-Konfiguration des Serviceprozessors (NWSCFG-Subtyp SRVPRC) kopieren, wenn Sie eine neue Konfiguration erstellen. Dies spart Zeit, wenn einige der neuen Attribute für die Konfiguration des Serviceprozessors den existierenden Attributen ähneln oder gleichen.

| Gehen Sie wie folgt vor, um mit iSeries Navigator einen Serviceprozessor auf der Basis eines bestehenden Prozessors zu konfigurieren:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Serviceprozessoren** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf eine Konfiguration des Serviceprozessors in der Liste.
- | 5. Wählen Sie **Neu basierend auf...** aus.
- | 6. Geben Sie den **Namen** für die neue Konfiguration des Serviceprozessors ein.
- | 7. Geben Sie alle anderen Attribute an, die sich von den Attributen der kopierten Serviceprozessorkonfiguration unterscheiden sollen.
- | 8. Klicken Sie auf **OK**.

| **Anmerkung:** Für diese Task gibt es keinen äquivalenten CL-Befehl.

| **Konfigurationseigenschaften des Serviceprozessors anzeigen**

| Ein Konfigurationsobjekt für Serviceprozessornetzserver (NWSCFG-Subtyp SRVPRC) enthält Konfigurationsdaten für einen Serviceprozessor oder ein Managementmodul eines xSeries- oder IBM BladeCenter-Servers, auf dem ein an iSCSI angeschlossener integrierter Server ausgeführt werden soll.

| Gehen Sie wie folgt vor, um mit iSeries Navigator die Attribute einer Serviceprozessorkonfiguration zu ändern:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Serviceprozessoren** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf eine Serviceprozessorkonfiguration in der Liste.
- | 5. Wählen Sie **Eigenschaften** aus.
- | 6. Klicken Sie auf die Indexungen der Eigenschaften, die Sie anzeigen wollen.
- | 7. Klicken Sie auf **OK**, um die Anzeige zu schließen.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter DSPNWSCFG oder WRKNWSCFG.

| **Konfigurationseigenschaften des Serviceprozessors ändern**

| Ein Konfigurationsobjekt für Netzserver ferner Systeme (NWSCFG-Subtyp SRVPRC) enthält Konfigurationsdaten für einen Serviceprozessor oder ein Managementmodul einer IBM xSeries- oder BladeCenter-Einheit, die verwendet werden, um einen an iSCSI angeschlossenen integrierten Server auszuführen.

| Gehen Sie wie folgt vor, um mit iSeries Navigator die Attribute einer Serviceprozessorkonfiguration zu ändern:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Serviceprozessoren** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf einen Serviceprozessor in der Liste.
- | 5. Wählen Sie **Eigenschaften** aus.
- | 6. Klicken Sie auf die Indexungen der Eigenschaften, die Sie ändern wollen.

| 7. Klicken Sie auf **OK**, um die Änderungen zu speichern.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter CHGNWSCFG oder WRKNWSCFG.

| **Serviceprozessor initialisieren**

| Ein Konfigurationsobjekt für Serviceprozessornetzserver (NWSCFG-Subtyp SRVPRC) enthält Konfigurationsdaten für einen Serviceprozessor oder ein Managementmodul eines xSeries- oder IBM BladeCenter-Einheit, die verwendet werden, um einen an iSCSI angeschlossenen integrierten Server auszuführen. Der Serviceprozessor muss initialisiert werden, bevor er zusammen mit einem integrierten Server verwendet werden kann. Sie möchten evtl. auch Benutzer, Kennwort und Zertifikat für die sichere Serviceprozessorverbindung neu generieren oder synchronisieren bzw. Benutzer oder Kennwort ändern, die für die Verbindung zum Serviceprozessor verwendet werden.

| Gehen Sie wie folgt vor, um mit iSeries Navigator einen Serviceprozessor zu initialisieren:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Serviceprozessoren** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf eine Serviceprozessorkonfiguration in der Liste.
- | 5. Wählen Sie **Initialisieren** aus.
- | 6. Wählen Sie eine der folgenden Optionen aus:
 - | • **Neuen Serviceprozessor initialisieren**
 - | • **Serviceprozessorzertifikat neu generieren**
 - | • **Serviceprozessorzertifikat synchronisieren**
 - | • **Benutzer-ID und Kennwort des Serviceprozessors ändern**
- | 7. Geben Sie, falls erforderlich, den **Benutzer** und das **Kennwort** ein.
- | 8. Klicken Sie auf **Initialisieren**, um die ausgewählte Option auszuführen.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter INZNWSCFG oder WRKNWSCFG.

| **Konfigurationsobjekt für einen Serviceprozessor löschen**

| Gehen Sie wie folgt vor, um mit iSeries Navigator eine Serviceprozessorkonfiguration zu löschen:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Serviceprozessoren** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf eine Serviceprozessorkonfiguration in der Liste.
- | 5. Wählen Sie **Löschen** aus.
- | 6. Klicken Sie in der Bestätigungsanzeige auf **Löschen**.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter DLTNWSCFG oder WRKNWSCFG.

| **Netzwerkserverkonfigurationen für Verbindungssicherheit verwalten**

| Die Objekte der Netzwerkserverkonfiguration für Verbindungssicherheit (NWSCFG-Subtyp CNNSEC) werden verwendet, um Richtlinien für die IP-Netzwerksicherheit (IPSec) zu definieren, die für Speicherungs- und Virtual Ethernet-Datenfluss zwischen iSeries- und xSeries- oder IBM BladeCenter-Blade-Servern gelten. Weitere Informationen finden Sie unter „Konfiguration für Verbindungssicherheit“ auf Seite 49.

| **Anmerkung:** Wenn die iSCSI-HBA-Hardware auf der iSeries- oder der xSeries/Center-Seite der iSCSI-
| Verbindung IPsec nicht unterstützt, kann IPsec nicht verwendet werden, um einen sicheren
| Datenfluss über das iSCSI-Netzwerk zu gewährleisten. Wenn die iSCSI-HBA-Hardware
| IPsec nicht unterstützt, muss zwar ein Verbindungssicherheitsobjekt erstellt werden, es soll-
| ten aber keine IP-Sicherheitsregeln definiert werden.

| Die folgenden Tasks können bei Verbindungssicherheitskonfigurationsobjekten ausgeführt werden:

- | • „Verbindungssicherheitskonfigurationsobjekt erstellen“
- | • „Objekt der Verbindungssicherheitskonfiguration auf der Basis eines anderen erstellen“
- | • „Konfigurationseigenschaften der Verbindungssicherheit anzeigen“ auf Seite 137
- | • „Konfigurationseigenschaften der Verbindungssicherheit ändern“ auf Seite 137
- | • „Verbindungssicherheitsobjekt löschen“ auf Seite 138

| **Verbindungssicherheitskonfigurationsobjekt erstellen**

| Ein Verbindungssicherheitskonfigurationsobjekt (NWSCFG-Subtyp CNNSEC) muss erstellt werden, das
| die Regeln der IP-Netzwerkssicherheit (IPsec) definiert, die für Speicherungs- und Virtual Ethernet-Datenfluss
| über das iSCSI-Netzwerk zwischen iSeries und xSeries oder IBM BladeCenter-Blade-Servern gelten.

| **Anmerkung:** Wenn die iSCSI-HBA-Hardware auf der iSeries-, xSeries- oder IBM BladeCenter-Seite der
| iSCSI-Verbindung IPsec nicht unterstützt, kann IPsec nicht verwendet werden, um einen
| sicheren Datenfluss über das iSCSI-Netzwerk zu gewährleisten. Wenn die iSCSI-HBA-Hard-
| ware IPsec nicht unterstützt, muss trotzdem ein Verbindungssicherheitsobjekt erstellt wer-
| den, es sollten aber nicht zu viele IP-Sicherheitsregeln definiert werden.

| Gehen Sie wie folgt vor, um mit iSeries Navigator eine Verbindungssicherheitskonfiguration zu erstellen:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Klicken Sie mit der rechten Maustaste auf **Verbindungssicherheit**.
- | 4. Wählen Sie **Neue Verbindungssicherheitskonfiguration** aus.
- | 5. Auf der Indexzunge **Allgemein**:
 - | • Geben Sie **Name** und **Beschreibung** ein.
 - | • Wählen Sie **Objektberechtigung** aus.
- | 6. Auf der Indexzunge **IP-Sicherheitsregeln**:
 - | • Wenn Ihre iSCSI-HBA-Hardware IPsec unterstützt, definieren Sie die IP-Sicherheitsregeln, die für
| den Speicherungs- und den Virtual Ethernet-Datenfluss über das iSCSI-Netzwerk gelten.
 - | • Sonst definieren Sie keine IP-Sicherheitsregeln.
- | 7. Klicken Sie auf **OK**.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter CRTNWSCFG oder
| WRKNWSCFG.

| **Objekt der Verbindungssicherheitskonfiguration auf der Basis eines anderen erstellen**

| Sie können ein Objekt einer bestehenden Konfiguration eines Verbindungssicherheitsobjekts für
| Netzwerkserver (NWSCFG-Subtyp CNNSEC) kopieren, wenn Sie ein neues Objekt erstellen. Dies spart
| Zeit, wenn einige der Attribute der neuen Verbindungssicherheitskonfiguration den existierenden Attribu-
| ten ähneln oder gleichen.

| Gehen Sie wie folgt vor, um mit iSeries Navigator eine neue Verbindungssicherheitskonfiguration auf der
| Basis einer bestehenden zu erstellen:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Verbindungssicherheit** aus.

- | 4. Klicken Sie mit der rechten Maustaste auf eine Verbindungssicherheitskonfiguration.
- | 5. Wählen Sie **Neu basierend auf...** aus.
- | 6. Geben Sie den **Namen** für die Verbindungssicherheitskonfiguration des fernen Systems ein.
- | 7. Geben Sie alle anderen Attribute an, die sich von den Attributen der kopierten Konfiguration unterscheiden sollen.
- | 8. Klicken Sie auf **OK**.

| **Anmerkung:** Für diese Task gibt es keinen äquivalenten CL-Befehl.

| **Konfigurationseigenschaften der Verbindungssicherheit anzeigen**

| Ein Verbindungssicherheitskonfigurationsobjekt (NWSCFG-Subtyp CNNSEC) enthält Regeln zur IP-Netzwerkssicherheit (IPSec), die für Speicherungs- und Virtual Ethernet-Datenfluss über das iSCSI-Netzwerk zwischen iSeries- und xSeries- oder IBM BladeCenter-Blade-Servern verwendet werden.

| Gehen Sie wie folgt vor, um mit iSeries Navigator die Attribute einer Verbindungssicherheitskonfiguration anzuzeigen:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Verbindungssicherheit** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf eine Verbindungssicherheitskonfiguration in der Liste.
- | 5. Wählen Sie **Eigenschaften** aus.
- | 6. Klicken Sie auf die Indexungen der Eigenschaften, die Sie anzeigen wollen.
- | 7. Klicken Sie auf **OK**, um die Anzeige zu schließen.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter DSPNWSCFG oder WRKNWSCFG.

| **Konfigurationseigenschaften der Verbindungssicherheit ändern**

| Ein Verbindungssicherheitskonfigurationsobjekt (NWSCFG-Subtyp CNNSEC) enthält Regeln zur IP-Netzwerkssicherheit (IPSec), die für Speicherungs- und Virtual Ethernet-Datenfluss über das iSCSI-Netzwerk zwischen iSeries- und xSeries- oder IBM BladeCenter-Blade-Servern verwendet werden.

| **Anmerkung:** Wenn die iSCSI-HBA-Hardware auf der iSeries- oder der BladeCenter-Seite der iSCSI-Verbindung IPSec nicht unterstützt, kann IPSec nicht verwendet werden, um einen sicheren Datenfluss über das iSCSI-Netzwerk zu gewährleisten. Wenn die iSCSI-HBA-Hardware IPSec nicht unterstützt, dann dürfen keine IP-Sicherheitsregeln definiert werden.

| Gehen Sie wie folgt vor, um mit iSeries Navigator die Attribute einer Verbindungssicherheitskonfiguration ändern:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Verbindungssicherheit** aus.
- | 4. **Klicken Sie mit der rechten Maustaste** auf eine Verbindungssicherheitskonfiguration in der Liste.
- | 5. Wählen Sie **Eigenschaften** aus.
- | 6. Klicken Sie auf die Indexungen der Eigenschaften, die Sie ändern wollen.
- | 7. Klicken Sie auf **OK**, um die Änderungen zu speichern.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter CHGNWSCFG oder WRKNWSCFG.

| **Verbindungssicherheitsobjekt löschen**

| Gehen Sie wie folgt vor, um mit iSeries Navigator ein Verbindungssicherheitsobjekt zu löschen:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Verbindungssicherheit** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf eine Verbindungssicherheitskonfiguration in der Liste.
- | 5. Wählen Sie **Löschen** aus.
- | 6. Klicken Sie in der Bestätigungsanzeige auf **Löschen**.

| Wenn Sie mit CL-Befehlen arbeiten wollen, finden Sie weitere Informationen unter DLTNWSCFG oder WRKNWSCFG.

| **Sicherheit zwischen i5/OS und Hosted Systemen konfigurieren**

| Um zu erfahren, welche der folgenden Sicherheitsmaßnahmen für Ihre Umgebung geeignet sind, siehe „Sicherheit für Systeme mit iSCSI-Anschluss“ auf Seite 51.

- | • „CHAP konfigurieren“
- | • „IPSec konfigurieren“ auf Seite 139
- | • „Serviceprozessor-SSL konfigurieren“ auf Seite 140
- | • „Serviceprozessorkennwort“ auf Seite 142
- | • „Firewall konfigurieren“ auf Seite 142

| **CHAP konfigurieren**

| **Anmerkung:** Sie müssen Sonderberechtigung als Sicherheitsadministrator (*SECADM) haben, um CHAP-Informationen zu erstellen, zu ändern oder anzuzeigen.

| Um CHAP zu konfigurieren oder die Berechtigungsnachweise zu ändern, gehen Sie wie folgt vor:

- | 1. Bei abgeschaltetem Server (NWSD ist abgehängt) verwenden Sie die unter „Konfigurationseigenschaften des fernen Systems ändern“ auf Seite 132 beschriebene Prozedur, um die Konfigurationseigenschaften des fernen Systems für den Server zu ändern. Klicken Sie auf die Indexzunge **CHAP-Authentifizierung**.
 - | • Um CHAP zu aktivieren, wählen Sie die Option **Folgende Werte für CHAP-Authentifizierung verwenden** aus, geben den **CHAP-Namen** ein und wählen dann die Option **Geheimen CHAP-Schlüssel einmal generieren** aus.
 - | • Um CHAP zu inaktivieren, wählen Sie die Option **CHAP nicht verwenden** aus.
- | 2. Verwenden Sie die unter „Konfigurationseigenschaften des fernen Systems anzeigen“ auf Seite 131 beschriebene Prozedur, um die Konfigurationseigenschaften des fernen Systems für den Server anzuzeigen.
 - | • Auf der Indexzunge **CHAP-Authentifizierung** geben Sie den **CHAP-Namen** und den **Geheimen CHAP-Schlüssel** ein.
 - | • Auf der Indexzunge **Bootparameter** geben Sie die Übergabemethode für Bootparameter ein,
- | 3. Dieser Schritt ist erforderlich, wenn die Übergabemethode des Bootparameters **Manuell auf fernem System konfiguriert** oder **Dynamisch über CHAP an fernes System übergeben** ist. Beim nächsten Start des Servers (NWSD anhängen) warten Sie, bis Sie auf der Konsole des Hosted Systems aufgefordert werden, STRG-Q zu drücken. Sobald Sie diese Eingabeaufforderung sehen, drücken Sie unverzüglich STRG-Q. Wählen Sie in dem mit STRG-Q aufgerufenen Dienstprogramm den Adapter aus, der für das Booten des Hosted OS konfiguriert ist. Geben Sie den CHAP-Namen und den geheimen Schlüssel für die Konfigurationseigenschaften des fernen Systems in die entsprechenden Felder der

Zielsicherheitskonfiguration des mit STRG-Q aufgerufenen Dienstprogramms ein. Geben Sie diese Informationen nicht auf der Initiator Konfigurationsanzeige des mit STRG-Q aufgerufenen Dienstprogramms ein.

Anmerkung: Alle nicht gebooteten iSCSI-HBAs im Hosted System werden automatisch von der i5/OS-Konfiguration konfiguriert.

IPSec konfigurieren

Anmerkung: Ein iSCSI-HBA für iSeries mit IPSec-Unterstützung ist erforderlich, wenn IPSec für den sicheren Datenfluss über das iSCSI-Netzwerk verwendet werden soll. Wenn die iSCSI-HBA-Hardware IPSec nicht unterstützt, muss trotzdem ein Verbindungssicherheitsobjekt erstellt werden, es sollten aber keine IP-Sicherheitsregeln definiert werden.

Um IPSec zu konfigurieren oder die IPSec-Berechtigungsanweisung zu ändern, gehen Sie wie folgt vor:

1. Dieser Schritt ist erforderlich, wenn Sie den ersten vorab bekannten gemeinsamen Schlüssel noch nicht generiert haben. Sie können diesen Schritt auch zu jeder anderen Zeit ausführen, um den vorab bekannten gemeinsamen Schlüssel zu ändern. Bei abgeschaltetem Server (NWSD ist abgehängt) gehen Sie wie unter „Konfigurationseigenschaften der Verbindungssicherheit ändern“ auf Seite 137 beschrieben vor, um die Eigenschaften der Verbindungssicherheitskonfiguration für den Server zu ändern.
 - Klicken Sie auf die Indexzunge **IP-Sicherheitsregeln**.
 - Klicken Sie auf die Schaltfläche **Hinzufügen**, und wählen Sie die Option **Vorab bekannten gemeinsamen Schlüssel generieren** aus.
 - Klicken Sie auf **OK**, um der Tabelle die neue IP-Sicherheitsregel hinzuzufügen. Klicken Sie erneut auf **OK**, um die Verbindungssicherheitskonfiguration zu sichern und den vorab bekannten gemeinsamen Schlüssel zu generieren.

Anmerkung: Sie müssen Sonderberechtigung als Sicherheitsadministrator (*SECADM) haben, um den vorab bekannten gemeinsamen Schlüssel zu erstellen, zu ändern oder anzuzeigen.

2. Verwenden Sie die unter „Konfigurationseigenschaften der Verbindungssicherheit anzeigen“ auf Seite 137 beschriebene Prozedur, um die Konfigurationseigenschaften der Verbindungssicherheit für den Server anzuzeigen.
 - Klicken Sie auf die Indexzunge **IP-Sicherheitsregeln**.
 - Die erste Zeile der Tabelle enthält einen zufällig von i5/OS generierten vorab bekannten gemeinsamen Schlüssel. Diese Informationen werden in Schritt 5 auf Seite 140 verwendet.
3. Mit iSeries Navigator:
 - Wählen Sie **Verwaltung integrierter Server -> Server** aus.
 - Klicken Sie mit der rechten Maustaste auf den integrierten Server, und wählen Sie die Option **Eigenschaften** aus.
 - Klicken Sie auf die Indexzunge **iSCSI-Sicherheit**.
 - Für die **Standard-IP-Sicherheitsregel** wählen Sie **1** und dann **OK** aus, um die Änderung zu speichern. Sie bewirkt, dass i5/OS Folgendes durchführt: Wenn ein **Standardwert** für die IP-Sicherheitsregel in den Servereigenschaften erscheint, wird der erste Wert in der Verbindungssicherheitskonfiguration verwendet (es ist der Wert **Verbindungssicherheitskonfiguration** in der Indexzunge **iSCSI-Sicherheit** der Servereigenschaften).
4. Dieser Schritt ist nur erforderlich, wenn IPSec nicht auf allen NWSD-Verbindungen des Servers aktiviert sein soll, oder wenn Regeln für ferne Schnittstellen geändert wurden und nicht mehr der Standardwert verwendet wird.

Mit iSeries Navigator:

 - Wählen Sie **Verwaltung integrierter Server -> Server** aus.

- Klicken Sie mit der rechten Maustaste auf den integrierten Server, und wählen Sie die Option **Eigenschaften** aus.
- Klicken Sie auf die Indexzunge **Speicherpfade**.
- Jede **IP-Sicherheitsregel für ferne Schnittstelle** entspricht einem iSCSI-HBA-Paar bestehend aus iSeries-Port und iSCSI-HBA-Port auf dem Hosted System.
Wiederholen Sie die folgenden Schritte für alle **IP-Sicherheitsregel für ferne Schnittstelle**-Spalten in den Indexzungen **Speicherpfade** und **Virtual Ethernet-Pfade**.

Anmerkung: Jeder NWSH, der mehr als einmal in einer NWS-Beschreibung verwendet wird, muss identische Gruppen von IP-Sicherheitsregeln für die ferne Schnittstelle in jedem der Speicherungs- oder Virtual Ethernet-Pfade aufweisen, die darauf verweisen.

Definieren Sie jede IP-Sicherheitsregel für ferne Schnittstellen als "Kein" oder "Standard", je nachdem, welche Angabe für das zu verwendende iSCSI-HBA-Portpaar verwendet werden soll:

- Wählen Sie **Kein** aus, wenn der Datenaustausch über das Netz zwischen den iSCSI-HBA-Ports erfolgen soll, ohne Rücksicht darauf, ob die iSCSI-HBAs IPSec unterstützen.
- Verwenden Sie **Standard**, wenn der entsprechende iSCSI-HBA für iSeries IPSec unterstützt und Sie nur verschlüsselten Datenverkehr erlauben wollen (bzw. gar keinen Datenverkehr, wenn der iSCSI-HBA-Port des Hosted Systems IPSec nicht unterstützt).

5. Dieser Schritt ist nur erforderlich, wenn die Übergabemethode in der Konfiguration des fernen Systems **Manuell auf fernem System konfiguriert** oder **Dynamisch über CHAP an fernes System übergeben** ist: Beim nächsten Start des Servers (NWSD anhängen) warten Sie, bis Sie auf der Konsole des Hosted Systems aufgefordert werden, STRG+Q zu drücken. Sobald Sie diese Eingabeaufforderung sehen, drücken Sie unverzüglich STRG-Q. Wählen Sie in dem mit STRG-Q aufgerufenen Dienstprogramm den Adapter aus, der für das Booten des OS konfiguriert ist. Geben Sie den vorab bekannten gemeinsamen Schlüssel aus den Konfigurationseigenschaften der Verbindungssicherheit in die Anzeige ein. „Booten über iSCSI ohne Plattenspeicher“ auf Seite 23 enthält weitere Informationen zu dem mit STRG-Q aufgerufenen Dienstprogramm.

Anmerkung: Alle nicht gebooteten iSCSI-HBAs im Hosted System werden automatisch von der i5/OS-Konfiguration konfiguriert.

Serviceprozessor-SSL konfigurieren

SSL und das Kennwort des Serviceprozessors schützen gemeinsam den Systemmanagementdatenverkehr zwischen einem LAN-Adapter eines iSeries-Systems und dem Serviceprozessor des Hosted Systems.

Um die SSL-Verbindung des Serviceprozessors zu initialisieren, können Sie die folgenden Methoden verwenden.

- „Automatische SSL-Initialisierung“
- „Manuelle SSL-Initialisierung“ auf Seite 141

Weitere Informationen zum Serviceprozessorkennwort finden Sie unter „Serviceprozessorkennwort“ auf Seite 142.

Automatische SSL-Initialisierung

Um SSL automatisch zu initialisieren, führen Sie die folgenden Schritte durch:

1. Wenn die Verbindung zwischen Serviceprozessor und iSeries über ein gemeinsam genutztes Netzwerk erfolgt, kann es sinnvoll sein, den Serviceprozessor und iSeries temporär über ein isoliertes Netz zu verbinden. Wenn Sie dies nicht tun, ist die automatische Methode in der kurzen Zeit geringfügig unsicherer als die manuelle Methode, die für die Initialisierungstask in Schritt 3 auf Seite 141 benötigt wird.
2. Verwenden Sie die unter „Konfigurationseigenschaften des Serviceprozessors ändern“ auf Seite 134 beschriebene Prozedur, um die Eigenschaften der Serviceprozessorkonfiguration für den Server zu

ändern. Wählen Sie auf der Indexzunge **Sicherheit** die Option **Benutzer automatisch konfigurieren und Zertifikat generieren** aus. Klicken Sie auf OK, um die Änderung zu speichern.

3. Verwenden Sie die unter „Serviceprozessor initialisieren“ auf Seite 135 beschriebene Prozedur, um den Serviceprozessor zu initialisieren.

- a. Wählen Sie die Option **Neuen Serviceprozessor angeben** aus.

Anmerkung: Verwenden Sie die Option **Zertifikat von Serviceprozessor synchronisieren**, wenn dies eine zusätzliche Konfiguration für den gleichen Serviceprozessor ist, der bereits für den Einsatz mit einem anderen integrierten Server initialisiert wurde.

- b. Geben Sie die Werte für **Benutzer** und **Kennwort** ein.


- c. Klicken Sie auf **Initialisieren**, um die Operation auszuführen.

Anmerkung: Der Serviceprozessor generiert automatisch ein selbst signiertes Zertifikat, das von i5/OS gespeichert wird. Das Zertifikat wird im Integrated File System-Verzeichnis /QIBM/UserData/Director/classes/com/ibm/sysmgmt/app/iide/ unter einem Dateinamen gespeichert, der dem Namen der Serviceprozessorkonfiguration entspricht. Die Erweiterung dieser Datei ist 'kdb'.

Manuelle SSL-Initialisierung

Um SSL manuell mit einem von einer anerkannten Zertifizierungsstelle unterzeichneten Zertifikat zu initialisieren, gehen Sie wie folgt vor:

1. Verwenden Sie die Webschnittstelle des Serviceprozessors, um ein SSL-Zertifikat von einer anerkannten Zertifizierungsstelle anzufordern. Für eine detaillierte Beschreibung der Prozedur klicken Sie auf den Link IBM Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's

Guide  (www.ibm.com/pc/support/site.wss/). Wählen Sie unter **Browse** die Optionen **Servers**, **Family: xSeries 236**, **Publications** aus.

Anmerkung: Das Zertifikat für die Zertifizierungsstelle muss sich im i5/OS *SYSTEM-Zertifikatsspeicher befinden.

2. Wenn Sie das neue Zertifikat von der Zertifizierungsstelle erhalten, verwenden Sie die Webschnittstelle des Serviceprozessors, um es in den Serviceprozessor zu importieren.

3. Verwenden Sie die unter „Konfigurationseigenschaften des Serviceprozessors ändern“ auf Seite 134 beschriebene Prozedur, um die Eigenschaften der Serviceprozessorkonfiguration für den Server zu ändern. Klicken Sie auf die Indexzunge **Sicherheit** und führen Sie die folgenden Schritte aus:

- a. Wählen Sie **Benutzer und Zertifikat manuell konfigurieren** aus.

- b. Bei **Komponente** wählen Sie entweder **Allgemeiner Name**, **E-Mail-Adresse** oder **Organisationseinheit** aus.

- c. Geben Sie als **Vergleichswert** die entsprechenden Informationen aus dem Zertifikat ein. So kann SSL zwischen Ihren Zertifikaten und Fremdzertifikaten im i5/OS-Zertifikatsspeicher *SYSTEM unterscheiden, die von vertrauenswürdigen Zertifikatsstellen unterzeichnet sind. Sie können z. B. die E-Mail-Adresse angeben, in der Sie ein Zertifikat von einer anerkannten Zertifizierungsstelle empfangen haben.

- d. Klicken Sie auf **OK**, um die Änderung zu speichern.

4. Ändern Sie das Kennwort und beenden Sie die Initialisierung. Weitere Informationen finden Sie unter „Serviceprozessorkennwort“ auf Seite 142.

Um SSL zu inaktivieren, wählen Sie die Option **Kein Zertifikat verwenden (physische Sicherheit erforderlich)** aus.

Serviceprozessorkennwort

Um das Serviceprozessorkennwort zu ändern, gehen Sie wie unter „Serviceprozessor initialisieren“ auf Seite 135 beschrieben vor.

1. Wählen Sie die Option **Benutzer-ID und Kennwort des Serviceprozessors ändern** aus.
2. Geben Sie den neuen Werte für **Benutzer, Kennwort und Neue Kennwortwerte bestätigen** ein.
3. Klicken Sie auf **Initialisieren**, um die Operation auszuführen.

Firewall konfigurieren

Wenn zwischen dem iSeries und dem iSCSI-Netzwerk eine Firewall vorhanden ist, muss sie so konfiguriert werden, dass ankommender iSCSI- und Virtual Ethernet-Datenverkehr zugelassen ist. Die u. a. Werte beeinflussen die Firewallkonfiguration.

Für Speicherpfade und Virtual Ethernet-Verbindungen, die durch die Firewall geschützt werden:

- **Ferne IP-Adresse:** Verwenden Sie die unter „Konfigurationseigenschaften des fernen Systems anzeigen“ auf Seite 131 beschriebene Prozedur, um die Konfigurationseigenschaften des fernen Systems für den Server anzuzeigen. Klicken Sie auf die Indexzunge **Netzwerkschnittstelle** und notieren Sie die Werte für **SCSI-Internetadresse** und **LAN-Internetadresse**.
- **Lokale IP-Adresse und TCP-Port:** Verwenden Sie die unter „Eigenschaften des NWS-Hostadapters anzeigen“ auf Seite 128 beschriebene Prozedur, um die Eigenschaften des NWS-Hostadapters anzuzeigen. Klicken Sie auf die Indexzunge **lokale Schnittstelle**, um die Informationen anzuzeigen, die der NWSH verwendet. Erfassen Sie die folgenden Werte:
 - Lokale SCSI-Interface: Internetadresse
 - Lokale SCSI-Schnittstelle: TCP-Port
 - Lokale LAN-Schnittstelle: Internetadresse
 - Lokale LAN-Schnittstelle: Unterer Virtual Ethernet-Port
 - Lokale LAN-Schnittstelle: Oberer Virtual Ethernet-Port

Anmerkung: Virtual Ethernet-Datenverkehr ist in UDP-Pakete eingebunden. Jedem Virtual Ethernet-Adapter wird automatisch ein UDP-Port aus einem Bereich zugeordnet, der mit der unteren Virtual Ethernet-Portnummer beginnt und an der oberen Nummer plus der Anzahl an konfigurierten Virtual Ethernet-Adaptoren endet. Jeder Virtual Ethernet-Adapter hat auch auf dem Windows-Server einen zugeordneten UDP-Port. UDP-Ports für Virtual Ethernet werden von Windows normalerweise automatisch zugeordnet. Wenn Sie die automatische Zuordnung außer Kraft setzen wollen, können Sie manuell einen UDP-Port zuordnen. Führen Sie an der Windows-Konsole folgende Schritte aus:

1. Navigieren Sie zum Fenster **Netzverbindungen**.
2. Doppelklicken Sie auf den **IBM iSeries Virtual Ethernet x-Adapter**, den Sie konfigurieren möchten.
3. Klicken Sie auf **Eigenschaften**.
4. Klicken Sie auf **Konfigurieren**.
5. Klicken Sie auf **Erweitert**.
6. Klicken Sie auf **Initiator-LAN-UDP-Port**.
7. Geben Sie den UDP-Port an, den der Virtual Ethernet-Adapter verwenden soll.

- **TCP-Ports, die allen lokalen IP-Adressen zugeordnet sind:**

Mit iSeries Navigator:

1. Erweitern Sie **Verwaltung integrierter Server**.
2. Wählen Sie **Server** aus.
3. Klicken Sie mit der rechten Maustaste auf den gewünschte Server in der Liste und wählen Sie **Eigenschaften** aus.

4. Klicken Sie auf die Indexzunge **System** und dann auf die Schaltfläche **Erweitern**.
5. Notieren Sie die folgenden Werte:
 - **TCP-Port für Systemabschluss**
 - **Virtual Ethernet-Steuerport**

Wenn mit IPSec gearbeitet wird, müssen weitere Dinge für die Firewalls zwischen iSCSI-HBA und iSCSI-Netzwerk berücksichtigt werden:

- **IPSec zulassen:** Diese Option steht nicht bei allen Firewalls zur Verfügung.
- Es sollten nur IP-Adressen verwendet werden, wenn Firewalls konfiguriert werden. TCP- und UDP-Ports werden von IPSec verschlüsselt; die Firewall kann daher diese Daten nicht verwenden.

iSCSI-Hostbusadapter verwalten

Gehen Sie wie folgt vor, um iSCSI-Hostadapter (NWSHs) zu verwalten.

- „Hot-Spare zwischen lokalen iSCSI-Hostadaptern“
- „iSCSI-HBA-Nutzung verwalten“ auf Seite 144
- „Überlegungen zur größten zu übertragenden Einheit (MTU)“ auf Seite 147
- „Integrierter DHCP-Server“ auf Seite 149

Hot-Spare zwischen lokalen iSCSI-Hostadaptern

Die Hardware der lokalen iSeries iSCSI-Hostadapter bietet Hot-Spare-Funktionalität, um die Zuverlässigkeit und die Wiederherstellbarkeit von Windows-Serverumgebungen zu verbessern. Wenn der lokale SCSI-Hostadapter fehlschlägt, den ein Windows-Server benutzt, können Sie den Server schnell auf einen anderen lokalen iSCSI-Hostadapter umschalten, den so genannten Hot-Spares. Die Hot-Spare-Unterstützung erhöht außerdem die Flexibilität, da ein Ersatzserver für den lokalen iSCSI-Hostadapter aktiviert wird, der zum Schutz mehrerer lokaler iSCSI-Hostadapter für die Produktion eingesetzt wird.

Anmerkung: Die Hot-Spare-Funktion des lokalen iSCSI-Hostadapters komplettiert die Hot-Spare-Funktionalität, die bei integrierter Server-Hardware zur Verfügung steht. Weitere Informationen finden Sie unter „Hot-Spare zwischen Server-Hardware“ auf Seite 166.

Um lokale iSCSI-Hostadapterhardware mit iSeries Navigator als Hot-Spare zu nutzen, gehen Sie wie folgt vor:

1. Erweitern Sie **Verwaltung integrierter Server**.
2. Erweitern Sie **iSCSI-Verbindungen**.
3. Wählen Sie **Lokale Hostadapter** aus.
4. Wenn der NWS-Hostadapter, für den Sie die Hardware umschalten wollen, noch nicht gestoppt ist:
 - Klicken Sie mit der rechten Maustaste auf den NWS-Hostadapter, und wählen Sie **Stoppen** aus.
 - Klicken Sie auf der Bestätigungsanzeige auf **Stoppen**.
 - Wenn die aktiven Server gerade den NWSH verwenden, wird eine Warnung angezeigt. Klicken Sie auf **Weiter**.
5. Um den NWS-Hostadapter so zu ändern, dass er auf den Hot-Spare-Adapter des lokalen iSCSI-Hosts zeigt:
 - Klicken Sie mit der rechten Maustaste auf den NWS-Hostadapter, und wählen Sie **Eigenschaften** aus.
 - Klicken Sie auf die Indexzunge **Allgemein**, und wählen Sie einen neuen Wert für die Eingabeaufforderung **Hardwareressource** aus.
 - Klicken Sie auf **OK**.
6. Um den NWS-Hostadapter zu starten, klicken Sie mit der rechten Maustaste auf ihn und wählen dann **Starten** aus.

| Sie können auch den Befehl VRYCFG verwenden, um den NWS-Hostadapter zu beenden. Mit dem CL-Befehl zum Ändern der Einheitenbeschreibung (NWSH) (CHGDEVNWSH) ändern Sie den Wert des Ressourcennamenparameters (RSRCNAME) so, dass er jetzt den Namen der neuen Hardwareressource angibt.

| **iSCSI-HBA-Nutzung verwalten**

| Sie können mehrere Hosted Systeme (xSeries-System oder IBM BladeCenter-Blades) an iSeries über einen einzigen iSeries-iSCSI-Hostbusadapter (iSCSI-HBA) anhängen. Sie können auch ein einzelnes Hosted System an iSeries anhängen und dabei mehrere iSCSI-HBAs für iSeries verwenden. Es gibt verschiedene Möglichkeiten, ein Hosted System so zu konfigurieren, dass es mehr als einen iSCSI-HBA für iSeries verwendet. Auch Kombinationen dieser Verfahren können verwendet werden.

| Weitere Informationen über einige allgemeine Konfigurationen enthalten die folgenden Abschnitte:

- | • „Einen iSCSI-HBA mit mehreren Hosted Servern gemeinsam benutzen“
- | • „Workload über mehrere iSCSI-HBAs verteilen“ auf Seite 145
- | • „Mehrere iSCSI-HBAs für Redundanz verwenden“ auf Seite 146
- | • „iSCSI-HBA-Zuordnung auf der Windows-Seite des iSCSI-Netzwerks verwalten“ auf Seite 147

| **Einen iSCSI-HBA mit mehreren Hosted Servern gemeinsam benutzen**

| Ein einzelner iSCSI-HBA für iSeries kann die Workload mehrerer Server bearbeiten, die für den LAN-Verkehr über SCSI und das Virtual Ethernet keine große Bandbreite benötigen. So kann z. B. ein iSCSI-HBA für iSeries von mehreren Entwicklungs- und Testservern gemeinsam genutzt werden, wenn deren Workload nicht sehr hoch ist.

| Die Anzahl der Speicher- und Virtual Ethernet-Pfade, die ein iSCSI-HBA unterstützen kann, ist begrenzt. Jeder aktive Serverspeicherpfad arbeitet mit einer Dateiserverressource im NWS-Hostadapterobjekt, das dem iSCSI-HBA entspricht. Genauso verwendet jeder Virtual Ethernet-Pfad eine Virtual Ethernet-Ressource im NWS-Hostadapterobjekt. Die Anzahl der Dateiserver- und Virtual Ethernet-Ressourcen, die ein NWS-Hostadapter unterstützen kann, ist begrenzt.

| Um mit dem iSeries Navigator den Grenzwert für die Dateiserver- und Ethernet-Ressourcenverwendung anzuzeigen, führen Sie die folgenden Schritte durch:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **iSCSI-Verbindungen**.
- | 3. Wählen Sie **Lokale Hostadapter** aus.
- | 4. Klicken Sie mit der rechten Maustaste auf einen NWS-Hostadapter in der Liste.
- | 5. Wählen Sie **Eigenschaften** aus.
- | 6. Klicken Sie auf die Indexzunge **Ressourcennutzung**.
- | 7. Die Tabelle zeigt die aktiven Server, die momentan den NWS-Hostadapter nutzen, und die Dateiserver- und Virtual Ethernet-Ressourcen, auf die sie gerade zugreifen. Unter der Tabelle ist angezeigt, wie viele Dateiserver- und Virtual Ethernet-Ressourcen noch zur Nutzung durch inaktive Server verfügbar sind und wie viele Dateiserver- und Virtual Ethernet-Ressourcen der NWS-Hostadapter unterstützt.
- | 8. Klicken Sie auf der Anzeige mit den Eigenschaften für den NWS-Hostadapter auf **Abbrechen**, um die Anzeige zu schließen.

| Wenn Sie einen CL-Befehl verwenden möchten, finden Sie weitere Informationen unter WRKDEVD oder DSPDEVD.

| Es gibt auch eine praktische Grenze für die Anzahl der Server, die ein iSCSI-HBA unterstützen kann. Sie wird durch die verfügbare Bandbreite des iSCSI-HBA und der Workload festgelegt, die durch den iSCSI-HBA läuft. Diese praktische Begrenzung liegt in den meisten Fällen unter der Anzahl der Hosted Sys-

teme, die der iSCSI-HBA unterstützen kann, bevor die oben beschriebenen Grenzen für Dateiserver- und Virtual Ethernet-Ressourcen erreicht werden. Die praktische Begrenzung hängt von der jeweiligen Serverkonfiguration und der Workload ab.

Workload über mehrere iSCSI-HBAs verteilen

Server, die eine hohe Bandbreite erfordern, benötigen evtl. mehr als einen iSCSI-HBA für iSeries, um die Workload abzuwickeln. Sie können dies noch detaillierter identifizieren, indem Sie feststellen, welche virtuellen Platten oder Virtual Ethernet-LANs hohe Bandbreite erfordern und welche nicht. Sie können z. B. einen iSCSI-HBA einem Datenträger zuordnen, der eine hohe Bandbreite benötigt, und einen anderen iSCSI-HBA für den Einsatz mit Datenträgern oder Servern einplanen, die keine hohe Bandbreite erfordern.

Um die Workload eines Servers bezüglich SCSI und Virtual Ethernet auf mehrere iSCSI-HBAs zu verteilen, definieren Sie mehrere Speicher- oder Virtual Ethernet-Pfade in der NWS-Beschreibung (NWS), und geben Sie an, welche virtuelle Platte und welches Virtual Ethernet die einzelnen Pfade benutzen.

Um mit iSeries Navigator zusätzliche Speicherpfade zu definieren, beenden Sie zunächst den Server (siehe „Integrierten Server starten und stoppen“ auf Seite 157); führen Sie dann die folgenden Schritte durch:

1. Erweitern Sie **Verwaltung integrierter Server**.
2. Erweitern Sie **Server**.
3. Klicken Sie mit der rechten Maustaste auf einen Server in der Liste.
4. Wählen Sie **Eigenschaften** aus.
5. Klicken Sie auf die Indexzunge **Speicherpfade**.
6. Klicken Sie auf die Schaltfläche **Hinzufügen**, um einen neuen Speicherpfad zu definieren.
7. Wählen Sie den NWS-Hostadapter aus, der dem iSCSI-HBA entspricht, der für den Speicherpfad verwendet werden soll.
8. Klicken Sie auf **OK**, um den Speicherpfad auf der Anzeige der Servereigenschaften hinzuzufügen.
9. Notieren Sie die Pfadnummer, die dem neuen Pfad zugeordnet wird. Diese Nummer wird verwendet, um diesen Pfad zu identifizieren, wenn später Platten verknüpft werden.
10. Klicken Sie auf der Anzeige der Servereigenschaften auf **OK**, um den neuen Speicherpfad in der NWS-Beschreibung (NWS) zu speichern.

Wenn Sie einen CL-Befehl verwenden möchten, finden Sie weitere Informationen unter dem Stichwort STGPTR des Befehls CHGNWS.

Nachdem der neue Speicherpfad jetzt definiert ist, müssen Sie die virtuelle Platte(n) des Servers erneut verbinden, damit der neue Speicherpfad genutzt werden kann. Heben Sie zunächst die Verbindung zur Platte auf (siehe „Verbindung von Plattenlaufwerken für integrierten Windows-Server aufheben“ auf Seite 177). Hängen Sie die Platte dann wieder am Server an (siehe „Plattenlaufwerk mit einem integrierten Server verbinden“ auf Seite 173). Verwenden Sie die neue Speicherpfadnummer.

Um mit iSeries Navigator zusätzliche Virtual Ethernet-Pfade zu definieren, beenden Sie zunächst den Server (siehe „Integrierten Server starten und stoppen“ auf Seite 157); führen Sie dann die folgenden Schritte durch:

1. Erweitern Sie **Verwaltung integrierter Server**.
2. Erweitern Sie **Server**.
3. Klicken Sie mit der rechten Maustaste auf einen Server in der Liste.
4. Wählen Sie **Eigenschaften** aus.
5. Klicken Sie auf die Indexzunge **Virtual Ethernets**.
6. Wählen Sie den Virtual Ethernet-Port aus, für den der Pfad verwendet werden soll, und klicken Sie dann auf die Schaltfläche **Eigenschaften**.

- | 7. Wählen Sie den NWS-Hostadapter, der für den Virtual Ethernet-Port verwendet werden soll.
- | 8. Klicken Sie auf **OK**, um die Informationen des Virtual Ethernet-Ports über die Anzeige mit den Servereigenschaften zu aktualisieren. Der Virtual Ethernet-Pfad für den Port wird dadurch implizit ebenfalls aktualisiert.
- | 9. Klicken Sie auf der Anzeige der Servereigenschaften auf **OK**, um die Änderungen in der NWS-Beschreibung (NWS) zu speichern.

| Wenn Sie einen CL-Befehl verwenden möchten, finden Sie weitere Informationen unter dem Stichwort VRTETHPTH des Befehls CHGNWSD.

| **Mehrere iSCSI-HBAs für Redundanz verwenden**

| Auch wenn die Bandbreitenanforderungen für einen Server nicht darauf schließen lassen, dass mehr als ein iSCSI-HBA für iSeries erforderlich ist, können Sie mehrere iSCSI-HBAs verwenden, um Fehlertoleranz und Redundanz bereitzustellen. Dadurch wird die Wahrscheinlichkeit von Systemausfällen reduziert, die auf den Ausfall des iSCSI-HBA oder einer der Netzkomponenten (z. B. Switches, Kabel etc.) zurückzuführen sind, die den iSeries mit dem Hosted System verbinden. Redundanz bietet iSCSI die Möglichkeit, E/A über mehrere Pfade (Multipath-E/A) durchzuführen (siehe „Erweiterte iSCSI-Unterstützung“ auf Seite 22). Um die Multipath-E/A nutzen zu können, erstellen Sie eine Multipath-Gruppe, die mindestens zwei iSCSI-HBAs identifiziert. Danach legen Sie fest, welche virtuellen Platten die Multipath-Gruppe verwenden sollen. Sie können außerdem die Multipath-Gruppe als Standardpfad für Verbindungen zu Plattenlaufwerken verwenden.

| Um mit iSeries Navigator eine Multipath-Gruppe zu definieren, beenden Sie zunächst den Server (siehe „Integrierten Server starten und stoppen“ auf Seite 157), und führen Sie dann die folgenden Schritte durch:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **Server**.
- | 3. Klicken Sie mit der rechten Maustaste auf einen Server in der Liste.
- | 4. Wählen Sie **Eigenschaften** aus.
- | 5. Klicken Sie auf die Indexzunge **Speicherpfade**.
- | 6. Definieren Sie mindestens zwei Speicherpfade (falls erforderlich, mit der Schaltfläche **Hinzufügen**).
- | 7. Unter der Tabelle mit den Speicherpfaden klicken Sie auf die Schaltfläche **Eigenschaften**.
- | 8. Verwenden Sie die Markierungsfelder, um zwei oder mehr der definierten Speicherpfade für Elemente der Multipath-Gruppe zu identifizieren.
- | 9. Klicken Sie auf **OK**, um die Informationen der Multipath-Gruppe auf der Anzeige mit den Servereigenschaften zu aktualisieren.
- | 10. **Optional:** Wählen Sie die Multipath-Gruppe als Standardpfad für alle Plattenlaufwerke aus.
- | 11. Klicken Sie auf der Anzeige der Servereigenschaften auf **OK**, um die Änderungen in der NWS-Beschreibung (NWS) zu speichern.

| Wenn Sie einen CL-Befehl verwenden möchten, finden Sie weitere Informationen unter den Stichwörtern MLTPHGRP und DFTSTGPTH des Befehls CHGNWSD.

| Nachdem die neue Multipath-Gruppe jetzt definiert ist, müssen Sie die virtuelle Platte(n) des Servers erneut verbinden, damit die neue Multipath-Gruppe genutzt werden kann. Heben Sie zunächst die Verbindung zur Platte auf (siehe „Verbindung von Plattenlaufwerken für integrierten Windows-Server aufheben“ auf Seite 177). Verbinden Sie die Platte wieder mit dem Server (siehe „Plattenlaufwerk mit einem integrierten Server verbinden“ auf Seite 173); geben Sie die Multipath-Gruppe entweder explizit an oder verwenden Sie den Standardpfad (wenn er für die Plattenlaufwerke als Multipath-Gruppe definiert wurde).

| **iSCSI-HBA-Zuordnung auf der Windows-Seite des iSCSI-Netzwerks verwalten**

| Ein Windows-Server kann mehrere physische Ports mit iSCSI-HBA- Ports haben. Über den iSCSI-HBA-Port kann Datenverkehr für iSeries-Speicherpfade und/oder Virtual Ethernet-Netzwerke laufen. Mehrere Faktoren beeinflussen den Datenverkehr, der durch jeden iSCSI-HBA-Port auf dem Windows-Server fließt.

| **IP-Adressen**

| iSCSI-HBA-Ports können eine SCSI-IP-Adresse und/oder eine LAN-Adresse haben. Ein Port mit einer SCSI-IP-Adresse ist ein Kandidat für die Übertragung von Speicherdatenverkehr. Ein Port mit einer LAN-IP-Adresse ist ein Kandidat für die Übertragung von Virtual Ethernet-Datenverkehr.

| **Speicherkonfiguration booten**

| Wählen Sie in dem mit STRG-Q aufgerufenen Dienstprogramm den iSCSI-HBA-Port aus, mit dem Windows gebootet wird. Nachdem Windows gebootet ist, stellt der ausgewählte iSCSI-HBA-Port weiter eine Verbindung zu dem iSeries-Speicherpfad zur Verfügung, der dem Systemlaufwerk entspricht.

| **iSCSI-HBA-Ports automatisch Virtual Ethernet- und Non-Boot-Speicherpfaden zuordnen**

| Die Windows-Umgebung auf iSeries schließt Programme ein, die unter Windows ausgeführt werden und automatisch die i5/OS-Objekte mit Serverkonfigurationsdaten lesen. Die iSCSI-HBAs für iSeries sind in den i5/OS-Objekten konfiguriert, aber die iSCSI-HBA-Ports für das Hosted System nicht. Stattdessen ordnet Programm die iSCSI-HBA-Ports automatisch den Virtual Ethernet- und Non-Boot-Speicherpfaden zu.

| **Virtual Ethernet-Adapter einem physischen iSCSI-HBA-Port manuell zuordnen**

| Wenn Sie die automatische Zuordnung außer Kraft setzen wollen, können Sie manuell einen iSCSI-HBA-Port zuordnen. Führen Sie an der Windows-Konsole folgende Schritte aus:

- | 1. Navigieren Sie zum Fenster **Netzverbindungen**.
- | 2. Doppelklicken Sie auf den **IBM iSeries Virtual Ethernet x-Adapter**, den Sie konfigurieren möchten.
- | 3. Klicken Sie auf **Eigenschaften**.
- | 4. Klicken Sie auf **Konfigurieren**.
- | 5. Klicken Sie auf **Erweitert**.
- | 6. Klicken Sie auf **Initiator LAN IP Address**.
- | 7. Geben Sie die IP-Adresse des iSCSI-HBA-Ports in Windows ein, den der Virtual Ethernet-Adapter für die physische Verbindung verwenden soll.

| **Überlegungen zur größten zu übertragenden Einheit (MTU)**

| **Anmerkung:** Die hier besprochenen Rahmengrößen schließen den 14 Byte großen MAC-Header (Ethernet) nicht ein.

| Anders als die 9000 Byte großen Jumbo-Rahmen (in an IXS und IXA angehängten Servern) hat das Virtual Ethernet bei Systemen, die an iSCSI-Netzwerken angeschlossen sind, standardmäßig kleinere Rahmen (Frames), die mit Ethernet-Standardframes (1500 Byte) transportiert werden können.

| Wenn das iSCSI-Netzwerk größere Rahmen verarbeiten kann, können Sie das Virtual Ethernet so konfigurieren, dass Rahmengrößen von bis zu 9000 Byte möglich sind; dies verbessert den Durchsatz. In einem komplexen iSCSI-Netzwerk können gemischte, maximale Rahmengrößen vorhanden sein, je nach Netztopologie und verwendeten Komponenten.

| **Anmerkung:** Die MTU-Eingabeaufforderungen im Befehl INSWNTSVR (Windows-Server installieren)
| haben keine Wirkung, außer bei LAN-Adaptern, die auf IES verwendet werden.

| Weitere Informationen zur MTU-Konfiguration enthalten die folgenden Themen:

- | • „Virtual Ethernet für maximale Leistung auf iSCSI-Netzwerken konfigurieren, die Rahmen über 1500 Byte unterstützen“
- | • „Virtual Ethernet für iSCSI-Netzwerk konfigurieren, deren maximale Rahmengröße geringer als 1500 Byte ist“
- | • „Virtual Ethernet so konfigurieren, dass ungewöhnliche Nicht-TCP-Anwendungen unterstützt werden, die keine MTU vereinbaren“ auf Seite 149

| **Virtual Ethernet für maximale Leistung auf iSCSI-Netzwerken konfigurieren, die Rahmen über 1500 Byte unterstützen**

| Führen Sie an der Windows-Konsole folgende Schritte durch:

- | 1. Navigieren Sie zum Fenster **Netzverbindungen**.
- | 2. Doppelklicken Sie auf den iSCSI-Adapter, der mit dem iSCSI-Netz verbunden ist und Rahmen über 1500 Byte unterstützt.
- | 3. Klicken Sie auf **Eigenschaften**.
- | 4. Klicken Sie auf **Konfigurieren**.
- | 5. Klicken Sie auf **Erweitert**.
- | 6. Klicken Sie auf **Ethernet Frame Size**.
- | 7. Wählen Sie einen Wert aus, der so groß wie möglich ist, ohne die max. Rahmengröße des iSCSI-Netzwerks zu übersteigen.

| **Anmerkung:** Zusammengehörige Konfigurationselement in der folgenden Liste sollte ihre Standardwerte behalten:

- | • Bei Windows nimmt der Virtual Ethernet-Adapter standardmäßig den Wert Maximum Frame Size "Auto" an. Auto bewirkt, dass das Virtual Ethernet eine maximale Rahmengröße berechnet, die auf Ethernet Frame Sizedes des verwendeten iSCSI-HBA-Ports basiert. Weitere Informationen zur Verwendung des iSCSI-HBA-Ports finden Sie unter „iSCSI-HBA-Zuordnung auf der Windows-Seite des iSCSI-Netzwerks verwalten“ auf Seite 147.
- | • In der Leitungsbeschreibung für das Virtual Ethernet bei i5/OS nimmt **Maximale Rahmengröße (MAXFRAME)** standardmäßig den Wert **8996** an.
- | • Bei TCP/IP-Schnittstellen für Virtual Ethernet auf i5/OS nimmt **Maximale Rahmengröße** standardmäßig einen Wert ***LIND** an.

| **Virtual Ethernet für iSCSI-Netzwerk konfigurieren, deren maximale Rahmengröße geringer als 1500 Byte ist**

| Führen Sie an der Windows-Konsole folgende Schritte durch:

- | 1. Navigieren Sie zum Fenster **Netzverbindungen**.
- | 2. Doppelklicken Sie auf **den IBM iSeries Virtual Ethernet x-Adapter**, der einen iSCSI-HBA verwenden soll, der am iSCSI-Netzwerk angeschlossen ist und eine maximale Rahmengröße von weniger als 1500 Byte hat.
- | 3. Klicken Sie auf **Eigenschaften**.
- | 4. Klicken Sie auf **Konfigurieren**.
- | 5. Klicken Sie auf **Erweitert**.
- | 6. Klicken Sie auf **Maximale Rahmengröße**.
- | 7. Wählen Sie einen Wert aus, der so groß wie möglich ist, ohne die max. Rahmengröße des iSCSI-Netzwerks zu übersteigen.

Virtual Ethernet so konfigurieren, dass ungewöhnliche Nicht-TCP-Anwendungen unterstützt werden, die keine MTU vereinbaren

Anmerkung: Um Auswirkungen auf normale Anwendungen zu vermeiden, die MTUs vereinbaren, muss vor der Ausführung dieser Prozedur evtl. ein separates Virtual Ethernet-Netzwerk oder separate IP-Adressen für die Anwendung definiert werden, die MTUs nicht vereinbaren.

1. Eine der folgenden Maßnahmen durchführen:

- a. Wenn alle Windows-Endpunkte ein iSCSI-Netzwerk mit einer maximalen Rahmengröße von 1500 Byte oder höher verwenden, konfigurieren Sie den iSCSI-HBA Ethernet frame size bei allen Windows-Endpunkten so, dass der Wert so groß wie möglich ist, ohne die maximale Rahmengröße des eingeschränkten iSCSI-Netzwerks zu beeinträchtigen.
- b. Wenn ein Windows-Endpunkt ein iSCSI-Netzwerk verwendet, dessen maximale Rahmengröße unter 1500 Byte liegt, muss das Virtual Ethernet Maximum frame size an allen Endpunkten mit einem Wert definiert werden, der so groß wie möglich ist, aber die maximale Rahmengröße des eingeschränkten iSCSI-Netzwerks nicht übersteigt.

2. Für andere Endpunkte setzen Sie MTU auf den Wert, den Sie erhalten, wenn Sie 116 vom kleineren der Werte Windows-iSCSI-HBA Ethernet frame size oder Maximum frame size für Virtual Ethernet abziehen. Für i5/OS-Endpunkte können Sie die folgende Prozedur ausführen.

- a. Verwenden Sie iSeries Navigator, um **Netzwerk**—>**TCP/IP-Konfiguration**— > **IPv4**—> **Schnittstellen** zu erweitern.
- b. Klicken Sie mit der rechten Maustaste auf die gewünschte IP-Adresse und Leitungsbeschreibung, und wählen Sie dann **Eigenschaften** aus.
- c. Geben Sie auf der Indexzunge **Erweitert** den berechneten Wert in das Feld "Größte zu übertragende Einheit" ein, und klicken Sie dann auf **OK**, um die Änderung zu speichern.

Anmerkung: Wenn Sie die Befehlszeilenschnittstelle verwenden möchte, verwenden Sie CFGTCP und wählen Option 1 (Mit TCP/IP-Schnittstellen arbeiten) aus.

Integrierter DHCP-Server

Der iSeries-Server mit iSCSI-Anschluss bietet einen integrierten DHCP-Server. Der Server wird verwendet, um Bootparameter des iSCSI-HBA im Hosted System zu implementieren, wenn die Option "Dem fernen System über DHCP dynamisch bereitgestellt" im fernen i5/OS-Systemkonfigurationsobjekt angegeben wurde, und AUTO oder DHCP im iSCSI-HBA des Hosted Systems.

Der integrierte DHCP-Server ist kein Allgemeinserver. Es ist ausschließlich für die Implementierung von Bootparametern für den iSCSI-HBA des Hosted-Servers vorgesehen. Der Server wird automatisch mit den Parametern konfiguriert, die in der Konfiguration des fernen Systems zur Verfügung gestellt werden, wenn eine NWSD (Netzwerkserverbeschreibung) angehängt wird.

Der DHCP-Server antwortet nur dem DHCP-Client des iSCSI-HBA des Hosted-Servers. Alle DHCP-Clientanforderungen des iSCSI-HBA arbeiten mit einer von IBM definierten Lieferanten-ID. Der Server ist so programmiert, dass er auf Anforderungen antwortet, die die Standardlieferanten-ID verwenden. Anforderungen von andere Einheiten im Netz werden vom DHCP-Server ignoriert.

Es ist sehr wichtig, dass die MAC-Adressen der iSCSI-HBAs des Hosted-Servers im Konfigurationsobjekt des fernen Systems zur Verfügung gestellt werden. Außer der bereits beschriebenen Lieferanten-ID verwendet der integrierte DHCP-Server die MAC-Adressen, um die Bootparameter korrekt zu implementieren. MAC-Adressen sind Teil des spezifischen Gültigkeitsbereichs, der für die korrekte Parameterimplementierung erforderlich ist.

Der durch Lieferanten-ID und MAC-Adresse definierte Gültigkeitsbereich kann geändert werden. Dies ist eine erweiterte Funktion; aber fortgeschrittene Benutzer können die Einstellungen noch spezifischer konfigurieren, falls dies nötig sein sollte. Die Standardlieferanten-ID kann nicht auf einen anderen Wert gesetzt werden. Konfigurationsanzeigen stehen in dem mit STRG-Q aufgerufenen Dienstprogramm des iSCSI-

| HBA für das Hosted System und dem Konfigurationsobjekt des fernen Systems zur Verfügung. Diese erweiterte Funktion ist kompatibel mit der Spezifikation RFC 2132. Weitere Details zur erweiterten Konfiguration finden Sie unter iSCSI Install Read Me First 

| Wenn eine DHCP-Anforderung beim integrierten DHCP-Server eingeht und der Gültigkeitsbereich abgeglichen ist, stellt der DHCP-Server dem DHCP-Client die IP-Adressen für die Bootzieleinheit zur Verfügung. Die Bootzieleinheit ist der NWS-Hostadapter (NWSH), auf dem die virtuelle Bootplatte konfiguriert ist. Der Server stellt auch die IP-Adresse für den Initiator oder den DHCP-Client zur Verfügung. Der Initiator ist der iSCSI-HBA im Hosted-Server, mit dem über iSCSI gebootet wird.

| Zusätzlich bietet der integrierte DHCP-Server global eindeutige qualifizierte iSCSI-Namen (IQNs), die für den iSCSI-HBA des Hosted Systems die Ziel- und Initiatoreinheiten darstellen.

| Beide Gruppen von IP-Adressen und IQNs werden in den iSeries-Konfigurationsobjekten für die Definition des Hosted-Servers verwendet. Die IP-Zieladresse wird im NWSH-Objekt definiert. Die IP-Initiatoradresse und der Initiator-IQN werden im Konfigurationsobjekt des fernen Systems definiert. Die Ziel-IQN wird automatisch im NWS-Objekt konfiguriert und definiert. Weitere Informationen zu diesen Objekten finden Sie unter „NWS-Beschreibung“ auf Seite 46.

| Der integrierte DHCP-Server ist die Schlüsselkomponente bei der Implementierung von Hot-Spares. Der DHCP-Bootmodus aktiviert die automatische Implementierung der erforderlichen Parameter, die in iSeries-Softwareobjekten definiert wurden; es ist daher nicht mehr nötig, Server manuell zu konfigurieren, wenn sich Bootparameter (IP-Adresse und IQNs) ändern.

| Fernen Server erkennen und verwalten

| IBM Director sowie Konfigurationsinformationen des fernen i5/OS-Systems und aus den Konfigurationsobjekten des Serviceprozessors werden verwendet, um zugeordnete Server zu lokalisieren und zu verwalten. Weitere Informationen enthalten die folgenden Abschnitte.

- | • „IBM Director installieren und konfigurieren“
- | • „Fernen Server und Serviceprozessor erkennen“ auf Seite 151
 - | – „Erkennungskonfiguration für Serviceprozessor“ auf Seite 151
 - | – „Dynamische IP-Adressierung (DHCP)“ auf Seite 153
 - | – „Erkennungsmethode für Serviceprozessor“ auf Seite 153
- | • „Managementmodul- oder RSA II-Webschnittstelle verwenden“ auf Seite 155

| IBM Director installieren und konfigurieren

| IBM Director wird für Erkennung und Verwaltung von Server mit iSCSI-Anschluss verwendet. Außer der IBM Director-Schnittstelle für das Installieren und Starten von IBM Director braucht keine weitere Schnittstelle verwendet zu werden. Weitere Informationen über die Installation von IBM Director finden Sie unter „Softwarevoraussetzungen“ auf Seite 64.

| Die Windows-Umgebung auf iSeries verwendet IBM Director für

- | • **Erkennung von fernem Server und Serviceprozessor**
| Server im Netz suchen.
- | • **Stromversorgung**
| Server einschalten oder Systemabschluss für das Betriebssystem für die entsprechenden i5/OS-Konfigurationsbefehle (Vary) ausführen.
- | • **Abfrage des Stromstatus**
- | • **Konfiguration des fernen Servers**
| Einige Funktionen des fernen Servers können mit iSeries über Remotezugriff zum Serviceprozessor des fernen Servers konfiguriert werden.

| IBM Director benötigt TCP/IP. TCP/IP muss aktiv sein, damit IBM Director arbeiten kann. Weil IBM Director ein i5/OS-TCP-Server ist, kann er so konfiguriert werden, dass er automatisch startet, wenn TCP gestartet wird. Es wird empfohlen, den IBM Director-TCP-Server mit automatischem Start zu konfigurieren. Dadurch ist sichergestellt, dass IBM Director verfügbar ist, wenn der iSCSI-HBA für iSeries ihn benötigt.

| Um den IBM Director-TCP-Server so zu konfigurieren, dass er automatisch gestartet wird, wenn TCP/IP startet, verwenden Sie iSeries Navigator, und führen Sie die folgenden Schritte aus:

- | 1. Wählen Sie **Netzwerk -> Server -> Benutzerdefiniert** aus.
- | 2. Klicken Sie mit der rechten Maustaste auf **IBM DIRECTOR**, und wählen Sie **Eigenschaften** aus.
- | 3. Wählen Sie die Option **Starten, wenn TCP/IP gestartet wird** aus.
- | 4. Klicken Sie auf **OK**.

| Sie können auch den Befehl CHGTCPSPVR (TCP/IP-Server ändern) verwenden.

| Wenn IBM Director nicht automatisch gestartet wird, verwenden Sie iSeries Navigator, um den IBM Director-TCP-Server zu starten:

- | 1. Wählen Sie **Netzwerk -> Server -> Benutzerdefiniert** aus.
- | 2. Klicken Sie mit der rechten Maustaste auf **IBM DIRECTOR**, und wählen Sie **Starten** aus.

| **Anmerkung:** Es dauert mindestens einige Minuten, bis der IBM Director-Server startet. Sie können den Status des Startvorgangs anzeigen, indem Sie die iSeries Navigator-Liste aktualisieren, bis der IBM DIRECTOR-Server den Status "Gestartet" hat.

| Fernen Server und Serviceprozessor erkennen

| i5/OS verwendet IBM Director, um ferne Server in einem lokalen Netz (LAN) zu lokalisieren und zu identifizieren, und kommuniziert dafür mit dem Serviceprozessor des fernen Servers. Ferne Systeme werden anhand von Informationen in ihrer Konfiguration und in den Konfigurationsobjekten des Serviceprozessors auf dem iSeries-Server identifiziert.

| Dies ist eine andere Verbindung als die Verbindung zwischen dem iSeries-Ziel-iSCSI-HBA und dem iSCSI-Initiatoradapter auf dem fernen Server. Der LAN-Adapter für den Serviceprozessor des fernen Servers muss an ein Netz angeschlossen sein, das über einen LAN-Adapter des iSeries-Server erreichbar ist.

| Die i5/OS Objekte und der Serviceprozessor müssen konfiguriert sein. Sie können die Erkennungsmethode konfigurieren, die in den Konfigurationsobjekten des i5/OS-Netzservers verwendet wird.

| Weitere Informationen enthalten die folgenden Abschnitte:

- | • „Erkennungskonfiguration für Serviceprozessor“
- | • „Dynamische IP-Adressierung (DHCP)“ auf Seite 153
- | • „Erkennungsmethode für Serviceprozessor“ auf Seite 153
- | • „Managementmodul- oder RSA II-Webschnittstelle verwenden“ auf Seite 155

| Erkennungskonfiguration für Serviceprozessor

| Die IP-Informationen des Serviceprozessors müssen so konfiguriert werden dass sie der i5/OS-Konfiguration entsprechen. Die Konfigurationsoptionen hängen von der Art des Serviceprozessors ab. Weitere Informationen über das Identifizieren des Serviceprozessortyps im xSeries-Server enthalten die von iSCSI

| unterstützten xSeries- und BladeCenter-Modelle 
| (www.ibm.com/servers/eserver/iseries/integratedxseries/iscsiservermodels/)



| Baseboard Management Controller (BMC)

| Der BMC-Serviceprozessor steht in einigen xSeries-Modellen zur Verfügung.

- | • Um den BMC zu konfigurieren, verwenden Sie das BIOS-Definitionsmenü.
- | • Der BMC unterstützt statische IP-Adressierung.
- | • Der BMC unterstützt Erkennung durch IP-Adresse. Weitere Informationen finden Sie unter „Erkennung durch IP-Adresse“ auf Seite 154.
- | • Der BMC unterstützt Absicherung durch Kennwort. Weitere Informationen finden Sie unter „Serviceprozessorkennwort“ auf Seite 142.

| Remote Supervisor Adapter II (RSA II)


| Der RSA II-Serviceprozessor steht in einigen xSeries-Modellen zur Verfügung.

- | • Um den RSA II zu konfigurieren, eine der folgenden Maßnahmen ausführen.
 - | – Verwenden Sie das Definitionsmenü des System-BIOS. Diese Methode kann nicht verwendet werden, um einen Hostnamen zu konfigurieren.
 - | – Weitere Informationen finden Sie unter „Managementmodul- oder RSA II-Webschnittstelle verwenden“ auf Seite 155.
- | • Der RSA II kann IP-Adressinformationen mit einer der beiden folgenden Methoden abrufen. Verwenden Sie die Methode, die für Netz sinnvoll ist.
 - | – „Dynamische IP-Adressierung (DHCP)“ auf Seite 153. Dies ist die werkseitige Voreinstellung.
 - | – Statische IP-Adressierung.
- | • Der RSA II unterstützt die folgenden Erkennungsmethoden. Verwenden Sie die Methode, die für Netz sinnvoll ist.
 - | – „Service Location Protocol (SLP) mit Multicastadressierung“ auf Seite 153.
 - | – „Erkennung durch IP-Adresse“ auf Seite 154.
 - | – „Erkennung durch Hostname“ auf Seite 155.
- | • Der RSA II unterstützt die folgenden Absicherungsmethoden:
 - | – Kennwort. Weitere Informationen zum Konfigurationsvorgang finden Sie unter „Serviceprozessorkennwort“ auf Seite 142.
 - | – SSL und Kennwort. Weitere Informationen finden Sie unter „Serviceprozessor-SSL konfigurieren“ auf Seite 140.
- | • Weitere Informationen über den RSA II finden Sie in den folgenden Abschnitten.
 - | – IBM Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II Installation Guide - Servers  (www.ibm.com/pc/support/site.wss/). Wählen Sie unter **Browse** die Optionen **Servers**, Family: **xSeries 236**, Type: **All Types**, **Continue** aus. Wählen Sie **Publications** aus.
 - | – IBM Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide - Servers  (www.ibm.com/pc/support/site.wss/). Wählen Sie unter **Browse** die Optionen **Servers**, Family: **xSeries 236**, Type: **All Types**, **Continue** aus. Wählen Sie **Publications** aus.

| Managementmodul

| Das Managementmodul steht in IBM BladeCenter-Servern zur Verfügung.

- | • Weitere Informationen zur Konfiguration des Managementmoduls finden Sie unter „Managementmodul- oder RSA II-Webschnittstelle verwenden“ auf Seite 155.
- | • Das Managementmodul kann IP-Adressinformationen mit einer der beiden folgenden Methoden abrufen. Verwenden Sie die Methode, die für Netz sinnvoll ist.
 - | – „Dynamische IP-Adressierung (DHCP)“ auf Seite 153. Dies ist die werkseitige Voreinstellung.
 - | – Statische IP-Adressinformationen.

- | • Das Managementmodul unterstützt die folgenden Erkennungsmethoden. Verwenden Sie die Methode, die für Netz sinnvoll ist.
- | – „Service Location Protocol (SLP) mit Multicastadressierung“
- | – „Erkennung durch IP-Adresse“ auf Seite 154.
- | – „Erkennung durch Hostname“ auf Seite 155
- | • Bei IBM BladeCenter-Servern gibt es zusätzliche Überlegungen bezüglich der Erkennung. Die ID des fernen Systems in der Konfiguration des fernen Systems muss immer auf die Seriennummer des IBM BladeCenter-Servers gesetzt sein, die auf einem Etikett des Servers steht. Informationen zum Ändern der Konfiguration des fernen Systems finden Sie unter „Konfigurationseigenschaften des fernen Systems ändern“ auf Seite 132. Die Gehäuse-Identität in der Serviceprozessorkonfiguration kann für jedes Blade auf die Seriennummer des IBM BladeCenter-Gehäuses (Chassis) gesetzt werden. Der Managementmodul-Serviceprozessor im IBM BladeCenter muss bekannt sein, bevor die Server-Blades erkannt werden können. Die Parameter in der Serviceprozessorkonfiguration legt die Erkennungsmethode für das Managementmodul fest. Weitere Informationen zum Ändern dieser Eigenschaften finden Sie unter „Konfigurationseigenschaften des Serviceprozessors ändern“ auf Seite 134. Nachdem das Managementmodul erkannt ist, sammelt IBM Director Informationen über die Server-Blades im Gehäuse. Die ID des fernen Systems wird in der zweiten Erkennungsphase verwendet, um das individuelle Blade zu identifizieren.
- | • Das Managementmodul unterstützt die folgenden Sicherheitsmethoden:
- | – Kennwort. Weitere Informationen finden Sie unter „Serviceprozessorkennwort“ auf Seite 142.
- | – SSL und Kennwort. Weitere Informationen finden Sie unter „Serviceprozessor-SSL konfigurieren“ auf Seite 140.
- | • Weitere Informationen finden Sie unter IBM BladeCenter Systems Management Redpaper  (www.redbooks.ibm.com/abstracts/redp3582.html) zum Thema IBM eServer BladeCenter-Systemmanagement.

| **Dynamische IP-Adressierung (DHCP)**

| Ein Serviceprozessor mit DHCP wird unverzüglich initialisiert, wenn der Server Strom erhält; er startet dann den DHCP-Prozess. Wenn eine Adresse mit DHCP nicht festgestellt werden kann, verwendet der Serviceprozessor die statische IP-Standardadresse 192.168.70.125.

| **Anmerkung:** Wenn der Serviceprozessor die IP-Adresse mit DHCP nicht feststellen kann, kann der Prozess nur durch Aus- und Einschalten der Einheit erneut gestartet werden.

| **Erkennungsmethode für Serviceprozessor**

| Es gibt verschiedene Methoden zur Serviceprozessorerkennung.

- | • „Service Location Protocol (SLP) mit Multicastadressierung“
- | • „Erkennung durch IP-Adresse“ auf Seite 154
- | • „Erkennung durch Hostname“ auf Seite 155

| **Service Location Protocol (SLP) mit Multicastadressierung:** Wenn Sie weder den Serviceprozessor-Hostnamen noch die Internetadresse verwenden, um den Server im Netz zu erkennen, wird Multicastadressierung mit Service Location Protocol (SLP) verwendet. Für SLP-Erkennung müssen Sie Ihren iSeries-Server konfigurieren. Gehen Sie dazu folgendermaßen vor:

- | 1. Gehen Sie wie im Abschnitt „Konfigurationseigenschaften des Serviceprozessors ändern“ auf Seite 134 beschrieben vor:
 - | a. Stellen Sie sicher, dass die Option **Serviceprozessorverbindung verwenden, um Gehäuse-identifikation für fernes System zu ermitteln** nicht ausgewählt ist.
 - | b. Geben Sie in das Feld **Seriennummer** die Nummer des Standalone-Servergehäuses oder des IBM BladeCenter-Chassis ein.
- | 2. Gehen Sie wie in Abschnitt „Konfigurationseigenschaften des fernen Systems ändern“ auf Seite 132 beschrieben vor, um sicherzustellen, dass die ID des fernen Systems korrekt definiert ist.
 - | a. Bei einem Standalone-Server wählen Sie **Gehäuseidentifikation aus Konfiguration für Serviceprozessor verwenden** aus.

- b. Für ein IBM BladeCenter-Blade wählen Sie die Option **Folgende Werte verwenden:** aus, und geben Sie seine Seriennummer ein.

Der Serviceprozessor zeigt sich mit einem SLP-Paket, das mit Multicastadressierung über das Netz gesendet wird. Dieses Paket enthält Attribute wie z. B. Seriennummer, Typ und Modell des fernen Servers. IBM Director empfängt dieses Paket und speichert die Informationen über den Server. Die Seriennummer der Gehäuse-ID aus der Serviceprozessorkonfiguration oder die ID des fernen Systems aus dessen Konfiguration wird auf die Attribute, die aus dem SLP-Erkennungsprozess stammen und einen bestimmten fernen Server identifizieren.

Vorteile:

- Es wird nur die Seriennummer (sie kann von einem Etikett auf dem Server stammen) benötigt, um den fernen Server zu erkennen.
- Wenn der Serviceprozessor seine IP-Adresse von einem DHCP-Server abrufen und da Netz IP-Multicasting unterstützt, kann die werkseitig vorgenommene Standardeinstellung für den Serviceprozessor verwendet werden.

Nachteile:

- SLP wird nur von den Serviceprozessoren für Remote Supervisor Adapter II und IBM BladeCenter-Managementmodul unterstützt. Von BMC-Serviceprozessoren (Baseboard Management Controller) wird es nicht unterstützt.
- Router und Switches, die sich zwischen dem Serviceprozessor und dem iSeries LAN-Adapter befinden, müssen konfiguriert werden, damit sie Multicastadressierung unterstützen. Wenn sie nicht korrekt konfiguriert sind, geben Router Multicastpakete nicht weiter. Hinweise zur Konfigurierung für Multicastadressierung von Routern finden Sie in den entsprechenden Dokumentationen. SLP (Service Location Protocol) verwendet die IP-Adresse 239.255.255.253 und die Portnummer 427. Diese Informationen sind evtl. erforderlich, um Router für die Unterstützung von SLP-Multicastpaketen zu konfigurieren.

Erkennung durch IP-Adresse: Diese Methode der Erkennung verwendet Unicastadressierung. Um Erkennung durch IP-Adresse zu konfigurieren, gehen Sie wie folgt vor:

1. Auf dem Hosted System konfigurieren Sie eine statische IP-Adresse, die für das Netz im Serviceprozessor geeignet ist. Dieser Schritt sollte durchgeführt werden, bevor der Serviceprozessor an das LAN angeschlossen wird. Verwenden Sie entweder das Definitionsmenü des System-BIOS oder die Webschnittstelle, je nachdem, was Ihr Serviceprozessor unterstützt. Weitere Informationen über den Einsatz eines Web-Browsers finden Sie unter „Managementmodul- oder RSA II-Webschnittstelle verwenden“ auf Seite 155.
2. Konfigurieren Sie auf dem iSeries-Server den Serviceprozessor.
 - a. Stellen Sie sicher, dass die Option **Serviceprozessorverbindung verwenden, um Gehäuseidentifikation für fernes System zu ermitteln** ausgewählt ist.
 - b. Wählen Sie die Option **Internetadresse** aus, und geben Sie die IP-Adresse des Serviceprozessors ein.
 - c. Optional: Geben Sie die Seriennummer des Standalone-Servers oder die Seriennummer eines IBM BladeCenter-Chassis ein. Ein Fehler tritt auf, wenn die von der IP-Adresse erkannte Seriennummer des Serviceprozessors nicht mit der Seriennummer in der Konfiguration übereinstimmt.
Weitere Informationen finden Sie unter „Konfigurationseigenschaften des Serviceprozessors ändern“ auf Seite 134.
3. Gehen Sie wie in Abschnitt „Konfigurationseigenschaften des fernen Systems ändern“ auf Seite 132 beschrieben vor, um sicherzustellen, dass die ID des fernen Systems korrekt definiert ist.
 - Bei einem Standalone-Server wählen Sie **Gehäuseidentifikation aus Konfiguration für Serviceprozessor verwenden** aus.
 - Für ein IBM BladeCenter-Blade wählen Sie die Option **Folgende Werte verwenden:** aus, und geben Sie seine Seriennummer ein.

| Vorteile:

- | • Diese Erkennungsmethode ist sehr einfach, wenn die IP-Adresse des Serviceprozessors bekannt ist und für den Serviceprozessor konfiguriert wird.

| Nachteile:

- | • Die IP-Adresse muss im Serviceprozessor konfiguriert werden.

| **Erkennung durch Hostname:** Diese Methode der Erkennung verwendet Unicastadressierung. Um Erkennung durch Hostname zu konfigurieren, gehen Sie wie folgt vor:

- | 1. Konfigurieren Sie auf dem Hosted System den Hostnamen des Serviceprozessors. Dieser Schritt sollte durchgeführt werden, bevor der Serviceprozessor an das LAN angeschlossen wird.
 - | a. Sie müssen für diesen Schritt die Webschnittstelle verwenden. Nutzen Sie die aktuelle IP-Adresse, um die Verbindung zur RSA II-Webschnittstelle herzustellen. Weitere Informationen über den Einsatz eines Web-Browsers finden Sie unter „Managementmodul- oder RSA II-Webschnittstelle verwenden“.
 - | b. Verwenden Sie Ihren Browser, um den Hostnamen so zu ändern, das er in das Netz passt.
 - | c. **Optional:** Sie können auch eine statische IP-Adresse konfigurieren, die den Angaben im Netz entspricht.
- | 2. Konfigurieren Sie auf Ihrem iSeries-Server den Serviceprozessor.
 - | a. Stellen Sie sicher, dass die Option **Serviceprozessorverbindung verwenden, um Gehäuseidentifikation für fernes System zu ermitteln** ausgewählt ist.
 - | b. Wählen Sie die Option **Hostname** aus, und geben Sie den Hostnamen des Serviceprozessors ein.
 - | c. **Optional:** Geben Sie die Seriennummer eines Standalone-Servers oder eines IBM BladeCenter-Chassis ein. Wenn die über den Hostnamen erkannte Seriennummer des Serviceprozessors nicht mit der Seriennummer übereinstimmt, tritt ein Fehler auf.
| Weitere Informationen finden Sie unter „Konfigurationseigenschaften des Serviceprozessors ändern“ auf Seite 134.
- | 3. Gehen Sie wie in Abschnitt „Konfigurationseigenschaften des fernen Systems ändern“ auf Seite 132 beschrieben vor, um sicherzustellen, dass die ID des fernen Systems korrekt definiert ist.
 - | • Bei einem Standalone-Server wählen Sie **Gehäuseidentifikation aus Konfiguration für Serviceprozessor verwenden** aus.
 - | • Für ein IBM BladeCenter-Blade wählen Sie die Option **Folgende Werte verwenden:** aus, und geben Sie seine Seriennummer ein.

| Vorteile:

- | • Wenn ein DNS-Server verfügbar ist, braucht in der Konfiguration des fernen i5/OS-Servers keine spezifische IP-Adresse verwaltet zu werden.

| Nachteile:

- | • Der Hostname muss im Serviceprozessor konfiguriert werden; dazu wird die Webschnittstelle des Serviceprozessors verwendet.
- | • Ein DNS-Server (Domain Name System) ist erforderlich.

| **Managementmodul- oder RSA II-Webschnittstelle verwenden**

| Die Managementmodul- bzw. die RSA II-Webschnittstelle kann für die folgenden Tasks verwendet werden:



- | • IP-Hostname des Serviceprozessors ändern
- | • Zertifikate für die manuelle Einstellung der Serviceprozessorkonfiguration verwalten
 - | – Anforderung zur Zertifikatssignierung durchführen, um ein Zertifikat von einer Zertifizierungsinstanz wie z. B. Verisign abzurufen.
 - | – Zertifikat in den Serviceprozessor importieren.

- Statische IP-Adressen konfigurieren
- RSA II-Firmware aktualisieren

Achtung: Die Webschnittstelle darf nicht verwendet werden, um den Benutzernamen oder das Kennwort des Serviceprozessors zu ändern. Wenn die Webschnittstelle für die Änderung von Benutzernamen oder Kennwort verwendet wird, haben die i5/OS-Objekte die alten Namen und Kennwörter. Das bedeutet, dass i5/OS die Verbindung zum Serviceprozessor nicht herstellen kann.

Verwenden Sie die in „Serviceprozessor initialisieren“ auf Seite 135 beschriebene Methode, um Benutzernamen und Kennwort zu ändern, bzw. den Befehl INZNWSCFG (NWS-Konfiguration initialisieren) mit der Option *CHGSPAUT. Dadurch bleiben die i5/OS-Objekte und die Werte für Benutzername und Kennwort des Serviceprozessors synchron.

Weitere Informationen über die Verwendung der Webschnittstelle zum Serviceprozessor finden Sie unter folgenden Links:

- Kapitel 2 des IBM Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide - Servers  (www.ibm.com/pc/support/site.wss/). Wählen Sie unter **Browse** die Optionen **Servers**, Family: **xSeries 236**, Type: **All Types**, **Continue** aus. Wählen Sie **Publications**
- IBM xSeries and BladeCenter Server Management, SG24-6495 

Mit Web-Browser Verbindung zu einem RSA II- oder IBM BladeCenter-Managementmodul herstellen

1. **Optional:** Um den Browser über einen Router mit RSA II zu verbinden, konfigurieren Sie zunächst die IP-Adresse von RSA II über die BIOS-Schnittstelle.
2. Geben Sie zuerst die IP-Adresse für RSA II oder das Managementmodul in den URL-Bereich des Web-Browsers ein.
3. Es sollte die Eingabeaufforderung für den RSA II- oder Managementmodul-Benutzernamen oder das Kennwort angezeigt werden. Geben Sie den Benutzernamen und das Kennwort für RSA II oder das Managementmodul ein. Für RSA II oder das Managementmodul werden standardmäßig der Benutzername "USERID" und das Kennwort "PASSWORD" (0 = Null) verwendet. Die werkseitige Voreinstellung für RSA II oder das Managementmodul sind die folgenden:
DHCP. Geben Sie DHCP ein. Wenn diese Angabe nicht funktioniert, verwenden Sie die statische IP-Konfiguration. Die statische IP-Adresse ist 192.168.70.125. Beachten Sie, dass es sich um eine Adresse handelt, die nicht weitergeleitet werden kann. Sie können daher den Browser nicht über einen Router mit RSA II oder dem Managementmodul verbinden und diese Adresse verwenden. Sie können evtl. einen Browser mit RSA II oder dem Managementmodul verbinden, wenn Sie die IP-Standardadresse verwenden; das gilt für die meisten (aber nicht alle) Arten von Switches und die meisten Ethernet-Hubs.

Wenn Verbindung zu RSA II/Managementmodul-Webschnittstellen besteht, können die folgenden Tasks durchgeführt werden:

- Wählen Sie "Netzschnittstellen" unter ASM-Steuerung aus. Geben Sie den Hostnamen ein. Es empfiehlt sich, das Hostnamensfeld auf den nichtqualifizierten Teil des IP-Hostnamens zu setzen. Der nichtqualifizierte IP-Hostname besteht aus den Angaben vor dem ersten Punkt des vollständig qualifizierten IP-Hostnamens. Beispiel: Der vollständig qualifizierte IP-Hostname ist `asmcard1.us.company.com`; der nichtqualifizierte IP-Hostname ist `asmcard1`.
- Wählen Sie "Anmeldeprofile" unter ASM-Steuerung aus, um den Benutzernamen und die Kennwörter zu ändern. Dies ist für den manuellen Sicherheitsmodus erforderlich.
- Wählen Sie "Firmware-Update" unter Tasks aus, um die RSA II- oder Managementmodul-Firmware auf den neuesten Stand zu bringen.

Kapitel 8. Integrierte Windows-Server verwalten

Die folgenden Abschnitte führen Sie durch einige allgemeine und im täglichen Betrieb anfallende Aufgaben, die für den integrierten Server ausgeführt werden müssen:

- „Integrierten Server starten und stoppen“
 - „Integrierten Windows-Server mit iSeries Navigator starten und stoppen“
 - „Integrierten Windows-Server über die zeichenorientierte Schnittstelle starten und stoppen“ auf Seite 158
 - „Integrierten Server über die Konsole des Windows-Servers beenden“ auf Seite 158
 - „iSeries mit integrierten Windows-Servern sicher herunterfahren“ auf Seite 158
- „Verbindung zur virtuellen seriellen Konsole für IXS Modell 4812 herstellen“ auf Seite 159
- „Konfigurationsdaten des integrierten Windows-Servers anzeigen oder ändern“ auf Seite 160
- „Nachrichtenprotokollierung“ auf Seite 161
- „Befehle für den integrierten Windows-Server im Fernzugriff ausführen“ auf Seite 161
 - „Richtlinien für die Übergabe ferner Befehle“ auf Seite 163
 - „Unterstützung des Befehls SBMNWSCMD und der Sicherung auf Dateiebene für Kerberos V5 und EIM“ auf Seite 165
- „Hot-Spare zwischen Server-Hardware“ auf Seite 166

Integrierten Server starten und stoppen

Ein integrierter Windows-Server ist nicht mit einem Netzschalter ausgestattet; sein Betriebszustand wird durch die iSeries gesteuert. Normalerweise verwenden Sie iSeries Navigator oder die zeichenorientierte Schnittstelle zum Starten oder Stoppen von integrierten Servern. Teilweise können Sie einen integrierten Server auch über sein eigenes Menü für **Start** —> **Beenden** beenden. Für seinen erneuten Start müssen Sie jedoch iSeries Navigator oder die zeichenorientierte Schnittstelle verwenden.

Stellen Sie sicher, dass alle integrierten Server abgehängt sind, bevor Sie die iSeries herunterfahren, da andernfalls Daten beschädigt werden können. Manche Befehle, die zum Herunterfahren der iSeries verwendet werden, leiten eine Beendigung der angeschlossenen integrierten Server ein und warten eine bestimmte Zeit, damit diese beendet werden können, bevor die iSeries heruntergefahren wird. Andere Befehle fahren die iSeries sofort herunter.

Wenn Sie das Programm QEZPWROFFP zum geplanten Ein-/Ausschalten verwenden, müssen Sie es so konfigurieren, dass es die integrierten Server berücksichtigt.

Die folgenden Abschnitte beschreiben die unterschiedlichen Methoden zum Starten und Beenden:

- „Integrierten Windows-Server mit iSeries Navigator starten und stoppen“
- „Integrierten Windows-Server über die zeichenorientierte Schnittstelle starten und stoppen“ auf Seite 158
- „Integrierten Server über die Konsole des Windows-Servers beenden“ auf Seite 158
- „iSeries mit integrierten Windows-Servern sicher herunterfahren“ auf Seite 158

Integrierten Windows-Server mit iSeries Navigator starten und stoppen

1. Um einen integrierten Server in iSeries Navigator zu stoppen, wählen Sie **Verwaltung integrierter Server** -> **Server** aus.
2. Klicken Sie mit der rechten Maustaste auf den Server, den Sie stoppen wollen, und wählen Sie die Option **Beenden** aus. Wenn alle integrierten Server beendet werden sollen, klicken Sie mit der rechten

Maustaste auf das Symbol "Integrierte xSeries-Server" im linken Navigationsbereich, und wählen Sie die Option **Alle beenden** aus. Der Status ändert sich in **Wird beendet...**, **Teilweise ausgeschaltet** und schließlich in **Beendet**.

3. Um einen integrierten Server zu starten, klicken Sie mit der rechten Maustaste auf den Server, und wählen Sie die Option **Starten** aus. Der Status ändert sich in **Wird gestartet...** und schließlich in **Gestartet**.

Integrierten Windows-Server über die zeichenorientierte Schnittstelle starten und stoppen

1. Um einen integrierten Server über die zeichenorientierte Schnittstelle zu stoppen, geben Sie den Befehl `WRKCFGSTS *NWS` ein.
2. Suchen Sie nach dem integrierten Server, den Sie stoppen wollen, und geben Sie eine 2 ein, um den Server *abzuhängen*.
3. Der Status ändert sich von **AKTIV** in **BEENDET** und dann in **ABGEHÄNGT**. Durch Drücken der Taste **F5** können Sie die Anzeige aktualisieren.

Anmerkung: Für an iSCSI angehängte Server ändert sich der Status von **AKTIV** in **ABGEHÄNGT**.

4. Zum Starten des integrierten Servers verwenden Sie ebenfalls den Befehl `WRKCFGSTS *NWS`, und geben Sie eine 1 ein, um den integrierten Server zu starten oder *anzuhängen*.
5. Um einen integrierten Server erneut zu starten, müssen Sie ihn manuell abhängen und dann wieder anhängen. Es gibt keinen Befehl, mit dem ein integrierter Server über die zeichenorientierte Schnittstelle automatisch erneut gestartet werden kann.

Integrierten Server über die Konsole des Windows-Servers beenden

Um einen integrierten Windows-Server über seine eigene Konsole zu beenden, wählen Sie im Windows-Menü die Optionen **Start** —> **Beenden** aus. Diese Methode ist jedoch nicht zu empfehlen, da ein integrierter Server hierbei nur zum Teil beendet wird. Das Windows-Betriebssystem wird gestoppt, und in der Anzeige erscheint die Nachricht *Sie können den Computer jetzt ausschalten*. Um einen kompletten Systemabschluss und einen Neustart durchzuführen, müssen Sie den Server jedoch mit iSeries Navigator oder über die zeichenorientierte Schnittstelle *abhängen*.

Im Gegensatz zur Beendigung stellt der **Neustart** eines integrierten Servers über seine eigene Konsole eine der effizientesten Methoden für diesen Zweck dar.

So gehen Sie vor:

1. Wählen Sie im Menü **Start** die Option **Beenden** aus.
2. Wählen Sie im Dropdown-Menü die Option **Neu starten** aus, und klicken Sie auf **OK**.

Anmerkung: Wenn Server mit iSCSI-Anschluss an der Windows-Serverkonsole beendet werden, wird die NWS-Beschreibung (NWS) nicht abgehängt. Der NWS-Status ändert sich von **AKTIV** in **ANGEHÄNGT**. Der Serverstatus kann mit dem iSeries Navigator oder mit dem Befehl `WRKNWSSTS` (Mit Netzwerkserverstatus arbeiten) abgefragt werden. Der Status wird jedes Mal abgerufen, wenn der Befehl ausgegeben wird. Der Windows-Server meldet seinen Status nicht automatisch zurück.

iSeries mit integrierten Windows-Servern sicher herunterfahren

Wenn Sie sicherstellen wollen, dass die integrierten Server sicher beendet werden, besteht die einfachste Methode darin, die Server immer manuell zu beenden, bevor die iSeries heruntergefahren wird. Dies ist allerdings mitunter umständlich und zeitaufwändig. Der CL-Befehl `PWRDWN SYS *CNTRLD` versucht, jeden einzelnen integrierten Server zu beenden, und stellt ihm dafür einen bestimmten Zeitraum (das NWS-Attribut `SHUTDTIMO` ist standardmäßig auf 15 Minuten gesetzt) zur Verfügung. Bitte beachten Sie, dass es keine Garantie dafür gibt, dass die Beendigung innerhalb dieses Zeitraums vollständig erfolgt.

Anmerkung: Der CL-Befehl PWRDWN SYS *IMMED sollte nicht verwendet werden. Er schaltet iSeries sofort ab, ohne zu versuchen, die integrierten Server herunterzufahren.

Table 2.

Aktion	Ergebnis
Integrierten Server manuell beenden	Der integrierte Server wird ordnungsgemäß abgehängt. Es besteht keine Gefahr eines Datenverlustes.
CL-Befehl pwrdw nsys *cntrl d absetzen	Dem integrierten Server wird für die Beendigung der Zeitraum zur Verfügung gestellt, der in seinem NWS D-Attribut "Zeitlimit bei Systemabschluss" angegeben ist. Anschließend fährt die iSeries mit der Beendigung fort.
CL-Befehl pwrdw nsys *immed absetzen	Die iSeries wird sofort heruntergefahren und beendet die integrierten Server nicht. Hierbei können Daten beschädigt werden.

Wenn Ihr i5/OS-System das geplante Ein-/Ausschalten verwendet, sollte das Exitprogramm für das Ausschalten (QEZPWROFFP) so geändert werden, dass alle NWS-Beschreibungen vor Aufrufen des Befehls PWRDWN SYS abgehängt werden. Der Zeitplan muss sorgfältig definiert werden, da Anzahl und Aktivität der Server den Zeitraum bestimmen, der zum vollständigen Abhängen der einzelnen Server benötigt wird. Verwenden Sie die Parameter SBMMLTJOB (Mehrere Jobs übergeben) und JOB D (Jobbeschreibung) des Befehls VRYCFG (Konfiguration ändern), um mehrere Server gleichzeitig im Stapelbetrieb an- bzw. abzuhängen. Das geplante Einschalten darf erst stattfinden, nachdem das System die Möglichkeit hatte, alle Server abzuhängen und den Befehl PWRDWN SYS abzusetzen. Weitere Informationen finden Sie unter Zeitplan für automatisches Ein- und Ausschalten aufstellen.

Verbindung zur virtuellen seriellen Konsole für IXS Modell 4812 herstellen

Die virtuelle serielle Konsole umfasst Windows-Konsolenfunktionen für einen Windows Server 2003-Server, der auf einem integrierten xSeries-Server (IXS) des Typs 4812 ausgeführt wird. Weitere Informationen zu Windows-Konsolen finden Sie in „Windows-Konsole“ auf Seite 24. Diese Konsolenverbindung kann verwendet werden, bevor TCP/IP auf dem Server konfiguriert wird.

Als virtuelle serielle Konsole können alle Telnet-Clients verwendet werden. Hierbei ist es möglich, dass mehrere Telnet-Clients gemeinsam auf dieselbe virtuelle serielle Konsole zugreifen. Um eine Konsolenverbindung herzustellen, müssen Sie über Telnet eine Verbindung zum Port 2301 der i5/OS-Partition aufbauen, die für die gemeinsame Ressourcenbenutzung konfiguriert wurde. TCP/IP muss auf dem System konfiguriert sein und in der logischen i5/OS-Partition ausgeführt werden.

Gehen Sie wie folgt vor, um über den IBM Personal Communications-Client eine Verbindung zu einer virtuellen seriellen Konsole herzustellen:

1. Klicken Sie auf **Start -> Programme -> IBM Personal Communications -> Sitzung starten oder konfigurieren**.
2. Wählen Sie im Dialogfeld zur Anpassung der Kommunikation im Feld für den **Hosttyp** die Einstellung **ASCII** aus.
3. Klicken Sie auf die Option für **Verbindungsparameter**.
4. Geben Sie im Telnet-ASCII-Dialog in das Feld **Primärer Hostname oder IP-Adresse** den Hostnamen oder die IP-Adresse der i5/OS-Partition ein, zu der eine Verbindung hergestellt werden soll.
5. Geben Sie im Feld für **Primäre Portnummer** den Wert 2301 ein.
6. Klicken Sie auf **OK**.
7. Klicken Sie nochmals auf **OK**. Der Sitzungsdialog wird geöffnet.

8. Wählen Sie im i5/OS-Menü für virtuelle Konsolen die Option für **Integrierte xSeries-Serverkonsolen** aus.
9. Wählen Sie im Dialog für die integrierten xSeries-Serverkonsolen den Namen der Hardwareressource für die IOA-Einheit vom Typ 4812 aus, die als Konsole angeschlossen werden soll. Zur Feststellung dieses Namens müssen Sie die NWS-Beschreibung des Servers aufrufen und den dort für den Ressourcennamenparameter angegebenen Wert verwenden.
10. Geben Sie die i5/OS-Service-Tools-ID und das Kennwort ein, um eine Verbindung zur virtuellen Konsole des integrierten xSeries-Servers herzustellen.

Wenn Sie die Verbindung zur virtuellen seriellen Konsole mit Hilfe von Telnet über eine DOS-Bedienerführung herstellen möchten, müssen Sie die folgenden Arbeitsschritte ausführen:

1. Geben Sie im Bedienerführungsdialg den Befehl `telnet partitionname 2301` ein. Hierbei steht *partitionname* für den Namen der i5/OS-Partition, zu der eine Verbindung hergestellt werden soll.
2. Drücken Sie die Eingabetaste.
3. Wählen Sie im i5/OS-Menü für virtuelle Konsolen die Option für **Integrierte xSeries-Serverkonsolen** aus.
4. Wählen Sie im Dialog für die integrierten xSeries-Serverkonsolen den Namen der Hardwareressource für die IOA-Einheit vom Typ 4812 aus, die als Konsole angeschlossen werden soll. Zur Feststellung dieses Namens müssen Sie die NWS-Beschreibung des Servers aufrufen und den dort für den Ressourcennamenparameter angegebenen Wert verwenden.
5. Geben Sie die i5/OS-Service-Tools-ID und das Kennwort ein, um eine Verbindung zur virtuellen Konsole des integrierten xSeries-Servers herzustellen.

Konfigurationsdaten des integrierten Windows-Servers anzeigen oder ändern

Mit iSeries Navigator können Sie einen Großteil der Konfigurationsdaten für den integrierten Server anzeigen und ändern.

1. Wählen Sie im iSeries Navigator **Verwaltung integrierter Server -> Server** aus.
2. Klicken Sie mit der rechten Maustaste auf einen integrierten Server, und wählen Sie die Option **Eigenschaften** aus.

| Für Server mit iSCSI-Anschluss können Sie zusätzliche Konfigurationsdaten anzeigen; verwenden Sie dazu iSeries Navigator wie folgt:

- | 1. Wählen Sie im iSeries Navigator **Verwaltung integrierter Server -> iSCSI-Anschlüsse** aus.
- | 2. Wählen Sie einen der folgenden Ordner aus, um die entsprechende Liste mit Objekten anzuzeigen.
| Klicken Sie in der Liste mit der rechten Maustaste auf ein Objekt, und wählen Sie **Eigenschaften** aus.
 - | • **Lokale Hostadapter**
 - | • **Ferne Systeme**
 - | • **Serviceprozessoren**
 - | • **Verbindungssicherheit**

Über die zeichenorientierte Schnittstelle können Sie alle Konfigurationsdaten des integrierten Servers anzeigen und ändern. Die folgende Tabelle gibt einen Überblick über die relevanten CL-Befehle.

Tabelle 3.

Aufgaben	CL-Befehl
Integrierte Server an- und abhängen, Status des integrierten Servers und der Objekte prüfen, die der NWSD zugeordnet sind	WRKCFGSTS CFGTYPE(*NWS)

Tabelle 3. (Forts.)

Integrierte Server verwalten.	WRKNWSD
Leitungsbeschreibungen verwalten, die bei der Installation des integrierten Servers erstellt werden	WRKLIND
TCP/IP-Schnittstellen verwalten, die während der Serverinstallation erstellt werden	Mit TCP/IP-Netzwerkstatus arbeiten, Auswahl 1 (NETSTAT), TCP/IP konfigurieren, Auswahl 1 (CFGTCP)
NWS-Speicherbereiche überwachen	WRKNWSSTG
Netzwerkserverkonfiguration verwalten	WRKNWSCFG
NWS-Hostadapter verwalten	WRKDEVD DEVD(*NWSH)

Nachrichtenprotokollierung

Die integrierten Windows-Server protokollieren Informationen an unterschiedlichen Stellen. Wenn ein Fehler auftritt, können Sie die Ursache möglicherweise anhand dieser Informationen bestimmen. Die folgenden Abschnitte beschreiben die unterschiedlichen Nachrichtenprotokolle.

Das **Jobprotokoll des Überwachungsjobs** ist eine wichtige Informationsquelle bei der Behebung von Fehlern des integrierten Servers. Es enthält Nachrichten, die von normalen Verarbeitungsereignissen bis hin zu detaillierten Fehlernachrichten reichen. Der Überwachungsjob wird immer im Subsystem QSYSWRK mit demselben Namen wie der integrierte Server ausgeführt.


So suchen Sie in iSeries Navigator nach dem Jobprotokoll:

1. Klicken Sie auf **Ablaufsteuerung** → **Aktive Jobs**.
2. Einer der im Abschnitt QSYSWRK aufgeführten Jobs hat denselben Namen wie der integrierte Server. Klicken Sie mit der rechten Maustaste auf den Job, und wählen Sie die Option **Jobprotokoll** aus.
3. Daraufhin wird das Jobprotokoll des integrierten Servers geöffnet. Doppelklicken Sie auf eine Nachrichten-ID, um Details anzuzeigen.

So suchen Sie in der zeichenorientierten Schnittstelle nach dem Jobprotokoll:

1. Geben Sie in einer i5/OS-Befehlszeile den Befehl `WRKACTJOB SBS(QSYSWRK)` ein.
2. Einer der aufgelisteten Jobs hat denselben Namen wie der integrierte Server. Wählen Sie Auswahl 5 (Mit Job arbeiten) aus.
3. Geben Sie eine 10 ein, und drücken Sie die Eingabetaste, um das Jobprotokoll anzuzeigen.
4. Drücken Sie F10, um die detaillierten Nachrichten anzuzeigen.

Es gibt jedoch noch weitere relevante Jobprotokolle, deren Prüfung ebenfalls von Nutzen sein kann. Im

Redbook, Microsoft Windows Server 2003 Integration with iSeries, SG24-6959  befindet sich ein sehr informativer Abschnitt zu den Ereignisprotokollen des integrierten Servers unter i5/OS und an der Windows-Konsole.

Befehle für den integrierten Windows-Server im Fernzugriff ausführen

Mit i5/OS können Sie Stapelbefehle für den integrierten Server im Fernzugriff übergeben. Windows-Server-Befehle, die ohne Benutzerinteraktion im Stapelmodus ausgeführt werden, können verwendet werden. Ermitteln Sie vor der Übergabe des fernen Befehls, ob folgende Voraussetzungen erfüllt sind:

- Der Server ist unter diesem i5/OS ein integrierter Windows-Server und aktiv.
- Ihr Benutzerprofil ist auf dem integrierten Windows-Server oder in der Domäne registriert, oder Sie melden sich mit dem Profil QSECOFR an.

- Sie sind berechtigt, den Befehl SBMNWSCMD auszuführen, d. h., Sie besitzen die Sonderberechtigung *JOBCTL. Darüber hinaus benötigen Sie zumindest eine Benutzungsberechtigung (*USE) für das Objekt QSYS/SBMNWSCMD *CMD.
- Ist der LCLPDMGT-Wert des Benutzerprofils auf *YES gesetzt, muss der Systemwert QRETSVRSEC auf 1 gesetzt und das Benutzerkennwort geändert werden, oder der Benutzer muss sich nach einer Änderung von QRETSVRSEC anmelden.
- Ist der LCLPDMGT-Wert des Benutzerprofils auf *NO gesetzt, wird die Netzwerkauthentifizierung (Kerberos) verwendet. Der Benutzer muss über Anwendungen mit Kerberos-Unterstützung auf den iSeries-Betrieb zugreifen (z. B. mit der Einzelmeldung von iSeries Navigator). Weitere Informationen finden Sie unter „Unterstützung des Befehls SBMNWSCMD und der Sicherung auf Dateiebene für Kerberos V5 und EIM“ auf Seite 165.
- Das Kennwort für das i5/OS-Benutzerprofil und das Windows-Kennwort müssen übereinstimmen. Die einfachste Möglichkeit, deren Konsistenz zu gewährleisten, bietet die Benutzer- und Gruppenregistrierung.

Unter Umständen empfiehlt sich in diesem Zusammenhang auch die Lektüre des Abschnitts „Richtlinien für die Übergabe ferner Befehle“ auf Seite 163.

Befehle für den integrierten Server über iSeries Navigator ausführen

1. Wählen Sie im iSeries Navigator **Verwaltung integrierter Server** — -> **Server** aus.
2. Klicken Sie mit der rechten Maustaste auf den Server, auf dem der Stapelbefehl ausgeführt werden soll, und wählen Sie **Befehl ausführen** aus.
3. Geben Sie in der Anzeige **Befehl ausführen** den Windows-Befehl ein, der ausgeführt werden soll (z. B. dir \).
Tipp: Sie können den Befehl in einer Liste mit den letzten 10 Befehlen auswählen, die zuvor auf dem Server ausgeführt wurden.
4. Klicken Sie auf **Ausführen**, um den Befehl auszuführen.

Anmerkung:

Befehle, die über die Anzeige "Befehl ausführen" ausgeführt werden, verwenden als Authentifizierungsdomäne *PRIMARY. Verwenden Sie für andere Domänen SBMNWSCMD.

Befehle für den integrierten Windows-Server über die zeichenorientierte Schnittstelle ausführen

1. Geben Sie CALL QCMD ein, und drücken Sie die Eingabetaste.
2. Geben Sie SBMNWSCMD ein, und drücken Sie die Taste F4.
3. Geben Sie den Befehl ein, der auf dem fernen Server ausgeführt werden soll. Blättern Sie vor.
4. Geben Sie die NWSD des Servers ein, auf dem der Befehl ausgeführt werden soll, und drücken Sie die Eingabetaste.
5. Der von Ihnen verwendete i5/OS-Account sollte auf dem integrierten Server registriert sein, damit die Authentifizierung für die Ausführung des fernen Befehls erteilt werden kann. Im Feld für die Authentifizierungsdomäne können Sie angeben, wo die Authentifizierung Ihrer Benutzer-ID vorgenommen werden soll.
6. Die vom Befehl zurückgegebene Ausgabe wird in der Konsole angezeigt. Drücken Sie F10, um alle Nachrichten anzuzeigen.

Richtlinien für die Übergabe ferner Befehle

Berücksichtigen Sie bei der fernen Übergabe von Befehlen für den integrierten Windows-Server die folgenden Richtlinien:

Anmerkung: Zahlreiche, in diesem Abschnitt erläuterte SBMNWSCMD-Parameter sind nicht verfügbar, wenn die Windows-Befehle mit iSeries Navigator ausgeführt werden. Wenn Sie einen Parameter verwenden möchten, der von iSeries Navigator nicht unterstützt wird, müssen Sie den Befehl SBMNWSCMD direkt verwenden.

- Der angeforderte Befehl wird unter dem Windows-Konsolenbefehl "cmd.exe" ausgeführt. SBMNWSCMD gibt die Steuerung erst dann an die aufrufende Komponente zurück, wenn der Befehl unter Windows abgeschlossen ist und die Ausführung des Programms cmd.exe beendet ist.
- Das Feld für die Authentifizierungsdomäne von SBMNWSCMD gibt die Windows-Domäne an, in der Ihre Benutzer-ID authentifiziert wird. Bei der Standardeinstellung *PRIMARY werden Sie in der primären Domäne des Servers angemeldet, wenn dieser ein Mitgliedsserver der Domäne ist. Wenn Sie *LOCAL angeben, werden Sie direkt am Server angemeldet. Zudem kann der Name der vertrauenswürdigen Domäne angegeben werden.
- Das Benutzerprofil QSECOFR wird anders als andere Benutzerprofile gehandhabt. Unter Windows wird keine Benutzerauthentifizierung durchgeführt, wenn SBMNWSCMD vom Profil QSECOFR ausgeführt wird. Der angeforderte Befehl wird unter dem lokalen Windows-Systemaccount ausgeführt. Der lokale Systemaccount wird auch dann verwendet, wenn das Profil QSECOFR registriert ist. Er hat kein Kennwort und keine Netzwerkzugriffsrechte.
- Verwenden Sie nicht den Parameter "/u" im Windows-Befehl "cmd".
- SBMNWSCMD unterstützt die Authentifizierung mit Kerberos V5 nur eingeschränkt. Kerberos wird nur dann verwendet, wenn das Benutzerprofilattribut LCLPWDMGT auf *NO gesetzt ist. Weitere Informationen hierzu finden Sie unter „Unterstützung des Befehls SBMNWSCMD und der Sicherung auf Dateiebene für Kerberos V5 und EIM“ auf Seite 165.
- Der Dienst "Remote Command" und SBMNWSCMD können zwischen ASCII-Ausgabedaten mit mehreren Byte und Unicode-Ausgabedaten unterscheiden und diese entsprechend konvertieren.
- Es besteht die Möglichkeit, Befehle für den integrierten Windows-Server mit Hilfe der Funktionen des Befehlsinterpreters "cmd.exe" von Windows zu einer Befehlszeichenfolge zusammenzufassen. Sie können in die SBMNWSCMD-Befehlszeile beispielsweise net statistics workstation && net statistics server eingeben, um Statistiken zu erstellen. Befehle, die in einer SBMNWSCMD-Anfrage kombiniert werden, dürfen jedoch keine gemischten Daten (z. B. eine Kombination aus ASCII- und Unicode-Daten) oder Daten in gemischten Codesätzen zurückgeben. Wenn der Befehl unterschiedliche Datentypen zurückgibt, wird SBMNWSCMD unter Umständen nicht ordnungsgemäß beendet und eine Nachricht, die Sie auf die Möglichkeit eines Problems bei der Datenkonvertierung aufmerksam macht, eingeblendet. Führen Sie die Befehle in diesem Fall separat aus.
- Verwenden Sie ausschließlich Zeichen, die auf der Standardtastatur des integrierten Servers zur Verfügung stehen. In seltenen Fällen kann es vorkommen, dass in der aktiven Codepage von Windows kein Äquivalent für ein EBCDIC-Zeichen im codierten Zeichensatz der aktiven Jobs vorhanden ist. Jede Windows-Anwendung liefert andere Konvertierungsergebnisse.
- Mit "NWS-Befehl übergeben" wird die Anmeldeumgebung nicht vollständig initialisiert. Die Umgebungsvariablen des Benutzers werden zwar eingerichtet, sie stimmen jedoch unter Umständen nicht vollkommen mit den von einer interaktiven Anmeldung bereitgestellten Variablen überein. Daher können Umgebungsvariablen, für die während einer interaktiven Anmeldung im Allgemeinen benutzerspezifische Werte eingestellt werden, nicht vorhanden sein oder Standardwerte des Systems enthalten. In diesem Fall werden Scripts oder Anwendungen, die benutzerspezifische Umgebungsvariablen nutzen, ggf. nicht korrekt ausgeführt.

- Wenn sich das Stammverzeichnis Ihrer Benutzer-ID auf dem integrierten Server auf einem lokalen Server befindet, wird bei Verwendung von "NWS-Befehl übergeben" das aktuelle Verzeichnis als Stammverzeichnis eingestellt. Andernfalls wird das standardmäßige Stammverzeichnis oder das lokale Systemlaufwerk verwendet.
- Wenn das LODUSRPRF-Schlüsselwort (Benutzerprofil laden) *YES ist und wenn ein Benutzerprofil existiert, versucht SBMNWSCMD, Ihr Windows-Profil zu laden. Anschließend können Sie Befehle verwenden, die die Profilabhängigkeiten nutzen oder ändern. Fehler beim Laden des Profils werden jedoch nicht angezeigt, abgesehen von Ereignisprotokollnachrichten, die ggf. von Windows erzeugt werden. Ein Windows-Profil kann nur in einer Windows-Anmeldesitzung aktiv sein.
- Mit Hilfe von SBMNWSCMD können Anwendungen für den integrierten Server ausgeführt werden, wenn keine Benutzereingriffe erforderlich sind. Die Befehle werden in einem Hintergrundfenster und nicht in der Konsole des integrierten Servers ausgeführt. Sind bei einer Anwendung Benutzereingriffe erforderlich, z. B. wenn ein Nachrichtenfenster eingeblendet wird, ist SBMNWSCMD blockiert, da auf das Beenden eines Befehls gewartet wird und keine Eingriffe möglich sind. Wenn Sie SBMNWSCMD unter i5/OS beenden, wird versucht, den blockierten Windows-Befehl abzuschließen. Die Hintergrundbefehle werden unabhängig davon, ob sie GUI- oder konsolenbasiert sind, beendet.
- Darüber hinaus können Sie Befehle ausführen, die die Eingabe von YES oder NO erfordern. Verwenden Sie für die Eingabe der Antwort eine Eingabepipesyntax. Beispiel: echo y|format f: /fs:ntfs ermöglicht die Fortsetzung der Formatierung, nachdem der Formatierungsbefehl gefragt hat, ob die **Formatierung fortgesetzt** werden soll. Beachten Sie, dass zwischen dem "y" und dem Pipesymbol "|" kein Leerzeichen steht. Nicht alle Windows-Stapelbefehle unterstützen allerdings eine Verkettung von eingegebenen Befehlen (z. B. der Befehl "net"). Versuche, eine Standardantwort weiterzugeben, sind ggf. nicht erfolgreich.
- Sie können verhindern, dass SBMNWSCMD den Befehl protokolliert. Gehen Sie wie folgt vor, wenn die Befehlszeichenfolge sensible Daten, z. B. Kennwörter, enthält, die in den Fehlernachrichten nicht protokolliert werden sollen:
 1. Geben Sie als Befehlszeichenfolge *NOLOGCMD ein.
 2. Geben Sie in das eingeblendete Feld Befehl (nicht protokolliert) den auszuführenden Befehl ein.

Beachten Sie jedoch, dass die Option *NOLOGCMD keine Auswirkung auf Daten hat, die der Befehl zurückgibt. Werden von diesem sensible Daten zurückgegeben, können sie mit Hilfe des Parameters CMDSTDOUT an einem sicheren Ort gespeichert werden (z. B. in einer Datei des Integrated File System).
- Sie können Standardausgaben des Befehls an das Jobprotokoll (*JOBLOG), eine Spooldatei (*PRINT) oder ein IFS-Objekt (Integrated File System) weiterleiten. Standardfehlerdaten werden immer an das Jobprotokoll übergeben.

Wenn Sie *PRINT angeben, wird in der Anzeige WRKSPLF (Mit Spooldateien arbeiten) im Feld "Benutzerdaten" für die Spooldatei SBMNWSCMD angezeigt. Wenn Sie Auswahl 8 zum Anzeigen der Attribute auswählen, werden die Namen der angegebenen Befehle für den integrierten Server und der Windows-Befehle im benutzerdefinierten Datenfeld angezeigt.

Bei Angabe eines Objekts im Integrated File System muss der Pfadname vorhanden sein. Wenn der Name des Objekts im Integrated File System noch nicht existiert, wird dieses von SBMNWSCMD erstellt.
- Im Feld zur Konvertierung der Standardausgabe kann *YES angegeben werden, um die Ausgabe vom codierten Windows-Zeichensatz in die ID des codierten Zeichensatzes (CCSID) des i5/OS-Jobs zu konvertieren.

Neue IFS-Dateien werden mit der Job-CCSID erstellt. Ausgaben, die an ein vorhandenes IFS-Objekt übertragen werden, werden in die CCSID des IFS-Objekts konvertiert. Ausgaben, die in eine neue Teildatei einer vorhandenen Datei im Dateisystem /QSYS.LIB übertragen werden, werden in die CCSID der vorhandenen Datei konvertiert.
- Wenn für die Konvertierung der Standardausgabe *NO angegeben wurde, wird die Windows-Standardausgabe in das IFS-Objekt oder eine Spooldatei mit CCSID-Konversion geschrieben.

Unterstützung des Befehls SBMNWSCMD und der Sicherung auf Dateiebene für Kerberos V5 und EIM

Sicherungsoperationen auf Dateiebene auf einem integrierten Windows-Server nutzen die Funktionen von iSeries NetClient und des Befehls SBNWSCMD (NWS-Befehl übergeben). Ab i5/OS V5R3 bieten diese Funktionen eine begrenzte Unterstützung für Kerberos V5 (wird auch als iSeries-Netzwerkauthentifizierung bezeichnet). Daher sollten Sie einige Aspekte bedenken, wenn Sie die Netzwerkauthentifizierung zusammen mit diesen Funktionen verwenden wollen.

1. Um die iSeries für die Authentifizierung über Kerberos zu aktivieren, müssen Sie auf dem iSeries-Server folgende Einstellungen konfigurieren:
 - iSeries Navigator-Komponente "Sicherheit"
 - Netzwerkauthentifizierungsservice
 - Enterprise Identity Mapping (EIM)
 - Cryptographic Access Provider (5722-AC2 oder AC3)
2. iSeries NetServer sollte für die Verwendung der Authentifizierung über Kennwort/Kerberos V5 konfiguriert sein; NetServer muss aktiv sein.
3. Die Kerberos-Instanz zur Schlüsselverteilung (Kerberos Key Distribution Center, KDC) muss ein Domänencontroller für das Windows Active Directory sein (Windows 2000 Server oder Windows Server 2003). Weitere Informationen finden Sie unter „Kerberos für Windows Server 2003 Active Directory Server aktivieren“ auf Seite 115.
4. Die Kerberos-Authentifizierung wird nur dann verwendet, wenn im Benutzerprofil des i5/OS-Jobs das Attribut LCLPWDMGT auf den Wert *NO gesetzt ist. Bei der Einstellung *YES für das Attribut LCLPWDMGT wird immer die Authentifizierung über ein Kennwort verwendet.
5. Die Benutzerregistrierung unterstützt die Zuordnung eines Windows-Benutzernamens zu einem abweichenden i5/OS-Profilnamen über EIM. Daher kann die Benutzerregistrierung nach einem EIM-Register suchen, das nach dem Domännennamen des Windows Active Directory benannt ist, oder nach einem EIM-Register, das nach dem integrierten Server benannt ist. Die Benutzerregistrierung verwendet die EIM-Zuordnung unabhängig davon, ob die Kerberos-Authentifizierung verwendet werden kann. SBMNWSCMD und NetClient verwenden einen über EIM zugeordneten Namen jedoch **nur**, wenn die Kerberos-Authentifizierung verwendet wird. Daher kann die Benutzerregistrierung einen lokalen Windows-Benutzer mit einem anderen Namen als das i5/OS-Profil erstellen (wie in der EIM-Zuordnung angegeben). SBMNWSCMD und NetClient verwenden den abweichenden Windows-Namen jedoch nur dann, wenn die Kerberos-Authentifizierung ausgeführt wird (für LCLPWDMGT ist die Einstellung *NO angegeben). Andernfalls wird versucht, die Authentifizierung mit einem Windows-Namen vorzunehmen, der mit dem i5/OS-Profilnamen identisch ist.
6. Damit Windows-Befehle, die mit SBMNWSCMD übergeben werden, bei Verwendung der Kerberos-Authentifizierung eine Verbindung zu anderen Netzwerkservers herstellen können, muss der Windows-Zielservers *für die Delegation anerkannt sein*. Unter Windows 2000 ist dies bei Domänencontrollern standardmäßig aktiviert. Bei Mitgliedsservers der Domäne ist dies jedoch standardmäßig inaktiviert. Die Aktivierung kann über das Verwaltungstool **Active Directory-Benutzer und -Computer** auf einem Domänencontroller geschehen. In diesem Tool klicken Sie auf **Computer**, und wählen Sie den entsprechenden Computer aus. Klicken Sie dann auf **Computer-Eigenschaften -> Allgemein**. Anschließend wählen Sie das Markierungsfeld **Computer für Delegierungszwecke vertrauen** aus, mit dem der Computer als vertrauenswürdig definiert wird.

Hot-Spare zwischen Server-Hardware

iSeries- und xSeries-Integration und Speichervirtualisierung sind Optionen, mit denen Sie die Zuverlässigkeit und Wiederherstellbarkeit der Windows-Server-Umgebung verbessern können. Bei Problemen mit dem Windows-Server kann die Konfiguration des Servers schnell und ohne großen Aufwand auf einen anderen xSeries-Hot-Spare-Server umgeschaltet werden, ohne dass Ihr iSeries-Server neu gestartet werden muss. Dies kann die Gesamtzahl der für die verbesserte Verfügbarkeit benötigten Intel-Server reduzieren. Dadurch wird außerdem die Flexibilität erhöht, weil ein Ersatzserver aktiviert wird, der zum Schutz mehrerer Produktionsserver eingesetzt wird.

Anmerkung: Bei Servern mit iSCSI-Anschluss können auch die lokalen iSCSI-Hostadapter die Hot-Spare-Unterstützung nutzen. Weitere Informationen finden Sie unter „Hot-Spare zwischen lokalen iSCSI-Hostadaptern“ auf Seite 143.

Wie Hot-Spares in die Hardware des Servers integriert werden, ist unten beschrieben.

Mit iSeries Navigator:

1. Erweitern Sie **Verwaltung integrierter Server**.
2. Wählen Sie **Server** aus.
3. Wenn der Server, für den Sie die Hardware umschalten wollen, noch nicht heruntergefahren ist:
 - Klicken Sie mit der rechten Maustaste auf den Server, und wählen Sie die Option **Beenden** aus.
 - Klicken Sie auf der Bestätigungsanzeige auf **Beenden**.
4. Ändern Sie die Serverkonfiguration so, dass sie auf die Hot-Spare-Serverhardware zeigt.
 - a. Klicken Sie mit der rechten Maustaste auf den Server, und wählen Sie die Option **Eigenschaften** aus.
 - b. Wählen Sie die Indexzunge **System** aus, und ändern Sie eine der folgenden Angaben:
 - Wählen Sie bei Nicht-iSCSI-Servern die Option **Ressourcenname und Typ** aus.
 - Wählen Sie bei iSCSI-Servern die Option **Name der fernen Systemkonfiguration** aus.

Klicken Sie auf **OK**.
5. Um einen integrierten Server zu starten, klicken Sie mit der rechten Maustaste auf den Server, und wählen Sie **Starten** aus.

Zeichenbasierte Schnittstelle verwenden

1. Wenn der Server, für den Sie die Hardware umschalten wollen, noch nicht heruntergefahren ist, verwenden Sie den Befehl **VRYCFG (Konfiguration ändern)**, um ihn zu beenden.
2. Um die Serverkonfiguration so zu ändern, dass sie auf die Hot-Spare-Serverhardware zeigt, verwenden Sie den Befehl **CHGNWSD (NWS-Beschreibung ändern)**. So können Sie eine der folgenden Angaben ändern:
 - Für Nicht-iSCSI-Server ändern Sie den Wert des Parameters **RSRCNAME (Ressourcenname)** in den neuen IXS- oder IXA-Hardwareressourcenamen.
 - Für iSCSI-Server ändern Sie den Wert des Elements **Name des fernen Systems** im Parameter **NWSCFG (NWS-Konfiguration)** in den neuen Objektnamen der NWS-Konfiguration.
3. Um den integrierten Server zu starten, verwenden Sie den Befehl **VRYCFG (Konfiguration ändern)**.

Kapitel 9. Speicherverwaltung

Integrierte Windows-Server verfügen nicht über eigene Festplattenlaufwerke, sondern verwenden für die Speicherung von Clientdaten und die Freigabe von Netzwerkdateien i5/OS-Plattenspeicher. i5/OS-Plattenspeicher, der einem integrierten Server zugeordnet ist, wird als *NWS-Speicherbereich* bezeichnet. Die funktionale Entsprechung zur Installation eines neuen Festplattenlaufwerks in einem PC-Server besteht in der Erstellung eines NWS-Speicherbereichs unter i5/OS und seiner Verbindung mit dem integrierten Server. Die Tatsache, dass der Plattenspeicher des integrierten Servers über i5/OS verwaltet wird, wirkt sich auf die verwendeten Laufwerksgrößen, Partitionierungen und Datenträgergrößen aus. Weitere Informationen finden Sie unter „i5/OS-Speicherverwaltung“. In den Abschnitten „Vordefinierte Plattenlaufwerke für integrierte Windows-Server“ auf Seite 171 und „Plattenlaufwerke für integrierte Windows-Server“ auf Seite 168 finden Sie ebenfalls entsprechende Angaben.

Die Windows-Umgebung für die iSeries unterstützt Sie in der folgenden Weise bei der Verwaltung von Datenspeicher:

- Über i5/OS können Sie „Plattenlaufwerke des integrierten Windows-Servers unter i5/OS verwalten“ auf Seite 172.
- Sie können „Windows-Programme zur Datenträgerverwaltung mit integrierten Windows-Servern verwenden“ auf Seite 178.

i5/OS-Speicherverwaltung

Die folgende Übersicht über die Speicherverwaltungskonzepte von i5/OS richtet sich an Administratoren, die mit der Speicherverwaltung des Windows-Servers vertraut sind. Das i5/OS Speicher anders verwaltet als ein PC-Server, sind einige Techniken aus der PC-Welt in der Windows-Umgebung für die iSeries überflüssig.

i5/OS und Plattenlaufwerke

Das auf einer iSeries verwendete Betriebssystem i5/OS muss Plattenlaufwerke nicht direkt verwalten. Unterhalb des Betriebssystems verdeckt eine Softwareebene (System Licensed Internal Code, SLIC) die Plattenlaufwerke und verwaltet die Speicherung von Objekten auf den Plattenlaufwerken. Ein virtueller Adressraum wird dem vorhandenen Plattenspeicherplatz zugeordnet und anstelle von Plattenlaufwerk-IDs, Zylindern und Sektoren für die Adressierung von Objekten verwendet. Benötigte Objekte werden aus dem Adressraum der Platte in den Adressraum des Hauptspeichers kopiert („eingelagert“).

Aufgrund der Art, wie i5/OS Daten verwaltet, müssen Sie sich im Allgemeinen keine Gedanken über die Partitionierung schnell wachsender Datenbanken, die Defragmentierung von Platten oder das einheitenübergreifende Lesen und Schreiben von Daten auf dem integrierten Server machen. Der integrierte Server verwendet Einheitentreiber, um die i5/OS-Plattenlaufwerke freizugeben. Diese Einheitentreiber senden und empfangen Daten im Speicherverwaltungssystem von i5/OS. Die Speicherverwaltung von i5/OS ist für die Festplattenlaufwerke zuständig, einschließlich der Verteilung von Images der Windows-Plattenlaufwerke auf mehrere Festplattenlaufwerke und der Anwendung von RAID und Dateispiegelungen (falls konfiguriert). Defragmentierungssoftware verwaltet die logische Dateifragmentierung der Festplattenimages. Da die i5/OS-Speicherverwaltung diese Aufgaben übernimmt, ist die Ausführung eines Defragmentierungsprogramms auf dem integrierten Server nur sinnvoll, wenn „kritische Dateisystemstrukturen“ defragmentiert werden können.

Plattenpools (ASPs)

Unter i5/OS werden physische Festplattenlaufwerke in einem gemeinsamen Speicherbereich, dem sogenannten Plattenpool, der auch als Zusatzspeicherpool (Auxiliary Storage Pool - ASP) bezeichnet wird,

zusammengefasst. Wenn im Dateisystem nicht mehr genügend Speicherplatz verfügbar ist, können Sie dem Plattenpool ein neues Festplattenlaufwerk zuordnen. Der neue Speicherbereich ist dann sofort verfügbar. Jedes System verfügt über mindestens einen Plattenpool, nämlich den Systemplattenpool. Der Systemplattenpool ist immer ASP 1. Sie können zusätzliche *Benutzerplattenpools* mit den Nummern 2 bis 255 konfigurieren. Mit Hilfe von Plattenpools lassen sich i5/OS-Daten auf unterschiedliche Platten-
gruppen verteilen. Darüber hinaus können mit dieser Methode weniger wichtige Anwendungen oder Daten auf ältere, langsamere Plattenlaufwerke verschoben werden. Die Unterstützung unabhängiger ASPs (33-255) wird von iSeries Navigator bereitgestellt. Sowohl im Information Center als auch in iSeries Navigator werden ASPs als Plattenpools bezeichnet.

Plattenschutz:

i5/OS-Platten können auf zweierlei Weise geschützt werden:

- | • **Standortübergreifende Spiegelung**
| Die Funktion der standortübergreifenden Spiegelung für IASPs spiegelt Daten auf Platten, die geogra-
| fisch weit voneinander entfernt sein können.
- | • **RAID-5**
| Die RAID-5-Technik gruppiert mehrere Platten zu einem Array. Jede Platte enthält Kontrollsummen-
| informationen der anderen Platten im gleichen Array. Wenn eine Platte ausfällt, kann der RAID-5-
| Plattencontroller die zugehörigen Daten anhand der Kontrollsummeninformationen über die anderen
| Datenträger wiederherstellen. Wird eine fehlerhafte Platte durch eine neue ersetzt, kann i5/OS die
| Informationen der fehlerhaften Platte auf der neuen (und daher leeren) Platte wiederherstellen.
- | • **Spiegelung**
| Mit Hilfe der Spiegelung werden zwei Kopien der Daten auf zwei verschiedenen Platten gespeichert.
| i5/OS schreibt gleichzeitig auf beide Platten und liest die Daten auf den beiden Platten eines gespiegel-
| ten Paares ebenfalls gleichzeitig. Wenn eine der beiden Platten ausfällt, verwendet i5/OS die Informati-
| onen auf der zweiten Platte. Wird die fehlerhafte Platte ersetzt, kopiert i5/OS die Daten von der intak-
| ten Platte auf die neue Platte.

Als weitere Sicherheitsmaßnahme können Sie die gespiegelten Platten an zwei unterschiedliche Platten-
controller anschließen. Wenn in diesem Fall ein Controller und somit ein Plattensatz ausfällt, sichert der
andere Controller die Betriebsbereitschaft des Systems. Bei größeren iSeries-Modellen können Controller
an mehr als einen Bus angeschlossen werden. Werden die beiden Plattencontroller, die ein gespiegeltes
Paar ergeben, an zwei verschiedene Busse angeschlossen, wird damit die Verfügbarkeit noch weiter ver-
bessert.

Plattenpools unter i5/OS können unterschiedliche Sicherheitsstufen oder keine Sicherheit zugewiesen
werden. Sie können Anwendungen und Daten je nach Wichtigkeit in dem Plattenpool mit der geeigneten
Sicherheitsstufe speichern. Weitere Informationen zum i5/OS-Plattenschutz und zu Verfügbarkeits-
optionen finden Sie unter Sicherung und Wiederherstellung.

Plattenlaufwerke für integrierte Windows-Server

Integrierte Server sind nicht mit eigenen Plattenlaufwerken ausgestattet. i5/OS erstellt NWS-Speicher-
bereiche in seinem eigenen Dateisystem. Diese Bereiche werden von den integrierten Servern wie normale
Festplattenlaufwerke verwendet.

- | Damit ein integrierter Windows-Server ein Plattenlaufwerk für integrierte Server (NWS-Speicherbereich)
- | als Festplattenlaufwerk erkennt, müssen Sie den Server mit dem Laufwerk verbinden. Vor der Verbin-
- | dung muss das Plattenlaufwerk jedoch erstellt werden. Entsprechende Anweisungen finden Sie unter
- | „Plattenlaufwerk für integrierten Server erstellen“ auf Seite 173 und „Plattenlaufwerk mit einem integrier-
- | ten Server verbinden“ auf Seite 173. Nachdem das neue Plattenlaufwerk für integrierte Server erstellt und
- | verbunden wurde, wird es auf dem integrierten Server als neue Festplatte angezeigt. Anschließend müs-
- | sen Sie das Laufwerk formatieren, bevor es verwendet werden kann. Weitere Informationen zu diesem
- | Thema finden Sie in „Plattenlaufwerke für integrierten Server formatieren“ auf Seite 175.

Plattenlaufwerke können auf folgende Arten mit Servern verbunden werden:

1. Feste (statische) Plattenlaufwerkverbindungen ermöglichen eine Verbindung von Plattenlaufwerken mit dem Server unter Verwendung benutzerdefinierter Verbindungsfolgepositionen. Die Reihenfolge, in der der Server die Laufwerke erkennt, wird von der relativen Reihenfolge der Verbindungsfolgepositionen bestimmt. Der Server muss abgehängt werden, wenn eine feste (statische) Plattenlaufwerkverbindung hinzugefügt wird.

Anmerkung: Statische Laufwerkverbindungen werden nicht für an iSCSI angeschlossene xSeries-Server verwendet.

2. Eine Verbindung des Quorum-Ressourcenplattenlaufwerks für den Cluster wird verwendet, um das Plattenlaufwerk, das als Quorum-Ressource dient, mit den Servern im Cluster zu verbinden.
3. Die Verbindung von im Cluster gemeinsam benutzten Plattenlaufwerken ermöglicht Plattenlaufwerke in Clustern aus integrierten Servern gemeinsam zu benutzen. Ein gemeinsam benutztes Laufwerk kann nur mit Knoten verbunden werden, die ein gemeinsames Quorum-Ressourcenlaufwerk verwenden. Laufwerke dieser Art stehen allen Knoten zur Verfügung, die über die Verbindungen der Quorum-Ressource des Clusters zusammengefasst sind. Alle Knoten können auf die gemeinsam benutzten Laufwerke zugreifen, die von den Windows-Clusterdiensten auf den einzelnen Knoten gesteuert werden.

Anmerkung: Laufwerke, die als gemeinsam benutzte Laufwerke verbunden werden, müssen mit ALLEN Knoten im Cluster verbunden werden.

4. Dynamische Plattenlaufwerkverbindungen ermöglichen eine Verbindung von zusätzlichen Plattenlaufwerken mit einem integrierten Server unter Verwendung dynamisch zugeordneter Verbindungsfolgepositionen. Diese werden bei der Verbindung eines Plattenlaufwerks mit einem aktiven Server dynamisch zugeordnet. Die Verbindungsfolgeposition des Laufwerks kann angegeben werden, wird jedoch erst beim Neustart des Servers verwendet. Der integrierte Server kann während des Hinzufügens einer dynamischen Plattenlaufwerkverbindung abgeschaltet oder aktiv sein.

Der integrierte Server erkennt die Plattenlaufwerke nach dem Start in der folgenden Reihenfolge:

1. Statisch verbundene Plattenlaufwerke.
2. Quorum-Ressourcenlaufwerk des Clusters.
3. Gemeinsam benutzte Plattenlaufwerke des Clusters.
4. Dynamisch verbundene Plattenlaufwerke.

Bei Servern mit iSCSI-Anschluss erscheint das Quorum-Laufwerk des Clusters am Ende der Liste der Plattenlaufwerke. Dynamisch verlinkte Platten und gemeinsam genutzte Clusterplatten werden evtl. nicht getrennt aufgelistet.

Innerhalb der einzelnen Verbindungstypkategorien werden die Laufwerke in der Reihenfolge ihrer benutzerdefinierten Verbindungsfolgepositionen angezeigt. Wenn ein Plattenlaufwerk mit einem aktiven Server dynamisch verbunden wird, erscheint das neue Laufwerk nach allen anderen verbundenen Plattenlaufwerken.

Die folgende Tabelle zeigt die Features der virtuellen iSeries-Plattenlaufwerke, die für die verschiedenen Server-NWSDs ab i5/OS V5R4 unterstützt werden.

Unterstützte Plattenfeatures

Feature	NWSD-Typ ⁵ *WINDOWSNT oder *IXSVR mit OS-Typ *WIN32	NWSD-Typ ⁵ *ISCSI mit OS-Typ *WIN32
Anzahl fester (statischer) Verbindungen	16	0
Anzahl dynamischer Verbindungen	16	63 ¹

Feature	NWSD-Typ ⁵ *WINDOWSNT oder *IXSVR mit OS-Typ *WIN32	NWSD-Typ ⁵ *ISCSI mit OS-Typ *WIN32
Anzahl Cluster-Quorum-Verbindungen	1	1
Anzahl gemeinsam genutzter Clusterverbindungen	15	61 ¹
Maximale Anzahl virtueller Platten, die mit dem Server verlinkt werden können	48 mit Clustering ² ; sonst 32	64 mit Clustering ² ; sonst 63
Maximale Kapazität pro virtueller Platte	1000 GB	1000 GB
Maximal Gesamtkapazität virtueller Platten bei angenommenen 1000 GB pro Platte	46,9 TB mit Clustering ² ; sonst 31,3 TB	62,5 TB mit Clustering ² ; sonst 61,5 TB
Verlinken bei aktivem Server möglich?	Ja Ausnahmen: Feste Verbindungen	Ja Ausnahmen: Dynamische Verbindungen
Verbindung aufheben bei aktivem Server möglich?	Ja Ausnahmen: Feste Verbindungen; Platte kann nicht Teil eines Datenträgersatzes sein; Platte kann nicht als Datenträger in einem Verzeichnis angehängt sein.	Ja Ausnahmen: Dynamische Verbindungen 1 - 2; Platte kann nicht Teil eines Datenträgersatzes sein; Platte kann nicht als Datenträger in einem Verzeichnis angehängt sein.
Zulässige virtuelle Plattenformat-typen für das Verlinken ³	*NTFS, *NTFSQR, *FAT, *FAT32, *OPEN	*NTFS, *NTFSQR, *FAT, *FAT32, *OPEN
Zulässige virtuelle Plattenzugriffstypen für das Verlinken	Exklusive Aktualisierung, gemeinsame Aktualisierung ⁴	Exklusive Aktualisierung, gemeinsame Aktualisierung ⁴
Plattenverbindungen, die exklusive Aktualisierungsadrestypen erfordern	Alle Festplattenverbindungen und alle dynamischen Verbindungen	Alle dynamischen Verbindungen
Plattenverbindungen, die gemeinsame Aktualisierungsadrestypen erfordern	Cluster-Quorum-Verbindung und alle gemeinsamen Plattenverbindungen auf dem Cluster	Cluster-Quorum-Verbindung und alle gemeinsamen Plattenverbindungen auf dem Cluster

Anmerkungen:

1. Bei Windows-iSCSI-Servern können die dynamischen und die gemeinsamen Cluster-Platten den gleichen Bereich von Verbindungsfolgepositionen verwenden und gemischt werden. Die kombinierte Gesamtzahl dynamischer und gemeinsamer Clusterplattenverbindungen ist 63.
2. Beim Windows-Server-Clustering muss der Zugriff auf die gemeinsam genutzte Platten im Cluster mit Microsoft Cluster Service (MSCS) gesteuert werden.
3. Weitere Informationen zu diesen Formattypen enthält die Hilfe für den Befehl RTNWSSTG (NWS-Speicherbereich erstellen).
4. Wenn mehrere Server über gemeinsam genutzte Aktualisierung mit einem Datenträger verbunden sind, kann jeweils nur ein Server tatsächlich auf diese Platte Schreibzugriff haben. Beispiel: Bei Windows-Servern wird Microsoft Cluster Service (MSCS) verwendet, um zu steuern, welcher Server im Cluster gerade Schreibzugriff auf den Datenträger hat.
5. Die Hilfe für den Befehl CRTNWS (NWS-Beschreibung erstellen) beschreibt die NWSD-Typen und die zugeordneten Betriebssystemtypen.

NWS-Speicherbereiche können sich auf dem Systemplattenpool (ASP 1) von i5/OS oder einem Benutzerplattenpool befinden. Plattenlaufwerke können kopiert werden, um sie in einen anderen Plattenpool zu verschieben.

| Nachdem ein NWS-Speicherbereich erstellt und mit einem integrierten Server verbunden wurde, müssen
| Sie ihn über die Windows-Konsole formatieren. Es stehen drei unterschiedliche Plattenformate zur Aus-
| wahl. Wahrscheinlich entscheiden Sie sich für NTFS, da dies das effizienteste und sicherste Format ist.
| Mit NTFS formatierte Partitionen können bis zu 1.024.000 MB groß sein. Ein weiteres Format ist FAT-32.
| Mit FAT-32 formatierte Partitionen können zwischen 512 und 32.000 MB groß sein. Das älteste dieser For-
| mate ist FAT. Die maximal mögliche Größe für eine FAT-Partition beträgt 2.047 MB. Die vordefinierte
| Installationsquellen-Laufwerkpartition (D), die das Format FAT aufweisen muss, ist daher auf eine Größe
| von 2.047 MB begrenzt.

NWS-Speicherbereiche sind einer der beiden Netzwerkspeichertypen, die von integrierten Servern ver-
wendet werden. Integrierte Server können zudem auf i5/OS-Ressourcen zugreifen, die ein Administrator
mit iSeries NetServer im Netzwerk zur gemeinsamen Benutzung freigegeben hat.

Die Installationsprozessunterstützung für integrierte IBM iSeries-Server erstellt mehrere Laufwerke, die
bei der Installation und Ausführung der integrierten Windows-Server eingesetzt werden. Weitere Infor-
mationen enthält der Abschnitt „Vordefinierte Plattenlaufwerke für integrierte Windows-Server“.

| Weitere Informationen zum Erstellen von Laufwerken finden Sie unter „Plattenlaufwerk für integrierten
| Server erstellen“ auf Seite 173

Vordefinierte Plattenlaufwerke für integrierte Windows-Server

Der Installationsprozess für IBM iSeries Integrated Server Support erstellt zwei Plattenlaufwerke (NWS-
Speicherbereiche) für die Installation und Ausführung der integrierten Server. Weitere Informationen fin-
den Sie unter „Plattenlaufwerke für integrierte Windows-Server“ auf Seite 168. i5/OS erstellt diese
Plattenlaufwerke standardmäßig im Systemplattenpool (ASP), Sie können während der Installation jedoch
eine andere Position auswählen. i5/OS verwendet diese Plattenlaufwerke darüber hinaus zum Laden und
Starten des integrierten Servers.

Server verfügen über die folgenden vordefinierten Plattenlaufwerke:

Boot- und Systemlaufwerk (C)

Dieses Laufwerk dient als Systemlaufwerk. i5/OS bezeichnet dieses Laufwerk als *Server1*, wobei
Server für den Namen der NWS-Beschreibung (NWSD) steht. Es befindet sich im Integrated File
System und wird automatisch als erstes benutzerdefiniertes Laufwerk verbunden.

Das Laufwerk C hat eine Größe von 1.024 bis 1.024.000 MB. Sie können es als FAT definiert las-
sen. Das Laufwerk C wird automatisch in NTFS konvertiert, wenn dies durch die Größe des
Speicherbereiches erforderlich wird.

Anmerkung: Wenn Sie NWSD-Konfigurationsdateien erstellen möchten, müssen Sie berücksichti-
gen, dass diese nur bei Plattenlaufwerken unterstützt werden, die als FAT oder
FAT32 formatiert wurden. Weitere Informationen finden Sie in Kapitel 15,
„Konfigurationsdateien für NWS-Beschreibung (NWSD)“, auf Seite 261. NWSD-
Konfigurationsdateien können nicht auf Systemlaufwerke zugreifen, die in NTFS
konvertiert wurden. Zusätzliche Angaben zu den unterschiedlichen Dateisystemen
können Sie unter „Vergleich der Dateisysteme FAT, FAT32 und NTFS“ auf Seite 96
nachlesen.

Installationsquellenlaufwerk (D)

Das Laufwerk D kann zwischen 200 und 2.047 MB groß sein. Es beinhaltet eine Kopie des Win-
dows-Server-Installationscodes und des Codes von IBM iSeries Integrated Server Support. i5/OS
bezeichnet dieses Laufwerk als *Server2*, wobei *Server* für den Namen der NWS-Beschreibung
(NWSD) steht. Es befindet sich im Integrated File System und wird automatisch als zweites Lauf-
werk verbunden. i5/OS formatiert das Laufwerk D als FAT-Datenträger (File Allocation Table).

Achtung: Dieses Laufwerk muss als FAT-Laufwerk erhalten bleiben. Nehmen Sie keine Änderungen an diesem Laufwerk vor. i5/OS verwendet dieses Laufwerk für Aktualisierungen, die durch eine Änderung des Laufwerks ggf. unmöglich werden.

Anmerkung: Weitere Informationen über Server, die von i5/OS-Systemen vor V4R5 aktualisiert wurden, finden Sie unter Vordefinierte Plattenlaufwerke für integrierte Windows-Server im V5R3 iSeries Information Center.

Plattenlaufwerke des integrierten Windows-Servers unter i5/OS verwalten

Die Verwaltung der Plattenlaufwerke des integrierten Servers (NWS-Speicherbereiche) unter i5/OS umfasst die folgenden Aufgaben:

- „Vom integrierten Server auf das i5/OS-Dateisystem zugreifen“
- „Informationen zu Plattenlaufwerken des integrierten Servers abrufen“
- „Plattenlaufwerke zu integrierten Windows-Servern hinzufügen“
- „Plattenlaufwerk kopieren“ auf Seite 175
- | • „Plattenlaufwerk erweitern“ auf Seite 176
- | • „Systemlaufwerk erweitern“ auf Seite 177
- „Verbindung von Plattenlaufwerken für integrierten Windows-Server aufheben“ auf Seite 177
- „Plattenlaufwerke für integrierten Windows-Server löschen“ auf Seite 178

Vom integrierten Server auf das i5/OS-Dateisystem zugreifen

Vom integrierten Server aus greifen Sie über die IBM iSeries-Unterstützung für Windows-Netzwerkumgebung (iSeries NetServer) auf das IFS (Integrated File System) von i5/OS zu. Auf diese Weise kann unter i5/OS problemlos mit Dateisystemressourcen gearbeitet werden. Weitere Informationen über das Verwenden von iSeries NetServer finden Sie unter:

- iSeries NetServer-Dateifreigabe erstellen
- PC-Client zur Verwendung von iSeries NetServer konfigurieren
- Mit einem Windows-Client auf iSeries NetServer-Dateifreigaben zugreifen

Weitere Informationen finden Sie unter „iSeries NetServer aktivieren“ auf Seite 68.

Informationen zu Plattenlaufwerken des integrierten Servers abrufen

i5/OS. bietet Informationen zur prozentualen Verfügbarkeit eines Plattenlaufwerks des integrierten Servers (NWS-Speicherbereichs) und zu dessen Format.

So können Sie die Informationen zum Plattenlaufwerk abrufen:

- | 1. Wählen Sie im iSeries Navigator **Verwaltung integrierter Server** — -> **Alle virtuellen Platten** aus.
2. Wählen Sie eines der verfügbaren Plattenlaufwerke in der Liste aus.
3. Klicken Sie mit der rechten Maustaste auf das Plattenlaufwerk, und wählen Sie die Option **Eigenschaften** aus, oder klicken Sie in der Symbolleiste von iSeries Navigator auf das entsprechende Symbol.

Wenn Sie den CL-Befehl verwenden möchten, finden Sie unter WRKNWSSTG (Mit NWS-Speicherbereichen arbeiten) weitere Informationen.

Plattenlaufwerke zu integrierten Windows-Servern hinzufügen

Zur Erstellung und Formatierung des Speichers, den der integrierte Server als Plattenlaufwerke für Anwendungen und Daten verwendet, müssen NWS-Speicherbereiche unter i5/OS erstellt werden.

Grundlegende Informationen zu NWS-Speicherbereichen finden Sie unter „Plattenlaufwerke für integrierte Windows-Server“ auf Seite 168. So fügen Sie ein Plattenlaufwerk für einen integrierten Server (NWS-Speicherbereich) hinzu:

1. „Plattenlaufwerk für integrierten Server erstellen“.
2. „Plattenlaufwerk mit einem integrierten Server verbinden“.
3. „Plattenlaufwerke für integrierten Server formatieren“ auf Seite 175.

Plattenlaufwerk für integrierten Server erstellen

Die Erstellung eines Plattenlaufwerks für den integrierten Server (NWS-Speicherbereich) ist der erste Schritt beim Hinzufügen von Speicherbereich zu einem integrierten Windows-Server. Die für die Erstellung des Plattenlaufwerks erforderliche Zeit verhält sich proportional zur Größe des Plattenlaufwerks. Nachdem das Plattenlaufwerk erstellt wurde, muss es mit der NWS-Beschreibung des integrierten Servers verbunden (Siehe „Plattenlaufwerk mit einem integrierten Server verbinden“) und formatiert werden. Weitere Informationen zu diesem Thema finden Sie in „Plattenlaufwerke für integrierten Server formatieren“ auf Seite 175.

So erstellen Sie ein Plattenlaufwerk für den integrierten Server:

1. Wählen Sie im iSeries Navigator **Verwaltung integrierter Server** aus.
2. Klicken Sie mit der rechten Maustaste auf den Ordner **Alle virtuellen Platten** und wählen Sie **Neue Platte** aus, oder klicken Sie in der Symbolleiste von iSeries Navigator auf das entsprechende Symbol.
3. Geben Sie den Namen und die Beschreibung eines Plattenlaufwerks an.
4. Sollen Daten von einer anderen Platte kopiert werden, müssen Sie **Platte mit Daten von einer anderen Platte initialisieren** auswählen. Geben Sie anschließend die Quellenplatte an, von der die Daten kopiert werden sollen.
5. Geben Sie die Plattenkapazität an.
6. Wählen Sie einen Plattenpool (Zusatzspeicherpool) aus, zu dem die Platte hinzugefügt werden soll.
7. Wählen Sie das für die Platte zu verwendende Dateisystem aus.

Anmerkung: Wenn Sie den Datenträger von Windows aus formatieren, können Sie, falls erforderlich, ein anderes Dateisystem auswählen.

8. Wenn Sie eine Quorum-Ressourcenplatte im Windows-Cluster erstellen, geben Sie die Clusterattribute an.
 9. Wenn Sie die Platte sofort nach der Erstellung mit einem Server verbinden wollen, klicken Sie **Platte mit Server verbinden**, und geben Sie Verbindungsattribute ein.
 10. Klicken Sie auf **OK**.
- Wenn Sie den CL-Befehl verwenden möchten, finden Sie unter CRTNWSSTG weitere Informationen.

Anmerkungen:

1. Um das neue Plattenlaufwerk in einer separaten Operation zu verknüpfen, lesen Sie „Plattenlaufwerk mit einem integrierten Server verbinden“.
2. Erstellte Platten müssen mit Windows-Plattenverwaltung partitioniert und formatiert werden, oder mit dem Befehlszeilendienstprogramm DISKPART.
3. Um einen Server mit einem Plattenlaufwerk in einem unabhängigen Plattenpool (ASP) zu erstellen oder zu starten, muss die ASP-Einheit verfügbar sein.

Plattenlaufwerk mit einem integrierten Server verbinden

Damit ein integrierter Windows-Server ein Plattenlaufwerk für integrierte Server (NWS-Speicherbereich) als Festplattenlaufwerk erkennt, müssen Sie den Server mit dem Laufwerk verbinden. Vor der Verbindung muss das Plattenlaufwerk jedoch erstellt werden. Entsprechende Anweisungen finden Sie unter „Plattenlaufwerk für integrierten Server erstellen“. Nachdem das neue Plattenlaufwerk für integrierte Server erstellt und verbunden wurde, wird es auf dem integrierten Server als neue Festplatte angezeigt.

Anschließend müssen Sie das Laufwerk formatieren, bevor es verwendet werden kann. Weitere Informationen zu diesem Thema finden Sie in „Plattenlaufwerke für integrierten Server formatieren“ auf Seite 175.

So verbinden Sie ein Plattenlaufwerk mit einem integrierten Server:

1. Wenn keine dynamische Verbindung erfolgt, müssen Sie den integrierten Server beenden. Entsprechende Anweisungen finden Sie unter „Integrierten Server starten und stoppen“ auf Seite 157.
2. Wählen Sie im iSeries Navigator **Verwaltung integrierter Server** — -> **Alle virtuellen Platten** aus.
3. Klicken Sie mit der rechten Maustaste auf ein verfügbares Laufwerk, und wählen Sie **Verbindung hinzufügen** aus, oder wählen Sie das Laufwerk aus, und klicken Sie auf das entsprechende Symbol in der Symbolleiste von iSeries Navigator.
4. Wählen Sie den Server aus, mit dem die Platte verbunden werden soll.
5. Wählen Sie einen verfügbaren Verbindungstyp und die Verbindungsfolgeposition aus.
6. Um die Platte mit einem Server mit iSCSI-Anschluss zu verbinden, wählen Sie die einen der verfügbaren Speicherpfade aus.
7. Wählen Sie einen der verfügbaren Datenzugriffstypen aus.
8. Klicken Sie auf **OK**.
9. Wenn keine dynamische Verbindung erfolgt, müssen Sie den integrierten Server starten. Entsprechende Anweisungen finden Sie unter „Integrierten Server starten und stoppen“ auf Seite 157.

Wenn Sie den CL-Befehl verwenden möchten, finden Sie unter ADDNWSSTGL weitere Informationen.

Informationen zu neuen, unformatierten Plattenlaufwerken finden Sie unter „Plattenlaufwerke für integrierten Server formatieren“ auf Seite 175.

Plattenlaufwerke verwalten, wenn alle Laufwerksbuchstaben verwendet wurden

Die maximale Anzahl der Plattenlaufwerke, die mit einem integrierten Server verbunden werden können, ist größer als die Zahl der Laufwerksbuchstaben, die unter Windows zur Verfügung stehen. Da nicht alle Laufwerke über einen Laufwerksbuchstaben verfügen können, müssen andere Methoden verwendet werden, um den gesamten mit dem Server verbundenen Speicher zu nutzen. Die beiden folgenden Möglichkeiten stehen zur Verfügung, um alle mit einem Server verbundenen Plattenlaufwerke zu nutzen.

1. Ein Laufwerksbuchstabe kann aus mehreren Plattenlaufwerken bestehen, indem ein übergreifender Datenträger verwendet wird.
Anmerkung: Wenn Sie eine Datenträgergruppe erstellen, werden alle Daten auf den Partitionen, die für die neue Datenträgergruppe verwendet werden, gelöscht. Wenn Sie Ihren Server konfigurieren, sollten Sie Datenträgergruppen in Betracht ziehen.
 - a. Klicken Sie unter **Datenträgerverwaltung** mit der rechten Maustaste auf die einzelnen Laufwerksnummern, und wählen Sie im eingeblendeten Kontextmenü **In dynamische Festplatte umwandeln...** aus.
 - b. Klicken Sie mit der rechten Maustaste auf eine Festplattenpartition, und wählen Sie im Kontextmenü **Datenträger erstellen...** aus.
 - c. Erstellen Sie mit Hilfe der Anleitung im Assistenten zum Erstellen von Datenträgern einen übergreifenden Datenträger, und fügen Sie die verschiedenen Laufwerke hinzu. Anmerkung: Diese Funktion versetzt Sie bei einem vollen Datenträger in die Lage, ein Laufwerk dynamisch hinzuzufügen, ohne den Server neu zu starten.
2. Ein Plattenlaufwerk kann über dem Unterverzeichnis eines vorhandenen Laufwerksbuchstabens angehängt werden.
 - a. Erstellen Sie ein Verzeichnis unter dem Buchstaben eines Laufwerks, das mit NTFS formatiert ist. Beispiel: MD C:\MOUNT1.
 - b. Klicken Sie unter **Datenträgerverwaltung** mit der rechten Maustaste auf die Festplattenpartition, die formatiert werden soll, und wählen Sie im Kontextmenü **Formatieren** aus.

- c. Klicken Sie nach der Formatierung des Laufwerks erneut mit der rechten Maustaste auf die Festplattenpartition, und wählen Sie im Kontextmenü **Laufwerkbuchstaben und -pfad ändern...** aus.
- d. Wählen Sie **Hinzufügen** aus.
- e. Markieren Sie das Optionsfeld **In diesem NTFS-Ordner bereitgestellt**.
- f. Über die Schaltfläche **Durchsuchen** können Sie das Verzeichnis C:\MOUNT1 suchen, das in Schritt 1 erstellt wurde.
- g. Klicken Sie auf **OK**, um dieses Verzeichnis als Mountpunkt für das Plattenlaufwerk einzurichten.

Plattenlaufwerke für integrierten Server formatieren

Plattenlaufwerke von integrierten Windows-Servern (NWS-Speicherbereiche) müssen formatiert werden, bevor sie verwendet werden können. Vor der Formatierung müssen die Plattenlaufwerke jedoch erstellt werden (siehe „Plattenlaufwerk für integrierten Server erstellen“ auf Seite 173) und verbunden werden (siehe „Plattenlaufwerk mit einem integrierten Server verbinden“ auf Seite 173). Anschließend müssen Sie den Windows-Server unter i5/OS starten (siehe „Integrierten Server starten und stoppen“ auf Seite 157).

| **Anmerkung:** Server können Plattenlaufwerke dynamisch verbinden, während der Server mit dem Parameter für die dynamische Speicherverbindung des Befehls ADDNWSSTGL (NWS-Speicherbereichsverbindung hinzufügen) angehängt wird.

So formatieren Sie Plattenlaufwerke:

1. Wählen Sie an der Konsole des integrierten Windows-Servers im Menü **Start** die Optionen **Programme, Verwaltung** und **Computerverwaltung** aus.
2. Doppelklicken Sie auf **Speicher**.
3. Doppelklicken Sie auf **Datenträgerverwaltung**.
4. Um eine neue Partition zu erstellen, klicken Sie mit der rechten Maustaste auf den nicht zugeordneten Platz auf der Basisplatte, auf dem die Partition angelegt werden soll. Klicken Sie dann auf **Neue Partition**.
5. Folgen Sie der Bedienerführung zur Formatierung des neuen Laufwerks.
 - a. Geben Sie den Speicherbereichsnamen für den Datenträgerkennsatz später an.
 - b. Wählen Sie das Dateisystem aus, das Sie bei der Erstellung des Plattenlaufwerks angegeben haben.
 - c. Wählen Sie die Schnellformatierung für den gerade erstellten Speicherbereich. Er wurde bereits durch i5/OS auf niedriger Ebene formatiert, als er zugeordnet wurde.

Plattenlaufwerk kopieren

Neue Plattenlaufwerke für integrierte Windows-Server (NWS-Speicherbereiche) können erstellt werden, indem Sie die Daten von einem vorhandenen Plattenlaufwerk kopieren.

So kopieren Sie ein Plattenlaufwerk:

1. Erweitern Sie **Verwaltung integrierter Server** —> **Alle virtuellen Platten**.
2. Wählen Sie eines der verfügbaren Plattenlaufwerke in der Liste aus.
3. Klicken Sie mit der rechten Maustaste auf das Plattenlaufwerk, und wählen Sie **Neu basierend auf...** aus, oder klicken Sie in der Symbolleiste von iSeries Navigator auf das entsprechende Symbol.
4. Geben Sie den Namen und die Beschreibung eines Plattenlaufwerks an.
5. Geben Sie die Plattenkapazität an. Die Onlinehilfe enthält detaillierte Informationen zu gültigen Plattengrößen für die verschiedenen Dateisystemformate. Wenn der Datenträger beim Kopieren vergrößert werden soll, kann ein höherer Wert eingegeben werden. Bei dem erweiterten Abschnitt der Platte handelt es sich um einen nicht partitionierten freien Speicherbereich.

Anmerkung: Das Befehlszeilendienstprogramm DISKPART kann verwendet werden, um eine bestehende Partition so zu erweitern, dass zusätzlicher freier Speicherbereich zur Verfügung steht. Die Artikel zum Thema DISKPART in der Microsoft Knowledge Base enthalten weitere Informationen über Einschränkungen.

6. Wählen Sie einen Plattenpool (Zusatzspeicherpool) aus, zu dem die Platte hinzugefügt werden soll.
7. Klicken Sie auf **OK**.

Wenn Sie den CL-Befehl verwenden möchten, finden Sie unter CRTNWSSTG (NWS-Speicherbereiche erstellen) weitere Informationen.

Plattenlaufwerk erweitern


Sie können ein virtuelles Plattenlaufwerk (NWS-Speicherbereich) erweitern, ohne das Plattenlaufwerk zu kopieren. Weitere Informationen zum Erweitern eines Bootdatenträgers finden Sie unter „Systemlaufwerk erweitern“ auf Seite 177.

So erweitern Sie ein Plattenlaufwerk:

1. Erweitern Sie **Verwaltung integrierter Server -> Alle virtuellen Platten**.
2. Wählen Sie eines der verfügbaren Plattenlaufwerke in der Liste aus.
3. Klicken Sie mit der rechten Maustaste auf das Plattenlaufwerk, und wählen Sie **Eigenschaften** aus, oder klicken Sie in der Symbolleiste von iSeries Navigator auf das entsprechende Symbol.
4. Klicken Sie auf die Indexzunge **Kapazität** des Arbeitsblatts mit dem Plattenlaufwerkmerkmalen.
5. Erhöhen Sie die Plattengröße im Feld **Neue Kapazität**. Die Onlinehilfe enthält detaillierte Informationen zu gültigen Plattengrößen für die verschiedenen Dateisystemformate. Bei dem erweiterten Abschnitt der Platte handelt es sich um einen nicht partitionierten freien Speicherbereich.
6. Klicken Sie nochmals auf **OK**.
7. Wenn die Platte mit einem aktiven Server verbunden wird, erscheint eine Bestätigungsanzeige. Sie informiert darüber, dass das Plattenlaufwerk temporär dem Server nicht zur Verfügung steht, während die Platte erweitert wird. Klicken Sie auf der Bestätigungsanzeige auf **Ändern**, um zu bestätigen, dass dies akzeptabel ist, oder klicken Sie auf **Abbrechen**, um die Plattenerweiterung zu stornieren.

Anmerkungen:


1. Die Platte kann nicht mit einem aktiven Server verbunden werden, während sie erweitert wird. Wenn der Server dynamische Verbindungsaufhebung unterstützt, kann die o. a. Prozedur ausgeführt werden, während er Server aktiv ist. In diesem Fall wird die Verbindung der Platte dynamisch aufgehoben, dann wird die Platte erweitert und danach wieder dynamisch mit dem Server verbunden. Wenn daher die Platte temporär nicht für den aktiven Server zur Verfügung steht, wird sie erweitert.
2. Das Befehlszeilendienstprogramm DISKPART kann verwendet werden, um eine bestehende Partition so zu erweitern, dass zusätzlicher freier Speicherbereich zur Verfügung steht.

Anmerkung: DISKPART ist standardmäßig bei Windows Server 2003 verfügbar. Das Programm kann auch heruntergeladen werden von Microsoft  (www.microsoft.com). Die Artikel zum Thema DISKPART in der Microsoft Knowledge Base enthalten weitere Informationen über Einschränkungen.

3. Bei der Erweiterung eines bestehenden NWS-Speicherbereichs gibt es einige Einschränkungen, die davon abhängen, wie der Speicherbereich am Anfang zugeordnet wurde.

Wenn Sie den CL-Befehl verwenden möchten, finden Sie weitere Informationen unter CHGNWSSTG (Netzwerk Speicherbereich ändern). Wenn die Platte mit CHGNWSSTG erweitert wird, kann sie nicht mit einem aktiven Server verbunden werden. CHGNWSSTG hebt die Verbindung nicht automatisch auf und stellt eine erneute Verbindung her, wenn der Server aktiv ist.

Systemlaufwerk erweitern

Achtung: Vor dem Erweitern sollten Sie für Ihr Systemlaufwerk einen Backup durchführen. Weitere Informationen enthält die Website Microsoft  (www.microsoft.com).

Gehen Sie wie folgt vor, um ein Systemlaufwerk zu erweitern.

1. Beenden Sie den Server. Entsprechende Anweisungen finden Sie unter „Integrierten Server starten und stoppen“ auf Seite 157.
2. Heben Sie die Verbindung zwischen Systemlaufwerk und Server auf. Entsprechende Anweisungen finden Sie unter „Verbindung von Plattenlaufwerken für integrierten Windows-Server aufheben“.
3. Ändern Sie die Größe der Platte. Weitere Informationen finden Sie unter „Plattenlaufwerk erweitern“ auf Seite 176.
4. Verbinden Sie die Platte mit einer temporären Netzserverbeschreibung als Datenträger. Weitere Informationen finden Sie unter „Plattenlaufwerk mit einem integrierten Server verbinden“ auf Seite 173.
5. Starten Sie den temporären Server. Entsprechende Anweisungen finden Sie unter „Integrierten Server starten und stoppen“ auf Seite 157.
6. Auf der Windows-Konsole des temporären Servers erweitern Sie die Plattenpartition mit DISKPART.
7. Beenden Sie den temporären Server. Entsprechende Anweisungen finden Sie unter „Integrierten Server starten und stoppen“ auf Seite 157.
8. Heben Sie die Verbindung zwischen Platte und temporärem Server auf. Entsprechende Anweisungen finden Sie unter „Verbindung von Plattenlaufwerken für integrierten Windows-Server aufheben“.
9. Verbinden Sie die erweiterte Platte mit dem ursprünglichen Server als Systemplatte. Weitere Informationen finden Sie unter „Plattenlaufwerk mit einem integrierten Server verbinden“ auf Seite 173.
10. Starten Sie den ursprünglichen Server. Entsprechende Anweisungen finden Sie unter „Integrierten Server starten und stoppen“ auf Seite 157.

Verbindung von Plattenlaufwerken für integrierten Windows-Server aufheben

Wenn die Verbindung von Plattenlaufwerken des integrierten Servers (NWS-Speicherbereichen) aufgehoben wird, werden diese vom integrierten Server getrennt, so dass Benutzer nicht mehr auf sie zugreifen können. Weitere Informationen darüber, wann die Verbindung von Laufwerken dynamisch aufgehoben werden kann, finden Sie unter „Plattenlaufwerke für integrierte Windows-Server“ auf Seite 168.

So heben Sie die Verbindung eines Plattenlaufwerks auf:

1. Wenn die Verbindung nicht dynamisch aufgehoben wird, müssen Sie den integrierten Server beenden. Entsprechende Anweisungen finden Sie unter „Integrierten Server starten und stoppen“ auf Seite 157.
2. Wählen Sie im iSeries Navigator **Verwaltung integrierter Server** —> **Alle virtuellen Platten** aus, oder erweitern Sie **Verwaltung integrierter Server** —> **Server** —> *Servername* —> **Verbundene virtuelle Platten**, wobei *Servername* der Name des Servers ist, mit dem die Platte verbunden ist.
3. Klicken Sie mit der rechten Maustaste auf das Plattenlaufwerk, dessen Verbindung aufgehoben werden soll, und wählen Sie **Verbindung entfernen** aus, oder wählen Sie die Platte aus und klicken auf das entsprechende Symbol in der iSeries Navigator-Symbolleiste.
4. **Optional:** Um die Reihenfolge der Laufwerk zu ändern, klicken Sie auf **Verbindungsfolge komprimieren**.
5. Klicken Sie auf **Entfernen**.

Wenn Sie den CL-Befehl verwenden möchten, finden Sie weitere Informationen unter RMVNWSSTGL (NNWS-Speicherbereichsverbindung entfernen).

Plattenlaufwerke für integrierten Windows-Server löschen

Beim Löschen von Plattenlaufwerken (NWS-Speicherbereichen) gehen die Daten auf dem Plattenlaufwerk verloren. Der iSeries-Plattenspeicher wird somit freigegeben und kann für andere Zwecke verwendet werden.

Vor dem Löschen eines Plattenlaufwerks muss die Verbindung mit dem integrierten Server aufgehoben werden. Entsprechende Anweisungen finden Sie unter „Verbindung von Plattenlaufwerken für integrierten Windows-Server aufheben“ auf Seite 177. Anschließend kann es gelöscht werden.

So löschen Sie ein Plattenlaufwerk:

1. Wählen Sie im iSeries Navigator **Verwaltung integrierter Server** — -> **Alle virtuellen Platten** aus.
2. Wählen Sie eines der verfügbaren Plattenlaufwerke in der Liste aus.
3. Klicken Sie mit der rechten Maustaste auf das Plattenlaufwerk, und wählen Sie die Option **Löschen** aus, oder klicken Sie in der Symbolleiste von iSeries Navigator auf das entsprechende Symbol.
4. Klicken Sie in der Bestätigungsanzeige auf **Löschen**.

Wenn Sie den CL-Befehl verwenden möchten, finden Sie unter DLTNWSSTG (Netzwerkspeicherbereich löschen) weitere Informationen.

Plattenlaufwerke beim Entfernen eines integrierten Servers löschen

Wenn Sie einen integrierten Server manuell entfernen, müssen Sie die Plattenlaufwerke (NWS-Speicherbereiche), die mit der NWS-Beschreibung (NWSID) für diesen Server verbunden sind, ebenfalls löschen. Außerdem müssen Sie Ihre eigenen benutzerdefinierten Plattenlaufwerke löschen.

Mit dem Befehl DLTWNTSVR (Windows-Server löschen) werden Objekte gelöscht, die mit dem Befehl INSWNTSVR (Windows-Server installieren) erstellt wurden. Er entfernt die NWS-Beschreibung (NWSID), Leitungsbeschreibungen (LIND), Speicherbereiche (NWSSTG), TCP-Schnittstellen, Controllerbeschreibungen (CTLD) und Einheitenbeschreibungen (DEVD). Dies ist die empfohlene Methode, um einen integrierten Server dauerhaft aus dem System zu entfernen.

1. Zudem müssen alle Plattenlaufwerke gelöscht werden, die i5/OS als Systemlaufwerk und Installationslaufwerk für den Server vordefiniert hat.

Informationen zur Ermittlung der Plattenlaufwerke, die dem Server zugeordnet sind, finden Sie unter „Informationen zu Plattenlaufwerken des integrierten Servers abrufen“ auf Seite 172.

Windows-Programme zur Datenträgerverwaltung mit integrierten Windows-Servern verwenden

Die Plattenlaufwerke (NWS-Speicherbereiche) können mit den Windows-Programmen zur Datenträgerverwaltung auf die gleiche Weise wie einzelne physische Plattenlaufwerke verwaltet werden. Es besteht die Möglichkeit, Laufwerksbuchstaben zuzuordnen, Laufwerke zu partitionieren und Datenträgersätze zu erstellen.

Beachten Sie bei der Verwendung von Windows-Programmen zur Datenträgerverwaltung Folgendes:

- Bei der Verbindung von Plattenlaufwerken können Sie den Laufwerken relative Positionen zuordnen oder die Zuordnung von i5/OS automatisch vornehmen lassen.
- Wird für die Zuordnung eines Laufwerksbuchstabens zum optischen Laufwerk nicht die Datenträgerverwaltung verwendet, erhält dieses den nächsten verfügbaren Laufwerksbuchstaben, nachdem alle Plattenlaufwerke auf dem integrierten Server zugeordnet wurden. Wenn mit der NWS-Beschreibung keine benutzerdefinierten Plattenlaufwerke verbunden werden, erscheint das optische Laufwerk als Laufwerk E.

Kapitel 10. Einheiten gemeinsam benutzen

Einer der Vorteile von integrierten Windows-Servern ist die Möglichkeit, iSeries-Einheiten verwenden zu können. Es können optische Laufwerke, Bandlaufwerke und Drucker der iSeries auf dem Windows-Server genutzt werden.

Der Zugriff auf iSeries-Einheiten umfasst die folgenden Aufgaben:

- i5/OS und der Windows-Server verwenden unterschiedliche Namen für die Einheiten. Sie müssen sich daher zunächst über die entsprechenden Einheitenbeschreibungen und Hardwareressourcennamen informieren, die verwendet werden sollen. Weitere Informationen finden Sie unter „Einheitenbeschreibung und Hardwareressourcennamen für iSeries-Einheiten bestimmen“.
- Um ein optisches Laufwerk auf einem integrierten Server zu verwenden, müssen Sie es unter i5/OS anhängen. Weitere Informationen finden Sie unter „Optische iSeries-Laufwerke mit integrierten Windows-Servern verwenden“.
- Der Abschnitt „iSeries-Bandlaufwerke mit integrierten Windows-Servern verwenden“ auf Seite 180 enthält Informationen zur Zuordnung von Laufwerken zu integrierten Windows-Servern, zur Formatierung von Bändern, zur Übertragung von Laufwerken zwischen Servern und zur Rückübertragung von Laufwerken an i5/OS.
- Lesen Sie außerdem den Abschnitt „Vom integrierten Windows-Server auf iSeries-Druckern drucken“ auf Seite 185.

Einheitenbeschreibung und Hardwareressourcennamen für iSeries-Einheiten bestimmen

Bei der Angabe von iSeries-Einheiten unter i5/OS muss der Name der Einheitenbeschreibung verwendet werden. Bei Angabe dieser Einheiten auf dem integrierten Windows-Server muss hingegen der Hardwareressourcenname verwendet werden. Wenn sich die Namen unterscheiden und der falsche Name angegeben wird, wird die falsche Einheit verwendet.

So ermitteln Sie den Hardwareressourcennamen, um die Übereinstimmung mit dem Namen der Einheitenbeschreibung zu überprüfen:

1. Geben Sie in der i5/OS-Befehlszeile `DSPDEVD` (*Name der Einheitenbeschreibung*) ein, und drücken Sie die Eingabetaste.
2. Im Feld Ressourcenname wird der Hardwareressourcenname der Einheit angegeben. Überprüfen Sie, ob dieser mit dem Namen im Feld Einheitenbeschreibung übereinstimmt. Unterscheiden sich die Namen, muss bei der Arbeit auf die Verwendung des korrekten Namens geachtet werden. Dieser ist davon abhängig, ob Sie mit dem integrierten Windows-Server oder unter i5/OS arbeiten.

Manche Bändeinheiten verwenden mehr als eine Einheitenbeschreibung. Kassettenarchive (3590, 3570 usw.) werden sowohl als Einheiten (TAPxx) als auch als Kassettenarchive (TAPMLBxx) verzeichnet. Dabei steht xx für eine Nummer. IBM Integrated Server Support unterstützt Kassettenarchive nicht. Daher müssen sich bei Verwendung einer Einheit mit Kassettenarchivbeschreibung sowohl die Bändeinheit als auch das Kassettenarchiv im abgehängten Modus befinden, bevor die Einheit auf dem Windows-Server gesperrt wird.

Optische iSeries-Laufwerke mit integrierten Windows-Servern verwenden

Der Windows-Server kann ein optisches Laufwerk der iSeries auf die gleiche Weise wie ein lokales optisches Laufwerk verwenden. Das optische Laufwerk der iSeries wird am Windows-Server als herkömmliches lokales optisches Laufwerk unter **Arbeitsplatz** angezeigt.

Verfügt die iSeries über logische Partitionen, wird das optische Laufwerk einer einzelnen Partition zugeordnet. Es kann ausschließlich von integrierten Servern in der gleichen Partition gemeinsam benutzt werden. Darüber hinaus muss das optische Laufwerk einer NWS-Beschreibung (NWSID) zugeordnet (gesperrt) werden, um genutzt werden zu können.

Das optische Laufwerk muss angehängt werden, bevor es einem integrierten Windows-Server zugeordnet werden kann. So hängen Sie das optische Laufwerk an, wenn es noch nicht angehängt wurde:

1. Geben Sie in der i5/OS-Befehlszeile WRKCFGSTS *DEV *OPT ein, und drücken Sie die Eingabetaste.
2. Geben Sie in der Spalte Auswahl neben dem entsprechenden optischen Laufwerk (zumeist OPT01) eine 1 ein, um es anzuhängen.
3. Drücken Sie die Eingabetaste, um das optische Laufwerk anzuhängen.

So sperren Sie ein optisches Laufwerk:

1. Klicken Sie auf **Start, Programme, IBM iSeries, IBM iSeries Integrated Server Support**.
2. Erweitern Sie **IBM iSeries Integrated Server Support**.
3. Erweitern Sie den Namen der NWS-Beschreibung.
4. Wählen Sie **iSeries-Einheiten** aus.
5. Wählen Sie den Einheitennamen aus.
6. Klicken Sie mit der rechten Maustaste, und wählen Sie **Alle Tasks** sowie **Einheit sperren** aus.

Sollten bei der Nutzung des optischen Laufwerks der iSeries auf dem integrierten Windows-Server Probleme auftreten, lesen Sie die weiterführenden Informationen in „Fehler bei optischen Einheiten“ auf Seite 224.

Anmerkung:

Tritt auf dem integrierten Server vor der Freigabe eines optischen Laufwerks ein Fehler auf, ist das optische Laufwerk für i5/OS und andere integrierte Server nicht verfügbar. Das optische Laufwerk muss in diesem Fall mittels WRKCFGSTS *DEV *OPT abgehängt und erneut angehängt werden, um die Sperre aufzuheben.

Steuerung eines optischen Laufwerks vom integrierten Server an die iSeries zurückgeben

Zur Verwendung des optischen Laufwerks unter i5/OS muss dieses zunächst auf dem integrierten Server freigegeben werden. Ein optisches Laufwerk kann auf dem integrierten Server nur von der Person freigegeben werden, die es gesperrt hat oder die über Administrator- oder Sicherheitsberechtigung verfügt.

So übertragen Sie die Steuerung eines optischen Laufwerks der iSeries von einem integrierten Server auf die iSeries:

1. Klicken Sie auf **Start, Programme**, dann auf **IBM iSeries** und **IBM iSeries Integrated Server Support**.
2. Erweitern Sie **IBM iSeries Integrated Server Support**.
3. Erweitern Sie den Namen der NWS-Beschreibung.
4. Wählen Sie **iSeries-Einheiten** aus.
5. Wählen Sie die freizugebende Einheit aus.
6. Klicken Sie mit der rechten Maustaste, und wählen Sie **Alle Tasks** und **Einheit freigeben** aus.

iSeries-Bandlaufwerke mit integrierten Windows-Servern verwenden

iSeries-Bandlaufwerke sind wesentlich schneller als Laufwerke, die im Normalfall an einen PC-Server angeschlossen werden. Sie können diese Laufwerke integrierten Servern zuordnen. Auf diese Weise erreichen Sie einen schnelleren Bandzugriff als auf PC-Servern. Weitere Informationen finden Sie unter „Unterstützte iSeries-Bandlaufwerke“ auf Seite 183.

Da mehrere integrierte Server eines iSeries-Systems auf das gleiche Bandlaufwerk zugreifen können (wenn auch nicht zur gleichen Zeit), reicht ein Bandlaufwerk für mehrere integrierte Server aus.

Anmerkungen:

1. Bandlaufwerke können zwar dem integrierten Server und i5/OS zugeordnet werden, es ist jedoch nicht möglich, dass beide Systeme gleichzeitig das gleiche Bandlaufwerk verwenden. Die beiden Betriebssysteme setzen unterschiedliche Bandformate voraus. Um für den integrierten Server und i5/OS das gleiche Band zu nutzen, muss dieses neu formatiert werden.
2. Verfügt die iSeries über logische Partitionen, wird das Bandlaufwerk einer einzelnen Partition zugeordnet. Es kann ausschließlich von integrierten Servern in der gleichen Partition gemeinsam benutzt werden.

Um ein iSeries-Bandlaufwerk auf einem integrierten Server verwenden zu können, müssen Sie die folgenden Aufgaben durchführen:

- „Band unter i5/OS für integrierte Windows-Server formatieren“.
- Sie müssen ein iSeries-Bandlaufwerk einem integrierten Server zuordnen, indem Sie es in i5/OS OS/400 abhängen und auf dem integrierten Server sperren. Weitere Informationen finden Sie unter „iSeries-Bandlaufwerk einem integrierten Windows-Server zuordnen“ auf Seite 182.
- Sie müssen die Steuerung eines iSeries-Bandlaufwerks auf einen anderen integrierten Server übertragen. Weitere Informationen hierzu finden Sie in „Steuerung von optischen Laufwerken und Bandlaufwerken der iSeries zwischen integrierten Windows-Servern übertragen“ auf Seite 184.
- Sie müssen die Steuerung eines Bandlaufwerks von einem integrierten Server zurückgeben, damit es von i5/OS verwendet werden kann. Stellen Sie sicher, dass das Band korrekt formatiert ist. Weitere Informationen finden Sie unter „Steuerung eines Bandlaufwerks vom integrierten Windows-Server an die iSeries zurückgeben“ auf Seite 182.

Bei Problemen mit einem iSeries-Bandlaufwerk finden Sie unter „Bandfehler“ auf Seite 225 weitere Informationen.

Bandeinheitentreiber installieren

| Weitere Informationen über exportierte Bandeinheitentreiber finden Sie unter Supported Tape Devices for Windows Servers.

| Für die Installation von Treibern sind keine besonderen Maßnahmen erforderlich. Die im Treiber enthaltenen Anweisungen sollten ausreichen. Mit den neuen Bandtreibern sehen Bandlaufwerke genau so aus wie Laufwerke, die für xSeries-Server zur Verfügung stehen. Die Einheiten werden noch nach Typmodellnummer im Dienstprogramm für das Sperren/Freigeben angezeigt.

| Nachdem die Bandeinheit einmal gesperrt und der Server erneut gestartet wurde, kann es so aussehen, als gäbe es eine zusätzliche Instanz dieser Einheit im Removable Storage Manager bzw. in anderen Sicherungsanwendungen. Dieses Verhalten ist normal. Diese zusätzliche Instanz kann wahrscheinlich gelöscht werden, ohne dass es zu Problemen kommt. Bitte prüfen Sie Ihre Dokumentation. Die neuesten

| Informationen finden Sie unter Tape Driver Migration  auf der Website der integrierten iSeries xSeries-Lösungen

| (www.ibm.com/servers/eserver/series/integratedxseries/windows/tape_driver_migration.html).

Band unter i5/OS für integrierte Windows-Server formatieren

Damit iSeries-Bandlaufwerke von integrierten Windows-Servern verwendet werden können, muss ein Bandformat verwendet werden, das von diesen erkannt wird. Ein Band ohne Kennsatz für Windows wird über den i5/OS-Befehl INZTAP (Band initialisieren) erstellt.

So formatieren Sie ein Band:

- Legen Sie das zu formatierende Band in das iSeries-Bandlaufwerk ein.

- Geben Sie in der i5/OS-Befehlszeile Folgendes ein:

```
INZTAP DEV(tap01) NEWVOL(*NONE) NEWOWNID(*BLANK) VOL(*MOUNTED)CHECK(*NO) DENSITY(*CTGTYPE) CODE(*EBCDIC)
```

Dabei steht *tap01* für den Namen des Bandlaufwerks. Drücken Sie die Eingabetaste.

iSeries-Bandlaufwerk einem integrierten Windows-Server zuordnen

Um ein iSeries-Bandlaufwerk über die Konsole des integrierten Windows-Servers zu verwenden, muss dieses unter i5/OS abgehängt und auf dem integrierten Server gesperrt werden. Die Einheit muss vor dem Starten von Anwendungen oder zugehörigen Diensten gesperrt werden.

Anmerkung:

Manche Bandeinheiten verwenden mehr als eine Einheitenbeschreibung. Kassettenarchive (3590, 3570 usw.) werden sowohl als Einheiten (TAPxx) als auch als Kassettenarchive (TAPMLBxx) verzeichnet. Dabei steht xx für eine Nummer. IBM iSeries Integrated Server Support unterstützt Bandarchive nicht. Daher müssen Sie bei Verwendung einer Einheit mit Kassettenarchivbeschreibung sowohl die Bandeinheit als auch das Kassettenarchiv abhängen, bevor die Einheit auf dem integrierten Server gesperrt wird.

So übertragen Sie die Steuerung eines iSeries-Bandlaufwerks an einen integrierten Server:

1. Hängen Sie das Bandlaufwerk unter i5/OS ab:

- Vorgehensweise in iSeries Navigator:
 - a. Klicken Sie auf **Konfiguration und Service** —> **Hardware** —> **Bandeinheiten**.
 - b. Klicken Sie auf **Standalone-Einheiten** oder **Bandkassettenarchive**.
 - c. Klicken Sie mit der rechten Maustaste auf eine Einheit oder ein Archiv, und wählen Sie die Option **Sperren** aus.
- Vorgehensweise in der zeichenorientierten Schnittstelle von i5/OS:
 - a. Geben Sie in der i5/OS-Befehlszeile den Befehl `WRKCFGSTS *DEV *TAP` ein, und drücken Sie die Eingabetaste. Die Anzeige "Mit Konfigurationsstatus arbeiten" wird aufgerufen.

Anmerkung:

Mit `WRKCFGSTS *DEV *TAPMLB` wird eine Liste der Kassettenarchiveinheiten angezeigt.

- b. Geben Sie in die Spalte Auswahl neben dem Einheitennamen des Bandlaufwerks eine 2 ein, um das Bandlaufwerk abzuhängen.
- c. Drücken Sie die Eingabetaste. Das Bandlaufwerk wird abgehängt.

2. Sperren Sie die Bandeinheit auf einem integrierten Server.

- a. Klicken Sie auf der Windows-Konsole auf **Start** —> **Programme** —> **IBM iSeries** —> **IBM iSeries Integrated Server Support**.
- b. Erweitern Sie **IBM iSeries Integrated Server Support**.
- c. Erweitern Sie den Namen der NWS-Beschreibung.
- d. Wählen Sie **iSeries-Einheiten** aus.
- e. Wählen Sie das zu sperrende Bandlaufwerk aus.
- f. Klicken Sie mit der rechten Maustaste, und wählen Sie **Alle Tasks - Einheit sperren** aus.

3. Weitere Informationen zur Erkennung einer Bandeinheit durch eine Anwendung finden Sie unter „iSeries-Bandlaufwerke für Anwendungen identifizieren“ auf Seite 183. Bei Problemen können Sie im Abschnitt „Bandfehler“ auf Seite 225 weitere Informationen finden.

Steuerung eines Bandlaufwerks vom integrierten Windows-Server an die iSeries zurückgeben

Zur Verwendung eines gegenwärtig auf einem integrierten Server gesperrten Bandlaufwerks unter i5/OS muss dieses zunächst auf dem integrierten Server freigegeben und anschließend unter i5/OS angehängt werden. Ein Bandlaufwerk kann am Windows-Server nur von der Person freigegeben werden, die es gesperrt hat oder die über Administrator- oder Sicherheitsberechtigung verfügt.

So übertragen Sie die Steuerung eines iSeries-Bandlaufwerks von einem integrierten Windows-Server an die iSeries:

1. Geben Sie die Bändeinheit über die Konsole des integrierten Windows-Servers frei.
 - a. Klicken Sie auf **Start, Programme**, dann auf **IBM iSeries** und **IBM iSeries Integrated Server Support**.
 - b. Erweitern Sie **IBM iSeries Integrated Server Support**.
 - c. Erweitern Sie den Namen der NWS-Beschreibung.
 - d. Wählen Sie **iSeries-Einheiten** aus.
 - e. Wählen Sie das zu sperrende Bandlaufwerk aus.
 - f. Wählen Sie **Aktion, Alle Tasks** und **Einheit freigeben** aus.
2. Machen Sie die Einheit über die i5/OS-Konsole für i5/OS verfügbar.
 - Vorgehensweise in iSeries Navigator:
 - a. Klicken Sie auf **Konfiguration und Service** —> **Hardware** —> **Bändeinheiten**.
 - b. Klicken Sie auf **Standalone-Einheiten** oder **Bandkassettenarchive**.
 - c. Klicken Sie mit der rechten Maustaste auf eine Einheit oder ein Archiv, und wählen Sie die Option **Verfügbar machen** aus.
 - Vorgehensweise in der i5/OS-Befehlszeilenschnittstelle:
 - a. Geben Sie in der i5/OS-Befehlszeile den Befehl `WRKCFGSTS *DEV *TAP` ein, und drücken Sie die Eingabetaste. Die Anzeige "Mit Konfigurationsstatus arbeiten" wird aufgerufen.
 - b. Geben Sie in die Spalte "Auswahl" neben dem Einheitennamen des Bandlaufwerks (z. B. TAP01) eine 1 ein, um das Bandlaufwerk anzuhängen.
 - c. Drücken Sie die Eingabetaste, um das Bandlaufwerk anzuhängen.
 - d. Ersetzen Sie das Band durch ein für i5/OS formatiertes Band.

Unterstützte iSeries-Bandlaufwerke

Die Möglichkeit, iSeries-Bandlaufwerke auf integrierten Windows-Servern zu verwenden, hängt von den Bändeinheitenmodellen, Bandcontroller und Datenträgertypen ab.

Angaben zu den unterstützten Bändeinheiten finden Sie auf der Website [Integrated xSeries Solutions](#) .

Kassettenarchive werden zwar nicht als Archive unterstützt, können jedoch gegebenenfalls als einzelne Einheiten unterstützt werden.

Kassettenlader (Auto Cartridge Facilities - ACF - und Auto Cartridge Loaders - ACL) werden sowohl im manuellen als auch im Automatikmodus unterstützt. Befindet sich die ACL oder ACF im Automatikmodus, wird das nächste Band automatisch geladen, wenn die Sicherungsanwendung das volle Band ausgibt. Das Windows-Sicherungsprogramm führt dies automatisch ohne Benutzereingriff durch. Die Backup-Exec von Veritas zeigt ein Dialogfenster an, das eine Aufforderung zum Herausnehmen des Datenträgers aus dem Laufwerk enthält und beantwortet werden muss. (Entnehmen Sie den Datenträger aus dem Laufwerk, und klicken Sie auf OK.) Durch Klicken auf **OK** in diesem Dialogfenster wird die Sicherung normal fortgesetzt.

iSeries-Bandlaufwerke für Anwendungen identifizieren

Anwendungen verwenden keine Einheitenbeschreibungen oder Hardwareressourcennamen für Bändeinheiten, wie dies bei i5/OS der Fall ist. Sie zeigen Bändeinheiten stattdessen in einer der drei folgenden Arten an:

- Modellnummer des Herstellers
- Gerätezuordnung
- Anschluss-Bus-Ziel ID-LUN

So ermitteln Sie diese Werte:

1. Klicken Sie in der Konsole des integrierten Windows-Servers auf **Start** —> **Programme** —> **Verwaltung** —> **Computerverwaltung**.
2. Klicken Sie auf **Systemprogramme**.
3. Klicken Sie auf **Geräte-Manager**.
4. Doppelklicken Sie auf **Bandeinheiten**.
5. Klicken Sie mit der rechten Maustaste auf eine Bandeinheit.
6. Wählen Sie **Eigenschaften** aus.
7. Das Dialogfeld "Eigenschaften" verfügt über zwei Indexungen mit den Namen **Allgemein** und **Treiber**. Die Indexzunge **Allgemein** zeigt den Namen, die Busnummer, die Ziel-ID und die LUN der Einheit an.

Unterscheiden sich die Typen aller iSeries-Bandeinheiten, können die Bandeinheiten mittels dieser Informationen in Windows-Anwendungen unterschieden werden. Sind mehrere Bandeinheiten mit der gleichen Modellnummer vorhanden, müssen die einzelnen Einheiten getestet werden, um die Bandlaufwerke voneinander zu unterscheiden.

Steuerung von optischen Laufwerken und Bandlaufwerken der iSeries zwischen integrierten Windows-Servern übertragen

Werden mehrere integrierte Server ausgeführt, kann jeweils nur ein Server das Bandlaufwerk oder optische Laufwerk der iSeries verwenden. Um die Steuerung eines Bandlaufwerks oder optischen Laufwerks an einen anderen Server zu übertragen, muss dieses auf dem einen Server gesperrt und auf dem anderen Server freigegeben werden.

Anmerkung:

Verfügt die iSeries über logische Partitionen, werden das Bandlaufwerk und das optische Laufwerk einer einzelnen Partition zugeordnet und können von integrierten Servern auf einer anderen Partition nicht verwendet werden.

So übertragen Sie die Steuerung eines Bandlaufwerks oder optischen Laufwerks der iSeries zwischen integrierten Servern:

Führen Sie über die Konsole des integrierten Servers, der das Laufwerk steuert, Folgendes aus:

1. Klicken Sie auf **Start, Programme**, dann auf **IBM iSeries** und **IBM iSeries Integrated Server Support**.
2. Erweitern Sie **IBM iSeries Integrated Server Support**.
3. Erweitern Sie den Namen der NWS-Beschreibung.
4. Wählen Sie **iSeries-Einheiten** aus.
5. Wählen Sie die freizugebende Einheit aus.
6. Wählen Sie **Aktion, Alle Tasks** und **Einheit freigeben** aus.


Sperren Sie das Bandlaufwerk oder optische Laufwerk über die Konsole des integrierten Servers, der die Steuerung übernehmen soll:

1. Klicken Sie auf **Start, Programme**, dann auf **IBM iSeries** und **IBM iSeries Integrated Server Support**.
2. Erweitern Sie **IBM iSeries Integrated Server Support**.
3. Erweitern Sie den Namen der **NWS-Beschreibung**.
4. Wählen Sie **iSeries-Einheiten** aus.
5. Wählen Sie die zu sperrende Einheit aus.
6. Wählen Sie **Aktion, Alle Tasks** und **Einheit sperren** aus.

Vom integrierten Windows-Server auf iSeries-Druckern drucken

Um einen Druckjob an i5/OS zu senden, muss der i5/OS-Drucker für TCP/IP-Druck konfiguriert werden. Darüber hinaus muss der integrierte Server mit dem LPD/LPR-Protokoll für die Verwendung dieses Druckers konfiguriert werden. Auf dem integrierten Server muss zudem der Netzwerkdienst **Microsoft TCP/IP Printing** installiert sein. Weitere Informationen zum TCP/IP-Druck enthält die Dokumentation von Windows.

So konfigurieren Sie einen integrierten Server für die Druckausgabe auf i5/OS-Druckern:

1. Konfigurieren Sie den i5/OS-Drucker für TCP/IP-Druck. Weitere Informationen finden Sie im Handbuch TCP/IP Configuration and Reference. 
2. Konfigurieren Sie den integrierten Server für die Druckausgabe auf i5/OS-Druckern:
 - a. Klicken Sie im Menü **Start** von Windows 2000 Server oder Windows Server 2003 auf **Einstellungen** und **Drucker**. Das Fenster **Drucker** wird geöffnet.
 - b. Doppelklicken Sie auf das Symbol **Neuer Drucker**. Der **Druckerinstallationsassistent** wird gestartet.
 - c. Klicken Sie auf die Schaltfläche **Netzwerkdrucker**.
 - d. Geben Sie in der Anzeige **Drucker suchen** den Namen des Druckers ein, oder klicken Sie auf **Weiter**, um den Drucker zu suchen.

Kapitel 11. Benutzer des integrierten Windows-Servers unter i5/OS verwalten


Einer der Hauptvorteile der Windows-Umgebung auf iSeries ist eine synchronisierte und vereinfachte Benutzeradministration. Vorhandene i5/OS-Benutzerprofile und -Profilgruppen können auf integrierten Windows-Servern registriert werden. Dies hat zur Folge, dass sich die Benutzer am Windows-Server mit derselben Kombination aus Benutzer-ID und Kennwort anmelden können, die auch zur Anmeldung an i5/OS verwendet wird. Wenn die Benutzer ihr i5/OS-Kennwort ändern, ändert sich das Windows-Kennwort ebenfalls.

Informationen zum entsprechenden Konzept finden Sie unter „Konzepte für Benutzer und Gruppen“ auf Seite 54.

Sie können beispielsweise die folgenden Aufgaben ausführen:

- „Einzeln i5/OS-Benutzer mit iSeries Navigator in der Windows-Umgebung registrieren“
- „i5/OS-Gruppe mit iSeries Navigator in der Windows-Umgebung registrieren“ auf Seite 188
- „i5/OS-Benutzer über die zeichenorientierte Schnittstelle in der Windows-Umgebung registrieren“ auf Seite 188
- „Benutzerschablonen erstellen“ auf Seite 189
- „Ausgangsverzeichnis in einer Schablone angeben“ auf Seite 190
- „Benutzerprofilattribut LCLPMDMGT ändern“ auf Seite 190
- „EIM (Enterprise Identity Mapping)“ auf Seite 191
- „Benutzerregistrierung in der Windows-Umgebung beenden“ auf Seite 192
- „Gruppenregistrierung in der Windows-Umgebung beenden“ auf Seite 193
- „Benutzer QAS400NT“ auf Seite 193
- „Registrierung und Weitergabe auf einem integrierten Windows-Server verhindern“ auf Seite 196

Einzelnen i5/OS-Benutzer mit iSeries Navigator in der Windows-Umgebung registrieren


Wenn noch kein i5/OS-Benutzerprofil für den Benutzer existiert, muss dieses erstellt werden. Informationen zur Erstellung von i5/OS-Benutzerprofilen finden Sie in der iSeries Security Reference. 

So registrieren Sie einen einzelnen Benutzer in der Windows-Umgebung:

1. Wählen Sie im iSeries Navigator **Verwaltung integrierter Server** —> **Server** oder **Domänen** aus.
2. Klicken Sie mit der rechten Maustaste in der Liste auf eine verfügbare Windows-Domäne oder einen Server, und wählen Sie die Option **Benutzer registrieren** aus.
Anmerkung: Wählen Sie keine Windows-Arbeitsgruppe aus. Die Registrierung in einer Arbeitsgruppe wird nicht unterstützt.
3. Geben Sie den Benutzernamen ein, oder wählen Sie den Benutzernamen in der Liste aus.
4. (Optional) Wenn eine Benutzerschablone als Grundlage für die Benutzereinstellungen verwendet werden soll, müssen Sie einen Windows-Benutzer angeben, der bei der Erstellung des Benutzers unter Windows als Schablone verwendet werden soll. Bitte denken Sie daran, dass eine Änderung der Benutzerschablone nach der Registrierung des Benutzers keine Auswirkung auf den Benutzer hat.
5. Klicken Sie auf **Registrieren**.

Falls bei der Registrierung von Benutzern Probleme auftreten, finden Sie unter „Fehler bei der Benutzer- und Gruppenregistrierung“ auf Seite 232 weitere Informationen.

i5/OS-Gruppe mit iSeries Navigator in der Windows-Umgebung registrieren

Mit der folgenden Prozedur werden alle Benutzer der i5/OS-Gruppe in der Windows-Umgebung registriert. Weitere Informationen zum Erstellen von i5/OS-Benutzerprofilen und -Gruppenprofilen finden Sie in der iSeries Security Reference .

So registrieren Sie eine i5/OS-Gruppe und deren Mitglieder in der Windows-Umgebung:

1. Erweitern Sie **Verwaltung integrierter Server** —>**Server oder Domänen**.
2. Klicken Sie mit der rechten Maustaste in der Liste auf eine verfügbare Windows-Domäne oder einen Server, und wählen Sie die Option **Gruppen registrieren** aus.
Anmerkung: Wählen Sie keine Windows-Arbeitsgruppe aus. Die Registrierung in einer Arbeitsgruppe wird nicht unterstützt.
3. Geben Sie einen Gruppennamen ein, oder wählen Sie eine nicht registrierte Gruppe in der Liste aus.
4. (Optional) Um neue Benutzer mit Hilfe einer Schablone zu erstellen, müssen Sie bei der Erstellung eines Benutzers in der Gruppe unter Windows einen Windows-Benutzer angeben, der als Schablone dient. Wird eine Benutzerschablone nach der Registrierung des Benutzers geändert, hat dies keine Auswirkung auf den Benutzer.
5. Wählen Sie **Global** aus, wenn die Gruppe in einer Domäne registriert wird und in der Domäne sichtbar sein soll. Wählen Sie andernfalls **Lokal** aus. Lokale Windows-Server-Gruppen können Benutzer und globale Windows-Server-Gruppen beinhalten, während globale Windows-Server-Gruppen ausschließlich Benutzer beinhalten können. Die Windows-Onlinehilfe enthält weitere Informationen zu Gruppenarten.
6. Klicken Sie auf **Registrieren**.

Falls bei der Registrierung von Gruppen Probleme auftreten, finden Sie unter „Fehler bei der Benutzer- und Gruppenregistrierung“ auf Seite 232 weitere Informationen.

i5/OS-Benutzer über die zeichenorientierte Schnittstelle in der Windows-Umgebung registrieren

Benutzer in der Windows-Umgebung registrieren

1. Geben Sie in der zeichenorientierten Schnittstelle von i5/OS den Befehl CHGNWSUSRA ein, und drücken Sie die Taste **F4**.
2. Geben Sie im Feld **Benutzerprofil** den Namen des i5/OS-Benutzerprofils ein, das in der Windows-Umgebung registriert werden soll.
3. Drücken Sie zwei Mal die **Eingabetaste**. Jetzt sollten weitere Felder angezeigt werden.
4. **Blättern Sie vor**, und geben Sie die Windows-Domänen und die lokalen Windows-Server ein, in denen der Benutzer registriert werden soll.
5. Drücken Sie die **Eingabetaste**, um die Änderungen zu übernehmen.

Tabelle der relevanten CL-Befehle

Tabelle 4.

WRKUSRPRF	Mit i5/OS-Benutzerprofilen arbeiten
WRKNWSENR	Mit i5/OS-Benutzerprofilen arbeiten, die in der Windows-Umgebung registriert sind.
CHGNSWUSRA	i5/OS-Benutzer in der Windows-Umgebung registrieren.

Benutzerschablonen erstellen

Eine Schablone für die Benutzerregistrierung ist ein Tool, mit dessen Hilfe i5/OS-Benutzer effizienter für die Windows-Umgebung registriert werden können. Statt viele neue Benutzer mit identischen Einstellungen manuell zu konfigurieren, können Sie Benutzer mit einer Schablone für die Benutzerregistrierung automatisch konfigurieren. Weitere Informationen zu Schablonen für die Benutzerregistrierung finden Sie unter Schablonen für die Benutzerregistrierung.

So erstellen Sie eine Windows-Schablone:

Bei einer Domäne von Windows 2000 Server oder Windows Server 2003:

1. Klicken Sie in der Konsole des integrierten Servers auf **Start** → **Programme** → **Verwaltung** → **Active Directory-Benutzer und -Computer**.
2. Klicken Sie auf den Domänennamen.
3. Klicken Sie mit der rechten Maustaste auf **Benutzer**, und wählen Sie dann **Neu** → **Benutzer** aus.
4. Geben Sie in den Feldern **Benutzername** und **Anmeldename** einen eindeutigen Namen für die Schablone ein, z. B. *stduser* oder *admtemp*. Klicken Sie auf **Weiter**.
5. Es empfiehlt sich, außerdem die Auswahl des Markierungsfeldes **Benutzer muss Kennwort bei der nächsten Anmeldung ändern** zurückzunehmen und die Markierungsfelder **Benutzer kann Kennwort nicht ändern**, **Kennwort läuft nie ab** und **Konto ist deaktiviert** auszuwählen. Auf diese Weise verhindern Sie, dass ein Benutzer unter Verwendung des eigentlichen Schablonenaccounts auf den integrierten Server zugreifen kann.
6. Geben Sie für einen Schablonenaccount kein Kennwort ein.
7. Klicken Sie auf **Fertig stellen**.
8. Gruppenzugehörigkeiten können durch Doppelklicken auf den Schablonennamen in der Liste der Domänenbenutzer und -gruppen im rechten Teilfenster definiert werden. Klicken Sie auf die Indexzeile **Mitglied von** und auf **Hinzufügen**, um die gewünschten Gruppen hinzuzufügen.

Bei einem Server mit Windows 2000 Server oder Windows Server 2003:

1. Vorgehensweise in der Konsole des integrierten Servers:
 - Klicken Sie unter Windows 2000 Server auf **Start** → **Programme** → **Verwaltung** → **Computerverwaltung** → **Lokale Benutzer und Gruppen**.
 - Klicken Sie unter Windows Server 2003 auf **Start** → **Programme** → **Verwaltung** → **Computerverwaltung** → **Systemprogramme** → **Lokale Benutzer und Gruppen**.
2. Wählen Sie **Systemprogramme** → **Lokale Benutzer und Gruppen** aus.
3. Klicken Sie mit der rechten Maustaste auf **Benutzer**, und wählen Sie **Neuer Benutzer** aus.
4. Geben Sie im Feld **Benutzername** einen eindeutigen Namen der Schablone ein, z. B. *stduser* oder *admtemp*.
5. Es empfiehlt sich, außerdem die Auswahl des Markierungsfeldes **Benutzer muss Kennwort bei der nächsten Anmeldung ändern** zurückzunehmen und die Markierungsfelder **Benutzer kann Kennwort nicht ändern**, **Kennwort läuft nie ab** und **Konto ist deaktiviert** auszuwählen. Auf diese Weise verhindern Sie, dass ein Benutzer unter Verwendung des eigentlichen Schablonenaccounts auf den Windows-Server zugreifen kann.
6. Klicken Sie auf **Erstellen** und dann auf **Schließen**.
7. Klicken Sie auf **Benutzer**, oder aktualisieren Sie die Ansicht, um die neue Benutzerschablone anzuzeigen.
8. Gruppenzugehörigkeiten können durch Doppelklicken auf den Schablonennamen in der Liste der Domänenbenutzer und -gruppen im rechten Teilfenster definiert werden. Klicken Sie auf die Indexzeile **Mitglied von** und auf **Hinzufügen**, um die gewünschten Gruppen hinzuzufügen.

Benutzerschablonen können zu jeder Windows-Gruppe hinzugefügt werden, und zwar unabhängig davon, ob diese Gruppe über i5/OS registriert wurde oder nicht. Es können auch Benutzer mit einer Schablone registriert werden, die einer Gruppe angehört, die nicht über i5/OS registriert wurde. In diesem Fall können Benutzer nur mit Hilfe des Programms "Benutzer-Manager" auf dem Windows-Server aus der Gruppe entfernt werden.

Eine neu erstellte Schablone, die zur Registrierung von Administratoren verwendet werden soll, kann auch zur Windows-Server-Gruppe *Administratoren* hinzugefügt werden. Wenn Sie ein versehentliches Löschen der Windows-Benutzer unter i5/OS verhindern wollen, registrieren Sie die Schablone in der Gruppe *Permanente_AS400_Benutzer* (bzw. *Permanente_OS400_Benutzer*).

Ausgangsverzeichnis in einer Schablone angeben

Damit die Windows-Umgebung auf der iSeries Benutzer mit der größtmöglichen Portierbarkeit verwalten kann, kann für jeden Benutzer ein Ausgangsverzeichnis definiert werden. In diesem Verzeichnis werden benutzerspezifische Informationen gespeichert, die von Anwendungen generiert werden. Um den erforderlichen Aufwand zu reduzieren, können Sie die Ausgangsverzeichnisse in den Schablonenaccounts angeben, damit für jedes neue Profil, das durch den Registrierungsprozess erstellt wird, automatisch ein Ausgangsverzeichnis eingerichtet wird. Zur Gewährleistung der Skalierbarkeit dürfen Ausgangsverzeichnisse nicht auf einem bestimmten Plattenlaufwerk gesperrt werden. Die Portierbarkeit wird durch die Verwendung von Namen sichergestellt, die die allgemeine Namenskonvention (Universal Naming Convention - UNC) befolgen.

So können Sie über die Konsole des integrierten Windows-Servers die Schablonenprofile durch Aufnahme eines Ausgangsverzeichnisses anpassen:

1. Erstellen Sie den Ausgangsverzeichnisordner auf dem entsprechenden Server, und geben Sie diesen Ordner für die gemeinsame Benutzung frei.
2. Klicken Sie in einer Domäne in der Konsole des Windows-Servers auf **Start -> Programme -> Verwaltung -> Active Directory-Benutzer und -Computer**. Auf einem lokalen Server klicken Sie auf **Start -> Programme -> Verwaltung -> Computerverwaltung -> Lokale Benutzer und Gruppen**.
3. Doppelklicken Sie auf die Schablone (das Benutzermodell), um ihre Eigenschaften anzuzeigen.
4. Klicken Sie auf die Indexzunge "Profil".
5. Klicken Sie im Abschnitt für den Ausgangsordner auf **Verbinden**. Wählen Sie einen Laufwerkbuchstaben aus (beispielsweise Z:). Wechseln Sie in den Dialog **Zu:**, und geben Sie den Verzeichnispfad des Ausgangsverzeichnisses unter Verwendung eines UNC-Namens an, z. B. `\\iSeriesWin\homedirs\%username%`. In diesem Beispiel ist **iSeriesWin** der Name des Servers, auf dem sich der Ausgangsverzeichnisordner befindet, und **homedirs** ist der Name des Ausgangsverzeichnisordners. Wenn Sie anstelle des Anmelde- oder des Benutzernamens die Variable `%username%` verwenden, ersetzt der Windows-Server bei jeder Erstellung eines neuen Accounts auf dem Windows-Server den Variablennamen durch den Namen des Benutzers. Außerdem wird ein Ausgangsverzeichnis für den Benutzer erstellt.

Benutzerprofilattribut LCLPWDMGT ändern

Dieser Artikel erläutert, wie das Benutzerprofilattribut LCLPWDMGT (Lokale Kennwortverwaltung) geändert werden kann. Weitere Informationen zum Attribut LCLPWDMGT können Sie unter „Konzepte für Benutzer und Gruppen“ auf Seite 54 und „Arten von Benutzerkonfigurationen“ auf Seite 56 nachlesen.

So können Sie das Benutzerprofilattribut LCLPWDMGT in der *zeichenorientierten Umgebung* von i5/OS ändern:

1. Geben Sie den Befehl **CHGUSRPRF** sowie den Namen des Benutzerprofils ein, das Sie ändern wollen.
2. Drücken Sie die Taste **F4**, um die Bedienerführung aufzurufen.
3. Drücken Sie die Taste **F9**, um alle Attribute anzuzeigen, sowie die Taste **F11**, um deren Abkürzungen anzuzeigen.

4. Suchen Sie nach dem Attribut LCLPDMGT, und setzen Sie es auf die Einstellung *YES oder *NO.
5. Drücken Sie die Eingabetaste.

EIM (Enterprise Identity Mapping)

Was ist EIM?

Dank EIM (Enterprise Identity Mapping) können die unterschiedlichen Benutzer-IDs und Kennwörter eines Benutzers in einem gemeinsamen Account konsolidiert werden. Mit Hilfe dieses Accounts muss sich der Benutzer nur ein Mal an einem System anmelden. Anschließend arbeitet EIM quasi hinter den Kulissen mit anderen Diensten zusammen, um den Benutzer für alle seine Accounts zu authentifizieren.

Dies wird als Umgebung mit Einzelanmeldung bezeichnet. Eine Authentifizierung findet weiterhin statt, wenn ein Benutzer versucht, auf ein neues System zuzugreifen. Er wird jedoch nicht mehr zur Angabe eines Kennworts aufgefordert. EIM reduziert für Benutzer den Aufwand, mehrere Benutzernamen und Kennwörter für den Zugriff auf andere Systeme im Netzwerk zu protokollieren und zu verwalten. Sobald ein Benutzer für das Netzwerk authentifiziert wurde, kann er im gesamten Unternehmen auf Dienste und Anwendungen zugreifen, ohne sich an den unterschiedlichen Systemen mit verschiedenen Kennwörtern anmelden zu müssen.

Im Information Center ist EIM ein ganzes Thema gewidmet. Weitere Informationen finden Sie unter Enterprise Identity Mapping.

Die unterschiedlichen Möglichkeiten für die Registrierung von Benutzern in der Windows-Umgebung sind unter „Arten von Benutzerkonfigurationen“ auf Seite 56 beschrieben.

Benutzerprofilattribut EIMASSOC

Das Benutzerprofilattribut EIMASSOC dient speziell zur Konfiguration von EIM. Geben Sie in der i5/OS-Eingabeaufforderung den Befehl CHGUSRPRF sowie den Namen des Benutzerprofils ein, und drücken Sie dann die Taste F4, um die Bedienungsführung aufzurufen. Blättern Sie dann bis zum Ende vor. Dort finden Sie einen Abschnitt namens EIM-Zuordnung. Hier eine Zusammenfassung der Felder:

- **Element 1: EIM-Kennung:** Dies ist die Benutzer-ID, die EIM für den jeweiligen Benutzer verwendet. Sie ist mit einer Art Haupt-ID vergleichbar, unter der alle anderen Benutzer-IDs gespeichert werden. Wenn Sie die Einstellung *USRPRF angeben, verwendet das System den Namen Ihres i5/OS-Benutzerprofils als EIM-Kennung. Alternativ können Sie aber auch jede beliebige gültige Zeichenfolge angeben. Wenn Sie in diesem Feld *DLT eingeben und die Eingabetaste drücken, wird eine Liste mit geänderten Optionen für das Löschen von EIM-Zuordnungen angezeigt.
- **Element 2: Zuordnungstyp:** Dieser Wert gibt an, wie dem i5/OS-Benutzerprofil, das gerade bearbeitet wird, die EIM-Kennung zugeordnet wird. Bei der Windows-Umgebung auf der iSeries können i5/OS-Zielzuordnungen und Windows-Quellenzuordnungen durch Angabe der Werte *TARGET, *TGTSRC oder *ALL automatisch erstellt oder gelöscht werden.
- **Element 3: Zuordnungsaktion:** Die Sonderwerte lauten:
 - *REPLACE - Die Windows-Quellenzuordnungen werden aus allen EIM-Kennungen entfernt, die diesem Benutzerprofil zugeordnet sind. Für den registrierten Benutzer wird eine neue Windows-Quellenzuordnung zur angegebenen EIM-Kennung hinzugefügt.
 - *ADD - Für den registrierten Benutzer wird eine Windows-Quellenzuordnung hinzugefügt.
 - *REMOVE - Die Windows-Quellenzuordnung wird entfernt.
- **Element 4: EIM-Kennung erstellen:** Dieser Wert gibt an, ob die EIM-Kennung erstellt werden soll, falls sie noch nicht vorhanden ist. Die zulässigen Sonderwerte lauten *NOCRTEIMID (es wird keine EIM-Kennung erstellt) und *CRTEIMID (die EIM-Kennung wird erstellt, wenn sie nicht vorhanden ist).

Automatische und manuelle EIM-Zuordnungen

In einer typischen Umgebung mit EIM-Konfiguration, die die Einzelanmeldung verwendet, werden i5/OS-Zielzuordnungen und Windows-Quellenzuordnungen auf eine bestimmte Weise definiert. Bei der Benutzeradministration für den integrierten Windows-Server kann der Systemadministrator festlegen, dass für registrierte Benutzer automatisch EIM-Zuordnungen definiert werden sollen. Wenn für einen registrierten Benutzer beispielsweise EIMASSOC(*USRPRF *TARGET *ADD *CRTEIMID) angegeben ist, erstellt i5/OS automatisch eine i5/OS-Zielzuordnung und eine Windows-Quellenzuordnung. Die EIMASSOC-Informationen werden nicht im Benutzerprofil gespeichert und auch nicht mit dem Benutzerprofil gesichert oder zurückgespeichert. Außerdem wird die Zuordnung nicht verarbeitet und die EIMASSOC-Informationen werden ignoriert, wenn das i5/OS-System nicht für EIM konfiguriert ist.

Ist i5/OS für die Verwendung von EIM konfiguriert und die Verarbeitung von EIMASSOC für den registrierten Benutzer definiert, erstellt oder löscht die Benutzeradministration auf dem integrierten Windows-Server automatisch die Windows-Quellenzuordnungen für den Benutzer im Windows-EIM-Register. Bei einem Benutzer, der in der Windows-Umgebung lokal registriert ist, wird der vollständig qualifizierte lokale DNS-Name (DNS = Domain Name System) als Windows-EIM-Registernamen verwendet. Der Windows-EIM-Registertyp ist mit Windows 2000 definiert. Für Benutzer, die in einer Windows-Domäne registriert sind, wird als Windows-Registernamen der vollständig qualifizierte DNS-Name verwendet, und als Windows-Registertyp ist Kerberos definiert (die Groß-/Kleinschreibung wird ignoriert). Wenn das Attribut EIMASSOC für einen Benutzer definiert, i5/OS für die Verwendung von EIM konfiguriert und das Windows-EIM-Register nicht vorhanden ist, erstellt die Benutzeradministration des integrierten Windows-Servers das Windows-EIM-Register.

Unterschiedliche Namen von Windows-Benutzerprofilen durch EIM-Zuordnungen ermöglichen

Mit EIM können Benutzerprofile in einem Verzeichnissystem zugeordnet werden. In EIM kann für eine EIM-Kennung ein i5/OS-Benutzerprofil als Zielzuordnung und ein Windows-Benutzerprofil als Quellenzuordnung definiert sein. Ein Benutzeradministrator hat die Möglichkeit, eine Windows-Quellenzuordnung mit einem Windows-Benutzerprofilnamen zu definieren, der vom Benutzerprofilnamen der i5/OS-Zielzuordnung abweicht. Die Benutzeradministration des integrierten Windows-Servers verwendet das in EIM für die Windows-Benutzerregistrierung definierte Windows-Benutzerprofil für die Windows-Quellenzuordnung, sofern es vorhanden ist. Die i5/OS -Zielzuordnung muss definiert sein. Bei Verwendung der EIM-Kennung muss die Windows-Quellenzuordnung durch den Administrator definiert werden. Die Windows-Quellenzuordnung muss für dieselbe EIM-Kennung mit dem korrekten Namen und Typ für das Windows-EIM-Register definiert sein. Bei einem Benutzer, der in Windows lokal registriert ist, wird der vollständig qualifizierte Name des lokalen DNS-Servers als Windows-EIM-Registernamen verwendet. Der Windows-EIM-Registertyp ist mit EIM_REGTYPE_WIN2K definiert. Für Benutzer, die in einer Windows-Domäne registriert sind, wird als Windows-Registernamen der vollständig qualifizierte DNS-Name der Domäne verwendet, und als Windows-Registertyp ist EIM_REGTYPE_KERBEROS-IG definiert.

Benutzerregistrierung in der Windows-Umgebung beenden

So beenden Sie die Registrierung eines Benutzers in den Domänen und auf den Servern der Windows-Umgebung über die Konsole des integrierten Windows-Servers:

1. Erweitern Sie **Verwaltung integrierter Server** —>**Server oder Domänen**.
2. Erweitern Sie die Domäne bzw. den Server mit dem Benutzer, dessen Registrierung beendet werden soll.
3. Wählen Sie **Registrierte Benutzer** aus.
4. Klicken Sie mit der rechten Maustaste auf den Benutzer, dessen Registrierung beendet werden soll.
5. Wählen Sie **Registrierung aufheben** aus.
6. Klicken Sie im Bestätigungsfenster auf **Registrierung aufheben**.

Auswirkungen bei der Beendigung einer Benutzerregistrierung in der Windows-Umgebung

Wenn Sie die Benutzerregistrierung in der Windows-Umgebung beenden, wird der Benutzer auch aus der Liste der registrierten Benutzer für den Windows-Server sowie aus der Gruppe "AS400_Benutzer" (bzw. "OS400_Benutzer") des Windows-Servers entfernt. Alle Benutzer, die nicht Mitglied der Windows-Server-Gruppe "Permanente_AS400_Benutzer" (bzw. "Permanente_OS400_Benutzer") sind, werden zudem aus der Windows-Umgebung gelöscht.

Mitglieder der Windows-Server-Gruppe "Permanente_AS400_Benutzer" (bzw. "Permanente_OS400_Benutzer") können durch das Beenden der Registrierung oder das Löschen des Benutzers unter i5/OS nicht entfernt werden. Der Benutzer wird lediglich aus der Liste der registrierten Windows-Server-Benutzer und aus der Windows-Server-Gruppe "AS400_Benutzer" (bzw. "OS400_Benutzer") gelöscht.

- | Benutzer können nach dem Beenden ihrer Registrierung unter i5/OS in der Windows-Umgebung beibe-
- | halten werden. Dieses Verfahren wird nicht empfohlen, weil man diese Benutzer i5/OS-Gruppen hinzu fü-
- | gen oder Kennwörter ändern kann, ohne dass diese Aktualisierungen in der Windows-Umgebung
- | erscheinen. Abweichungen dieser Art erschweren die Überwachung von Benutzern auf beiden Systemen.

Die Benutzerregistrierung kann auf unterschiedliche Weise beendet werden. Beispiel:

- Absichtliches Beenden der Registrierung eines Benutzers.
- Löschen des i5/OS-Benutzerprofils.
- Beenden der Registrierung aller i5/OS-Gruppen, denen der Benutzer angehört.
- Entfernen des Benutzers aus der registrierten i5/OS-Gruppe, wenn der Benutzer keiner anderen registrierten Gruppe angehört.

Gruppenregistrierung in der Windows-Umgebung beenden

Wenn die Registrierung einer Gruppe in der Windows-Umgebung beendet wird, wird auch die Registrierung aller Benutzer beendet, die nur in dieser Gruppe registriert sind. Beinhaltet die Gruppe ausschließlich Mitglieder, die über sie registriert wurden, wird die Gruppe aus der Windows-Umgebung gelöscht.

Wenn die Gruppe hingegen über Mitglieder verfügt, die nicht von i5/OS aus registriert, sondern über die Windows-Umgebung hinzugefügt wurden, wird sie nicht gelöscht. Die Gruppe kann jedoch nur noch nicht registrierte Benutzer enthalten.

So beenden Sie die Registrierung einer Gruppe in den Domänen und auf den Servern der Windows-Umgebung über iSeries Navigator:

- | 1. Erweitern Sie **Verwaltung integrierter Server** —>**Server oder Domänen**.
- 2. Erweitern Sie die Domäne bzw. den Server mit der Gruppe, deren Registrierung beendet werden soll.
- 3. Wählen Sie **Registrierte Gruppen** aus.
- 4. Klicken Sie mit der rechten Maustaste auf die Gruppe, deren Registrierung beendet werden soll.
- 5. Wählen Sie **Registrierung aufheben** aus.
- 6. Klicken Sie im Bestätigungsfenster auf **Registrierung aufheben**.

Benutzer QAS400NT

In den folgenden Fällen müssen Sie den Benutzer QAS400NT definieren, damit ein i5/OS-Benutzerprofil oder -Gruppenprofil erfolgreich in einer Domäne oder auf einem lokalen Server registriert werden kann:

- Sie nehmen die Registrierung in einer Domäne über einen Mitgliedsserver vor.
- Sie nehmen die Registrierung auf einem lokalen Server vor und verwenden hierbei eine Schablone, die einen Ausgangsverzeichnispfad angibt (siehe „Ausgangsverzeichnis in einer Schablone angeben“ auf Seite 190).

- Sie nehmen die Registrierung in einer Domäne über eine i5/OS-Partition vor, die sowohl Domänencontroller als auch Mitgliedsserver der gleichen Domäne enthält.

In den folgenden Fällen müssen Sie den Benutzer QAS400NT nicht definieren, damit ein i5/OS-Benutzerprofil oder -Gruppenprofil erfolgreich in einer Domäne oder auf einem lokalen Server registriert werden kann:

- Sie nehmen die Registrierung in einer Domäne über eine i5/OS-Partition vor, die einen Domänencontroller, aber keine Mitgliedsserver in der gleichen Domäne enthält.
- Sie nehmen die Registrierung auf einem lokalen Server (oder lokal auf einem Mitgliedsserver) vor und verwenden hierbei eine Schablone, die keinen Ausgangsverzeichnispfad angibt.

So können Sie den Benutzer QAS400NT bei Bedarf definieren:

1. Erstellen Sie unter i5/OS das Benutzerprofil QAS400NT mit der Benutzerklasse *USER. Notieren Sie sich das Kennwort. Sie benötigen es im nächsten Schritt. Vergewissern Sie sich, dass das Kennwort die Regeln für Windows-Kennwörter einhält, wenn Sie die Registrierung in einer Domäne vornehmen. Weitere Informationen finden Sie unter „Überlegungen zu Kennwörtern“ auf Seite 59.
2. Erstellen Sie den Benutzeraccount QAS400NT in der Windows-Konsole des integrierten Windows-Servers, über den die Registrierung erfolgt. Bitte beachten Sie, dass die Kennwörter für das i5/OS-Benutzerprofil und den Windows-Benutzeraccount beim Benutzer QAS400NT identisch sein müssen.
 - a. QAS400NT auf einem Domänencontroller definieren

So erstellen Sie den Benutzeraccount QAS400NT auf dem Domänencontroller der Domäne, für die Sie die Registrierung einrichten:

- 1) Vorgehensweise in der Konsole des integrierten Servers:

- a)

- Klicken Sie unter Windows 2000 Server auf **Start -> Programme -> Verwaltung -> Computerverwaltung -> Lokale Benutzer und Gruppen**.
- Klicken Sie unter Windows Server 2003 auf **Start -> Programme -> Verwaltung -> Computerverwaltung -> Systemprogramme -> Lokale Benutzer und Gruppen**.

- b) Wählen Sie **Systemprogramme -> Lokale Benutzer und Gruppen** aus.

- 2) Klicken Sie mit der rechten Maustaste auf den Ordner **Benutzer** (oder auf den Ordner, zu dem der Benutzer gehört), und wählen Sie **Neu -> Benutzer** aus.
- 3) Geben Sie die folgenden Einstellungen ein:

Vollständiger Name: qas400nt
Benutzeranmeldename: qas400nt

- 4) Klicken Sie auf "Weiter". Geben Sie die folgenden Einstellungen ein:

Kennwort: (Geben Sie dasselbe Kennwort ein, das Sie für den Benutzer QAS400NT unter i5/OS verwendet haben.)
Markierungsfeld "Benutzer muss Kennwort bei der nächsten Anmeldung ändern": Auswahl zurücknehmen
Markierungsfeld "Benutzer kann Kennwort nicht ändern": Auswählen
Markierungsfeld "Kennwort verfällt nie": Auswählen

- 5) Klicken Sie auf "Weiter" und dann auf "Fertig stellen".
- 6) Klicken Sie mit der rechten Maustaste auf das Benutzersymbol QAS400NT, und wählen Sie "Eigenschaften" aus.
- 7) Klicken Sie auf die Indexzunge **Mitglied von** und dann auf "Hinzufügen".
- 8) Geben Sie im Feld Domänen-Admins ein, und klicken Sie zwei Mal auf "OK". Hierdurch erhält der Benutzeraccount QAS400NT die erforderlichen Berechtigungen zum Erstellen von Benutzern.

- b. QAS400NT auf einem lokalen Server definieren

So erstellen Sie den Benutzeraccount QAS400NT auf dem lokalen Server, für den Sie die Registrierung einrichten (bzw. auf dem Mitgliedsserver, wenn Sie die Registrierung lokal vornehmen):

- 1) Vorgehensweise in der Konsole des integrierten Servers:

- Klicken Sie unter Windows 2000 Server auf **Start -> Programme -> Verwaltung -> Computerverwaltung -> Lokale Benutzer und Gruppen**.

- Klicken Sie unter Windows Server 2003 auf **Start** —> **Programme** —> **Verwaltung** —> **Computerverwaltung** —> **Systemprogramme** —> **Lokale Benutzer und Gruppen**.
 - 2) Klicken Sie mit der rechten Maustaste auf den Ordner **Benutzer**, und wählen Sie **Neuer Benutzer...** aus.
 - 3) Geben Sie die folgenden Einstellungen ein:
 - Benutzername: qas400nt
 - Vollständiger Name: qas400nt
 - Kennwort: (Geben Sie dasselbe Kennwort ein, das Sie für den Benutzer QAS400NT unter i5/OS verwendet haben.)
 - Markierungsfeld "Benutzer muss Kennwort bei der nächsten Anmeldung ändern": Auswahl zurücknehmen
 - Markierungsfeld "Benutzer kann Kennwort nicht ändern": Auswählen
 - Markierungsfeld "Kennwort verfällt nie": Auswählen
 - 4) Klicken Sie auf "Erstellen" und dann auf "Schließen".
 - 5) Klicken Sie mit der rechten Maustaste auf das Benutzersymbol QAS400NT, und wählen Sie "Eigenschaften" aus.
 - 6) Klicken Sie auf die Indexzunge "Mitglied von" und dann auf "Hinzufügen".
 - 7) Geben Sie im Feld "Administratoren" ein, und klicken Sie dann zwei Mal auf "OK". Hierdurch erhält der Benutzeraccount QAS400NT die Berechtigungen für den Benutzeradministrationsdienst.
3. Registrieren Sie das i5/OS-Benutzerprofil QAS400NT mit iSeries Navigator oder mit dem Befehl CHGNWSUSRA in der Domäne oder auf dem lokalen Server. Eine entsprechende Beschreibung können Sie unter „Einzelnen i5/OS-Benutzer mit iSeries Navigator in der Windows-Umgebung registrieren“ auf Seite 187 nachlesen. Versuchen Sie nicht, bei der Registrierung von QAS400NT eine Schablone zu verwenden.
 4. Prüfen Sie mit iSeries Navigator oder mit dem Befehl WRKNWSEN, ob QAS400NT erfolgreich registriert wurde. Jetzt können Sie i5/OS-Benutzerprofile über Domänencontroller oder Mitgliedsserver in der Domäne registrieren.

Anmerkungen:

- Sie können das Kennwort von QAS400NT unter i5/OS ändern, da dieser Benutzer jetzt registriert ist.
- Falls mehrere integrierte Server zu unterschiedlichen Domänen auf einer gemeinsamen i5/OS-Partition gehören, müssen Sie QAS400NT für jede Domäne definieren. Alle QAS400NT-Benutzeraccounts müssen dasselbe Kennwort wie das i5/OS-Benutzerprofil haben. Eine andere Möglichkeit besteht darin, das Active Directory oder Vertrauensbeziehungen zwischen Domänen zu nutzen und die Benutzer in nur einer Domäne zu registrieren.
- Wenn Sie mehrere i5/OS-Partitionen und mehrere integrierte Server verwenden, können die Kennwörter für QAS400NT in den verschiedenen i5/OS-Partitionen unterschiedlich sein, sofern jede Domäne ausschließlich integrierte Server enthält, die nicht auf mehreren i5/OS-Partitionen definiert sind. Regelmäßig müssen alle i5/OS-Benutzerprofile QAS400NT und die entsprechenden Windows-Benutzeraccounts in einer Domäne dasselbe Kennwort verwenden.
- Das Benutzerprofil QAS400NT darf unter i5/OS nicht gelöscht werden, und sein Kennwort darf nicht verfallen. Um das Risiko eines Kennwortverfalls für QAS400NT auf einer von mehreren i5/OS-Partitionen in derselben Windows-Domäne zu verringern, empfiehlt es sich, die Weitergabe von Änderungen am Benutzerprofil QAS400NT nur auf einer i5/OS-Partition zuzulassen. Eine entsprechende Beschreibung können Sie unter „Registrierung und Weitergabe auf einem integrierten Windows-Server verhindern“ auf Seite 196 nachlesen.
- Wenn Sie mehrere i5/OS-Partitionen verwenden, die jeweils einen integrierten Windows-Server in der gleichen Domäne enthalten, kann es zu Problemen bei der Registrierung kommen, wenn das Kennwort für QAS400NT nicht auf allen i5/OS-Partitionen synchronisiert wird. Um dieses Problem nach Möglichkeit zu vermeiden, empfiehlt es sich, die Weitergabe von Änderungen am Kennwort von QAS400NT nur auf einer i5/OS-Partition zuzulassen, den anderen Partitionen jedoch die erforderliche Berechtigung für die Registrierung von Benutzern zu erteilen.

Wenn daraufhin auf einer der anderen Partitionen vergessen wird, ein Kennwort zu ändern, verhindert dies die Benutzerregistrierung nur auf dieser Partition. Eine entsprechende Beschreibung können Sie unter „Registrierung und Weitergabe auf einem integrierten Windows-Server verhindern“ nachlesen.

Registrierung und Weitergabe auf einem integrierten Windows-Server verhindern

Es gibt mehrere Gründe, aus denen es sinnvoll sein kann, die Weitergabe von i5/OS-Benutzerprofilen an einen bestimmten integrierten Server zu verhindern:

- Falls sich mehrere integrierte Server, die zur gleichen Domäne gehören, auf derselben i5/OS-Partition befinden, arbeitet die Registrierung von Benutzerprofilen standardmäßig alle integrierten Server dieser Partition durch. Zur Verringerung des Datenaustausches im Netzwerk können Sie die Registrierung für alle integrierten Server in der Domäne inaktivieren und nur noch auf einem Server zulassen. Normalerweise handelt es sich bei diesem integrierten Server um den Domänencontroller, wenn er sich in der Partition befindet.
- Falls sich mehrere integrierte Server, die zur gleichen Domäne gehören, auf unterschiedlichen i5/OS-Partition befinden, besteht die Gefahr, dass die Kennwörter von QAS400NT nicht mehr synchron sind und Probleme bei der Registrierung von Benutzerprofilen verursachen. Indem Sie die Weitergabe von QAS400NT-Benutzerprofilen auf nur einer i5/OS-Partition zulassen und auf allen anderen Partitionen verhindern, können Sie das Risiko von Registrierungsproblemen verringern. Bitte denken Sie daran, den anderen i5/OS-Partitionen die erforderliche Berechtigung für die Registrierung von Benutzern zu erteilen. Wenn daraufhin auf einer der anderen Partitionen vergessen wird, ein Kennwort zu ändern, verhindert dies die Benutzerregistrierung nur auf dieser Partition.

Es gibt zwei Methoden, mit denen Sie die Weitergabe von i5/OS-Benutzerprofilen an einen bestimmten integrierten Server verhindern können:

- Verwenden Sie hierzu den Parameter PRPDMNUSR (Domänenbenutzer weitergeben). Entsprechende Anweisungen finden Sie weiter unten.
- Erstellen Sie Datenbereiche mit dem Befehl CRTDTAARA (Datenbereich erstellen). Entsprechende Anweisungen finden Sie weiter unten.

Registrierung in einer Domäne über einen bestimmten integrierten Server mit dem Parameter PRPDMNUSR verhindern

Mit dem Parameter PRPDMNUSR (Domänenbenutzer weitergeben) des Befehls CHGNWSD (NWS-Beschreibung ändern) können Sie die Benutzerregistrierung in einer Domäne über einen bestimmten integrierten Server verhindern. Sie können diesen Parameter auch bei der Installation eines integrierten Servers mit dem Befehl INSWNTSVR (Windows-Server installieren) festlegen. Diese Option kann hilfreich sein, wenn eine einzige i5/OS-Partition mehrere integrierte Windows-Server steuert, die zur gleichen Domäne gehören, weil auf diese Weise die Registrierung nur noch auf einem der integrierten Server zugelassen und auf allen anderen integrierten Servern inaktiviert werden kann.

So verhindern Sie die Benutzerregistrierung mit dem Parameter PRPDMNUSR:

1. Wählen Sie mit dem Befehl WRKNWSD (Mit NWS-Beschreibung arbeiten) den integrierten Server aus, auf dem Sie die Registrierung stoppen wollen. (Es ist hierzu nicht erforderlich, den Server abzuhängen.)
2. Geben Sie den folgenden Befehl ein: CHGNWSD NWSD(nwsdname) PRPDMNUSR(*NO)

Anmerkungen:

- Inaktivieren Sie die Registrierung nicht auf allen integrierten Servern in der Domäne. Andernfalls werden dadurch möglicherweise alle Benutzer in den Status *UPDPND (Aktualisierung anstehend) versetzt, und es findet keine Weitergabe mehr statt.
- Es ist sinnvoll, die Benutzerregistrierung auf zwei integrierten Servern aktiviert zu lassen, damit Änderungen immer noch möglich sind, selbst wenn einer der Server ausfällt.

Registrierung von QAS400NT auf einem bestimmten integrierten Server mit dem Befehl CRTDTAARA verhindern

Mit dem Befehl CRTDTAARA (Datenbereich erstellen) können Sie die Registrierung des Benutzerprofils QAS400NT auf nur einem bestimmten integrierten Server verhindern. Die Weitergabe anderer Benutzerprofile ist hiervon nicht betroffen. Diese Option kann hilfreich sein, wenn mehrere integrierte Server zur gleichen Domäne gehören, sich jedoch auf unterschiedlichen i5/OS-Partitionen befinden. In diesem Fall ist es sinnvoll, wenn Benutzerprofile aus diesen unterschiedlichen i5/OS-Partitionen registriert werden, aber nicht mehrere QAS400NT-Benutzerprofile ihre Kennwörter an die Domäne weitergeben. So gehen Sie vor:

1. Wählen Sie eine i5/OS-Partition aus, die Sie für die Registrierung von QAS400NT in der Domäne verwenden wollen. Vergewissern Sie sich, dass QAS400NT in dieser i5/OS-Partition registriert ist.
2. Falls QAS400NT auf anderen i5/OS-Partitionen registriert ist, gehen Sie folgendermaßen vor:
 - a. Fügen Sie auf dem Domänencontroller den QAS400NT-Benutzeraccount zur Gruppe "Permanente_OS400_Benutzer" hinzu, damit er nicht gelöscht werden kann.
 - b. Löschen Sie das Benutzerprofil QAS400NT auf den i5/OS-Partitionen, auf denen Sie die Registrierung von QAS400NT verhindern wollen.
3. Erstellen Sie auf den i5/OS-Partitionen, auf denen Sie die Registrierung von QAS400NT verhindern wollen, mit dem folgenden Befehl einen Datenbereich:

```
CRTDTAARA DTAARA(QUSRSYS/nwsdnameAU) TYPE(*CHAR) LEN(10) VALUE( *NOPROP )
```

Hierbei steht **nwsdname** für den Namen der NWS-Beschreibung des integrierten Servers. Das Schlüsselwort ***NOPROP** gibt an, dass die Parameter des Benutzerprofils QAS400NT (einschließlich des Kennworts) von dieser i5/OS-Partition nicht weitergegeben werden.

4. Erstellen und registrieren Sie das Benutzerprofil QAS400NT auf allen i5/OS-Partitionen, auf denen Sie den Datenbereich erstellt haben. Denken Sie daran, dass das Kennwort von QAS400NT auf allen diesen i5/OS-Partitionen immer aktuell sein muss (also nicht verfallen darf), damit andere Benutzerprofile als QAS400NT weiterhin registriert werden können. Da das Kennwort von QAS400NT nicht weitergegeben wird, ist sein konkreter Wert ohne Bedeutung. Wichtig ist lediglich, dass das Kennwort nicht verfällt.


Kapitel 12. Integrierte Windows-Server sichern und zurückspeichern

Da die Windows-Umgebung auf der iSeries zwei Betriebssysteme (Windows 2000 Server oder Windows Server 2003 und i5/OS) verbindet, können Sicherungen mit Hilfe von i5/OS- oder Windows-Server-Dienstprogrammen oder mit Dienstprogrammen beider Systeme verwaltet werden. Weitere Informationen zur Planung der Sicherungsstrategie finden Sie unter *Sicherung, Wiederherstellung und Verfügbarkeit* sowie in der Dokumentation von Microsoft.

Zur Sicherung eines integrierten Servers auf der iSeries stehen die folgenden Basismethoden zur Verfügung:

- Sie führen eine vollständige Systemdatensicherung unter i5/OS durch. Weitere Informationen finden Sie unter *Server sichern*.
- Sie sichern die NWS-Beschreibung und die Plattenlaufwerke, die dem integrierten Server auf der iSeries zugeordnet sind. Weitere Informationen finden Sie unter *„Einem integrierten Windows-Server zugeordnete NWS-Beschreibungen und andere Objekte sichern“*.
- Sie sichern einzelne Dateien des integrierten Servers mit den i5/OS-Befehlen SAV und RST und i5/OS NetServer oder einem Sicherungsdienstprogramm. Weitere Informationen finden Sie unter *„Einzelne Dateien und Verzeichnisse des integrierten Windows-Servers sichern“* auf Seite 205.

Die Rückspeichermöglichkeiten hängen von der Art der Systemsicherung und der Art der zurückzuspeichernden Daten ab.

- Muss das gesamte System zurückgespeichert werden, erhalten Sie in dem Buch *Sicherung und Wiederherstellung*  weitere Informationen.
- Müssen eine NWS-Beschreibung und die zugeordneten i5/OS-Plattenlaufwerke zurückgespeichert werden, finden Sie unter *„NWS-Beschreibung und Plattenlaufwerke eines integrierten Windows-Servers zurückspeichern“* auf Seite 209 weitere Informationen.
- Müssen Daten des Windows-Servers (Dateien, Verzeichnisse, Freigaben und die Windows-Registrierung), die über den Befehl SAV (Sichern) gesichert wurden, zurückgespeichert werden, finden Sie unter *„Dateien des integrierten Windows-Servers zurückspeichern“* auf Seite 214 weitere Informationen.
- Verwenden Sie diese Programme zum Zurückspeichern von Dateien, die mit Sicherungsprogrammen von Windows gesichert wurden.

Einem integrierten Windows-Server zugeordnete NWS-Beschreibungen und andere Objekte sichern

Wenn ein integrierter Server installiert wird, erstellt i5/OS eine NWS-Beschreibung und vordefinierte Plattenlaufwerke für den Server, die gesichert werden müssen. Weitere Informationen finden Sie unter *„Vordefinierte Plattenlaufwerke für integrierte Windows-Server“* auf Seite 171. Einige der Plattenlaufwerke sind systembedingt (Installations- und Systemlaufwerke), andere sind benutzerdefiniert. Da der Windows-Server alle Plattenlaufwerke als einheitliches System ansieht, müssen alle Plattenlaufwerke und die NWS-Beschreibung gesichert werden, um ein ordnungsgemäßes Zurückspeichern zu ermöglichen.

Das Betriebssystem Microsoft Windows und die zum Starten des integrierten Servers erforderlichen Dateien befinden sich auf den Laufwerken C und D des Servers. Die Windows-Umgebung auf der iSeries ermöglicht es Ihnen, diese Laufwerke als NWS-Speicherbereichsobjekte des i5/OS-Netzwerkserverns zu sichern und zurückzuspeichern. Diese Objekte werden als Teil des i5/OS-Systems gesichert, wenn eine

vollständige i5/OS-Systemdatensicherung erfolgt. Es ist auch möglich, die NWS-Beschreibung und die zugeordneten Speicherbereiche explizit zu sichern. Es ist empfehlenswert, das Systemlaufwerk täglich zu sichern.

Das Sichern von Speicherbereichen ist die schnellste, aber unflexibelste Methode zum Sichern des integrierten Servers, da Dateien nicht einzeln zurückgespeichert werden können. Alternativ können Sie bestimmte einzelne Dateien und Verzeichnisse sichern, um die Sicherungen der BOOT-Platte, RDISK und Registrierung zu eliminieren, die bei PC-gestützten Windows-Servern ausgeführt würden. Weitere Informationen finden Sie unter „Einzelne Dateien und Verzeichnisse des integrierten Windows-Servers sichern“ auf Seite 205.

Die folgenden Abschnitte enthalten Informationen zur Sicherung der NWS-Beschreibung und der integrierten Servern zugeordneten Plattenlaufwerke:

- „NWS-Beschreibung eines integrierten Windows-Servers sichern“.
- „iSCSI-NWSCFGs und Prüflisten sichern“
- „Vordefinierte Plattenlaufwerke für integrierte Windows-Server sichern“ auf Seite 201.
- „Benutzerdefinierte Plattenlaufwerke für einen integrierten Windows-Server sichern“ auf Seite 202.
- „Benutzerregistrierungsdaten sichern und zurückspeichern“ auf Seite 203.
- Eine Tabelle der Benutzer- und Systemobjekte, die gesichert werden können, finden Sie unter „Zu sichernde Objekte und ihre Positionen unter i5/OS“ auf Seite 203.

NWS-Beschreibung eines integrierten Windows-Servers sichern

Wenn die zugeordneten Speicherbereichsobjekte eines integrierten Windows-Servers gesichert werden, muss auch die NWS-Beschreibung (NWSD) gesichert werden. Andernfalls ist der Windows-Server möglicherweise nicht in der Lage, Elemente wie beispielsweise Windows-Server-Dateisystemberechtigungen erneut zu erstellen. Mit dem Befehl SAVCFG (Konfiguration sichern) können Sie eine NWS-Beschreibung sichern:

1. Geben Sie in der i5/OS-Befehlszeile SAVCFG ein.
2. Drücken Sie die Eingabetaste, damit i5/OS die NWS-Beschreibung sichert.

| **Anmerkung:** Der Befehl SAVCFG (Konfiguration sichern) sichert die der NWS-Beschreibung zugeordneten Objekte.

| NWSH-Konfiguration eines Windows-Servers mit iSCSI-Anschluss sichern

| Mit dem Befehl SAVCFG (Konfiguration sichern) können Sie eine NWSH-Konfiguration sichern:

- | 1. Geben Sie in der i5/OS-Befehlszeile SAVCFG ein.
- | 2. Drücken Sie die Eingabetaste, damit i5/OS die NWSH-Konfiguration sichert.

| iSCSI-NWSCFGs und Prüflisten sichern

Die zusätzlichen Konfigurationsobjekte für Server mit iSCSI HBA-Anschluss werden in der Bibliothek QUSRSYS gespeichert. Zu diesen Objekten gehören die NWS-Konfigurationsobjekte (Typ *NWSCFG) und ein zugeordnetes Prüflistenobjekt (Typ *VLDDL).

Anmerkung: Die *NWSCFG- und *VLDDL-Objekte haben den gleichen Namen.

Um die NWS-Konfigurations- und Prüflistenobjekte zu sichern, wird der Befehl **SAVOBJ (Objekt sichern)** verwendet:

1. Erfolgt die Sicherung auf Band, muss gewährleistet sein, dass ein für i5/OS formatiertes Band eingelegt wurde.
2. Fahren Sie den Windows-Server herunter, um alle Objektsperren freizugeben.

3. Geben Sie in einer i5/OS-Befehlszeile den Befehl SAV0BJ ein, und drücken Sie F4.
4. Geben Sie im Feld **Objekte** die NWSCFG-Namen an. Wenn Standardnamen verwendet wurden, geben Sie den generischen Namen nwsdname* an.
5. Geben Sie im Feld **Bibliothek** den Wert QUSRSYS an.
6. Werden die Objekte auf Band gesichert, muss der Name der Bändeinheit im Feld **Einheit** angegeben werden (z. B. TAP01). Soll eine Sicherungsdatei anstelle des Bandes verwendet werden, geben Sie *SAVF als Einheit an, und aktivieren Sie die Datenkomprimierungsoption.
7. Geben Sie im Feld **Objektart** sowohl *NWSCFG als auch *VLDL an.
8. Wird eine Sicherungsdatei verwendet, drücken Sie F10, um zusätzliche Parameter anzuzeigen.
9. Geben Sie im Feld **Sicherungsdatei** den Pfad der Sicherungsdatei ein (z. B. winbackup/nwscfg).
10. Wird eine Sicherungsdatei verwendet, müssen Sie vorblättern und den Wert für "Datenkomprimierung" in *YES ändern.

Vordefinierte Plattenlaufwerke für integrierte Windows-Server sichern

Wenn ein integrierter Server installiert wird, erstellt i5/OS das System- und das Installationsquellenlaufwerk (C und D) als vordefinierte Laufwerke, die gesichert werden müssen. Weitere Informationen finden Sie unter „Vordefinierte Plattenlaufwerke für integrierte Windows-Server“ auf Seite 171.

Anmerkungen:

1. Eine Windows-NWS-Beschreibung, ihre vordefinierten Plattenlaufwerke und alle benutzerdefinierten Plattenlaufwerke, die ihr zugeordnet sind, müssen als eine Einheit angesehen werden. Sie müssen gleichzeitig gesichert und zurückspeichert werden. Sie bilden zusammen ein vollständiges System und sollten auch als solches behandelt werden. Andernfalls ist der integrierte Server möglicherweise nicht in der Lage, Elemente wie beispielsweise Windows-Server-Dateisystemberechtigungen erneut zu erstellen.
2. Wurde der Server unter OS/400 vor V4R5 erstellt, siehe Vordefinierte Plattenlaufwerke für integrierte Windows-Server sichern, die unter OS/400 vor V4R5 erstellt wurden im iSeries Information Center für V5R3.

So sichern Sie Plattenlaufwerke (NWS-Speicherbereiche), die sich im Systemplattenpool (System-ASP) unter i5/OS befinden:

1. Erfolgt die Sicherung auf Band, muss gewährleistet sein, dass ein für i5/OS formatiertes Band eingelegt wurde.
2. Beenden Sie den integrierten Server, um zu verhindern, dass andere Benutzer die Dateien während der Sicherung aktualisieren. Entsprechende Anweisungen finden Sie unter „Integrierten Server starten und stoppen“ auf Seite 157.
3. Geben Sie in der i5/OS-Befehlszeile den Befehl SAV ein, und drücken Sie F4.
4. Wird der Speicherbereich auf Band gesichert, müssen Sie den Namen der Bändeinheit (z. B. /QSYS.LIB/TAP01.DEVD) im Feld *Einheit* angeben.
Wird der Speicherbereich in einer Sicherungsdatei statt auf Band gesichert, müssen Sie den Pfad der Sicherungsdatei als Einheit angeben. Wird beispielsweise eine Sicherungsdatei namens MYSAVF in der Bibliothek WINBACKUP verwendet, muss /QSYS.LIB/WINBACKUP.LIB/MYSAVF.FILE als Einheit angegeben werden.
5. Im Feld Name unter Objekte: muss /QFPNWSSTG/stgsp' angegeben werden, wobei stgspc für den Namen des NWS-Speicherbereichs steht.
 - Für das Systemlaufwerk (C) muss /QFPNWSSTG/nwsdname1 verwendet werden.
 - Um Laufwerk D zu sichern, verwenden Sie den Befehl /QFPNWSSTG/nwsdname2.
 - Für Speicherbereiche, die in einem Benutzerplattenpool (Benutzer-ASP) erstellt wurden, muss /QFPNWSSTG/stgspc sowie dev/QASPnn/stgspc.UDFS verwendet werden, wobei stgspc für den Namen des NWS-Speicherbereichs und nn für die Nummer des Benutzer-ASP steht.

- Für einen unabhängigen Plattenpool (ASP) muss /QFPNWSSTG/stgspc sowie dev/independent ASP name/stgspc.UDFS verwendet werden, wobei independent ASP name für den Namen des unabhängigen ASP und stgspc für den Namen des NWS-Speicherbereichs steht.
6. Geben Sie die Werte für alle anderen gewünschten Parameter an, und drücken Sie die Eingabetaste, um den Speicherbereich zu sichern.
 7. Starten Sie dann den integrierten Server. Weitere Informationen hierzu finden Sie in „Integrierten Server starten und stoppen“ auf Seite 157.

Der Abschnitt „Zu sichernde Objekte und ihre Positionen unter i5/OS“ auf Seite 203 enthält weitere Informationen.

Benutzerdefinierte Plattenlaufwerke für einen integrierten Windows-Server sichern

Die Plattenlaufwerke, die für den integrierten Server erstellt werden, befinden sich im Integrated File System (IFS). Um diese Speicherbereiche aus dem Benutzer-ASP unter i5/OS zu sichern, verwenden Sie den Befehl SAV (Sichern).

Anmerkung:

Eine NWS-Beschreibung (NWSD), ihre vordefinierten Plattenlaufwerke und alle benutzerdefinierten Plattenlaufwerke, die ihr zugeordnet sind, müssen als eine Einheit angesehen werden. Sie müssen gleichzeitig gesichert und zurückgespeichert werden. Sie bilden zusammen ein vollständiges System und sollten auch als solches behandelt werden. Andernfalls ist der integrierte Server möglicherweise nicht in der Lage, Elemente wie beispielsweise Windows-Server-Dateisystemberechtigungen erneut zu erstellen.

So sichern Sie Plattenlaufwerke in einem Benutzer-ASP unter i5/OS:


1. Erfolgt die Sicherung auf Band, muss gewährleistet sein, dass ein für i5/OS formatiertes Band eingelegt wurde.
2. Bei NWS-Speicherbereichen, die in einem unabhängigen Plattenpool erstellt wurden, muss sichergestellt werden, dass die ASP-Einheit vor der Sicherung des Objekts "dev/independent ASP name/stgspc.UDFS" angehängt wurde.
3. Beenden Sie den integrierten Server durch Abhängen der NWS-Beschreibung, um zu verhindern, dass andere Benutzer die Dateien während der Sicherung aktualisieren. Weitere Informationen hierzu finden Sie in „Integrierten Server starten und stoppen“ auf Seite 157.
4. Geben Sie in der i5/OS-Befehlszeile den Befehl SAV ein, und drücken Sie F4.
5. Wird der Speicherbereich auf Band gesichert, müssen Sie den Namen der Bandeinheit (z. B. /QSYS.LIB/TAP01.DEVD) im Feld *Einheit* angeben.
Wird der Speicherbereich in einer Sicherungsdatei statt auf Band gesichert, müssen Sie den Pfad der Sicherungsdatei als Einheit angeben. Wird beispielsweise eine Sicherungsdatei namens MYSAVF in der Bibliothek WINBACKUP verwendet, muss /QSYS.LIB/WINBACKUP.LIB/MYSAVF.FILE als Einheit angegeben werden. Verwenden Sie andernfalls den Namen der Einheit (z. B. /QSYS.LIB/TAP01.DEVD).
6. Im Feld *Name* unter Objekte: muss /QFPNWSSTG/stgspc sowie dev/QASPnn/stgspc.UDFS angegeben werden, wobei stgspc für den Namen des NWS-Speicherbereichs und *nn* für die Nummer des Plattenpools steht.
 - Für Speicherbereiche, die in einem Benutzerplattenpool (Benutzer-ASP) erstellt wurden, muss /QFPNWSSTG/stgspc sowie dev/QASPnn/stgspc.UDFS verwendet werden, wobei stgspc für den Namen des NWS-Speicherbereichs und *xx* für die Nummer des Benutzer-ASP steht.
 - Für einen unabhängigen Plattenpool (ASP) muss /QFPNWSSTG/stgspc sowie dev/independent ASP name/stgspc.UDFS verwendet werden, wobei independent ASP name für den Namen des unabhängigen ASP und stgspc für den Namen des NWS-Speicherbereichs steht.
7. Geben Sie die Werte für alle anderen gewünschten Parameter an, und drücken Sie die Eingabetaste, um den Speicherbereich zu sichern.

8. Starten Sie den Windows-Server. Entsprechende Anweisungen finden Sie unter „Integrierten Server starten und stoppen“ auf Seite 157.

Weitere Informationen zum Sichern von Systemobjekten und zu den entsprechenden Sicherungsbefehlen finden Sie unter Sicherung, Wiederherstellung und Verfügbarkeit.

Die oben beschriebene Vorgehensweise ermöglicht das Sichern und Zurückspeichern vollständiger NWS-Speicherbereiche. Zum Sichern und Zurückspeichern einzelner Dateien kann nun die neue Funktion verwendet werden, die unter „Einzelne Dateien und Verzeichnisse des integrierten Windows-Servers sichern“ auf Seite 205 beschrieben ist.

Benutzerregistrierungsdaten sichern und zurückspeichern

In gewissen Fällen müssen die Benutzerprofile und deren Registrierungsdaten zurückgespeichert werden. Im Folgenden werden die Befehle von i5/OS und die API zur Sicherung und Rückspeicherung von Benutzerprofilen für die Registrierung auf dem integrierten Windows-Server beschrieben. Weitere Informationen zur Sicherung und Rückspeicherung von Sicherheitsdaten unter i5/OS finden Sie unter "Backup and Recovery of Security Information" in der iSeries Security Reference .

Benutzerprofile können mit Hilfe des Befehls SAVSECDTA oder der API QRSRAVO gesichert werden. Zur Unterstützung der Registrierung auf dem integrierten Windows-Server muss der i5/OS-Systemwert QRETSVRSEC auf 1 gesetzt werden. Benutzerprofile, die mit dem Befehl SAVSECDTA oder der API QRSRAVO gesichert wurden, können über den Befehl RSTUSRPRF und die Angabe des Parameters USRPRF(*ALL) zurückgespeichert werden. Wurde der Parameter USRPRF(*ALL) nicht angegeben, können Benutzerprofile unter Verwendung des Parameters und Wertes SECDTA(*PWDGRP) zurückgespeichert werden.

Wenn Sie Benutzerprofile mit der API QRSRAVO sichern und ein vorheriger Zielreleasewert verwendet wird, werden die Definitionen für die Benutzerprofilregistrierung nicht zurückgespeichert. Nach dem Zurückspeichern der Benutzerprofile muss daher die Registrierung definiert werden. Verwenden Sie zur Definition der Registrierung iSeries Navigator oder den Befehl CHGNWSUSRA (NWS-Benutzerattribute ändern).

Benutzerprofile müssen mittels der oben angegebenen Methoden für die Registrierung auf dem integrierten Windows-Server gesichert und zurückgespeichert werden. Benutzerprofile, die mit anderen Befehlen oder APIs gesichert oder zurückgespeichert wurden, werden für Windows nicht unterstützt.

Zu sichernde Objekte und ihre Positionen unter i5/OS

Als Ergebnis der Installation der Windows-Umgebung für die iSeries werden viele Objekte erstellt. Einige dieser Objekte sind systembedingt, andere sind benutzerbezogen. Alle diese Objekte müssen gesichert werden, wenn sie korrekt zurückgespeichert werden sollen. Diese Objekte können mit Hilfe der Auswahlmöglichkeiten des i5/OS-Befehls GO SAVE gesichert werden. Auswahl 21 sichert das gesamte System. Auswahl 22 sichert Systemdaten. Auswahl 23 sichert die gesamten Benutzerdaten (einschließlich der Objekte in QFPNWSSTG).

Wenn ein bestimmtes Objekt gesichert werden soll, kann dessen Position unter i5/OS anhand einer der folgenden Tabellen ermittelt werden. Die Tabelle enthält außerdem den zu verwendenden Befehl. Das Thema Manuelles Sichern von Teilen des Systems enthält weitere Informationen zur Verwendung der Sicherungsbefehle. Zusätzlich zum Sichern des gesamten Laufwerks (Speicherbereich) können auch einzelne Dateien und Verzeichnisse gesichert und zurückgespeichert werden. Weitere Informationen finden Sie unter „Einzelne Dateien und Verzeichnisse des integrierten Windows-Servers sichern“ auf Seite 205.

Zu sichernde Objekte

Objekthalt	Objektname	Objektposition	Objektart	Sicherungsbefehl
Boot- und Systemlaufwerk des integrierten Servers	nwsdname1	/QFPNWSSTG	Vordefinierte NWS-Speicherbereiche im Systemplattenpool	GO SAVE, Auswahl 21 oder 23 SAV OBJ('/QFPNWSSTG/nwsdname1') DEV('/QSYS.LIB/TAP01.DEVD')
Boot- und Systemlaufwerk des integrierten Servers	nwsdname1	/QFPNWSSTG	Vordefinierte NWS-Speicherbereiche im Benutzerplattenpool	SAV OBJ('/QFPNWSSTG/nwsdname1') ('/dev/QASPnn/nwsdname1.UDFS') DEV('/QSYS.LIB/TAP01.DEVD')
Installationsquellenlaufwerk des integrierten Servers	nwsdname2	/QFPNWSSTG	Vordefinierter NWS-Speicherbereich im Systemplattenpool	GO SAVE, Auswahl 21 oder 23 SAV OBJ('/QFPNWSSTG/nwsdname2') DEV('/QSYS.LIB/TAP01.DEVD')
Installationsquellenlaufwerk des integrierten Servers	nwsdname2	/QFPNWSSTG	Vordefinierte NWS-Speicherbereiche im Benutzerplattenpool	GO SAVE, Auswahl 21 oder 23 SAV OBJ('/QFPNWSSTG/nwsdname2') ('/dev/QASPnn/nwsdname2.UDFS') DEV('/QSYS.LIB/TAP01.DEVD')
Installationsquellenlaufwerk des integrierten Servers	nwsdname2	/QFPNWSSTG	Vordefinierte NWS-Speicherbereiche im unabhängigen Plattenpool (ASP)	GO SAVE, Auswahl 21 oder 23 SAV OBJ('/QFPNWSSTG/nwsdname2') ('/dev/independent ASP name/nwsdname2.UDFS') DEV('/QSYS.LIB/TAP01.DEVD')
Benutzerdaten und Anwendungen	Verschieden	/QFPNWSSTG	Benutzerdefinierte NWS-Speicherbereiche im Systemplattenpool	GO SAVE, Auswahl 21 oder 23 SAV OBJ('/QFPNWSSTG/stgspc') DEV('/QSYS.LIB/TAP01.DEVD')
Benutzerdaten und Anwendungen	Verschieden	/QFPNWSSTG	Benutzerdefinierte NWS-Speicherbereiche im Benutzerplattenpool	GO SAVE, Auswahl 21 oder 23 SAV OBJ('/QFPNWSSTG/stgspc') ('/dev/QASPnn/stgspc.UDFS') DEV('/QSYS.LIB/TAP01.DEVD')
Benutzerdaten und Anwendungen	Verschieden	/QFPNWSSTG	Benutzerdefinierte NWS-Speicherbereiche im unabhängigen Plattenpool	GO SAVE, Auswahl 21 oder 23 SAV OBJ('/QFPNWSSTG/stgspc') ('/dev/independent ASP name/stgspc.UDFS') DEV('/QSYS.LIB/TAP01.DEVD')
Nachrichten des integrierten Servers	Verschieden	Verschieden	Nachrichtewarteschlange	GO SAVE, Auswahl 21 oder 23 SAVOBJ OBJ(msgq) LIB(library) DEV(TAP01) OBJTYPE(*MSGQ)
i5/OS-Konfigurationsobjekte für integrierte Server	Verschieden	QSYS	Einheitenkonfigurationsobjekte	GO SAVE, Auswahl 21, 22 oder 23 SAVCFG DEV(TAP01)
Auf i5/OS und auf Windows basierender Code für IBM iSeries Integrated Server Support	QNTAP, NTAP und Unterverzeichnisse	QSYS und /QIBM/ProdData/NTAP	Bibliothek und Verzeichnis	SAVLICPGM LICPGM(5722SS1) OPTION(29)
Windows-Server-Dateifreigaben	QNTC und Unterverzeichnisse	/QNTC/Servername /Freigabename	Verzeichnis	GO SAVE, Auswahl 21 oder 22 SAV
i5/OS TCP-Schnittstellen	QATOCIFC	QUSRSYS	Physische Datei	GO SAVE, Auswahl 21 oder 23 SAVOBJ OBJ(QATOCIFC) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*FILE)
i5/OS TCP-Schnittstellen	QATOCLIFC	QUSRSYS	Logische Datei	GO SAVE, Auswahl 21 oder 23 SAVOBJ OBJ(QATOCLIFC) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*FILE)
iSCSI-NWSCFG und zugeordnete Prüfliste	Verschieden	QUSRSYS	NWS-Konfiguration und zugeordnete Werte	SAVOBJ LIB(QUSRSYS) OBJTYPE(*NWSCFG *VLDDL)
Zertifikatsspeicher für iSCSI-Pfad	nwsdname.*	/QIBM/UserData/NWSDCert	Zertifikatsspeicherdatei	GO SAVE, Auswahl 21 oder 23 SAV OBJ('/QIBM/UserData/NWSDCert/nwsdname.*')
Zertifikatsspeicher für iSCSI-Serviceprozessor	nwscfgname.kdb	/QIBM/UserData/Director/classes/com/ibm/sysmgmt/app/iide	Zertifikatsspeicherdatei. Sichern, wenn Initialisierungsmethode für Sicherheit 'Zertifikat automatisch generieren' lautet.	GO SAVE, Auswahl 21 oder 23 SAV OBJ('/QIBM/UserData/Director/classes/com/ibm/sysmgmt/app/iide/nwscfgname.kdb')

Anmerkung: Für integrierte Windows-Server, die auf Systemen vor V4R5 erstellt wurden, siehe Zu sichernde Objekte und ihre Positionen unter OS/400 im iSeries Information Center für V5R3.

Einzelne Dateien und Verzeichnisse des integrierten Windows-Servers sichern

IBM iSeries Integrated Server Support ermöglicht die gemeinsame Sicherung von Daten des integrierten Servers (Dateien, Verzeichnisse, Freigaben und die Windows-Registrierung) und anderen i5/OS-Daten auf einem Band, einem optischen Datenträger oder einer Festplatte, sowie das getrennte Zurückspeichern der Daten. Dieser Ansatz sollte jedoch nicht als Hauptsicherungsverfahren eingesetzt werden. Das Gesamtsystem und die NWS-Beschreibung, die dem Windows-Server zugeordnet ist, sollten weiterhin für den Katastrophenfall regelmäßig gesichert werden. Anschließend können die Dateien des integrierten Servers, die sich geändert haben, täglich gesichert werden. Weitere Informationen finden Sie unter „Einem integrierten Windows-Server zugeordnete NWS-Beschreibungen und andere Objekte sichern“ auf Seite 199.

Weitere Informationen zu der Funktion für die Sicherung auf Dateiebene erhalten Sie unter folgenden Themen:

- Lesen Sie zunächst den Abschnitt „Einschränkungen für Sicherungen auf Dateiebene“.
- Vor der Sicherung des integrierten Servers auf Dateiebene müssen Sie die Aufgaben ausführen, die im Abschnitt „Vorbereitende Konfigurationsaufgaben“ auf Seite 206 beschrieben sind.
- „Dateien sichern“ auf Seite 208

Zudem können Dienstprogramme wie das mit Windows ausgelieferte Sicherungsprogramm (siehe „Windows-Sicherungsdienstprogramm“ auf Seite 209) zur Sicherung der Dateien des integrierten Servers eingesetzt werden. Weitere Informationen über Sicherungs- und Wiederherstellungsoptionen für die Dateien des integrierten Windows-Servers finden Sie im Abschnitt zum Backup für Windows-Server auf der Website IBM Integrated xSeries Solutions.

Einschränkungen für Sicherungen auf Dateiebene

Bei Verwendung der Sicherung auf Dateiebene müssen folgende Einschränkungen und Anforderungen berücksichtigt werden:

Einschränkungen:

- Diese Unterstützung ist für Standalone-Windows-Server nicht verfügbar, da der Code zusammen mit IBM i5/OS Integrated Server Support bereitgestellt wird.
- Die Methode sichert keine Dateien, die Bestandteil des Codes von IBM iSeries Integrated Server Support sind.
- Sie können nicht verhindern, dass sich Benutzer anmelden und während der Ausführung des Befehls SAV (Sichern) oder RST (Zurückspeichern) auf Daten des Servers zugreifen. IBM iSeries Integrated Server Support kann im Gebrauch befindliche Dateien sichern, sofern diese gelesen werden können. Dateien des integrierten Servers sollten daher zu einem Zeitpunkt gesichert werden, zu dem nur wenige Benutzer auf das System zugreifen. Ein Hinweis an die Benutzer, den Zugriff auf das System zu vermeiden, stellt eine gute Vorsichtsmaßnahme dar.
- Windows Server 2003 stellt diese Funktion mit dem Volume Shadow Copy Service (VSS) zur Verfügung. Wenn die Sicherung auf Dateiebene verwendet wird, haben Anwendungen mit diesem Service die Möglichkeit, Dateien zu sichern, während diese weiterhin im Gebrauch sind.
- Das Benutzerprofil QSECOFR sollte nicht für Sicherungen auf Dateiebene verwendet werden. Selbst nach der Registrierung auf dem integrierten Server kann das Benutzerprofil QSECOFR nicht zum Sichern der Dateien eingesetzt werden. Stattdessen wird der lokale Windows-Systemaccount verwendet. Er verfügt unter Umständen nicht über die erforderlichen Berechtigungen, um alle angeforderten Dateien zu sichern.
- Ist der LCLPMDMGT-Wert des Benutzerprofils auf *YES gesetzt, muss der Systemwert QRETSVRSEC auf 1 gesetzt und das Benutzerkennwort geändert werden, oder der Benutzer muss sich nach einer Änderung von QRETSVRSEC anmelden.

- Ist der LCLPMDMGT-Wert des Benutzerprofils auf *NO gesetzt, wird die Netzwerkauthentifizierung (Kerberos) verwendet. Der Benutzer muss über eine EIM-kompatible Anwendung auf den iSeries-Betrieb zugreifen (z. B. mit der Einzelanmeldung von iSeries Navigator). Weitere Informationen finden Sie unter „Unterstützung des Befehls SBMNWSCMD und der Sicherung auf Dateiebene für Kerberos V5 und EIM“ auf Seite 165.

Anforderungen:

- Der integrierte Server muss aktiv sein und über eine betriebsbereite Virtual Punkt-zu-Punkt TCP/IP-Ethernet-Verbindung zu i5/OS verfügen. Um die verbleibenden i5/OS-Dateien zu sichern, müssen die Dateien des integrierten Servers gesichert werden, bevor der Systemstatus auf eingeschränkten Betrieb gestellt wird oder nachdem die Aufgaben im eingeschränkten Betrieb abgeschlossen wurden.
- Bei dieser Prozedur ist es erforderlich, dass Ihre Benutzer-ID und Ihr Kennwort auf dem integrierten Server und unter i5/OS identisch sind.
- Der Benutzeraccount des integrierten Servers muss Mitglied der Administratorengruppe sein.
- Die Sicherung auf Dateiebene verwendet zur Auflistung der zu speichernden Dateien das QNTC-Dateisystem (NetClient). QNTC sucht unter Verwendung von iSeries NetServer nach Servern in der Domäne. Der iSeries NetServer muss sich in derselben Domäne befinden (siehe „Zugehörigkeit von iSeries NetServer und integriertem Windows-Server zur selben Domäne sicherstellen“ auf Seite 207) wie der integrierte Server, von dem Daten gesichert werden sollen.
- Beim Zurückspeichern aller Dateien auf allen Laufwerken, die zuvor über das QNTC-Dateisystem gesichert wurden, ist Vorsicht geboten. Gewisse Systemdateien aus Windows (z. B. bestimmte Dateien im Papierkorb) können nach der Rückspeicherung unerwünschte Ergebnisse zur Folge haben.
- Unter Windows 2000 Server oder Windows Server 2003 muss dem Schutz der Systemdateien besondere Aufmerksamkeit geschenkt werden, wenn Windows-Systemdateien gesichert und zurückgespeichert werden. Weitere Informationen finden Sie in der Dokumentation von Microsoft.

Vorbereitende Konfigurationsaufgaben

Bevor die Dateien des integrierten Windows-Servers auf Dateiebene gesichert werden können, müssen einige vorbereitende Konfigurationsaufgaben durchgeführt werden:

1. Die Person, die die Dateien sichert und zurückspeichert, muss unter i5/OS und auf dem integrierten Server das gleiche Kennwort verwenden. Die einfachste Methode ist unter „Einzelnen i5/OS-Benutzer mit iSeries Navigator in der Windows-Umgebung registrieren“ auf Seite 187 beschrieben. Stellen Sie außerdem sicher, dass der Benutzer Mitglied der Administratorengruppe ist. Weitere Informationen finden Sie unter „Benutzerschemata erstellen“ auf Seite 189.
2. Erstellen Sie Freigaben für alle Laufwerke oder Datenträger, die gesichert werden sollen, wenn die Auswahl, alle Dateien auf einem Windows-Server zu sichern, getroffen wird. IBM iSeries Integrated Server Support greift auf das Dateisystem zu und setzt diese Freigaben in Pfadnamen um. Weitere Informationen hierzu finden Sie in „Freigaben auf integrierten Windows-Servern erstellen“ auf Seite 207.
3. Der Datei QAZLCSAVL in QUSRSYS müssen Teildateien hinzugefügt werden, die die zu sichernden Freigabennamen enthalten. Weitere Informationen finden Sie unter „Teildateien zur Datei QAZLCSAVL hinzufügen“ auf Seite 207.
4. Stellen Sie sicher, dass sich iSeries NetServer in derselben Domäne befindet wie der integrierte Server, für den Dateien gesichert werden sollen. Weitere Informationen finden Sie unter „Zugehörigkeit von iSeries NetServer und integriertem Windows-Server zur selben Domäne sicherstellen“ auf Seite 207.
5. Vergewissern Sie sich, dass die Person, die das Sichern und Zurückspeichern ausführt, über die Berechtigung *ALLOBJ verfügt, die dem Benutzer uneingeschränkten Zugriff auf die Programme und Einheiten erlaubt, die für den Sicherungs- oder Wiederherstellungsprozess benötigt werden. Wenn die Berechtigung *ALLOBJ nicht erteilt werden kann, muss der Benutzer zumindest über die Berechtigung *USE für das Objekt QNTAP/QVNASBM verfügen, damit die Anforderung zum Sichern oder Zurückspeichern an den Windows-Server übertragen werden kann.

Freigaben auf integrierten Windows-Servern erstellen

Um eine Sicherung und Rückspeicherung auf Dateiebene von Dateien des integrierten Servers unter i5/OS zu ermöglichen, muss für alle Verzeichnisse mit Daten, die gesichert werden sollen, eine Freigabe erstellt werden. So erstellen Sie über die Konsole des integrierten Servers Freigaben auf integrierten Servern:

1. Klicken Sie auf das Symbol **Arbeitsplatz**, um den Windows Explorer zu öffnen.
2. Klicken Sie mit der rechten Maustaste auf das gewünschte Laufwerk oder den gewünschten Datenträger.
3. Wählen Sie im Kontextmenü **Freigabe** aus.
4. Klicken Sie auf die Option **Diesen Ordner freigeben**. Geben Sie einen **Freigabennamen** an. (Die Zeichen des Namens müssen im eingeschränkten Zeichensatz der Codepage 500 enthalten sein.) Der Standardfreigabename entspricht dem letzten Teil des Verzeichnisnamens. Freigabennamen dürfen maximal 12 Zeichen umfassen und können Leerzeichen aufweisen.
5. Sie können einen uneingeschränkten Zugriff auswählen oder die Anzahl der Benutzer, die gleichzeitig auf die Freigabe zugreifen können, beschränken. Zudem kann über die Schaltfläche **Berechtigungen** die Freigabestufe (Kein Zugriff, Lesen, Ändern oder Vollzugriff) gewählt werden.
6. Klicken Sie auf **Anwenden**, um die Freigabe zu erstellen.

Teildateien zur Datei QAZLCSAVL hinzufügen

Um die Sicherung und Rückspeicherung auf Dateiebene unter i5/OS zu ermöglichen, muss der Datei QAZLCSAVL in QUSRSYS eine Teildatei für jeden integrierten Server hinzugefügt werden. Verwenden Sie als Teildateinamen den NWSD-Namen des Servers (*nwsdname*).

So fügen Sie eine Teildatei hinzu:

1. Geben Sie in der i5/OS-Befehlszeile Folgendes ein:
ADDPFM FILE(QUSRSYS/QAZLCSAVL) MBR(*nwsdname*) TEXT('description') EXPDATE(*NONE) SHARE(*NO) SRCTYPE(*NONE)
2. Listen Sie in der soeben erstellten Teildatei alle Freigaben auf, die gesichert werden sollen. Jeder Freigabename, der für den Server definiert wurde, muss in einer separaten Zeile angeführt werden. Der Windows-Freigabename darf maximal 12 Zeichen umfassen. Freigabennamen können eingebettete Leerzeichen enthalten. Wenn Sie auf WINSVR1 beispielsweise die Freigaben cshare, dshare, eshare, fshare, gshare und my share definiert haben, sieht die Teildatei namens WINSVR1 folgendermaßen aus:

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

Anmerkung:

Wurden mehrere Freigabennamen erstellt, die auf das gleiche Verzeichnis auf dem integrierten Server verweisen, sichert i5/OS die Daten bei der Anforderung, alle Dateien zu sichern, mehrfach. Um eine Duplizierung der Dateien beim Sichern zu vermeiden, sollten keine Freigaben hinzugefügt werden, die die gleichen Verzeichnisse oder Daten beinhalten.

Zugehörigkeit von iSeries NetServer und integriertem Windows-Server zur selben Domäne sicherstellen

Zur Sicherung von Dateien des integrierten Servers auf Dateiebene muss sich iSeries NetServer in derselben Domäne wie die zu sichernden Dateien befinden.

1. Überprüfen Sie die Domäne des integrierten Servers:
 - a. Wählen Sie im iSeries Navigator —> **Server** aus.
 - b. Suchen Sie den integrierten Server in der Liste im rechten Teilfenster. Die Domäne dieses Servers wird in der gleichnamigen Spalte angegeben.

2. Überprüfen Sie die Domäne für iSeries NetServer:
 - a. Wählen Sie in iSeries Navigator die Optionen **Netzwerk** → **Server** → **TCP/IP** aus.
 - b. Suchen Sie in der Liste der TCP/IP-Server nach iSeries NetServer.
 - c. Klicken Sie mit der rechten Maustaste auf **iSeries NetServer**, und wählen Sie **Eigenschaften** aus (oder doppelklicken Sie auf **iSeries NetServer**, und wählen Sie dann **Datei** und **Eigenschaften** aus). Der Domänenname für iSeries NetServer wird auf der Indexzunge **Allgemein** der Informationsdatei angezeigt.
3. Befindet sich iSeries NetServer in einer anderen Domäne als der integrierte Server, muss die Domäne für iSeries NetServer geändert werden:
 - a. Klicken Sie auf die Schaltfläche **Nächster Start**.
 - b. Geben Sie im Feld **Domänenname** den Namen der Windows-Server-Domäne ein.
 - c. Stoppen Sie iSeries NetServer, und starten das Programm erneut. (Klicken Sie hierzu mit der rechten Maustaste auf iSeries NetServer, und wählen Sie erst **Stoppen** und dann **Starten** aus.)

Dateien sichern

Nach Abschluss der erforderlichen Vorbereitungen (siehe „Vorbereitende Konfigurationsaufgaben“ auf Seite 206) können die Dateien des integrierten Servers unter i5/OS gesichert werden. Um Verzeichnisse oder Dateien anhand des Freigabennamens zurückzuspeichern, muss der Freigabe- bzw. Dateiname im Befehl SAV explizit angegeben werden.

Anmerkung:

Nehmen Sie die Angaben der zu sichernden Daten im Befehl SAV sorgfältig vor, um eine Duplizierung von Daten zu vermeiden. Werden mehrere Freigabennamen angegeben, die auf das gleiche Verzeichnis auf dem integrierten Server verweisen, sichert i5/OS die Daten mehrfach.

So geben Sie an, welche Daten i5/OS sichern soll:

1. Stellen Sie sicher, dass der integrierte Server aktiv ist (siehe „Integrierten Server starten und stoppen“ auf Seite 157). Stellen Sie des Weiteren sicher, dass die Subsysteme QSYSWRK, QSERVER und TCP/IP aktiv sind (verwenden Sie zu diesem Zweck den Befehl WRKACTJOB (Mit aktiven Jobs arbeiten)).
2. Geben Sie in der i5/OS-Befehlszeile den Befehl SAV ein, und drücken Sie F4.
3. Geben Sie im Feld Einheit die Einheit an, auf der i5/OS die Daten sichern soll. Bei Angabe von QSYS.LIB/TAP01.DEVD werden die Daten beispielsweise auf einem Band gesichert.
4. Geben Sie im Feld Objekt an, welche Daten i5/OS sichern soll. Verwenden Sie hierbei das Format `/QNTC/servername/sharename`.
Platzhalterzeichen sind zulässig. Im Abschnitt „Beispiele: Komponenten eines integrierten Windows-Servers angeben“ ist beschrieben, wie Sie bestimmte Komponenten des integrierten Servers angeben können.
5. Geben Sie im Feld Verzeichnisunterstruktur an, ob untergeordnete Strukturen eines Verzeichnisses gesichert werden sollen. In der Standardeinstellung werden alle Verzeichnisse gesichert.
6. Um Änderungen seit der letzten Sicherung zu sichern, geben Sie im Feld Zeitraum der letzten Änderung *LASTSAVE ein. Es kann darüber hinaus ein bestimmter Datums- und Zeitbereich eingegeben werden.
7. Drücken Sie die Eingabetaste, um die definierten Freigaben zu sichern.

Beispiele: Komponenten eines integrierten Windows-Servers angeben

Diese Beispiele zeigen, wie mit dem Befehl SAV oder RST auf bestimmte Komponenten des integrierten Servers für einen Server namens *server1* verwiesen werden kann:

Zu sichernde oder zurückzuspeichernde Objekte:	Erforderliche Angabe:
Alle Objekte des integrierten Servers	OBJ('/QNTC/*') SUBTREE(*ALL)
Alle Objekte für <i>server1</i> .	OBJ('/QNTC/server1/*') SUBTREE(*ALL)

Zu sichernde oder zurückzuspeichernde Objekte:	Erforderliche Angabe:
Alle Objekte für <i>server1</i> , die seit der letzten Dateisicherung geändert wurden.	OBJ('/QNTC/server1/*') SUBTREE(*ALL) CHGPERIOD(*LASTSAVE)
Alle Objekte für <i>server1</i> , die innerhalb eines bestimmten Zeitraums geändert wurden (in diesem Fall zwischen dem 19.10.99 und 25.10.99).	OBJ('/QNTC/server1/*') SUBTREE(*ALL) CHGPERIOD('10/19/99' '00:00:00' '10/25/99' '23:59:59')
Alle Verzeichnisse, Dateien und Freigaben, auf die eine bestimmte Freigabe verweist (z. B. 'fshare'). Das Verzeichnis, über das die Freigabe erstellt ist, wird von i5/OS nicht gesichert und zurückgespeichert.	OBJ('/QNTC/server1/fshare/*') SUBTREE(*ALL)
Nur Dateien, auf die die angegebene Freigabe (z. B. 'fshare') verweist und die dem angegebenen Muster (pay*) entsprechen. i5/OS sichert weder Verzeichnisse noch Freigaben.	OBJ('/QNTC/server1/fshare/pay*')
Nur Verzeichnisse und Freigaben (keine Objekte) für 'fshare' und die unmittelbar untergeordneten Komponenten.	OBJ('/QNTC/server1/fshare') SUBTREE(*DIR)
Verzeichnisse, Freigaben und Dateien für 'terry' und die zugehörigen Unterverzeichnisstrukturen (nicht Verzeichnis 'terry').	OBJ('/QNTC/server1/fdrive/terry/*') SUBTREE(*ALL)
Nur die angegebene Datei 'myfile.exe'.	OBJ('/QNTC/server1/gdrive/myfile.exe')
Registrierung des integrierten Servers	OBJ('/QNTC/server1/\$REGISTRY')

Windows-Sicherungsdienstprogramm

Mit Hilfe des Windows-Sicherungsdienstprogramms und eines iSeries-Bandlaufwerks können Sicherungen vom integrierten Windows-Server aus erstellt werden. Weitere Informationen hierzu finden Sie in „iSeries-Bandlaufwerke mit integrierten Windows-Servern verwenden“ auf Seite 180.

So starten Sie das Sicherungsdienstprogramm:

1. Klicken Sie in der Konsole des integrierten Servers auf **Start**.
2. Wählen Sie **Zubehör** —> **Systemprogramme** —> **Sicherung** aus.

Informationen zur Sicherung und Rückspeicherung unter Verwendung von am LAN angeschlossenen Massenspeichereinheiten finden Sie in der Dokumentation zum Windows-Server von Microsoft.

NWS-Beschreibung und Plattenlaufwerke eines integrierten Windows-Servers zurückspeichern

Eine Methode zum Zurückspeichern von Daten des integrierten Servers besteht im Zurückspeichern der NWS-Beschreibung (NWS-D) und der Plattenlaufwerke, die i5/OS diesem Server zuordnet. Dies ist die schnellste Methode für das Zurückspeichern großer Datenmengen. Wenn Sie die Sicherung auf Dateiebene verwenden, können Sie auch bestimmte Dateien des integrierten Servers zurückspeichern.

Werden gesicherte Objekte unter i5/OS zurückgespeichert, müssen folgende Punkte beachtet werden:

Anmerkungen:

1. Eine NWS-Beschreibung (NWSID), ihre vordefinierten Plattenlaufwerke (siehe „Vordefinierte Plattenlaufwerke für integrierte Windows-Server“ auf Seite 171) und alle benutzerdefinierten Plattenlaufwerke, die ihr zugeordnet sind, müssen als eine Einheit angesehen werden. Sie sollten gleichzeitig zurückgespeichert werden. Andernfalls ist der integrierte Server möglicherweise nicht in der Lage, Elemente wie beispielsweise Windows-Server-Dateisystemberechtigungen erneut zu erstellen.
2. Damit i5/OS die zurückgespeicherten Plattenlaufwerke im Integrated File System (IFS) automatisch erneut verbindet (Relink), muss die NWS-Beschreibung zurückgespeichert werden, nachdem die Plattenlaufwerke zurückgespeichert wurden.
3. Wird eine NWS-Beschreibung zurückgespeichert, bevor die vordefinierten und benutzerdefinierten Plattenlaufwerke im IFS (Integrated File System) zurückgespeichert wurden, müssen diese Plattenlaufwerke erneut verbunden werden (Relink). Dies erfolgt mit Hilfe des Befehls ADDNWSSTGL (NWS-Speicherbereichsverbindung hinzufügen) für jedes Plattenlaufwerk, das der NWS-Beschreibung zugeordnet ist:

```
ADDNWSSTGL NWSSTG(Speicherbereichsname) NWSID(NWSID-Name)
```

4. Wird ein Domänencontroller zurückgespeichert, muss sichergestellt werden, dass die Domänen-datenbank auf diesem Server mit den anderen Domänencontrollern synchronisiert wird. Wenn gemeinsam von einem Windows-Clusterknoten benutzte Plattenlaufwerke zurückgespeichert werden, müssen die gemeinsam benutzten Laufwerke möglicherweise manuell erneut verbunden werden. Beginnen Sie mit dem Verbinden der gemeinsam benutzten Quorum-Ressource. Verwenden Sie hierfür den folgenden Befehl:

```
ADDNWSSTGL  
NWSSTG(Quorum-Name) NWSID(NWSID-Name) ACCESS(*SHRUPD) DYNAMIC(*YES) DRVSEQNBR(*QR)
```

Nach dem erneuten Verbinden der Quorum-Ressource können die restlichen gemeinsam benutzten Laufwerke ebenfalls verbunden werden. Verwenden Sie hierzu den folgenden Befehl:

```
ADDNWSSTGL  
NWSSTG(Shared-Name) NWSID(NWSID-Name) ACCESS(*SHRUPD) DYNAMIC(*YES) DRVSEQNBR(*CALC)
```

Führen Sie zu diesem Zweck die normalen Windows-Prozeduren durch, und verwenden Sie bei Bedarf die Dokumentation von Microsoft.

5. Das Zurückspeichern einer NWS-Beschreibung von bestimmten Hardwaretypen auf bestimmte andere Hardwaretypen ist möglicherweise nicht zulässig. Weitere Informationen finden Sie unter „NWS-Beschreibungen von integrierten Windows-Servern zurückspeichern“ auf Seite 212.

Die folgenden Abschnitte erläutern, wie Sie die NWS-Beschreibung und Plattenlaufwerke eines integrierten Servers zurückspeichern:

- „Vordefinierte Plattenlaufwerke für integrierte Windows-Server zurückspeichern“
- „Benutzerdefinierte Plattenlaufwerke für integrierte Windows-Server zurückspeichern“ auf Seite 211
- „NWS-Beschreibungen von integrierten Windows-Servern zurückspeichern“ auf Seite 212

Vordefinierte Plattenlaufwerke für integrierte Windows-Server zurückspeichern

Plattenlaufwerke mit dem Windows-Betriebssystem und der Registrierung befinden sich im integrierten Dateisystem (IFS). Diese vordefinierten Plattenlaufwerke werden auf die gleiche Weise zurückgespeichert wie benutzerdefinierte Plattenlaufwerke. Zum Zurückspeichern der Plattenlaufwerke im IFS von i5/OS muss der Befehl RST (Zurückspeichern) verwendet werden:

1. Erfolgt das Zurückspeichern von einem Sicherungsdaträger, muss gewährleistet werden, dass der Datenträger eingelegt ist.

2. Sind derzeit keine NWS-Speicherbereiche auf dem System vorhanden (bei Verwendung des Befehls WRKNWSSTG erscheinen keine Speicherbereiche), muss das Verzeichnis /QFPNWSSTG erstellt werden, bevor NWS-Speicherbereiche zurückgespeichert werden können, die unterhalb dieses Verzeichnisses gesichert wurden. So erstellen Sie das Verzeichnis /QFPNWSSTG:
 - a. Geben Sie in der i5/OS-Befehlszeile den Befehl CRTNWSSTG ein, um einen NWS-Speicherbereich zu erstellen, und drücken Sie F4.
 - b. Geben Sie einen Namen für den Speicherbereich an.
 - c. Verwenden Sie die zulässige Mindestgröße, und geben Sie den entsprechenden ASP an.
 - d. Drücken Sie die Eingabetaste, um den Speicherbereich zu erstellen. i5/OS erstellt den Speicherbereich im Verzeichnis /QFPNWSSTG.
3. Um den Speicherbereich zurückzuspeichern, geben Sie den Befehl RST ein, und drücken Sie F4.
4. Geben Sie im Feld Name unter Objekte: die Werte '/QFPNWSSTG/stgspc' und 'dev/QASPnn/stgspc.UDFS' an. Hierbei steht *stgspc* für den Namen des NWS-Speicherbereichs und *nn* für die Nummer des Plattenpools.

Anmerkung: Zur Rückspeicherung des .UDFS-Objekts auf einem unabhängigen Plattenpool (ASP) muss die ASP-Einheit angehängt werden. Geben Sie *dev/independent ASP name/stgspc.UDFS* an. Hierbei steht *independent ASP name* für den Namen des unabhängigen Plattenpools und *stgspc* für den Namen des NWS-Speicherbereichs.

Speichern Sie das Systemlaufwerk (C) mit dem Befehl /QFPNWSSTG/*newsdname1* zurück. Laufwerk D wird mit dem Befehl /QFPNWSSTG/*newsdname2* zurückgespeichert.

5. Geben Sie die Werte für alle anderen gewünschten Parameter an, und drücken Sie die Eingabetaste, um den Speicherbereich zurückzuspeichern.
6. Die benutzerdefinierten Plattenlaufwerke, die dem Server zugeordnet sind, und die NWS-Beschreibung (NWS D) müssen ebenfalls zurückgespeichert werden. Weitere Informationen finden Sie unter „Benutzerdefinierte Plattenlaufwerke für integrierte Windows-Server zurückspeichern“. Nachdem die NWS-Beschreibung (NWS D) und alle zugeordneten Plattenlaufwerke zurückgespeichert wurden, müssen Sie den integrierten Server anhängen.

Anmerkung: Wurde der Server vor V4R5 installiert, siehe Vordefinierte Plattenlaufwerke für integrierte Windows-Server zurückspeichern, die vor V4R5 erstellt wurden im iSeries Information Center für V5R3.

Benutzerdefinierte Plattenlaufwerke für integrierte Windows-Server zurückspeichern

Obwohl jetzt die Sicherung einzelner Dateien und Verzeichnisse möglich ist (siehe „Einzelne Dateien und Verzeichnisse des integrierten Windows-Servers sichern“ auf Seite 205), besteht bei großen Datenmengen die schnellste Möglichkeit darin, den gesamten Speicherbereich zurückzuspeichern. Wenn der benutzer-eigene Speicherbereich aus dem Verzeichnis \QFPNWSSTG gesichert wurde, kann nur der gesamte Speicherbereich zurückgespeichert werden. Weitere Informationen finden Sie unter „Benutzerdefinierte Plattenlaufwerke für einen integrierten Windows-Server sichern“ auf Seite 202. Es ist nicht möglich, einzelne Dateien aus dieser Sicherung zurückzuspeichern.

So speichern Sie Plattenlaufwerke im IFS zurück:

1. Erfolgt das Zurückspeichern von einem Sicherungsdatenträger, muss gewährleistet werden, dass der Datenträger eingelegt ist.
2. Sind derzeit keine Speicherbereiche auf dem System vorhanden (bei Verwendung des Befehls WRKNWSSTG erscheinen keine Speicherbereiche), muss das Verzeichnis /QFPNWSSTG erstellt werden, bevor NWS-Speicherbereiche zurückgespeichert werden können, die unterhalb dieses Verzeichnisses gesichert wurden. So erstellen Sie das Verzeichnis /QFPNWSSTG:

- a. Geben Sie in der i5/OS-Befehlszeile den Befehl CRTNWSSTG ein, um einen NWS-Speicherbereich zu erstellen, und drücken Sie F4.
 - b. Geben Sie einen Namen für den Speicherbereich an.
 - c. Verwenden Sie die zulässige Mindestgröße, und geben Sie den entsprechenden ASP an.
 - d. Drücken Sie die Eingabetaste, um den Speicherbereich zu erstellen. i5/OS erstellt den Speicherbereich im Verzeichnis /QFPNWSSTG.
3. Um den Speicherbereich zurückzuspeichern, geben Sie den Befehl RST ein, und drücken Sie F4.
 4. Geben Sie im Namensfeld für Objekte: die Namen /QFPNWSSTG/stgspc und dev/QASPnn/stgspc.UDFS an. Dabei steht stgspc für den Namen des NWS-Speicherbereichs und "nn" für die Nummer des Plattenpools.

Anmerkung:

Zur Rückspeicherung des .UDFS-Objekts auf einem unabhängigen Plattenpool (ASP) muss die ASP-Einheit angehängt werden. Geben Sie dev/independent ASP name/stgspc.UDFS an. Hierbei steht independent ASP name für den Namen des unabhängigen ASP und stgspc für den Namen des NWS-Speicherbereichs.

5. Geben Sie die Werte für alle anderen gewünschten Parameter an, und drücken Sie die Eingabetaste, um den Speicherbereich zurückzuspeichern.
6. Die vordefinierten Plattenlaufwerke, die dem Server zugeordnet sind, und die NWS-Beschreibung (NWSD) müssen ebenfalls zurückgespeichert werden. Weitere Informationen finden Sie unter „NWS-Beschreibungen von integrierten Windows-Servern zurückspeichern“. Nachdem die NWS-Beschreibung (NWSD) und alle zugeordneten Plattenlaufwerke zurückgespeichert wurden, müssen Sie den integrierten Server anhängen.

NWS-Beschreibungen von integrierten Windows-Servern zurückspeichern

Bei einer Wiederherstellung nach einem Katastrophenfall werden alle Konfigurationsobjekte zurückgespeichert, darunter auch die NWS-Beschreibung (NWSD) für den integrierten Windows-Server. In einigen Situationen, wenn beispielsweise eine Migration auf neue Hardware des integrierten xSeries-Servers erfolgt, muss die NWS-Beschreibung ausdrücklich zurückgespeichert werden. Damit i5/OS die zurückgespeicherten Plattenlaufwerke im Integrated File System (IFS) automatisch erneut verbindet (Relink), muss die NWS-Beschreibung zurückgespeichert werden, nachdem die Plattenlaufwerke zurückgespeichert wurden. Verwenden Sie zum Zurückspeichern der NWS-Beschreibung (NWSD) den Befehl RSTCFG (Konfiguration zurückspeichern):

1. Geben Sie in der i5/OS-Befehlszeile den Befehl RSTCFG ein, und drücken Sie F4.
2. Geben Sie im Feld Objekte den Namen der NWSD ein.
3. Geben Sie im Feld Einheit den Einheitennamen an, wenn das Zurückspeichern von einem Datenträger erfolgt. Erfolgt das Zurückspeichern von einer Sicherungsdatei, müssen Sie *SAVF und den Namen sowie die Bibliothek für die Sicherungsdatei in den entsprechenden Feldern angeben.
4. Drücken Sie die Eingabetaste, damit i5/OS die NWS-Beschreibung zurückspeichert.
5. Nachdem die NWS-Beschreibung (NWSD) und alle ihr zugeordneten Speicherbereiche zurückgespeichert wurden, müssen Sie den integrierten Server starten. Entsprechende Anweisungen finden Sie unter „Integrierten Server starten und stoppen“ auf Seite 157.

Anmerkung: Beim Zurückspeichern einer NWS-Beschreibung (NWSD) müssen alle zugeordneten Leitungs-, und Einheitenbeschreibungen ebenfalls zurückgespeichert werden. Zudem müssen alle Leitungsbeschreibungen zurückgespeichert werden, für die TCP/IP-Schnittstellen definiert waren.

NWSHs von integrierten Windows-Servern zurückspeichern

Bei einer Wiederherstellung nach einem Katastrophenfall werden alle Konfigurationsobjekte zurückgespeichert, darunter auch der NWS-Hostadapter (NWSH). Verwenden Sie zum Zurückspeichern des NWSH den Befehl RSTCFG (Konfiguration zurückspeichern):

1. Geben Sie in der i5/OS-Befehlszeile den Befehl RSTCFG ein, und drücken Sie F4.
2. Geben Sie im Feld **Objekte** den Namen und des Typ des NWSH ein.
3. Geben Sie im Feld **Einheit** den Einheitennamen an, wenn das Zurückspeichern von einem Datenträger erfolgt. Erfolgt das Zurückspeichern von einer Sicherungsdatei, müssen Sie *SAVF und den Namen sowie die Bibliothek für die Sicherungsdatei in den entsprechenden Feldern angeben.
4. Drücken Sie die Eingabetaste, damit i5/OS den NWSH zurückspeichert.

Anmerkungen:

1. Wenn Sie einen NWSH zurückspeichern, muss er vor dem integrierten Server gestartet werden.

NWSCFGs von integrierten Windows-Servern für Server zurückspeichern, die über iSCSI angeschlossen sind

Die zusätzlichen Konfigurationsobjekte für Server mit iSCSI-HBA-Anschluss müssen in die Bibliothek QUSRSYS zurückgespeichert werden. Zu diesen Objekten gehören die NWS-Konfigurationsobjekte (Typ *NWSCFG) und ein zugeordnetes Prüflistenobjekt (Typ *VLDDL).

Anmerkung: Die *NWSCFG- und *VLDDL-Objekte haben den gleichen Namen.

Um Serverspeicherbereiche zurückzuspeichern, muss der Befehl RSTOBJ (Objekt zurückspeichern) verwendet werden:

1. Geben Sie in einer i5/OS-Befehlszeile den Befehl RSTOBJ ein, und drücken Sie F4.
2. Erfolgt das Zurückspeichern von einem Sicherungsdatenträger, muss gewährleistet werden, dass der Datenträger eingelegt ist.
3. Geben Sie im Feld **Objekte** den Namen der NWS-Konfiguration an. (Wenn Sie mehrere NWS-Konfigurationen zurückspeichern möchten, geben Sie den generischen Namen „nwsdname“ ein. Sie können die Objektnamen auch explizit angeben, indem Sie + eingeben und die Eingabetaste drücken.)
 - Um die standardmäßige NWS-Konfiguration für die Verbindungssicherheit zurückzuspeichern, geben Sie den Namen der NWSD gefolgt von CN ein.
 - Um die standardmäßige NWS-Konfiguration für den Serviceprozessor zurückzuspeichern, geben Sie den Namen der NWSD gefolgt von SP ein.
 - Um die standardmäßige NWS-Konfiguration für den fernen Server zurückzuspeichern, geben Sie den Namen der NWSD gefolgt von RM ein.
4. Geben Sie im Feld für die **Sicherungsbibliothek** den Wert QUSRSYS an.
5. Geben Sie im Feld **Einheit** entweder den Namen der Einheit, in die der Sicherungsdatenträger eingelegt wurde, oder den Befehl *SAVF an, wenn das Zurückspeichern von einer Sicherungsdatei erfolgt.
6. Geben Sie im Feld **Objektart** sowohl *NWSCFG als auch *VLDDL ein.
7. Erfolgt das Zurückspeichern von einer Sicherungsdatei, müssen Sie den Namen und die Bibliothek für die Sicherungsdatei angeben.
8. Drücken Sie die Eingabetaste, um die NWS-Konfiguration und die zugehörige Prüfliste zurückzuspeichern.

Dateien des integrierten Windows-Servers zurückspeichern

IBM iSeries Integrated Server Support unterstützt das Sichern und Zurückspeichern von Dateien auf Dateiebene. Sie sind somit in der Lage, eine einzelne Datei von i5/OS zurückzuspeichern, ohne das gesamte Plattenlaufwerk zurückzuspeichern. Vor Einsatz dieser Methode sollte jedoch die zurückzuspeichernde Datenmenge überprüft werden. Bei großen Datenmengen ist das Zurückspeichern eines gesamten Plattenlaufwerks wesentlich schneller als das Zurückspeichern einzelner Dateien auf dem Plattenlaufwerk. Um eine geringe Datenmenge zurückzuspeichern, ist diese Methode jedoch ideal.

Das Verzeichnis sollte zuerst zurückgespeichert werden, gefolgt von den Dateien und der Registrierung. Starten Sie den Windows-Server anschließend neu, um die neuen Registrierungseinträge zu übernehmen. Dateien, die mittels dieser Methode gesichert wurden, können über den Befehl RST zurückgespeichert werden:

1. Stellen Sie sicher, dass der integrierte Windows-Server und TCP/IP ausgeführt werden.
2. Geben Sie in der i5/OS-Befehlszeile den Befehl RST ein, und drücken Sie F4.
3. Geben Sie im Feld Einheit die Einheit an, auf der die Daten zur Verfügung stehen. (Bei Angabe von QSYS.LIB/TAP01.DEVD werden beispielsweise auf Band gesicherte Daten zurückgespeichert.)
4. Geben Sie im Feld Objekt an, welche Daten i5/OS zurückspeichern soll. Verwenden Sie hierbei das Format `/QNTC/servername/sharename`.
Platzhalterzeichen sind zulässig. Im Abschnitt „Beispiele: Komponenten eines integrierten Windows-Servers angeben“ auf Seite 208 ist beschrieben, wie Sie bestimmte Komponenten eines integrierten Windows-Servers angeben können. Windows-Systemdateien sollten nicht mit dieser Methode zurückgespeichert werden, da dies zu unvorhersehbaren Situationen führen kann.
5. Geben Sie im Feld Name den Pfad des zurückzuspeichernden Objekts an.
6. Über das Feld Einschließen oder auslassen können Objekte mit dem Muster, das im Abschnitt Name das Parameters Objekt definiert wurde, eingeschlossen oder ausgeschlossen werden.
7. Der im Feld Neuer Objektname angegebene Name kann übernommen werden, oder es kann ein neuer Pfadname angegeben werden. Auf den neuen Pfadnamen muss durch eine Freigabe verwiesen werden, die auf dem integrierten Windows-Server vorhanden ist.

Anmerkung:

Wird ein Verzeichnis mit übergeordneten Freigaben gesichert, sichert i5/OS die Freigabedaten zusammen mit dem Verzeichnis. Diese Freigaben werden nicht erneut erstellt, wenn beim Zurückspeichern des Verzeichnisses ein neuer Objektname angegeben wird.

8. Geben Sie im Feld Verzeichnisunterstruktur an, ob untergeordnete Strukturen eines Verzeichnisses zurückgespeichert werden sollen. In der Standardeinstellung werden alle Verzeichnisse zurückgespeichert.
9. Um Dateien zurückzuspeichern, die innerhalb eines bestimmten Zeitraums gesichert wurden, müssen im Feld Zeitraum der letzten Änderung die Start- und Enddaten und -zeiten angegeben werden.
10. Geben Sie weitere Daten ein, die i5/OS beim Zurückspeichern der Dateien verwenden soll, und drücken Sie die Eingabetaste.
11. Starten Sie den integrierten Server nach dem Zurückspeichern der Dateien neu, um neue Registrierungseinträge zu übernehmen.

Kapitel 13. Betriebssystem des Windows-Servers von der Hardware des integrierten Servers deinstallieren

Sie können mit dem Befehl DLTWNTSVR (Windows-Server löschen) den Windows-Server vom integrierten xSeries-Server deinstallieren. Vor der Ausführung des Befehls DLTWNTSVR müssen Sie den integrierten Windows-Server von i5/OS aus beenden. Entsprechende Anweisungen finden Sie unter „Integrierten Server starten und stoppen“ auf Seite 157.

Der Befehl DLTWNTSVR (Windows-Server löschen) löscht die angegebene NWS-Beschreibung des Windows-Servers und die zugehörigen Objekte, die mit dem Befehl INSWNTSVR (Windows-Server installieren) erstellt wurden. Zu diesen Objekten gehören die NWS-Beschreibung, Leitungsbeschreibungen, TCP/IP-Schnittstellen und vom System erstellte NWS-Speicherbereiche. Der Netzwerkserver muss abgehängt werden, bevor dieser Befehl abgesetzt wird.

- Wenn der Befehl DLTWNTSVR nicht benutzt werden kann (z. B. wenn das NWSD-Objekt des Servers nicht mehr vorhanden ist, einige der zugeordneten Objekte aber bereinigt werden müssen), können Sie den Server und die zugeordneten Objekte auch manuell löschen. Gehen Sie dazu folgendermaßen vor:
1. Beenden Sie den integrierten Server (siehe „Integrierten Server starten und stoppen“ auf Seite 157).
 2. „Verbindung von Plattenlaufwerken für integrierten Windows-Server aufheben“ auf Seite 177.
 3. „Plattenlaufwerke für integrierten Windows-Server löschen“ auf Seite 178.
 4. „NWS-Beschreibung eines integrierten Servers löschen“.
 5. „Leitungsbeschreibungen eines integrierten Servers löschen“ auf Seite 216.
 6. „TCP/IP-Schnittstellen löschen, die einem integrierten Windows-Server zugeordnet sind“ auf Seite 216.
 7. „Einem integrierten Windows-Server zugeordnete Controllerbeschreibungen löschen“ auf Seite 217.
 8. „Einem integrierten Windows-Server zugeordnete Einheitenbeschreibungen löschen“ auf Seite 217.
 9. „Einem integrierten iSCSI Windows-Server zugeordnete NWS-Konfigurationen löschen“ auf Seite 217

Wenn alle Windows- und Linux-Server, die ein bestimmtes NWSH-Objekt (NWSH = Netzwerkserver-Hostadapter) verwenden, aus i5/OS entfernt wurden und keine weiteren Server installiert werden sollen, die den NWSH verwenden, kann dieser gelöscht werden. Weitere Informationen finden Sie unter „NWS-Hostadapter löschen“ auf Seite 130.

Wenn alle Windows- und Linux-Server aus i5/OS entfernt wurden und keine neuen installiert werden sollen, kann IBM iSeries Integrated Server Support gelöscht werden, um den von diesem Produkt belegten Speicherplatz freizugeben. Weitere Informationen finden Sie unter „IBM i5/OS Integrated Server Support, i5/OS-Option 29 (5722-SS1) löschen“ auf Seite 218.

NWS-Beschreibung eines integrierten Servers löschen

Bevor Sie eine NWS-Beschreibung (NWSD) löschen, müssen Sie für alle mit dieser NWSD verbundenen Plattenlaufwerke die Verbindung aufheben (siehe „Verbindung von Plattenlaufwerken für integrierten Windows-Server aufheben“ auf Seite 177) und die Speicherbereiche löschen (siehe „Plattenlaufwerke für integrierten Windows-Server löschen“ auf Seite 178). Anschließend kann die NWSD gelöscht werden.

1. Um die Verbindung des Speicherbereichs für das Systemlaufwerk für NWSDs aufzuheben, die ab V4R5 erstellt wurden, muss in der i5/OS-Befehlszeile `RMVNWSSTGL NWSSTG(nwsdname1) NWSD(nwsdname)` eingegeben werden. Drücken Sie die Eingabetaste.
2. Um die Verbindung eines Speicherbereichs für das Installationsquellenlaufwerk aufzuheben, muss `RMVNWSSTGL NWSSTG(nwsdname2) NWSD(nwsdname)` eingegeben und die Eingabetaste gedrückt werden.

3. Darüber hinaus können zu diesem Zeitpunkt benutzerdefinierte Speicherbereiche entfernt werden, die mit der NWSD verbunden wurden. Verwenden Sie für jeden Speicherbereich den Befehl `RMVNWSTGL NWSSTG(nwsstgname) NWSD(nwsdname)`, und drücken Sie die Eingabetaste.
4. Das NWS-Speicherbereichsobjekt für das Systemlaufwerk wird gelöscht, indem Sie den Befehl `DLTNWSTG NWSSTG(nwsdname1)` eingeben und die Eingabetaste drücken.
5. Das NWS-Speicherbereichsobjekt für das Installationsquellenlaufwerk wird gelöscht, indem Sie `DLTNWSTG NWSSTG(nwsdname2)` eingeben und die Eingabetaste drücken.
6. Alle weiteren überflüssigen Speicherbereiche werden entfernt, indem Sie den Befehl `DLTNWSTG NWSSTG(nwsstgname)` eingeben und die Eingabetaste drücken.

So löschen Sie die NWS-Beschreibung (NWSD) eines integrierten Servers:

1. Geben Sie unter i5/OS den Befehl `WRKNWSD` ein, und drücken Sie die Eingabetaste.
2. Geben Sie im Feld Auswahl links neben dem Netzwerkserver eine 8 ein, und drücken Sie die Eingabetaste. Die Anzeige "Mit Konfigurationsstatus arbeiten" wird aufgerufen.
3. Wenn der Status der NWSD nicht "abgehängt" lautet, müssen Sie im Feld Auswahl links neben dem Netzwerkserver eine 2 eingeben und die Eingabetaste drücken. Fahren Sie andernfalls mit dem nächsten Schritt fort.
4. Drücken Sie F3, um zum vorherigen Dialog zurückzukehren.
5. Geben Sie im Feld Auswahl links neben dem Netzwerkserver eine 4 ein, und drücken Sie die Eingabetaste.
6. Drücken Sie in der Anzeige Löschen der NWS-Beschreibungen bestätigen die Eingabetaste.

Anmerkung: Wenn Sie eine NWSD löschen, die vor V4R5 erstellt wurde, lesen Sie die Informationen im Abschnitt über das Löschen der NWSD eines integrierten Windows-Servers im V5R3 iSeries Information Center.

Leitungsbeschreibungen eines integrierten Servers löschen

So löschen Sie alle Leitungsbeschreibungen eines integrierten Servers:

1. Geben Sie unter i5/OS den Befehl `WRKLIND` ein, und drücken Sie die Eingabetaste.
2. Blättern Sie bis zu der Leitungsbeschreibung vor, die gelöscht werden soll.

Anmerkung:

Der Name der Leitungsbeschreibung setzt sich aus dem Namen der NWS-Beschreibung (NWSD) gefolgt von 00, 01, 02, PP, V0, V1, V2, V3, V4, V5, V6, V7, V8 oder V9 zusammen. Dies ist von der Nummer des Ports abhängig, dem sie zugeordnet ist.

3. Geben Sie im Feld Auswahl links neben der Leitungsbeschreibung eine 4 ein, und drücken Sie die Eingabetaste. Wiederholen Sie diesen Schritt für alle Leitungsbeschreibungen, die der NWSD zugeordnet sind.

Anmerkung:

Anstelle der Schritte 1 und 2 kann auch der Befehl `WRKLIND NWSD-Name*` eingesetzt werden. Dabei steht NWSD-Name für den Namen der verbundenen NWS-Beschreibung.

TCP/IP-Schnittstellen löschen, die einem integrierten Windows-Server zugeordnet sind

So löschen Sie die TCP/IP-Schnittstellen, die einem integrierten Server zugeordnet sind:

1. Geben Sie an der i5/OS-Konsole den Befehl `CFGTCP` ein.
2. Wählen Sie im Menü TCP/IP konfigurieren die Auswahl 1. Mit TCP/IP-Schnittstellen arbeiten aus.
3. Geben Sie im Feld Auswahl neben der TCP/IP-Schnittstelle, die Sie entfernen wollen, eine 4 ein, und drücken Sie die Eingabetaste.

Die mit der NWS-Beschreibung verbundenen TCP/IP-Schnittstellen können anhand des Namens der zugeordneten Leitungsbeschreibungen identifiziert werden. Dieser setzt sich aus dem NWSD-Namen und einer Nummer zusammen.

4. Wiederholen Sie Schritt 3 für alle der NWSD zugeordneten TCP/IP-Schnittstellen.

Einem integrierten Windows-Server zugeordnete Controllerbeschreibungen löschen

So löschen Sie alle Controllerbeschreibungen für einen integrierten Server:

1. Geben Sie unter i5/OS den Befehl WRKCTLD ein, und drücken Sie die Eingabetaste.
2. Blättern Sie bis zu der Controllerbeschreibung vor, die gelöscht werden soll.

Anmerkung:

Der Name der Controllerbeschreibung beginnt mit den ersten fünf Zeichen des NWSD-Namens gefolgt von NET und einer zweistelligen Zahl. Lautet der NWSD-Name beispielsweise MYSERVER, heißt die Controllerbeschreibung MYSERVERNET01.

3. Geben Sie im Feld Auswahl links von der Controllerbeschreibung eine 4 ein, und drücken Sie die Eingabetaste. Wiederholen Sie diesen Schritt für alle Controllerbeschreibungen, die der NWSD zugeordnet sind.

| **Anmerkung:**

| Anstelle der Schritte 1 und 2 kann auch der Befehl WRKCTLD MYSER* verwendet werden.
| Dabei steht MYSER für die ersten 5 Zeichen des NWSD-Namens.

| **Achtung:** Wenn Sie nach dieser Methode vorgehen, verifizieren Sie, dass Sie wirklich alle
| NWSDs auf Ihrem System löschen möchten, die mit diesen 5 Zeichen beginnen.

Einem integrierten Windows-Server zugeordnete Einheitenbeschreibungen löschen

So löschen Sie alle Einheitenbeschreibungen für einen integrierten Server:

1. Geben Sie unter i5/OS den Befehl WRKDEVD ein, und drücken Sie die Eingabetaste.
2. Blättern Sie bis zu der Einheitenbeschreibung vor, die gelöscht werden soll.

Anmerkung:

Der Name der Einheitenbeschreibung beginnt mit den ersten fünf Zeichen des NWSD-Namens gefolgt von TCP und einer zweistelligen Zahl. Lautet der NWSD-Name beispielsweise MYSERVER, heißt die Einheitenbeschreibung MYSERVERTCP01.

3. Geben Sie im Feld Auswahl links von der Einheitenbeschreibung eine 4 ein, und drücken Sie die Eingabetaste. Wiederholen Sie diesen Schritt für alle Einheitenbeschreibungen, die der NWSD zugeordnet sind.

Anmerkung:

Auf einem System können zahlreiche Einheiten existieren. Über den Befehl WRKDEVD MYSE-
ERTCP* oder WRKDEVD *NET erhalten Sie eine vollständige Liste der Netzwerkeinheiten, die
gelöscht werden müssen.

Einem integrierten iSCSI Windows-Server zugeordnete NWS-Konfigurationen löschen

| So löschen Sie NWS-Konfigurationen, die einem integrierten Server zugeordnet sind:

- | 1. Geben Sie an der i5/OS-Konsole den Befehl WRKNWSCFG ein.
- | 2. Suchen Sie nach NWS-Konfigurationen, die der NWSD zugeordnet sind. Sie werden normalerweise als nwsdname* bezeichnet.

- | 3. Geben Sie im Feld Auswahl neben den NWS-Konfigurationen, die Sie entfernen wollen, eine 4 ein.
- | 4. Drücken Sie die **Eingabetaste**.

IBM i5/OS Integrated Server Support, i5/OS-Option 29 (5722-SS1) löschen

- | Wenn Sie alle integrierten Windows- und nicht-partitionierten Linux-Server von der iSeries entfernen und keine anderen erneut installieren möchten, sollten Sie auch IBM i5/OS Integrated Server Support, Option 29, aus i5/OS entfernen. Auf diese Weise wird der Speicherbereich, den dieses Programm unter i5/OS belegt hat, wieder freigegeben.

Anmerkung:


Durch das Entfernen des Programms werden vorhandene NWS-Beschreibungen oder benutzerdefinierte Plattenlaufwerke nicht automatisch gelöscht. Diese werden jedoch unbrauchbar. Weitere Informationen zum Löschen von NWS-Beschreibungen und Plattenlaufwerken finden Sie in Kapitel 13, „Betriebssystem des Windows-Servers von der Hardware des integrierten Servers deinstallieren“, auf Seite 215.

So löschen Sie IBM i5/OS Integrated Server Support:

- 1. Geben Sie unter i5/OS den Befehl `G0 LICPGM` ein, und drücken Sie die Eingabetaste.
- 2. Geben Sie im Menü Mit Lizenzprogrammen arbeiten die Auswahl 12 ein, und drücken Sie die Eingabetaste.
- | 3. Blättern Sie in der Liste der Lizenzprogramme bis zur Beschreibung Integrated Server Support vor.
- 4. Geben Sie im Feld Auswahl links neben der Option eine 4 ein. Drücken Sie die Eingabetaste. Die Option wird daraufhin von i5/OS gelöscht.




Kapitel 14. Fehlerbehebung bei integrierten Windows-Servern

Falls der integrierte Server nicht ordnungsgemäß funktioniert, führen Sie die folgenden Schritte aus, um den Fehler zu beheben:

1. Versuchen Sie, den integrierten Server erneut zu starten. Weitere Informationen hierzu finden Sie in „Integrierten Server starten und stoppen“ auf Seite 157.
2. Zeigen Sie die Informationen zur NWS-Beschreibung und zu den ihr zugeordneten Leitungen, Controllern und Einheiten an. Weitere Informationen finden Sie unter „Konfigurationsdaten des integrierten Windows-Servers anzeigen oder ändern“ auf Seite 160.
3. Bleibt das Problem bestehen, suchen Sie in den Protokollen nach hilfreichen Informationen. Entsprechende Anweisungen finden Sie unter „Nachrichten und Jobprotokolle prüfen“.
4. Suchen Sie anschließend im Abschnitt „Fehler auf integrierten Windows-Servern“ auf Seite 222 nach diesem speziellen Problem.
5. Lesen Sie außerdem in den APARs die neuesten Tipps und Serviceinformationen. Diese finden Sie auf der Website IBM Integrated xSeries Solutions .
6. Wenn auf dem integrierten Server Fehler auftreten, können Sie den Verlust von Anwendungen und Benutzerdaten unter Umständen verhindern, wenn Sie den integrierten Server erneut installieren. Weitere Informationen finden Sie unter „Integrierten Windows-Server erneut installieren“ auf Seite 257.
7. Weitere Informationen zur Erfassung von Servicedaten, die an die Benutzerunterstützung weitergeleitet werden können, finden Sie unter „Servicedaten des integrierten Windows-Servers erfassen“ auf Seite 257.

Weitere Optionen zur Fehlerbehebung

Wird in den Abschnitten zur Fehlerbehebung dieses Kapitels keine Lösung für das vorliegende Problem angeboten, können eventuell auch andere Serviceoptionen zur Problemlösung beitragen.

- Weitere Informationen finden Sie unter Troubleshooting  auf der Website Integrated xSeries solutions (www.ibm.com/servers/eserver/iserries/integratedxseries/troubleshooting.html).
- Bei Problemen mit bestimmten Anwendungen wenden Sie sich an den Anwendungslieferanten.
- Bei Hardwarefehlern des integrierten xSeries-Servers oder bei Serverinstallationsproblemen wenden Sie sich an den IBM Service.
- Bei nicht behebbaren Serverfehlern (z. B. Systemabsturzanzeigen) finden Sie möglicherweise weitere Informationen auf den folgenden Websites:
 - Support for the iSeries family  (www.ibm.com/servers/eserver/support/iserries/).
 - Microsoft Help and Support  (<http://support.microsoft.com>).

Falls Sie Serviceverträge mit IBM abgeschlossen haben und zusätzliche Unterstützung benötigen, hilft Ihnen der IBM Service bei der Suche nach der richtigen Problemlösung. Fordern Sie die Unterstützung über die IBM Support Line an.

Nachrichten und Jobprotokolle prüfen

Informationen zu den integrierten Windows-Servern werden an unterschiedlichen Stellen protokolliert. Wenn ein Fehler auftritt, können Sie die Ursache möglicherweise anhand dieser Informationen bestimmen.

Protokoll des Überwachungsjobs

Im Protokoll des Überwachungsjobs (siehe „Überwachungsjob“ auf Seite 221) werden normale Verarbeitungereignisse bis hin zu detaillierten Fehlernachrichten aufgezeichnet. So prüfen Sie dieses Protokoll:

1. Geben Sie in der i5/OS-Befehlszeile den Befehl WRKACTJOB (Mit aktivem Job arbeiten) ein, und suchen Sie im Subsystem QSYSWRK den Job, der denselben Namen hat wie Ihr Netzwerkservers. Falls der Job nicht in dieser Anzeige erscheint, wurde er entweder bereits beendet oder gar nicht erst gestartet.
2. Wenn Sie den Job finden, verwenden Sie Auswahl 5, um mit dem Job zu arbeiten, und Auswahl 10, um das Jobprotokoll anzuzeigen.
3. Drücken Sie F10, um detaillierte Nachrichten anzuzeigen.
4. Falls das Protokoll hilfreiche Informationen enthält, notieren Sie die Job-ID (alle drei Bestandteile: Name, Benutzer und Jobnummer). Drucken Sie anschließend das Protokoll mit dem folgenden Befehl aus: DSPJOBLOG JOB(Nummer/Benutzer/Name) OUTPUT(*PRINT)

Anmerkung:

Wurde der Überwachungsjob durch das Problem beendet oder versuchen Sie gerade, ein früher aufgetretenes Problem zu beheben, dann suchen Sie im vorherigen Jobprotokoll nach einer Spooldatei, die entsprechende Informationen enthält. Mit dem folgenden Befehl kann nach Spooldateien gesucht werden, die sich auf den Netzwerkservers beziehen: WRKSPLF SELECT(QSYS *ALL *ALL NWS-Name)

Jobprotokoll QVNAVARY

- | Das Jobprotokoll QVNAVARY enthält Nachrichten, die sich auf das Ab- und Abhängen der IXS oder über
 - | IXA angeschlossenen NWS-Beschreibung und erneuten Starten des Windows-Servers beziehen. So prüfen
 - | Sie dieses Protokoll auf Fehler, die beim Herunterfahren oder Starten auftreten:
1. Geben Sie in der i5/OS-Befehlszeile den Befehl WRKACTJOB (Mit aktivem Job arbeiten) ein, und suchen Sie im Subsystem QSYSWRK nach dem Job QVNAVARY.
 2. Verwenden Sie Auswahl 5, um mit dem Job zu arbeiten, und Auswahl 10, um das Jobprotokoll anzuzeigen.

Stattdessen kann auch WRKJOB JOB(QVNAVARY) verwendet werden.

- | Für IXS oder xSeries-Server mit IXA-Anschluss wird ein Stapeljob unter der Bezeichnung BTnwsdname
- | übergeben, um das Ab- und Anhängen auszuführen, das für den Warmstart (Reboot) des Servers erforderlich ist.
- | Identifizieren Sie den qualifizierten Namen des Jobs, der im Jobprotokoll QVNAVARY übergeben wurde.
- | Lokalisieren Sie das Jobprotokoll für den übergebenen Warmstartjob, indem Sie den Jobnamen vollständig
- | durch Angabe von WRKSPLF SELECT(*ALL) JOB(qualjobname) qualifizieren.
- | Listen Sie alle Warmstartjobs mit WRKSPLF SELECT(*ALL) JOB(BTnwsdname) auf.

Jobprotokoll des Jobs, der ein An- oder Abhängen eingeleitet hat

Wenn von einem Stapeljob oder einem interaktiven Benutzer im i5/OS das An- oder Abhängen einer NWS eingeleitet wurde, liefert das Protokoll für diesen Job unter Umständen hilfreiche Informationen. Beispiel: Wenn Sie den Befehl VRYCFG oder WRKCFGSTS benutzt haben, können Sie mit dem Befehl DSPJOB (Job anzeigen) und Auswahl 10 das Jobprotokoll anzeigen.

Servernachrichtwarteschlange

Haben Sie bei der Installation eine Nachrichtwarteschlange für den Netzwerkservers angegeben, liefert diese Nachrichtwarteschlange unter Umständen hilfreiche Informationen.

1. Um nachzuprüfen, ob eine Nachrichtenwarteschlange angegeben ist, geben Sie in der i5/OS-Befehlszeile DSPNWS NWS(NWS-Name) ein, und drücken Sie die Eingabetaste. Ist der Wert auf *NONE gesetzt, werden nur Nachrichten über schwer wiegende Fehler in der Nachrichtenwarteschlange QSYSOPR aufgezeichnet.
2. Ist eine Nachrichtenwarteschlange angegeben, verwenden Sie den folgenden Befehl unter i5/OS, um die Nachrichten anzuzeigen: DSPMSG MSGQ(Bibliothek/Warteschlange)

Nachrichtenwarteschlange des Systembedieners

Der integrierte Server aktualisiert die Nachrichtenwarteschlange des Systembedieners (QSYSOPR) mit Fehlermeldungen sowie mit normalen Start- und Beendigungsnachrichten. Um diese Nachrichten in der zeichenorientierten Schnittstelle anzuzeigen, geben Sie den Befehl DSPMSG QSYSOPR ein.

| DFV-Nachrichtenwarteschlange

| Server mit iSCSI-Anschluss enthalten einen Parameter für die DFV-Nachrichtenwarteschlange. Haben Sie bei der Installation eine DFV-Nachrichtenwarteschlange für den Netzwerkservers angegeben, liefert diese Nachrichtenwarteschlange unter Umständen hilfreiche Informationen über den Verbindungsstatus.

- | 1. Um nachzuprüfen, welche Nachrichtenwarteschlange angegeben wurde, geben Sie in der i5/OS-Befehlszeile DSPNWS NWS(NWS_Name) ein, und drücken Sie die Eingabetaste. Lautet der Wert für die DFV-Nachrichtenwarteschlange *SYSOPR, werden Nachrichten in der Nachrichtenwarteschlange QSYSOPR aufgezeichnet.
- | 2. Ist eine DFV-Nachrichtenwarteschlange angegeben, verwenden Sie den folgenden Befehl unter i5/OS, um die Nachrichten anzuzeigen: DSPMSG MSGQ(Bibliothek/Warteschlange).

Jobprotokoll für die Profilsynchronisation

Das Jobprotokoll für die Profilsynchronisation enthält Nachrichten, die von EIM und der Benutzerprofilregistrierung zurückgegeben werden. Dieses Protokoll können Sie überprüfen, indem Sie den Befehl WRKJOB QPRFSYNCH eingeben.

Überwachungsjob

Jeder aktive integrierte Windows-Server verfügt über einen Überwachungsjob, der gleichzeitig mit dem Server gestartet wird. Der Überwachungsjob läuft im Subsystem QSYSWRK unter dem Benutzerprofil QSYS. Der Jobname entspricht dem Namen der NWS-Beschreibung, die von ihm überwacht wird.

Beim Starten des Überwachungsjobs sendet i5/OS die Informationsnachricht CPIA41B an die Nachrichtenwarteschlange QSYSOPR. Diese Nachricht enthält die Job-ID des Überwachungsjobs. Mit Hilfe dieser Job-ID und dem Befehl WRKJOB (Mit Job arbeiten) können Sie das Jobprotokoll des Überwachungsjobs und andere jobbezogene Informationen für den Überwachungsjob finden.

| Zusätzliche Protokolle und Nachrichten für Server mit iSCSI-Anschluss

| Jobprotokoll für NWS-Hostadapter

| NWS-Hostadapter werden von i5/OS zu bestimmten Systemjobs zugeordnet. Das Jobprotokoll des Systemjobs, der dem NWS-Hostadapter zugeordnet ist, kann hilfreiche Informationen liefern.

- | 1. Um den Namen des Systemjobs festzustellen, geben Sie in der i5/OS-Befehlszeile DSPDEV DEV(NWS-Name) ein, und drücken Sie die Eingabetaste. Blättern Sie vor bis zu den Jobnamen.
- | 2. Verwenden Sie den Befehl DSPJOB (Job anzeigen) und Auswahl 10, um das Jobprotokoll für den genannten Job anzuzeigen.

| Nachrichtenwarteschlange der NWS-Hosteinheit

| NWS-Hostadapter enthalten einen Parameter für die Nachrichtenwarteschlange. Diese Nachrichtenwarteschlange kann hilfreiche Informationen liefern.

1. Informationen darüber, wie Sie feststellen können, welche Nachrichtenwarteschlange verwendet wird, finden Sie unter „Eigenschaften des NWS-Hostadapters anzeigen“ auf Seite 128. Klicken Sie auf die Indexzunge **Datenübertragung**, und notieren Sie den Namen der Nachrichtenwarteschlange und der Bibliothek.
2. Gehen Sie wie folgt vor, um die Nachrichtenwarteschlange im iSeries Navigator anzuzeigen:
 - a. Erweitern Sie **Basisoperation**—> **Nachrichten**.
 - b. Klicken Sie mit der rechten Maustaste auf **Nachrichten**, und wählen Sie **Ansicht anpassen**—> **Einschließen...**
 - c. Wählen Sie die Option **Nachrichtenwarteschlange** aus, und geben Sie den Namen der Nachrichtenwarteschlange und der Bibliothek ein, die sich auf der Anzeige der Eigenschaften des NWS-Hostadapters befinden.

Anmerkung: Wird „Systembediener“ auf der Anzeige der NWSH-Eigenschaften angezeigt, geben Sie QSYSOPR als Nachrichtenwarteschlange an.

Produktaktivitätenprotokoll (PAL)


Einige Fehler, die das iSCSI-Netzwerk betreffen, wie beispielsweise CHAP-Authentifizierungsfehler, werden im PAL protokolliert. So greifen Sie auf das PAL zu:

1. Führen Sie den CL-Befehl STRSST (Systemserviceprogramme starten) aus.
2. Wählen Sie **Serviceprogramm starten** aus.
3. Wählen Sie **Produktaktivitätenprotokoll** aus.

Fehler auf integrierten Windows-Servern




Arbeitet der integrierte Windows-Server nicht korrekt, prüfen Sie, ob der Fehler in der folgenden Liste aufgeführt ist:

- „STOP oder Blue-Screen-Fehler“ auf Seite 223
- Angaben zu Fehlern bei der Ausführung des Programms für die Softwarepflege finden Sie unter „Snap-in-Programm von IBM iSeries Integrated Server Support“ auf Seite 235
- **Laufwerkfehler**
 - „Zu wenig Speicherplatz auf dem Systemlaufwerk des integrierten Servers“ auf Seite 223
- **Einheitenfehler**
 - „Fehler bei optischen Einheiten“ auf Seite 224
 - „Bandfehler“ auf Seite 225
- **Fehler beim Starten/Stoppen**
 - „Fehler beim Starten eines integrierten Windows-Servers“ auf Seite 227
 - „Fehler beim Hot-Sparing zwischen Servern“ auf Seite 228
 - „Fehler in der NWS-D-Konfigurationsdatei“ auf Seite 231
- **Extern angeschlossene xSeries-Server**
 - „DASD in Servern mit IXa- oder iSCSI-Anschluss“ auf Seite 232
- **Fehler bei Benutzer- und Gruppenregistrierung**
 - „Fehler bei der Benutzer- und Gruppenregistrierung“ auf Seite 232
 - „Berechtigungsfehler bei der Benutzerregistrierung“ auf Seite 233
 - „Kennwortfehler“ auf Seite 234
- **xSeries- oder IBM BladeCenter-Server mit iSCSI-Anschluss**
 - „Fehler auf Servern mit iSCSI-Anschluss“ auf Seite 236
 - „Netzplananalyse für Boot- und Speicherpfade“ auf Seite 238
 - „Pfadzertifikate verwalten“ auf Seite 238
 - „Fehlerbehebung für IBM Director“ auf Seite 239

- | - „Fehler bei der Erkennung“ auf Seite 240
- | - „Fehler bei SSL-Verbindungen“ auf Seite 240
- | - „Virtual Ethernet-Fehler bei Servern mit iSCSI-Anschluss“ auf Seite 242
- **Netzwerkfehler**
 - „Virtual Ethernet-Fehler bei IXS und Servern mit IXA-Anschluss“ auf Seite 244
 - „Fehler bei externen Netzwerken“ auf Seite 248
 - „LAN-Treiber auf dem integrierten Windows-Server manuell aktualisieren“ auf Seite 249
 - „IP-Adressenkonflikte bei Virtual Ethernet-Punkt-zu-Punkt“ auf Seite 251
 - „IFS-Zugriffsfehler“ auf Seite 254
 - „Fehler bei TCP/IP über Virtual Ethernet“ auf Seite 253
 - „Fehler beim Zugriff auf Freigaben von Windows Server 2003 mit dem Dateisystem QNTC“ auf Seite 254
- | • „Fehler bei der gemeinsamen Nutzung von Hardware für Hosted Systeme“ auf Seite 229
- „Fehler beim Sichern von Dateien des integrierten Windows-Servers“ auf Seite 254
- „Nicht lesbare Nachrichten in der Servernachrichtenwarteschlange“ auf Seite 255
- „Fehler beim Erstellen eines Windows-Systemspeicherauszugs“ auf Seite 256
- | Wenn Ihnen die oben genannten Abschnitte bei Ihrem Problem nicht weiterhelfen konnten, rufen Sie auf
- | die Webseite xSeries solutions Troubleshooting  unter
- | <http://www.ibm.com/servers/eserver/iserie/integratedxseries/troubleshooting.html> auf. Auf dieser
- | Webseite finden Sie weitere Quellen mit Fehlerbehebungsinformationen.

STOP oder Blue-Screen-Fehler

Treten Blue-Screen-Fehler auf, führen Sie folgende Schritte durch, um die Fehlerursache zu bestimmen und geeignete Fehlerbehebungsmaßnahmen zu finden:

1. Geben Sie in der i5/OS-Befehlszeile DSPMSG QSYSOPR ein.
2. Drücken Sie die Eingabetaste. Die Nachrichtenwarteschlange QSYSOPR wird angezeigt.
3. Prüfen Sie, ob eine der Nachrichten einen Anhaltspunkt für den Blue-Screen-Fehler liefert.
4. Starten Sie den integrierten Server erneut, indem Sie ihn über i5/OS ab- und wieder anhängen (siehe „Integrierten Server starten und stoppen“ auf Seite 157).
5. Überprüfen Sie das Ereignisprotokoll unter Windows auf Fehler, die Art des Stoppcodes und andere Diagnoseinformationen.
- | 6. Prüfen Sie, ob PAL-Einträge und VLOGs vorhanden sind.
7. Wenn das Problem weiterhin besteht, überprüfen Sie die Datenbank mit technischen Informationen auf der Webseite  **server** IBM iSeries Support . Wird dort keine L"sung angeboten, wenden Sie sich an die technische Unterstützung.
- | 8. Informationen für Server mit iSCSI-Anschluss finden Sie auf der Webseite iSCSI troubleshooting  (www.ibm.com/servers/eserver/iserie/integratedxseries/iscsireadme/troubleshooting.html).

Zu wenig Speicherplatz auf dem Systemlaufwerk des integrierten Servers


Auf dem Systemlaufwerk befindet sich das Betriebssystem des Windows-Servers, wobei es zusätzlich noch Anwendungen und Daten enthalten kann. Wenn auf dem Laufwerk nicht mehr genug Speicherplatz frei ist, kann dies dazu führen, dass entsprechende Nachrichten ausgegeben werden oder Fehler bei der Auslagerungsdatei auftreten.

Mit einem oder mehreren der folgenden Schritte können Sie verhindern, dass das Systemlaufwerk zu voll wird:

- Vergrößern Sie das Systemlaufwerk bei der Installation des Windows-Servers.
- Installieren Sie Anwendungen statt auf dem standardmäßig angegebenen Systemlaufwerk in einem benutzerdefinierten Speicherbereich.
- Versetzen Sie die Auslagerungsdatei des Windows-Servers in einen benutzerdefinierten Speicherbereich, statt sie standardmäßig auf dem Systemlaufwerk zu halten. Wird die Auslagerungsdatei versetzt, kann kein Speicherauszug des Systemspeichers erstellt werden, wenn ein STOP- oder Blue-Screen-Fehler auftritt. Gehen Sie zum Versetzen der Auslagerungsdatei folgendermaßen vor:
 1. Klicken Sie mit der rechten Maustaste auf das Symbol **Arbeitsplatz**, und wählen Sie **Eigenschaften** aus.
 2. Wählen Sie die Indexzunge **Erweitert** aus.
 3. Klicken Sie auf die Schaltfläche **Systemleistungsoptionen**.
 4. Klicken Sie auf die Schaltfläche **Ändern**, um das Fenster **Virtueller Arbeitsspeicher** anzuzeigen.
 5. Wählen Sie einen benutzerdefinierten Speicherbereich aus, auf dem ausreichend freier Speicherplatz verfügbar ist.
 6. Klicken Sie auf **OK**.
- Versetzen Sie den Speicherauszug des Windows-Servers in einen benutzerdefinierten Speicherbereich, statt ihn standardmäßig auf dem Systemlaufwerk zu halten. Gehen Sie dazu folgendermaßen vor:
 1. Klicken Sie auf **Start, Einstellungen** und **Systemsteuerung**.
 2. Klicken Sie auf die Indexzunge **Starten/Herunterfahren**.
 3. Wählen Sie im Abschnitt **Wiederherstellung** in diesem Fenster die Option **Debug-Info festhalten in** aus.
 4. Wählen Sie einen benutzerdefinierten Speicherbereich aus, auf dem ausreichend freier Speicherplatz vorhanden ist (um ca. 12 MB größer als der RAM). Zusätzliche Empfehlungen und Anforderungen an die Größe der Auslagerungsdatei sind in der Windows-Dokumentation zu finden.
 5. Klicken Sie auf **OK**.

Anmerkung:



Wird der Hauptspeicherauszug des Windows-Servers in einen benutzerdefinierten Speicherbereich versetzt, muss die Speicherauszugsdatei zur Weiterleitung an die technische Unterstützung auf Band kopiert werden.

- Wenn das Problem weiterhin besteht, überprüfen Sie die Datenbank mit technischen Informationen auf der Webseite [@server IBM iSeries Support](#) . Wird dort keine Lösung angeboten, wenden Sie sich an die technische Unterstützung.

Fehler bei optischen Einheiten

Wenn die optische Einheit von i5/OS mit einem integrierten Windows-Server nicht funktioniert, führen Sie folgende Schritte durch:

1. Vergewissern Sie sich, dass die optische Einheit unter i5/OS angehängt ist. Weitere Informationen zum Anhängen der optischen Einheit finden Sie unter „Optische iSeries-Laufwerke mit integrierten Windows-Servern verwenden“ auf Seite 179.
2. Vergewissern Sie sich, dass das optische Laufwerk dem integrierten Server zugeordnet ist.
3. Prüfen Sie, ob ein optischer Datenträger in das Laufwerk eingelegt ist.
4. Verfügt das System über logische Partitionen, müssen Sie überprüfen, ob die optische Einheit derselben Partition zugeordnet ist wie der integrierte Server.
5. Prüfen Sie das Ereignisprotokoll auf Fehler, die sich auf die optische Einheit beziehen.
6. Prüfen Sie, ob die optische Einheit unter **Arbeitsplatz** auf dem Windows-Server angezeigt wird.
7. Fehlerbehebungsmaßnahmen für optische Einheiten:

- a. Schließen Sie das Snap-in-Programm von IBM iSeries Integrated Server Support.
 - b. Hängen Sie die optische Einheit auf der iSeries ab.
 - c. Hängen Sie die optische Einheit an.
 - d. Ordnen Sie die Einheit dem integrierten Server erneut zu.
8. Wenn das Problem weiterhin besteht, überprüfen Sie die Datenbank mit technischen Informationen auf der Webseite  **server** IBM iSeries Support .
9. Wird dort keine Lösung angeboten, wenden Sie sich an die technische Unterstützung.

Tritt auf dem integrierten Server vor der Freigabe eines optischen Laufwerks ein Fehler auf, ist das optische Laufwerk für i5/OS und andere integrierte Server nicht verfügbar. Weitere Informationen finden Sie unter „Sperre der optischen Einheit bei ausgefallenem Server“.



Sperre der optischen Einheit bei ausgefallenem Server

Tritt auf dem integrierten Server vor der Freigabe eines optischen Laufwerks (bzw. dem Abhängen des Servers) ein Fehler auf, ist das optische Laufwerk für i5/OS und andere Windows-Server nicht verfügbar. Das optische Laufwerk muss in diesem Fall mittels WRKCFGSTS *DEV *OPT abgehängt und erneut angehängt werden, um die Sperre aufzuheben.

Bandfehler

Wenn das iSeries-Bandlaufwerk auf dem integrierten Windows-Server nicht funktioniert, führen Sie folgende Schritte durch:

1. Das Bandlaufwerk muss unter i5/OS abgehängt und auf einem integrierten Server gesperrt werden (siehe „iSeries-Bandlaufwerk einem integrierten Windows-Server zuordnen“ auf Seite 182). Einheiten können unter Umständen aus einem der folgenden Gründe nicht zugeordnet (bzw. gesperrt) werden:
 - Die Bändeinheit oder das zugehörige Kassettenarchiv ist angehängt.
 - Der Einheits-treiber ist nicht geladen.
 - Die Bändeinheit wird nicht unterstützt.
 - Bestehen Probleme beim Sperren der Einheit, prüfen Sie, ob der Einheits-treiber auf dem integrierten Server geladen ist. Dies geschieht in der Regel automatisch. Weitere Informationen finden Sie unter „Prüfen, ob der Einheits-treiber für Bandlaufwerke geladen ist“ auf Seite 226.
 - Prüfen Sie, ob das Bandlaufwerk unterstützt wird. Weitere Informationen finden Sie unter „Unterstützte iSeries-Bandlaufwerke“ auf Seite 183.
2. Durch komplexere Anwendungen werden Einheiten eventuell bestimmten Diensten zugeordnet, die auch nach dem Verlassen der Anwendungsschnittstelle fortgesetzt werden. Dadurch wird verhindert, dass andere Anwendungen die Einheit benutzen können. Diese Dienste werden nach einem Systemwiederanlauf möglicherweise automatisch neu gestartet und ordnen die Einheit wieder der Anwendung zu. So zeigen Sie die Dienste einer Anwendung (wie z. B. Seagate und Computer Associates) an:
 - a. Klicken Sie auf **Start, Programme, Verwaltung und Komponentendienste**.
 - b. Doppelklicken Sie auf **Dienste**.
 - c. Falls erforderlich, können Dienste über das Fenster **Dienste** auch gestoppt werden.
3. Möglicherweise verwenden Sie mehrere integrierte Server. Ist dies der Fall, prüfen Sie, ob das Bandlaufwerk auf allen Servern freigegeben ist, mit Ausnahme des Servers, auf dem es benutzt werden soll (siehe „Steuerung von optischen Laufwerken und Bandlaufwerken der iSeries zwischen integrierten Windows-Servern übertragen“ auf Seite 184).
4. Verfügt das System über logische Partitionen, müssen Sie prüfen, ob das Bandlaufwerk derselben Partition zugeordnet ist wie der integrierte Server.
5. Vergewissern Sie sich, dass das Laufwerk ein korrekt formatiertes Band enthält. Weitere Informationen finden Sie unter „Band unter i5/OS für integrierte Windows-Server formatieren“ auf Seite 181.
6. Stellen Sie mit dem Befehl DSPNWS (NWS-Beschreibung anzeigen) sicher, dass das Laufwerk nicht in der Liste der eingeschränkten Einheiten unter i5/OS aufgeführt ist.

7. Prüfen Sie das Ereignisprotokoll auf Bandfehler.
8. Stellen Sie fest, ob die Bandeinheit in der Geräteliste enthalten ist:
 - a. Klicken Sie auf **Start, Programme, Verwaltung und Computerverwaltung**.
 - b. Wählen Sie **Systemprogramme** und dann **Geräte-Manager** aus.
 - c. Prüfen Sie, ob das Bandlaufwerk in der **Geräteliste** enthalten ist.
9. Wenn das Problem weiterhin besteht, überprüfen Sie die Datenbank mit technischen Informationen auf der Webseite  **server** IBM iSeries Support . Wird dort keine L"sung angeboten, wenden Sie sich an die technische Unterstützung.

Prüfen, ob der Einheits-treiber für Bandlaufwerke geladen ist

Bevor Anwendungen, die auf dem integrierten Server ausgeführt werden, das iSeries-Bandlaufwerk benutzen können, muss der Einheits-treiber auf den integrierten Server geladen werden. Dies geschieht in der Regel automatisch. Weitere Informationen über unterstützte Bandlaufwerke finden Sie unter „Unterstützte iSeries-Bandlaufwerke“ auf Seite 183.

So können Sie prüfen, ob der Bandeinheit-treiber geladen ist:

1. Klicken Sie in der Taskleiste des Windows-Servers auf **Start, Programme und Verwaltung**.
2. Klicken Sie auf **Computerverwaltung, Systemprogramme und Geräte-Manager**.
3. Erweitern Sie das Symbol mit dem Namen Ihres Computers. Wenn eine Bandeinheit geladen ist, erscheint ein Symbol für das Bandgerät.
4. Erweitern Sie das Symbol **Band-einheit**, um die geladenen Bandeinheit-treiber anzuzeigen.

Wenn Sie über ein IBM iSeries-Bandlaufwerk verfügen, das keinen Treiber eines Drittherstellers benötigt, und Sie die Einheits-treiber manuell laden müssen, führen Sie diese Schritte an der Konsole des integrierten Servers aus.

1. Klicken Sie auf **Start, Einstellungen und Systemsteuerung**.
2. Klicken Sie auf **Hardware**.
3. Klicken Sie im Hardware-Assistenten auf **Weiter**.
4. Wählen Sie **Gerät hinzufügen bzw. Problem beheben** aus, und klicken Sie auf **Weiter**.
5. Wählen Sie im Abschnitt **Gerät wählen** des Fensters "Hardware-Assistent" die Option **Neues Gerät hinzufügen** aus, und klicken Sie auf **Weiter**.
6. Wählen Sie im Abschnitt **Suche nach neuen Hardwarekomponenten** des Fensters "Hardware-Assistent" die Option "Nein, die Hardwarekomponenten selbst in der Liste auswählen" aus, und klicken Sie auf **Weiter**.
7. Blättern Sie im Kombinationsfeld des Abschnitts "Hardwaretyp" bis zu **Bandlaufwerke**, wählen Sie diese Option aus, und klicken Sie auf **Weiter**.
8. Wählen Sie im Teilfenster "Hersteller" des Abschnitts "Gerätetreiber auswählen" **IBM** aus. Wählen Sie im Teilfenster "Modelle" **IBM iSeries Bandlaufwerk** aus, und klicken Sie auf **Weiter**.
9. Klicken Sie im Abschnitt "IBM iSeries-Bandlaufwerk" dieses Fensters auf **Weiter**.
10. Erscheint das Markierungsfeld "Erforderliche Dateien", geben Sie im Feld "Dateien kopieren von" %SystemRoot%\System32\drivers ein, wobei C: das Systemlaufwerk ist. Klicken Sie auf **OK**.
11. Klicken Sie im Abschnitt "Fertigstellen des Assistenten" des Fensters "Hardware-Assistent" auf **Fertigstellen**. Damit müssten alle Bandeinheiten geladen sein.
12. Wiederholen Sie nach dem Neustart des Computers die Schritte 1 bis 4, um sicherzustellen, dass die Einheiten geladen wurden.

Informationen über das Laden anderer Bandeinheit-treiber finden Sie unter „Band-einheit-treiber installieren“ auf Seite 181.

Fehler beim Starten eines integrierten Windows-Servers

Kann der integrierte Server nicht gestartet werden, führen Sie die folgenden Schritte durch, um den Fehler zu beheben.

1. Überprüfen Sie den Status des Servers. Der aktuelle Status der NWSD muss ABGEHÄNGT sein. Ist dies nicht der Fall, hängen Sie die NWSD ab. Versuchen Sie anschließend, den Server erneut zu starten. Weitere Informationen hierzu finden Sie in „Integrierten Server starten und stoppen“ auf Seite 157. Lautet der Status des Servers ANHÄNGEN ANSTEHEND, obwohl der integrierte Server nicht gestartet wurde, besteht möglicherweise ein Problem mit dem Einheitentreiber.
2. Suchen Sie im Jobprotokoll nach Fehlnachrichten und möglichen Fehlerbehebungsmaßnahmen, die sich auf das Anhängen der NWSD beziehen.
3. Suchen Sie in der Nachrichtenwarteschlange QSYSOPR nach Fehlnachrichten und möglichen Fehlerbehebungsmaßnahmen.
4. Werden die Fehler durch die von Ihnen erstellte Serverkonfigurationsdatei verursacht, versuchen Sie, diese zu korrigieren oder zurückzusetzen. Weitere Informationen finden Sie unter „Fehler in der NWSD-Konfigurationsdatei“ auf Seite 231.
5. Haben Sie am integrierten Server einen Neustart eingeleitet, führen Sie die folgenden Schritte aus.
 - a. Geben Sie unter i5/OS den Befehl WRKACTJOB SBS(QSYSWRK) ein.
 - b. Drücken Sie die Eingabetaste.
 - c. Suchen Sie den Job QVNAVARY.
 - d. Verwenden Sie Auswahl 5, um mit dem Job zu arbeiten.
 - e. Ist der Job aktiv oder befindet er sich in der Jobwarteschlange, verwenden Sie Auswahl 10, um das Jobprotokoll anzuzeigen. Suchen Sie nach Fehlnachrichten und möglichen Fehlerbehebungsmaßnahmen.
 - f. Haben Sie den Job beendet, geben Sie WRKSPLF SELECT(*CURRENT *ALL *ALL QVNAVARY) ein, um die Spooldatei anzuzeigen.
6. Geben Sie den Befehl WRKPRB ein, um die protokollierten Probleme aufzulisten.

| Für IXS oder xSeries-Server mit IXA-Anschluss wird ein Stapeljob unter der Bezeichnung BTnwsdname
| übergeben, um das Ab- und Anhängen auszuführen, das für den Warmstart (Reboot) des Servers erforderlich ist.

| Identifizieren Sie den qualifizierten Namen des Jobs, der im Jobprotokoll QVNAVARY übergeben wurde.
| Lokalisieren Sie das Jobprotokoll für den übergebenen Warmstartjob, indem Sie den Jobnamen vollständig
| durch Angabe von WRKSPLF SELECT(*ALL) JOB(qualjobname) qualifizieren.

| Listen Sie alle Warmstartjobs mit WRKSPLF SELECT(*ALL) JOB(BTnwsdname) auf.

Notfallmaßnahmen

Wenn der Fehler aufgrund eines fehlerhaften Systemlaufwerks bestehen bleibt, Sie jedoch eine Sicherung dieses Laufwerks besitzen, versuchen Sie, den Fehler mit Hilfe dieser Notfallmaßnahmen zu beheben. Führen Sie die folgenden Schritte durch, um verloren gegangene Daten wiederherzustellen und das System wieder betriebsbereit zu machen.

Anmerkung:

In diesen Beispielen wird eine NWSD namens *ERS* mit einem Systemlaufwerk namens *ERS1* verwendet.

1. Trennen Sie die Verbindung zu dem fehlerhaften Systemlaufwerk (normalerweise Laufwerk C:) mit dem folgenden Befehl: `RMVNWSSSTGL NWSSTG(ERS1) NWSD(ERS)`
2. Kopieren Sie das fehlerhafte Systemlaufwerk mit dem folgenden Befehl unter einem neuen Namen: `CRTNWSSTG NWSSTG(ERSBKP) FROMNWSSTG(ERS1)`
3. Speichern Sie die letzte Sicherung des Systemlaufwerks zurück.

4. Stellen Sie eine Verbindung zu dem zurückgespeicherten Systemlaufwerk mit dem folgenden Befehl her: `ADDNWSSTGL NWSSTG(ERS1) NWS(ERS)`
5. Stellen Sie eine Verbindung zu dem fehlerhaften Systemlaufwerk aus Schritt 1 mit dem folgenden Befehl her: `ADDNWSSTGL NWSSTG(ERS1BKP) NWS(ERS)`
6. Hängen Sie die NWS mit dem folgenden Befehl an: `VRYCFG CFGOBJ(ERS) CFGTYPE(*NWS) STATUS(*ON)`
7. Kopieren Sie alle wichtigen Dateien, wie z. B. Datendateien, von dem fehlerhaften Systemlaufwerk, die sich seit der letzten Sicherung geändert haben.
8. Installieren Sie alle Anwendungen, die Sie seit der letzten Sicherung hinzugefügt oder für die Sie einen Upgrade durchgeführt haben.
9. Hängen Sie die NWS mit dem folgenden Befehl ab: `VRYCFG CFGOBJ(ERS1) CFGTYPE(*NWS) STATUS(*OFF)`
10. Trennen Sie die Verbindung zu dem fehlerhaften Systemlaufwerk aus Schritt 5 mit dem folgenden Befehl: `RMVNWSSTGL NWSSTG(ERS1BKP) ERS(ERS1)`
11. Sie können die Verbindung zu dem fehlerhaften Systemlaufwerk so oft wiederherstellen (Schritt 5) und weitere Dateien auf das wiederhergestellte Laufwerk kopieren, bis Sie sicher sind, dass Sie alle Daten von dem fehlerhaften Laufwerk entfernt haben. Nachdem Sie alle Daten von dem fehlerhaften Systemlaufwerk entfernt haben, erstellen Sie eine neue Sicherung aller Speicherbereiche. Die Schritte bei der Sicherung von Speicherbereichen sind unter „Vordefinierte Plattenlaufwerke für integrierte Windows-Server sichern“ auf Seite 201 beschrieben. Löschen Sie anschließend das fehlerhafte Systemlaufwerk mit dem folgenden Befehl: `DLTNWSSTG NWSSTG(ERS1BKP)`

| Fehler beim Hot-Sparing zwischen Servern

| Unterschiede bei der Hardware sind die Hauptursache dafür, dass das Hot-Sparing zwischen integrierten Servern nicht funktioniert. Die Aktivierung von Windows Server 2003 kann ebenfalls zu Problemen führen. Weitere Informationen finden Sie in den folgenden Abschnitten.

| Kompatibilität der Hot-Spare-Hardware

| Der Wechsel eines Windows-Servers von einer Hardwaregruppe auf eine andere ist vergleichbar mit der Migration des Windows-Systemlaufwerks von einem PC auf einen anderen. Unterschiede bei der erforderlichen HAL (Hardware Abstraction Layer), der BIOS-Version (Basic Input/Output System) oder den auf den beiden PCs installierten Einheiten können zu Problemen bei der Migration führen. Hardwareunterschiede werden beim einleitenden Booten von Windows auf dem zweiten PC festgestellt und auf eine der folgenden Arten behandelt:

- | • Einige Hardwareunterschiede können automatisch via Plug and Play aufgehoben werden.
- | • Bei einigen Hardwareunterschieden kann ein manueller Eingriff, wie beispielsweise die Installation eines neuen Einheitentreibers, erforderlich sein.
- | • Zu große Unterschiede bei der Hardware können dazu führen, dass der zweite PC nicht gebootet werden kann. Dies kann der Fall sein, wenn für beide PCs HAL-Versionen erforderlich sind, die nicht kompatibel sind.

| Die Informationen zur Hardwarekompatibilität in den vorherigen Abschnitten gelten gleichermaßen für das Hot-Sparing zwischen IXS-Servern, xSeries-Servern mit IXA-Anschluss und IBM xSeries- oder BladeCenter-Servern mit iSCSI-Anschluss. Damit die Hot-Spare-Migration erfolgreich durchgeführt werden kann, müssen die Hardwarekonfigurationen der beiden Server weitestgehend übereinstimmen.

| Hot-Spare für integrierte xSeries-Server (IXS)

| Damit Hot-Spare zwischen IXS-Servern funktioniert, müssen die Server kompatible Typen, vergleichbare LAN-Adapterkonfigurationen u.s.w. aufweisen. Die Konfigurationstabelle für den integrierten xSeries-Server auf der nachfolgend genannten Webseite enthält die speziellen IXS-Hot-Spare-Konfigurationen, die unterstützt werden: http://www.ibm.com/eserver/iserie/integratedxseries/ixs_system_config.html.

| Hot-Spare für xSeries- oder IBM BladeCenter-Server

| Damit Hot-Spare zwischen xSeries-Servern mit IXA-Anschluss oder zwischen xSeries- oder IBM BladeCenter-Servern mit iSCSI-Anschluss funktioniert, wird dringend empfohlen, den gleichen xSeries- oder IBM BladeCenter-Blade-Servertyp zu verwenden. So kann beispielsweise eine xSeries Modell 236 als Hot-Spare für eine andere xSeries Modell 236 dienen. Außerdem sollten die xSeries-Server die gleiche PCI-Adapterkonfiguration u.s.w. aufweisen.

| **Anmerkung:** Es besteht zwar die Möglichkeit, dass auch ein Hot-Spare zwischen zwei xSeries- oder Blade-Servern unterschiedlicher Modelle funktioniert, doch es bestehen oft erhebliche Hardwareunterschiede zwischen den xSeries- oder Blade-Modellen. Deshalb sollten Sie die Kombination aus xSeries- oder Blade-Servermodellen testen, die Sie in diesem Fall für ein Hot-Spare verwenden möchten. Mit dem Test können Sie verifizieren, dass die Hardwarekonfigurationen der xSeries- oder Blade-Servermodelle kompatibel sind und nahtlos untereinander migriert werden können, bevor Sie sie in einer Produktionsumgebung für den Server-Backup im Hot-Spare-Verfahren einsetzen.

| Aktivierung von Windows Server 2003

| Jedes Mal, wenn die Speicherbereiche eines Windows Server 2003 auf einen anderen integrierten Hot-Spare-Server umgeschaltet werden, kann die Windows-Aktivierung ausgelöst werden. Pro Lizenzschlüssel steht eine begrenzte Anzahl freier Aktivierungen zur Verfügung. Wurde die Aktivierung entsprechend oft ausgelöst, kann ein Telefonanruf bei Microsoft erforderlich sein, damit eine Reaktivierung veranlasst wird. Die Geschwindigkeit mit der ein Server reaktiviert wird, kann dadurch herabgesetzt werden. In diesem Fall kann die Lizenzierung für große Bestellvolumen von Windows Server 2003 hilfreich sein, da die Reaktivierung dann nicht erforderlich ist.

| Fehler bei der gemeinsamen Nutzung von Hardware für Hosted Systeme

| Die folgenden Links enthalten Informationen über Probleme bei der gemeinsamen Nutzung von Hardware für Hosted Systeme.

- | • „Mehrere NWSDs für gemeinsame Nutzung von Hardware für Hosted Systeme definiert“
- | • „Besonderheiten bei Systemen mit iSCSI-Anschluss“ auf Seite 230

| Mehrere NWSDs für gemeinsame Nutzung von Hardware für Hosted Systeme definiert

| Es besteht die Möglichkeit, mehrere NWS-Beschreibungen (NWSDs) für die Hardwaresteuerung eines bestimmten integrierten xSeries-Servers (IXS), xSeries-Systems oder IBM BladeCenter-Blades zu definieren. Bei Servern ohne iSCSI-Anschluss müssen sich diese NWSDs in derselben iSeries-Partition befinden. Bei Servern mit iSCSI-Anschluss können diese NWSDs hingegen in derselben iSeries-Partition, in einer anderen Partition im selben iSeries-System oder in einem gänzlich anderen iSeries-System definiert werden. Sie können beispielsweise eine NWSD definieren, die das xSeries-System für den Produktionsprozess während der üblichen Geschäftszeiten verwendet, und eine andere NWSD, die dasselbe xSeries-System zu anderen Zeiten verwendet.

| Eine bestimmte Server-Hardware kann jeweils nur von einer NWSD verwendet werden. Wenn mehrere NWSDs zur Ausführung auf ein und derselben Hardware definiert sind, und eine dieser Beschreibungen diese Hardware derzeit nutzt, dürfen daher die übrigen Beschreibungen erst dann starten, wenn diese NWSD beendet (abgehängt) wird. Auf diese Weise wird verhindert, dass eine NWSD unabsichtlich die Hardware übernimmt, die von einer anderen NWSD benutzt wird.

| Wenn es beim Starten einer NWSD Probleme gibt und die Server-Hardware derzeit von einer anderen NWSD benutzt wird, sollte die Steuerung der Hardware folgendermaßen von einer NWSD auf eine andere übertragen werden: Beenden Sie zunächst die NWSD, die die Hardware derzeit benutzt, und starten Sie dann die NWSD, die die Hardware als Nächstes benutzen muss.

| **Besonderheiten bei Systemen mit iSCSI-Anschluss**

| Bei Servern mit iSCSI-Anschluss wird der Zugriff auf die Hardware über den Status der Server-Hardware gesteuert; der Status stellt auch sicher, dass die Hardware nur von jeweils einer NWSD benutzt wird.

| Wenn die NWSD gestartet (angehängt) wird, richtet sich das Verhalten eines Servers mit iSCSI-Anschluss nach dem jeweiligen Serviceprozessortyp:

- | • Bei xSeries-Servern mit einem BMC-Serviceprozessor muss sich die Hardware zunächst im ausgeschalteten Status befinden.
- | • Bei xSeries-Servern mit einem RSA II oder einem IBM BladeCenter mit einem Managementmodul darf die Hardware nicht unter einem Betriebssystem (z. B. DOS oder Windows) gebootet werden. Ein xSeries-System, bei dem die Eingabeaufforderung zum Einlegen einer Diskette angezeigt wird, ist zulässig, wird jedoch eine Weile warten, um sicherzustellen, dass kein weiteres System versucht, auf das System zuzugreifen.

| Andernfalls kommt es zum Fehler bei der Startoperation. Wenn die NWSD beendet (abgehängt) wird, verbleibt die NWSD-Hardware der xSeries oder des BladeCenter-Blades im ausgeschalteten Status.

| Abgesehen von der Benutzung der Server-Hardware durch eine NWSD gibt es noch weitere mögliche Ursachen, warum sich die Server-Hardware im eingeschalteten Status befindet. So könnte die Server-Hardware beispielsweise für Setup-Tasks wie das Laden von Firmware oder Ändern von BIOS-Einstellungen eingeschaltet worden sein. Ein weiteres Beispiel: Wenn das Serverbetriebssystem auf einen nicht behebbaren Fehler gestoßen ist, der zum Ausfall des Servers führte, die Hardware aber im eingeschalteten Zustand gelassen hat. In den beschriebenen Fällen könnte das normale Starten der NWSD misslingen, da sich die Server-Hardware nicht im ausgeschalteten Zustand befindet, oder der Serviceprozessor meldet, dass noch ein Betriebssystem aktiv ist.

| Für die genannten Fälle stehen zahlreiche Lösungen zur Verfügung:

- | • Wenn eine NWSD die Hardware benutzt, das Serverbetriebssystem jedoch ausgefallen ist, versuchen Sie, den Server herunterzufahren. In den meisten Fällen wird dadurch die Server-Hardware ausgeschaltet und wieder für diese oder eine andere NWSD verfügbar gemacht. Wenn das Problem nicht durch Beenden der NWSD behoben werden kann, versuchen Sie es mit der folgenden Methode.
- | • Beim Starten der NWSD steht eine Option zum Zurücksetzen des Systems zur Verfügung, mit der ein Zurücksetzen der Server-Hardware während des NWSD-Starts erzwungen wird. Sie können diese Option verwenden, um eine NWSD zu starten, die Server-Hardware benutzt, die sich in einem Zustand befindet, der normalerweise das Starten (Anhängen) des Servers verhindern würde.

| **Achtung:** Verwenden Sie die Option zum Zurücksetzen des Systems nur dann, wenn Sie sicher sind, dass die Server-Hardware derzeit nicht von einer anderen NWSD benutzt wird. In diesem Fall würde diese andere NWSD nämlich fehlschlagen, was den Verlust oder die Zerstörung von Daten zur Folge haben kann.

| So setzen Sie ein fernes System mit dem iSeries Navigator zurück:

- | 1. Erweitern Sie **Verwaltung integrierter Server**.
- | 2. Erweitern Sie **Server**.
- | 3. Wählen Sie durch Klicken mit der rechten Maustaste einen der verfügbaren Server in der Liste aus.
- | 4. Wählen Sie **Mit Optionen starten...** aus.
- | 5. Markieren Sie die Option **Fernes System zurücksetzen**.
- | 6. Klicken Sie auf **Start**. Es wird eine Bestätigungsanzeige angezeigt.
- | 7. Klicken Sie in dieser Anzeige auf **Start**, um das ferne System zu starten und zurückzusetzen.

| Wenn Sie einen CL-Befehl verwenden möchten, geben Sie das Schlüsselwort RESETSYS (System zurücksetzen) für den Befehl VRYCFG (Konfiguration an-/abhängen) ein.

Fehler in der NWSD-Konfigurationsdatei

Wenn Sie vermuten, dass eine von Ihnen erstellte NWSD-Konfigurationsdatei einen Fehler verursacht, versuchen Sie, den NWSD-Konfigurationsdateiparameter auf *NONE zurückzusetzen. Weitere Informationen finden Sie unter „NWSD-Konfigurationsdateiparameter zurücksetzen“. Wird der Fehler dadurch behoben, liegt das Problem höchstwahrscheinlich in Ihrer NWSD-Konfigurationsdatei.

Werden durch die NWSD-Konfigurationsdatei Fehler verursacht, haben Sie folgende Optionen.

- Arbeit ohne Ihre NWSD-Konfigurationsdatei fortsetzen
- „Frühere Version der Datei des integrierten Servers verwenden“
- „NWSD-Konfigurationsdatei korrigieren“

NWSD-Konfigurationsdatei korrigieren

Wenn Sie die NWSD-Konfigurationsdatei korrigieren und die Fehler beheben wollen, haben Sie die folgenden Möglichkeiten:

1. Suchen Sie in den Protokollen nach Fehlern und Informationen zur Fehlerbehebung. Weitere Informationen finden Sie unter „Nachrichten und Jobprotokolle prüfen“ auf Seite 219.
2. Editieren Sie die NWSD-Konfigurationsdatei.
3. Führen Sie einen Neustart aus. Entsprechende Anweisungen finden Sie unter „Integrierten Server starten und stoppen“ auf Seite 157.

NWSD-Konfigurationsdateiparameter zurücksetzen

Sie können den Konfigurationsdateiparameter der NWSD auf *NONE setzen, um zu verhindern, dass die Änderungen, die Fehler verursachen, an die Datei des integrierten Servers weitergegeben werden. So verhindern Sie, dass i5/OS Ihre NWSD-Konfigurationsdatei verwendet:

1. Geben Sie in der i5/OS-Befehlszeile WRKNWSD ein, um mit NWS-Beschreibungen (NWSD) zu arbeiten.
2. Geben Sie in der Zeile mit dem Netzwerkserver, bei dem die Probleme aufgetreten sind, Auswahl 2 (Ändern) ein.
3. Wählen Sie im Feld Konfigurationsdatei *NONE aus.
4. Hängen Sie den Netzwerkserver an, und prüfen Sie, ob der Fehler behoben ist.

Anmerkung:

Vorhandene Änderungen in Dateien, die von der Konfigurationsdatei verarbeitet werden, bleiben unverändert. Es existiert eine .BKU-Datei mit dem Dateiinhalt vor der letzten Änderung, die durch Anhängen des Servers vorgenommen wurde. Diese Datei kann verwendet werden, um die geänderte Version zu ersetzen, oder Sie speichern die Datei anhand einer vorherigen Sicherung zurück, falls eine solche vorhanden ist.

Frühere Version der Datei des integrierten Servers verwenden

Wenn Sie über eine funktionierende Version der Datei des integrierten Servers verfügen, können Sie die Datei in diese Version zurück ändern. Gehen Sie dazu wie folgt vor:

1. Setzen Sie den Konfigurationsdateiparameter der NWSD auf *NONE zurück, um zu verhindern, dass Änderungen, die Fehler verursachen, in der Datei des integrierten Servers vorgenommen werden. Weitere Informationen finden Sie unter „NWSD-Konfigurationsdateiparameter zurücksetzen“.
2. Wählen Sie die Datei aus, die auf eine frühere Version zurückgesetzt werden soll.
3. Ist der Server betriebsbereit und angehängt, melden Sie sich am Server an, oder verwenden Sie einen fernen Befehl (siehe „Befehle für den integrierten Windows-Server im Fernzugriff ausführen“ auf Seite 161) an der i5/OS-Konsole, um die Dateien umzubenennen:
 - Benennen Sie die Datei, die die Probleme verursacht, um.
 - Ändern Sie die frühere Version der Datei zurück in ihren ursprünglichen Namen.
4. Hängen Sie den integrierten Server ab- und wieder an, damit er die frühere Version der Datei benutzt.

DASD in Servern mit IXa- oder iSCSI-Anschluss

Auf einem xSeries-Server werden lokale Festplattenlaufwerke nicht unterstützt, wenn er direkt über einen integrierten xSeries-Adapter an die iSeries angeschlossen ist. Auf einem IBM xSeries- oder BladeCenter-Server werden lokale Festplattenlaufwerke nicht unterstützt, wenn er über einen iSCSI-HBA an die iSeries angeschlossen ist. In den meisten Fällen wird das lokale Festplattenlaufwerk nicht angezeigt. Wird es doch angezeigt und auch verwendet, können unvorhersehbare Ergebnisse die Folge sein. Wird ein xSeries- oder IBM BladeCenter-Server im Direktanschlussmodus über einen IXA oder iSCSI-HBA mit der iSeries verbunden, muss sichergestellt sein, dass alle Festplattenlaufwerke vorher entfernt wurden.

Fehler bei der Benutzer- und Gruppenregistrierung

Wenn Gruppen oder Benutzer in der Windows-Umgebung auf der iSeries nicht registriert werden können, können Sie den Fehler mit Hilfe der folgenden Prozedur bestimmen.

Unter i5/OS:

- Überprüfen Sie das Nachrichtenprotokoll für diese NWS-Beschreibung (NWSID) auf Fehler. (Während der Serverinstallation wurde entweder die Nachrichtenwarteschlange QSYSOPR, ein benutzerdefiniertes Nachrichtenprotokoll oder ein Benutzerjobprotokoll zugeordnet.) Befolgen Sie die Fehlerbehebungsmaßnahmen in den Fehlernachrichten, um den Fehler zu korrigieren. Fehlercodes sind auch in der Anzeige "Mit NWS-Benutzerregistrierung arbeiten" (WRKNWSENR) zu finden.
- Enthält das Nachrichtenprotokoll die Angabe NTA0282 Fehler bei Benutzeradministration, lesen Sie den Abschnitt „Berechtigungsfehler bei der Benutzerregistrierung“ auf Seite 233.
- Vergewissern Sie sich, dass sich der Server im Status ANGEHÄNGT befindet.
- Überprüfen Sie den Registrierungsstatus (siehe „Einzelnen i5/OS-Benutzer mit iSeries Navigator in der Windows-Umgebung registrieren“ auf Seite 187), und suchen Sie nach Fehlernachrichten. Aktualisieren Sie den Status mit F5.
- Prüfen Sie, ob i5/OS so eingerichtet ist, dass Kennwörter gesichert werden (QRETSVRSEC ist auf 1 gesetzt). Stellen Sie außerdem sicher, dass Benutzer, die versuchen, sich zu registrieren, sich erst bei i5/OS anmelden, **nachdem** dieser Wert festgelegt wurde.
- Erstellen Sie eine Nachrichtenwarteschlange für die NWSID, und geben Sie diese an; überprüfen Sie die Warteschlange auf Nachrichten.
- Geben Sie unter i5/OS den Befehl WRKACTJOB ein. Prüfen Sie den Job QPRFSYNCH im Subsystem QSYSWRK. Prüfen Sie das Jobprotokoll, indem Sie F10 drücken, um detailliertere Nachrichten zu erhalten.
- Geben Sie unter i5/OS den Befehl WRKJOB *nwsdname* ein, wobei *nwsdname* der Name der NWSID für den integrierten Server ist. Ist der Job aktiv, zeigen Sie das Jobprotokoll an. (Drücken Sie F10, um detailliertere Nachrichten anzuzeigen.) Wenn Sie den Job beenden, zeigen Sie die Spooldatei an.

Vorgehensweise auf dem integrierten Windows-Server:

Sie können den Fehler auch mit den folgenden Schritten bestimmen.

- Prüfen Sie, ob der Benutzeradministrationsdienst aktiv ist.
 1. Wählen Sie im Menü **Start** des integrierten Servers **Programme, Verwaltung und Komponentendienste** aus.
 2. Wählen Sie **Systemverwaltung** und dann **Dienste** aus.
 3. Prüfen Sie, ob die **iSeries-Benutzeradministration** in der Liste der Dienste erscheint.
 4. Wenn der Dienst **iSeries-Benutzeradministration** aufgelistet ist, aber nicht den Status "Gestartet" hat, klicken Sie mit der rechten Maustaste auf **iSeries-Benutzeradministration**, und wählen Sie dann im Menü **Starten** aus.
 5. Ist die **iSeries-Benutzeradministration** nicht aufgelistet, gehen Sie folgendermaßen vor, um diesen Dienst erneut zu installieren:
 - a. Wählen Sie im Menü **Start** die Option **Ausführen**, und geben Sie `command` ein, um ein Eingabeaufforderungsfenster zu öffnen.

- b. Wechseln Sie zu Laufwerk C: (oder zum aktuellen Windows-Laufwerk).
- c. Geben Sie %SystemRoot%\as400wsv\admin\qvnadaem /install ein, und drücken Sie die Eingabetaste.
- d. Schließen Sie das Fenster **Dienste**.
- e. Öffnen Sie das Fenster **Dienste** erneut.
- f. Falls die **iSeries-Benutzeradministration** nicht gestartet ist, klicken Sie auf **Starten**.

Wenn die Fehlernachricht ausgegeben wird, dass kein Windows-Domänencontroller gefunden werden kann, haben Sie möglicherweise versucht, Benutzer in einer Windows-Arbeitsgruppe zu registrieren. Beim Windows-Netzwerkbetrieb können Gruppen von lokalen Servern in Windows-Arbeitsgruppen flexibel zusammengefasst werden. Wenn Sie beispielsweise die Position "Netzwerkumgebung" öffnen und auf "Arbeitsgruppencomputer anzeigen" klicken, wird eine Liste der Computer angezeigt, die zur gleichen Arbeitsgruppe gehören. In iSeries Navigator entsteht manchmal der Eindruck, dass OS/400-Benutzer in diesen Windows-Arbeitsgruppen registriert werden können. Ein entsprechender Versuch führt jedoch zu einem Fehler. Anders als bei einer Windows-Domäne gibt es keine separate Liste von Benutzern in Windows-Arbeitsgruppen.

Berechtigungsfehler bei der Benutzerregistrierung

Wird der Fehler NTA0282 ausgegeben, der auf eine unzureichende Berechtigung für das Erstellen und Aktualisieren von Benutzern des integrierten Servers hinweist, sollten Sie entsprechend vorgehen.

- Versuchen Sie zum ersten Mal, Benutzer und Gruppen in einer Domäne zu registrieren, müssen Sie die Benutzer-ID QAS400NT anlegen, um über die erforderliche Berechtigung zu verfügen. Dies wird unter „Benutzer QAS400NT“ auf Seite 193 beschrieben. Stellen Sie außerdem sicher, dass der Benutzer als herkömmlicher Benutzer konfiguriert ist, also ein iSeries-Kennwort angeben muss und die lokale Kennwortverwaltung verwendet. Weitere Informationen enthält der Abschnitt „Arten von Benutzerkonfigurationen“ auf Seite 56.
- Wenn Sie bereits zuvor erfolgreich Benutzer und Gruppen registriert haben, prüfen Sie, ob eventuell das i5/OS-Kennwort für den Benutzer QAS400NT abgelaufen ist. Wenn das Benutzerkennwort für QAS400NT abläuft, läuft auch der Account auf dem integrierten Server ab. So können Sie dieses Problem lösen:
 1. Aktivieren Sie den Account auf dem integrierten Server.

Führen Sie auf einem Domänencontroller Folgendes aus:

 - a. Öffnen Sie **Start** → **Programme** → **Verwaltung**.
 - b. Wählen Sie **Active Directory-Benutzer und -Computer** aus.
 - c. Klicken Sie mit der rechten Maustaste auf **Benutzer**, und doppelklicken Sie dann auf **QAS400NT**.
 - d. Klicken Sie oben im Fenster **Benutzereigenschaften** auf die Indexzunge **Konto**.
 - e. Ändern Sie das Datum bei **Konto läuft ab** in ein Datum in der Zukunft, und klicken Sie auf **Nie**.

Führen Sie auf einem lokalen integrierten Windows-Server Folgendes aus:



 - a. Öffnen Sie **Start, Programme, Verwaltung**.
 - b. Wählen Sie **Computerverwaltung** aus.
 - c. Erweitern Sie **Systemprogramme** und anschließend **Lokale Benutzer und Gruppen**.
 - d. Klicken Sie mit der rechten Maustaste in der Liste auf **QAS400NT**.
 - e. Klicken Sie oben im Fenster **Benutzereigenschaften** auf die Indexzunge **Konto**.
 - f. Ändern Sie das Datum bei **Konto läuft ab** in ein Datum in der Zukunft, und klicken Sie auf **Nie**.
 2. Verwenden Sie unter i5/OS den Befehl CHGUSRPRF (Benutzerprofil ändern) oder CHGPWD (Kennwort ändern), um das Benutzerkennwort für QAS400NT zu ändern.
 3. Starten Sie die iSeries-Benutzeradministration erneut.
 - a. Klicken Sie auf **Start, Programme, Verwaltung** und **Komponentendienste**.

- b. Klicken Sie auf **Dienste**.
- c. Klicken Sie auf **iSeries-Benutzeradministration**, und klicken Sie dann mit der rechten Maustaste auf **Stoppen**, um den Dienst zu stoppen.
- d. Klicken Sie auf **iSeries-Benutzeradministration**, und klicken Sie dann mit der rechten Maustaste auf **Starten**, um den Dienst erneut zu starten.


Durch erneutes automatisches Starten des Dienstes wird die Registrierung der Benutzer und Gruppen erneut versucht.

Sie können dieses Problem vermeiden, indem Sie das Kennwort für QAS400NT unter i5/OS in regelmäßigen Abständen ändern, damit es nicht abläuft.

Wenn mehrere iSeries-Systeme mit mehreren integrierten Servern vorhanden sind, die zu einer Windows-Domäne gehören, können Sie Probleme mit abgelaufenen Kennwörtern vermeiden, indem Sie die Schritte im Abschnitt „Benutzer QAS400NT“ auf Seite 193 ausführen.

- Wenn das Problem weiterhin besteht, überprüfen Sie die Datenbank mit technischen Informationen auf der Webseite IBM  iSeries Support Web.  Wird dort keine Lösung angeboten, wenden Sie sich an die technische Unterstützung.

Kennwortfehler



Bisher waren alle Zeichen, die in i5/OS-Kennwörtern zulässig waren, auch in Windows-Kennwörtern zulässig. Jetzt werden unter i5/OS längere Kennwörter und mehr Zeichen unterstützt als unter Windows. Deshalb sollten für i5/OS-Kennwörter nur die Zeichen und die Kennwortlänge verwendet werden, die für Windows-Kennwörter zulässig sind, wenn Benutzer dort registriert werden sollen. Weitere Informationen über die Stufen der i5/OS-Kennwortsicherheit sind im Abschnitt "Planning Password Level Changes" der iSeries Security Reference zu finden. .

Verfällt ein Kennwort täglich, nachdem es über die Konsole des integrierten Servers geändert wurde, bedeutet dies, dass der Benutzer vergessen hat, dass das Kennwort unter i5/OS geändert werden muss. Das Ändern des i5/OS-Kennwort verhindert dieses Problem.

Stimmen das i5/OS- und das Windows-Server-Kennwort nicht überein, führen Sie folgende Schritte aus, um den Grund dafür herauszufinden:

1. Überprüfen Sie, ob der Benutzer als Windows-Benutzer konfiguriert ist. Weitere Informationen enthält der Abschnitt „Arten von Benutzerkonfigurationen“ auf Seite 56.
 - a. Geben Sie in der i5/OS-Befehlszeile den Befehl WRKUSRPRF ein.
 - b. Geben Sie die richtige Benutzer-ID ein.
 - c. Prüfen Sie, ob das Attribut LCLPWDMGT (Lokale Kennwortverwaltung) auf *NO gesetzt ist. Wenn dies der Fall ist, ist für den Benutzer das i5/OS-Kennwort *NONE konfiguriert, und die Kennwörter für i5/OS und Windows sind nicht identisch.
2. Prüfen Sie, ob i5/OS so eingerichtet ist, dass Kennwörter gespeichert werden:
 - a. Geben Sie in der i5/OS-Befehlszeile WRKSYSVAL SYSVAL(QRETSVRSEC) ein.
 - b. Geben Sie im Feld Auswahl eine 2 ein, und drücken Sie die Eingabetaste.
 - c. Prüfen Sie, ob Server-Sicherheitsdaten sichern auf 1 gesetzt ist. Falls nicht, ändern Sie die Einstellung in 1.
3. Vergewissern Sie sich, dass auf dem integrierten Windows-Server der Benutzeradministrationsdienst ausgeführt wird. Entsprechende Informationen finden Sie unter „Fehler bei der Benutzer- und Gruppenregistrierung“ auf Seite 232.
4. Prüfen Sie die i5/OS-Kennwortunterstützungsstufe:
 - a. Geben Sie in der i5/OS-Befehlszeile WRKSYSVAL SYSVAL(QPWDLV) ein.
 - b. Geben Sie im Feld Auswahl eine 5 ein, und drücken Sie die Eingabetaste.

Die Kennwortstufe unter i5/OS kann so festgelegt werden, dass Benutzerprofilkennwörter mit einer Länge von 1-10 Zeichen oder mit einer Länge von 1-128 Zeichen zulässig sind. Die i5/OS-Kennwortstufe 0 oder 1 unterstützt Kennwörter mit 1-10 Zeichen und begrenzt den Zeichensatz. Auf Stufe 0 oder 1 konvertiert i5/OS die Kennwörter für den Windows-Server in Kleinbuchstaben. Die i5/OS-Kennwortstufen 2 oder 3 unterstützen Kennwörter mit 1-128 Zeichen sowie zusätzliche Zeichen, u. a. Groß- und Kleinschreibung. Auf Stufe 2 oder 3 von i5/OS bleibt die Groß-/Kleinschreibung der Kennwörter für den Windows-Server erhalten. Eine Änderung der i5/OS-Kennwortstufe wird beim nächsten IPL wirksam.

5. Prüfen Sie den Registrierungsstatus des Benutzers. Dabei muss vor der Registrierung des Benutzers sichergestellt werden, dass er nicht bereits mit einem anderen Kennwort in der Windows-Umgebung vorhanden ist (siehe „Einzelnen i5/OS-Benutzer mit iSeries Navigator in der Windows-Umgebung registrieren“ auf Seite 187). War der Benutzer bereits mit einem anderen Kennwort vorhanden, misslingt die Registrierung. Ändern Sie das Windows-Kennwort so, dass es mit dem i5/OS-Kennwort übereinstimmt. Wiederholen Sie anschließend das Registrierungsverfahren.
6. Wenn das Problem weiterhin besteht, überprüfen Sie die Datenbank mit technischen Informationen auf der Webseite  IBM iSeries Support . Wird dort keine Lösung angeboten, wenden Sie sich an die technische Unterstützung.

Snap-in-Programm von IBM iSeries Integrated Server Support

Beim Versuch, das Snap-in-Programm von IBM iSeries Integrated Server Support auszuführen, kann ein Fehler auftreten. Möglicherweise wird das Programm nicht gestartet bzw. stellt unerwartete Informationen bereit, oder bei der Ausführung treten Fehler auf.

Wenn die Anzeige des Snap-in-Programms von IBM iSeries Integrated Server Support nie erscheint, gehen Sie folgendermaßen vor, um die Fehlerursache festzustellen.



- Prüfen Sie, ob bereits eine Instanz des Snap-in-Programms von IBM iSeries Integrated Server Support oder des Programms Lvsync auf dem System vorhanden ist. Es kann jeweils nur eine Instanz dieser Programme ausgeführt werden. Wenn bereits eine Instanz dieser Programme ausgeführt wird, wird ein weiterer Programmaufruf zurückgegeben. Beenden Sie das derzeit benutzte Programm, bevor Sie versuchen, eine neue Instanz zu starten.
- Vergewissern Sie sich, dass der Benutzer über die Berechtigung als Administrator und die entsprechenden Sonderberechtigungen verfügt. Für Snap-in-Programme von IBM iSeries Integrated Server Support sind diese Berechtigungen erforderlich. Versuchen Sie, das Programm mit Administratorberechtigung erneut zu starten.
- Vergewissern Sie sich, dass iSeries NetServer gestartet wurde. iSeries NetServer wird automatisch mit dem Subsystem QSERVER unter i5/OS gestartet. Starten Sie iSeries NetServer, wenn i5/OS noch nicht gestartet wurde.
- Vergewissern Sie sich, dass das Gastbenutzerprofil unter iSeries NetServer aktiviert wurde. Ist dies nicht der Fall, aktivieren Sie das Gastbenutzerprofil, so dass Gastbenutzer auf iSeries NetServer zugreifen können (siehe „Gastbenutzerprofil für iSeries NetServer erstellen“ auf Seite 68). Wenn Sie den Gastzugriff aktiviert haben, beenden und starten Sie iSeries NetServer erneut. Versuchen Sie anschließend, das Snap-in-Programm von IBM iSeries Integrated Server Support erneut auszuführen.
- Überprüfen Sie das Systemereignisprotokoll auf dem Windows-Server auf Nachrichten, die sich auf das Snap-in-Programm von IBM iSeries Integrated Server Support beziehen.

Die Anzeige des Snap-in-Programms von IBM iSeries Integrated Server Support wird möglicherweise aufgerufen, unter Umständen werden von i5/OS jedoch nicht die von Ihnen erwarteten Informationen angezeigt. Ist dies der Fall, führen Sie die folgenden Schritte aus, um den Fehler zu bestimmen:

- Überprüfen Sie, ob das neueste Service-Pack-PTF verfügbar und unter i5/OS aktiviert ist. Sie können hierzu den Befehl DSPPTF (PTF anzeigen) verwenden.
- Überprüfen Sie, ob das von Ihnen erwartete Service-Pack auch tatsächlich auf dem integrierten Server installiert ist.

- Überprüfen Sie das System- und Anwendungsereignisprotokoll auf dem integrierten Server auf Nachrichten, die sich auf das Snap-in-Programm von Integrated Server Support beziehen.

Beim Ausführen einer Aktion mit dem Snap-in-Programm von IBM iSeries Integrated Server Support können Fehler auftreten. Die folgende Liste hilft Ihnen bei der Behebung von Fehlern, die auftreten können, nachdem Sie auf die Schaltfläche **OK** geklickt haben.

- Damit das Snap-in-Programm von IBM iSeries Integrated Server Support fortgesetzt werden kann, muss ein Laufwerksbuchstabe verfügbar sein. Dieser Laufwerksbuchstabe muss nur vorübergehend verfügbar sein. Wenn alle Laufwerksbuchstaben belegt sind, müssen Sie einen Laufwerksbuchstaben für das Snap-in-Programm von IBM iSeries Integrated Server Support freigeben und die Ausführung des Programms erneut starten.
- Das Snap-in-Programm von IBM iSeries Integrated Server Support führt die angegebene Aktion aus. Abhängig davon, welche Dateien aktualisiert wurden, wird das System unter Umständen erneut gestartet. Es dauert möglicherweise einen Moment, bis das System heruntergefahren wird und neu startet.
- Überprüfen Sie das System- und Anwendungsereignisprotokoll auf dem integrierten Server auf Nachrichten, die sich auf das Snap-in-Programm von IBM iSeries Integrated Server Support beziehen.
- Wenn das Problem weiterhin besteht, überprüfen Sie die Datenbank mit technischen Informationen auf der Webseite  IBM iSeries Support . Wird dort keine Lösung angeboten, wenden Sie sich an die technische Unterstützung.

Fehler auf Servern mit iSCSI-Anschluss

Wenn eines der unten beschriebenen Probleme auftritt, können Sie die Fehlerbehebung mit Hilfe der aufgeführten Maßnahmen starten. Diese Liste ist nicht vollständig, so dass für einige Probleme Maßnahmen erforderlich sein können, die hier nicht aufgeführt sind. Weiterführende Informationen zur Fehlerbehebung finden Sie unter „Nachrichten und Jobprotokolle prüfen“ auf Seite 219.

Initialisieren der Serviceprozessorkonfiguration schlägt fehl

Wenn die Nachrichtenwarteschlange des Systembedieners (QSYSOPR) die Nachricht CPDC4xx oder CPFC4xx enthält, oder das Jobprotokoll des Stapeljobs oder des interaktiven Benutzers betroffen ist, lesen Sie die Informationen unter „Fehlerbehebung für IBM Director“ auf Seite 239.


Bei der Installation oder dem Start des Servers bleibt der NWS-Status VARIED OFF (abgehängt)

- Vergewissern Sie sich, dass alle erforderlichen konfigurierten NWS-Hostadapter für den Server angehängt sind, bevor Sie einen Server installieren oder starten. Wenn sich ein NWS-Hostadapter nicht anhängen lässt, schauen Sie nach, ob die Nachrichtenwarteschlange für die NWS-Hosteinheit entsprechende Nachrichten enthält.
- Wenn die Nachrichtenwarteschlange des Systembedieners (QSYSOPR) die Nachricht CPDC4xx oder CPFC4xx enthält, oder das Jobprotokoll des Stapeljobs oder des interaktiven Benutzers betroffen ist, lesen Sie die Informationen unter „Fehlerbehebung für IBM Director“ auf Seite 239.

Server startet nicht, solange das Hosted System eingeschaltet ist.


Weitere Informationen finden Sie unter „Fehler bei der gemeinsamen Nutzung von Hardware für Hosted Systeme“ auf Seite 229.

Auf der Konsole des Hosted Systems wird 'Keine iSCSI-Einheiten gefunden' oder eine Aufforderung für eine Diskette angezeigt

- Der im Hosted System konfigurierte Boot-iSCSI-HBA konnte nicht booten.
- Möglicherweise liegt ein iSCSI-Konfigurationsproblem vor. Siehe iSCSI Troubleshooting  (www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/troubleshooting.html).

- Wenn im Produktaktivitätenprotokoll Nachricht CPPC056 enthalten ist, liegt wahrscheinlich ein CHAP-Konfigurationsproblem vor.
- Möglicherweise gibt es ein Netzproblem zwischen dem Boot-iSCSI-HBA des Hosted Systems und dem iSeries-HBA, der dem Pfad entspricht, der für den NWS-D-Speicherbereich des Systemlaufwerks konfiguriert wurde. Weitere Informationen finden Sie unter „Netzplananalyse für Boot- und Speicherpfade“ auf Seite 238.

Der NWS-D-Status ist VARIED ON (angehängt), aber Windows bootet nicht.

- Möglicherweise liegt ein iSCSI-Konfigurationsproblem vor. Siehe iSCSI Troubleshooting  (www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/troubleshooting.html).
- Wenn im Produktaktivitätenprotokoll Nachricht CPPC056 enthalten ist, liegt wahrscheinlich ein CHAP-Konfigurationsproblem vor.
- Möglicherweise gibt es ein Netzproblem zwischen dem Boot-iSCSI-HBA des Hosted Systems und dem iSeries-HBA, der dem Pfad entspricht, der für den NWS-D-Speicherbereich des Systemlaufwerks konfiguriert wurde. Weitere Informationen finden Sie unter „Netzplananalyse für Boot- und Speicherpfade“ auf Seite 238.


Der NWS-D-Status ist DEGRADED

Vergewissern Sie sich, dass alle erforderlichen konfigurierten NWS-Hostadapter für den Server angehängt sind. Wenn sich ein NWS-Hostadapter nicht anhängen lässt, schauen Sie nach, ob die Nachrichtenwarteschlange für die NWS-Hosteinheit entsprechende Nachrichten enthält.

Speicher, der einen anderen als den Boot-Pfad verwendet, wird nicht in Windows angezeigt.

- Möglicherweise gibt es ein Netzproblem zwischen dem Hosted System und dem iSCSI-HBA in der iSeries, der dem nicht für den Boot vorgesehenen Pfad entspricht. Weitere Informationen finden Sie unter „Netzplananalyse für Boot- und Speicherpfade“ auf Seite 238.
- Wenn im Produktaktivitätenprotokoll Nachricht CPPC056 enthalten ist, liegt ein CHAP-Konfigurationsproblem vor. In diesem Fall wird das Problem wahrscheinlich von den digitalen Zertifikaten verursacht, die für die Windows-Umgebung auf der iSeries benötigt werden, um die eigenen schutzwürdigen Daten zwischen i5/OS und Windows auszutauschen. Weitere Informationen finden Sie unter „Pfadzertifikate verwalten“ auf Seite 238.

Speicher, der einen anderen als den Boot-Pfad verwendet, wird gelegentlich erst spät in Windows angezeigt.

- Dies ist normal, wenn der Server zum ersten Mal gestartet wird, nachdem bestimmte i5/OS-Konfigurationsdaten geändert wurden (z. B. die lokale SCSI-Schnittstelle im NWS-Hostadapter oder CHAP-Daten in der Konfiguration des fernen Systems).
- Dies ist normal, wenn ein iSCSI-HBA im Hosted System noch nie zuvor mit dieser speziellen NWS-D benutzt wurde. Das wäre der Fall, wenn ein iSCSI-HBA im Hosted System ausgetauscht oder ein anderes Hosted System als Hot-Spare verwendet wird.
- Wenn zu Ihrer Anwendung ein automatischer Startservice gehört, der auf die oben genannten Situationen empfindlich reagiert, lesen Sie die Informationen auf der Webseite Advanced iSCSI tasks  (www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/advancedtasks.html).

Benutzerregistrierung oder Übergabe eines fernen Befehls schlägt mit NTA02BB, NTA028A, NTA028B fehl

- Es gibt ein Problem mit den digitalen Zertifikaten, die für die Windows-Umgebung auf der iSeries benötigt werden, um die eigenen schutzwürdigen Daten zwischen i5/OS und Windows auszutauschen. Weitere Informationen finden Sie unter „Pfadzertifikate verwalten“ auf Seite 238.


- Vergewissern Sie sich bei NTA028A und NTA028B dass Datum und Uhrzeit auf dem Hosted System nicht zu stark vom Datum auf der iSeries abweichen, da andernfalls digitale Zertifikate als ungültig erscheinen können.

Netzplananalyse für Boot- und Speicherpfade

Weitere Informationen über diese Schritte sowie weitere Fehlerbehebungsprozeduren finden Sie unter

iSCSI troubleshooting 

(www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/troubleshooting.html).

- Verwenden Sie auf dem Hosted System das mit STRG-Q aufgerufene Dienstprogramm, um die iSCSI-HBA-MAC-Adressen des Hosted Systems anzuzeigen. Vergewissern Sie sich, dass die Werte mit denen für den SCSI-Schnittstellenadapter in der i5/OS-Konfiguration für den fernen Server übereinstimmen. Dieser Schritt kann übersprungen werden, wenn Sie an diese Stelle verwiesen wurden, weil ein manuell konfigurierter Bootvorgang fehlgeschlagen ist.
- Verwenden Sie die Sicht des mit STRG-Q aufgerufenen Dienstprogramms oder des Einheitenmanagers des SCSI-Treibers, um die SCSI-IP-Adresse des entsprechenden iSCSI-HBAs für die iSeries mit PING zu überprüfen.
- Wenn der PING fehlschlägt, führen Sie die folgenden Schritte aus.
 - Vergewissern Sie sich, dass das physische Netzwerk richtig angeschlossen ist, und dass die Einheiten im Netzwerk, wie beispielweise Switches, funktionieren.
 - Vergewissern Sie sich, dass die in „iSCSI-Netzwerk“ auf Seite 30 definierten Voraussetzungen erfüllt werden.
 - Wenn eine Firewall oder eine ähnliche Paketfilterfunktion vorhanden ist, vergewissern Sie sich, dass die Firewall ICMP-Pakete (Internet Control Message Protocol) passieren lässt. Im Unterschied zu SCSI-IP-Adressen können LAN-Adressen von der unter Windows laufenden Firewall-Software betroffen sein.
 - Wenn für Ihre NWSD andere IPSec-Regeln (IP-Sicherheitsregeln) als *NONE gelten, lesen Sie die Informationen auf der Webseite iSCSI Troubleshooting  (www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/troubleshooting.html).
- Wenn der PING erfolgreich ist, führen Sie die folgenden Schritte aus.
 - Wenn eine Firewall oder eine ähnliche Paketfilterfunktion vorhanden ist, lesen Sie die Informationen in „Firewall konfigurieren“ auf Seite 142. Im Unterschied zu SCSI-IP-Adressen können LAN-Adressen von der unter Windows laufenden Firewall-Software betroffen sein.
 - Wenn der DHCP-Boot fehlschlägt und ein Netzwerk mit Routern betroffen ist, vergewissern Sie sich, dass ein entsprechend konfigurierter DHCP-Weitergabeagent (Relay Agent), der auch als BOOTP Relay Agent bezeichnet wird, im Netzwerk vorhanden ist.

Pfadzertifikate verwalten

Anmerkung: Dieser Abschnitt bezieht sich nur auf Systeme mit iSCSI-Anschluss.

Normalerweise generiert die Windows-Umgebung auf der iSeries automatisch die digitalen Zertifikate, die sie benötigt, um die eigenen schutzwürdigen Daten zwischen i5/OS und Windows auszutauschen. Diese Zertifikate werden als Pfadzertifikate bezeichnet. Wenn Sie vermuten, dass es ein Problem mit den Pfadzertifikaten gibt, gehen Sie folgendermaßen vor:

- Vergewissern Sie sich, dass 5722-SS1 Option 34 (Digital Certificate Manager) installiert ist.
- Vergewissern Sie sich, dass die digitalen i5/OS- und Windows-Zertifikate kompatibel sind, indem Sie beim Starten des Servers neue Zertifikate generieren. Diese Vorgehensweise ist nur in außergewöhnlichen Situationen angebracht, also beispielsweise, wenn eine alte Version eines Speicherbereichs für ein Windows-Systemlaufwerk wiederhergestellt wird, ohne gleichzeitig auch den i5/OS-Zertifikatsspeicher wiederherzustellen. So generieren Sie neue Pfadzertifikate mit iSeries Navigator:
 1. Erweitern Sie **Verwaltung integrierter Server**.
 2. Erweitern Sie **Server**.

- | 3. Wählen Sie durch Klicken mit der rechten Maustaste einen der verfügbaren Server in der Liste aus.
- | 4. Wählen Sie **Mit Optionen starten...** aus.
- | 5. Markieren Sie die Option **Pfadzertifikate regenerieren**.
- | 6. Klicken Sie auf **Start**.

| Wenn Sie einen CL-Befehl verwenden möchten, geben Sie das Schlüsselwort GENPTHCERT (Pfadzertifikat generieren) für den Befehl VRYCFG (Konfiguration an-/abhängen) ein.

| Fehlerbehebung für IBM Director

| **Anmerkung:** Dieser Abschnitt bezieht sich nur auf Systeme mit iSCSI-Anschluss.

| Wenn Sie keine Verbindung zu IBM Director herstellen können (z. B. wenn Sie einen Server starten oder herunterfahren), gehen Sie folgendermaßen vor:

- | • Wiederholen Sie die Operation nach fünf Minuten.
- | • Stoppen Sie IBM Director und starten Sie ihn erneut.
 - | – Geben Sie in der i5/OS-Befehlszeile ENDTCPVR SERVER(*DIRECTOR) ein.
 - | – Bis der Director-Server endgültig gestoppt wird, vergehen ein paar Minuten. Der Status des Ausschaltprozesses kann abgerufen werden, indem /qibm/userdata/director/bin/twgstat in qsh ausgeführt wird. Nach ein paar Minuten sollte der Status „inaktiv“ gemeldet werden.
 - | – Starten Sie den qsh-Interpreter durch Eingabe von qsh in der i5/OS-Befehlszeile.
 - | – Führen Sie in qsh /qibm/userdata/director/bin/twgstart aus.
- | • Verifizieren Sie die Konfiguration der IBM Director-Eigenschaftendatei.

| Die IBM Director-Eigenschaftendatei wird während der Installation von IBM Director in /QIBM/ProdData/Director/classes/com/ibm/sysmgmt/app/iide/IIDETask.properties installiert.

| Prüfen Sie, ob die IBM Director-Eigenschaftendatei vorhanden ist. Wenn sie nicht vorhanden ist, installieren Sie IBM Director erneut, oder wenden Sie sich an den Kundendienst.
- | • Prüfen Sie, ob in der IBM Director-Eigenschaftendatei ein Port angegeben ist.

| Die Eigenschaftendatei sollte eine Zeile mit der Angabe „port = **xxxxx**“ enthalten; **xxxxx** ist die Portnummer. Wenn diese Zeile nicht vorhanden ist, führen Sie folgende Schritte aus:

 - | 1. Editieren Sie die Datei, und fügen Sie die Zeile „port = 5779“ hinzu. 5779 ist der Standardport für die Verbindung zwischen i5/OS und IBM Director.
 - | 2. Starten Sie IBM Director erneut.
- | • Prüfen Sie, ob der von IBM Director verwendete Port nicht von einer weiteren Anwendung benutzt wird.


| Prüfen Sie nach dem Starten von IBM Director, ob der in der IBM Director-Eigenschaftendatei angegebene Port nicht von einer weiteren Anwendung benutzt wird.

 - | 1. Erweitern Sie im iSeries Navigator **Netzwerk**—>**TCP/IP-Konfiguration**—>**IPv4**—> **Verbindungen**.
 - | 2. Klicken Sie mit der rechten Maustaste auf den Listeneintrag, für den in der Spalte **Lokaler Port** der gleiche Port angegeben ist, wie in der IBM Director-Eigenschaftendatei, und wählen Sie **Jobs** aus.
 - | 3. Suchen Sie in der Jobliste nach einem Job mit dem Jobnamen **Qcpmgtsvr** und dem Benutzer **Qcpmgtdir**. Es sollte der einzige Job sein, der den angegebenen Port verwendet.

| Sollten noch weitere Jobs den Port verwenden, müssen Sie den von IBM Director verwendeten Port folgendermaßen ändern:

 - | 1. Ändern Sie in der IBM Director-Eigenschaftendatei die in der Zeile „port = **xxxxx**“ angegebene Portnummer **xxxxx**.
 - | 2. Starten Sie IBM Director erneut.

| **Fehler bei der Erkennung:** Wenn eine Nachricht protokolliert wird, die besagt, dass der ferne Server
| oder das ferne Gehäuse nicht gefunden wurde, war die IBM Director-Schnittstelle nicht in der Lage, den
| als Ziel vorgesehenen Serviceprozessor auf dem Netzwerk auszumachen. Weitere Informationen finden
| Sie unter „Fernen Server erkennen und verwalten“ auf Seite 150.

| Wenn Sie mit einem Remote Supervisor II-Serviceprozessor arbeiten, stellen Sie sicher, dass Sie die neu-
| este Firmware benutzen. Weitere Informationen finden Sie in iSCSI install read me first 

| (www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme)

| **Wenn Sie zur Erkennung des Serviceprozessors keine Unicast-Adressierung verwenden, führen Sie die
| folgenden Schritte aus:**

- | • Prüfen Sie, ob der iSeries-Server über eine physische Netzwerkverbindung mit dem Serviceprozessor
| des fernen Systems verbunden ist.
 - | – Weitere Informationen finden Sie im Abschnitt über Ping vom iSeries Navigator in der Themen-
| sammlung zur TCP/IP-Fehlerbehebung.
- | • Wenn der iSeries-Server über eine physische Netzwerkverbindung zum Serviceprozessor verfügt, über-
| prüfen Sie die Firewall-Einstellungen für die Router oder Switches auf dem iSCSI-Netzwerk. Netzwer-
| krouter oder Switches zwischen der iSeries-LAN-Schnittstelle und dem Serviceprozessor unterstützen
| m"glicherweise keine Multicastadressierung oder sind nicht für die Zulassung der Multicastadressie-
| rung konfiguriert.
| Netzwerkrouter oder Firewalls k"nnen Multicastpakete blockieren. Die Router oder Firewalls müssen
| ggf. so konfiguriert werden, dass sie der SLP-IP-Adresse (SLP = Service Location Protocol)
| 239.255.255.253 oder der Portnummer 427 erlauben, SLP-Pakete durchzulassen.
- | • Konfigurieren Sie den Serviceprozessor so, dass er die Unicast-Adressierung zulässt.
| Sie müssen für den Serviceprozessor einen statischen Hostnamen oder eine statische IP-Adresse konfi-
| gurieren. Verwenden Sie dazu das BIOS-Dienstprogramm für einen RSA II oder die Serviceprozessor-
| Webschnittstelle. Der Abschnitt „Managementmodul- oder RSA II-Webschnittstelle verwenden“ auf
| Seite 155 enthält Anweisungen dafür, wie die Serviceprozessor-Webschnittstelle zur Konfiguration des
| Serviceprozessors genutzt wird.
| Ändern Sie die Serviceprozessorkonfiguration so, dass sie die Unicast-Adressierung verwendet, die den
| Hostnamen oder die IP-Adresse übernimmt, die im oben beschriebenen Serviceprozessor festgelegt
| wurden. Weitere Informationen finden Sie unter „Konfigurationseigenschaften des Serviceprozessors
| ändern“ auf Seite 134.

| **Wenn Sie zur Erkennung des Serviceprozessors die Unicast-Adressierung verwenden, führen Sie die
| folgenden Schritte aus:**

- | • Prüfen Sie, ob die IP-Adresse oder der Hostname sowohl im Serviceprozessor des fernen Systems als
| auch in der Serviceprozessorkonfiguration unter i5/OS richtig konfiguriert ist.
- | • Unter dem Thema zur TCP/IP-Fehlerbehebung finden Sie allgemeine Vorgehensweisen zur TCP/IP-
| Fehlerbehebung.

| **Fehler bei SSL-Verbindungen:** Es kann zu einer Reihe unterschiedlicher Probleme kommen, wenn die
| SSL (Secure Sockets Layer)-Verbindung zum Serviceprozessor konfiguriert wird. Weitere Informationen
| hierzu finden Sie in „Serviceprozessor-SSL konfigurieren“ auf Seite 140.

| **Das Zertifikat wird nicht in den richtigen i5/OS-Zertifikatsspeicher importiert.**

| Wenn Sie den manuellen Sicherheitsmodus verwenden, prüfen Sie, ob sich die Root-CA (CA = Zertifizie-
| rungsstelle) des Serviceprozessors im iSeries-Zertifikatsspeicher *SYSTEM befindet.

- | 1. Stellen Sie eine Verbindung zur Webschnittstelle des Serviceprozessors her.
- | 2. Zeigen Sie das Zertifikat an. Notieren Sie die Zertifizierungsstelle im Feld „Ausgestellt von“.
- | 3. Stellen Sie eine Verbindung zur iSeries-Schnittstelle für Digital Certificate Manager (DCM) her, um
| festzustellen, ob die CA als Zertifikat im Zertifikatsspeicher *SYSTEM aufgeführt wird.

- a. Bestimmen Sie die Root-CA des Zertifikats, das im Serviceprozessor installiert wurde.
 - 1) Stellen Sie mit Ihrem Web-Browser eine Verbindung zur Webschnittstelle des Serviceprozessors her, indem Sie `http://Hostname` (`Hostname` ist der Hostname des Serviceprozessors) oder `http://ipaddress` (`ipaddress` ist die IP-Adresse des Serviceprozessors) aufrufen.
 - 2) Befolgen Sie die Hilfeanweisungen des Browsers, um das Sicherheitszertifikat anzuzeigen, das die Identität der Website bestätigt.
 - 3) Befolgen Sie die Hilfeanweisungen des Browsers, um die Zertifikathierarchie anzuzeigen.
 - 4) Der oberste Eintrag in der Hierarchie ist das Root-CA-Zertifikat.
 - 5) Notieren Sie den Namen des Root-CA-Zertifikats. Er wird in Schritt h ben"tigt.
- b. Stellen Sie eine Verbindung zur iSeries-Schnittstelle für Digital Certificate Manager (DCM) her. Siehe den Abschnitt über das Starten von DCM unter dem Thema "Digital Certificate Manager".
- c. Klicken Sie auf **Zertifikatsspeicher auswählen**.
- d. Wählen Sie ***SYSTEM** aus, und klicken Sie auf **Weiter**.
- e. Geben Sie das Kennwort für den Zertifikatsspeicher ***SYSTEM** ein.
- f. Klicken Sie im linken Teilfenster auf **Fast Path**.
- g. Wählen Sie **Mit CA-Zertifikaten arbeiten** aus, und klicken Sie auf **Weiter**.
- h. Suchen Sie auf der Seite **Mit CA-Zertifikaten arbeiten** nach einem Eintrag im Feld "Zertifizierungsstelle (CA)", der mit dem Namen des Root-CA-Zertifikats aus Schritt a übereinstimmt.
- i. Lautet das Feld **Status** für diesen Eintrag **Aktiviert**, ist die CA richtig konfiguriert.
- j. Lautet das Feld **Status** für diesen Eintrag **Inaktiviert**, muss die CA mit den folgenden Schritten aktiviert werden:
 - 1) Wählen Sie den Radioknopf links von dem CA-Eintrag aus, der aktiviert werden muss.
 - 2) Wählen Sie die Schaltfläche "Aktivieren" am unteren Tabellenrand aus.
 - 3) Die CA ist jetzt richtig konfiguriert.
- k. Wenn das Feld "Zertifizierungsstelle (CA)" keinen Eintrag enthält, der mit dem Namen des Root-CA-Zertifikats aus Schritt a übereinstimmt, fügen Sie die CA folgendermaßen hinzu:
 - 1) Nehmen Sie die Original-E-Mail, die Sie von Ihrer Zertifizierungsstelle (CA) erhalten haben, als Vorlage. Diese E-Mail sollte das Zertifikat (das in den Serviceprozessor importiert wurde) und das zugehörige Trusted-Root-Zertifikat enthalten.
 - 2) Übertragen Sie das Trusted-Root-Zertifikat mittels FTP in ein Verzeichnis im IFS-Dateisystem auf der iSeries, und notieren Sie den vollständigen Pfad- und Dateinamen.
 - 3) Wählen Sie im linken Teilfenster **Zertifikate verwalten** aus, um eine Taskliste anzuzeigen.
 - 4) Wählen Sie in der Taskliste **Zertifikat importieren** aus.
 - 5) Wählen Sie **Zertifizierungsstelle (CA)** als Zertifikatstyp aus, und klicken Sie auf **Weiter**.
 - 6) Geben Sie den vollständig qualifizierten Pfad- und Dateinamen der CA-Zertifikatsdatei an, und klicken Sie auf **Weiter**. Es wird eine Nachricht angezeigt, die entweder bestätigt, dass der Importprozess erfolgreich war, oder die Fehlerinformationen enthält, falls der Prozess fehlgeschlagen ist.
 - 7) Die CA ist jetzt richtig konfiguriert.

Die Konfiguration des Serviceprozessors ist nicht initialisiert

Wenn Sie den automatischen Sicherheitsmodus verwenden, muss die Konfiguration des Serviceprozessors nach der Konfiguration des Sicherheitsmodus initialisiert werden.

Führen Sie die folgenden Schritte aus:

- Wenn der Serviceprozessor des fernen Systems zum ersten Mal initialisiert wird, befolgen Sie die Anweisungen in „Serviceprozessor initialisieren“ auf Seite 135, um einen neuen Serviceprozessor zu initialisieren.

- Wenn der Serviceprozessor des fernen Systems zuvor bereits initialisiert wurde, befolgen Sie die Anweisungen in „Serviceprozessor initialisieren“ auf Seite 135, um den Benutzer, das Kennwort und das Zertifikat aus der Serviceprozessorkonfiguration des fernen Systems und die Serviceprozessorkonfiguration zu synchronisieren.

Die ID des Serviceprozessorzertifikats wird nicht erkannt

Wenn Sie den manuellen Sicherheitsmodus verwenden, prüfen Sie, ob das Feld für das Serviceprozessorzertifikat mit der ID des Serviceprozessorzertifikats in der Konfiguration des Serviceprozessors übereinstimmt.

1. Zeigen Sie die Konfiguration des Serviceprozessors an (siehe „Konfigurationseigenschaften des Serviceprozessors anzeigen“ auf Seite 134), und klicken Sie auf die Indexzunge **Sicherheit**. Notieren Sie die Komponentenwerte für die ID des Serviceprozessorzertifikats und die Vergleichswerte. Die Komponentenwerte entsprechen den Zertifikatsfeldern folgendermaßen:
 - Allgemeiner Name – Ausgestellt für (Subjekt) Allgemeiner Name (CN)
 - E-Mail-Adresse – Ausgestellt für (Subjekt) (E)
 - Organisationseinheit – Ausgestellt für (Subjekt) Organisationseinheit (OU)
2. Greifen Sie auf die Webschnittstelle des Serviceprozessors zu.
3. Zeigen Sie das Sicherheitszertifikat für den Serviceprozessor an.
4. Vergleichen Sie die Zertifikatsfelder mit den Vergleichswerten aus der Serviceprozessorkonfiguration.
5. Wenn die Werte nicht übereinstimmen, geben Sie den richtigen Wert mit Hilfe der unter „Konfigurationseigenschaften des Serviceprozessors ändern“ auf Seite 134 beschriebenen Methode ein. Lesen Sie anschließend unter „Serviceprozessor initialisieren“ auf Seite 135 nach, wie das Zertifikat für den Serviceprozessor des fernen Systems mit der Serviceprozessorkonfiguration synchronisiert wird.

Anmerkung: In der Serviceprozessorkonfiguration können Sie angeben, dass das Serviceprozessorzertifikat nicht verwendet werden soll.

Der Serviceprozessor unterstützt kein SSL

- Wenn eine sichere Verbindung nicht erforderlich ist, folgen Sie den Anweisungen unter „Konfigurationseigenschaften des Serviceprozessors ändern“ auf Seite 134. Wählen Sie auf der Indexzunge **Sicherheit** die Option **Kein Zertifikat verwenden (physische Sicherheit erforderlich)** aus, und speichern Sie die Änderungen.
- Prüfen Sie, ob der Serviceprozessor SSL unterstützt.
 1. Weitere Informationen finden Sie unter „Fernes Server und Serviceprozessor erkennen“ auf Seite 151.
 2. Wenn der Serviceprozessor SSL-fähig ist, wenden Sie sich an den Kundendienst, um festzustellen, ob ein Firmware- oder Hardwareupdate erforderlich ist, um die SSL-Unterstützung hinzuzufügen.

Virtual Ethernet-Fehler bei Servern mit iSCSI-Anschluss

Geben Sie in einer Windows-Befehlsanzeige **ipconfig /all** ein, um Informationen über die Verbindungen aufzurufen, die für den Windows-TCP/IP-Stack verfügbar sind. Es sollten Informationen über folgende Komponenten angezeigt werden:

- Externe Netzadapter
- Die LAN-Schnittstellen für die iSCSI-HBA-Ports
- Virtual Ethernet-Adapter für den iSeries-Server

Vergleichen Sie die Ergebnisse des Befehls **ipconfig** mit einer der folgenden Fehlersituationen, und führen Sie die vorgeschlagenen Fehlerbehebungsmaßnahmen durch.

| In ipconfig fehlt eine konfigurierte LAN-IP-Adresse

| Das ist der Fall, wenn eine Internetadresse für eine LAN-Schnittstelle in der fernen i5/OS-Konfiguration
| nicht mit einer der IP-Adressen übereinstimmt, die ipconfig für die iSCSI-HBAs anzeigt. Anweisungen für
| das Anzeigen der Konfiguration des fernen Systems finden Sie unter „Konfigurationseigenschaften des
| fernen Systems anzeigen“ auf Seite 131.

- | • Suchen Sie in den ipconfig-Ergebnissen nach den physischen Adressen (MAC-Adressen) der iSCSI-HBAs. Wenn eine der angezeigten physischen Adressen von der Adapteradresse für die LAN-Schnittstelle in der Konfiguration des fernen i5/OS-Systems abweicht, führen Sie die folgenden Schritte aus:
 - | 1. Fahren Sie den Server an der Windows-Konsole herunter.
 - | 2. Hängen Sie die NWS-D unter i5/OS ab. Entsprechende Anweisungen finden Sie unter „Integrierten Server starten und stoppen“ auf Seite 157.
 - | 3. Ändern Sie die Adapteradresse für die LAN-Schnittstelle in der Konfiguration des fernen Systems.
 - | 4. Starten Sie die NWS-D unter i5/OS (hängen Sie sie an). Weitere Informationen hierzu finden Sie in „Integrierten Server starten und stoppen“ auf Seite 157.
- | • Öffnen Sie nacheinander **Systemsteuerung**, **Verwaltungstools** und **Services**. Vergewissern Sie sich, dass **iSeries Shutdown Manager** mit dem Status **Gestartet** in der Liste der Services aufgeführt wird. Dieser Service ordnet automatisch Informationen über die LAN-IP-Schnittstelle aus der Konfiguration des fernen i5/OS-Systems den Ports mit den konfigurierten MAC-Adressen zu.
- | • Suchen Sie im **Anwendungsereignisprotokoll** in Windows nach Ereignissen mit der Quelle **iSeries Shutdown Manager**.
- | • Schließen Sie alle Fenster mit dem Titel "Eigenschaften für Netzwerk", die über eine Indexzeile **Allgemein**, **Authentifizierung** und **Erweitert** verfügen, denn diese Fenster sperren Ressourcen, die für die Zuordnung von IP-Adressen erforderlich sind. Nachdem Sie diese Fenster geschlossen haben, warten Sie etwa 30 Sekunden, bis iSeries Shutdown Manager die fehlende IP-Adresse zugeordnet hat, und geben Sie dann erneut **ipconfig /all** ein.
- | • Wenn keins der ipconfig-Ergebnisse einen installierten iSCSI-HBA beschreibt, öffnen Sie den Geräte-Manager in Windows, und vergewissern Sie sich, dass der Netztreiber für den iSCSI-HBA installiert und aktiviert ist. Wenn der Treiber mit einem gelben '!' markiert oder abgeblendet ist, sehen Sie nach, ob das Systemereignisprotokoll Ereignisse mit der Quelle QL40xx enthält, und vergewissern Sie sich, dass der iSCSI-HBA nicht vom Setup-Menü des System-BIOS inaktiviert wurde.


| Ipconfig zeigt eine konfigurierte iSCSI-HBA-Verbindung mit dem Status "Verbindung getrennt" an.

| Dies ist der Fall, wenn ipconfig eine iSCSI-HBA-Verbindung anzeigt, die sich im Status "Verbindung
| getrennt" befindet und über eine physische Hardwareadresse verfügt, die mit einer Adapteradresse in der
| Konfiguration des fernen i5/OS-Systems übereinstimmt.

- | • Vergewissern Sie sich, dass das physische Netzwerk richtig angeschlossen ist, und dass die Einheiten im Netzwerk, wie beispielweise Switches, an der physischen Verbindung zum iSCSI-HBA des Hosted Systems funktionieren.

| Ipconfig zeigt eine IBM iSeries Virtual Ethernet-Verbindung mit dem Status "Verbindung getrennt" an.

- | • Für Virtual Ethernet ist ein betriebsfähiges iSCSI-Netzwerk erforderlich, daher müssen iSCSI-HBA Probleme zuerst gelöst werden. Vergewissern Sie sich, dass ipconfig die LAN-Adressen in der Konfiguration des fernen i5/OS-Systems anzeigt, bevor Sie fortfahren.
- | • Vergewissern Sie sich, dass das physische Netzwerk richtig angeschlossen ist, und dass die Einheiten im Netzwerk, wie beispielweise Switches, über die physische Verbindung zum iSCSI-HBA des Hosted Systems hinaus funktionieren.
- | • Vergewissern Sie sich, dass die in „iSCSI-Netzwerk“ auf Seite 30 definierten Voraussetzungen erfüllt werden.

- Öffnen Sie nacheinander **Systemsteuerung**, **Verwaltungstools** und **Services**. Vergewissern Sie sich, dass **iSeries Manager**, **iSeries Shutdown Manager** und **iSeries Virtual Ethernet Manager** mit dem Status **Gestartet** in der Liste aufgeführt werden.
- Suchen Sie im **Anwendungsereignisprotokoll** in Windows nach Ereignissen mit der Quelle **iSeries Virtual Ethernet Manager**.
- Wenn eine Firewall oder eine ähnliche Paketfilterfunktion vorhanden ist, lesen Sie die Informationen „Firewall konfigurieren“ auf Seite 142. LAN-IP-Schnittstellen im der Konfiguration des fernen i5/OS-Systems können von der unter Windows laufenden Firewall-Software betroffen sein.
- Wenn für Ihre NWSD andere IPSec-Regeln als *NONE gelten, lesen Sie die Informationen auf der Webseite iSCSI troubleshooting  (www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme/troubleshooting.html).

Ipconfig zeigt eine IBM iSeries Virtual Ethernet-Verbindung mit einer falschen IP-Adresse an.

- Konfigurieren Sie die IP-Adresse in Windows manuell. Entsprechende Anweisungen für Virtual Ethernet-Punkt-zu-Punkt finden Sie unter „IP-Adressenkonflikte bei Virtual Ethernet-Punkt-zu-Punkt“ auf Seite 251. Für andere Virtual Ethernet-Netzwerke gelten nur die Schritte 1 - 5 dieser Prozedur.

‘Virtual Ethernet x’ ist in i5/OS konfiguriert, aber ‘IBM iSeries Virtual Ethernet x’ fehlt in ipconfig

- Prüfen Sie in i5/OS, ob die Leitungsbeschreibung für das betreffende Virtual Ethernet vorhanden ist. Entsprechende Anweisungen für Virtual Ethernet-Punkt-zu-Punkt finden Sie unter „Virtual Ethernet-Punkt-zu-Punkt-Netzwerke anzeigen und ändern“ auf Seite 123.
- Öffnen Sie nacheinander **Systemsteuerung**, **Verwaltungstools** und **Services**. Vergewissern Sie sich, dass **iSeries Virtual Ethernet Manager** mit dem Status **Gestartet** in der Liste der Services aufgeführt wird. Dieser Service erstellt und entfernt automatisch IBM iSeries Virtual Ethernet-Adapter, um eine Übereinstimmung mit der Konfiguration der Leitungsbeschreibung in i5/OS zu erzielen.
- Vergewissern Sie sich, dass das System nicht so eingestellt ist, dass es die Installation nicht signierter Treiber blockiert. Details finden Sie in den Schritten 1-4 von „Installation oder Aktualisierung des LAN-Treibers beginnen“ auf Seite 249. Wenn Sie die Einstellung **Blockieren** ändern, starten Sie **iSeries Virtual Ethernet Manager** erneut, warten 30 Sekunden und geben dann erneut **ipconfig /all** ein.
- Öffnen Sie den **Geräte-Manager** in Windows und vergewissern Sie sich, dass der Netztreiber für den betreffenden IBM iSeries Virtual Ethernet-Adapter installiert und aktiviert ist. Wenn neben dem Treiber ein gelbes ‘!’ steht, sehen Sie nach, ob das **Systemereignisprotokoll** in Windows Ereignisse mit der Quelle **Qvndvimp** enthält.

Die Ipconfig-Ergebnisse scheinen OK zu sein, aber bei umfangreichen Übertragungen treten Fehler auf

- Vergewissern Sie sich, dass die Konfiguration der IBM iSeries Virtual Ethernet-Adapter und der ‘LAN’-Seite der iSCSI-HBA-Ports keinen Wert als „größte zu übertragende Einheit“ enthält, der größer ist, als der vom iSCSI-Netzwerk unterstützte Wert. So unterstützen beispielsweise nicht alle Switches Jumbo-Frames mit einer Größe von 9000 Byte. Überprüfen Sie die Spezifikationen Ihrer Netzeinheit. Weitere Informationen finden Sie unter „Überlegungen zur größten zu übertragenden Einheit (MTU)“ auf Seite 147.

Virtual Ethernet-Fehler bei IXS und Servern mit IXA-Anschluss

Für die Zwecke dieses Abschnitts werden die Ports 0-9 für das Virtual PTP-Ethernet-LAN und für das Virtual Ethernet alle als Virtual Ethernet-Adapter oder Virtual Ethernet-Ports betrachtet.

Es gibt zwei Arten von Virtual Ethernet-Einheitentreibern: einen Virtual Ethernet-Adapter (VE) und einen Virtual Ethernet-Datentransport (DT).

- Der Virtual Ethernet-Adapter entspricht dem Treiber, der als Adapter erscheint und als „virtuell“ bezeichnet wird, da ihm keine NIC-Hardware zugeordnet ist.

- Der Virtual Ethernet-Datentransport ist der Treiber, der eine Verbindung zum Systembus herstellt und alle Virtual Ethernet-Netzwerke miteinander verbindet.

Wenn ein VE-Port nicht über den Systembus kommunizieren kann, gibt er eine Meldung aus, die besagt, dass das Kabel für den Port nicht eingesteckt ist. Dies ist wichtig für die Fehlerbehebung beim Virtual Ethernet.

Die Virtual Ethernet-Ports unter Windows werden automatisch vom Virtual Ethernet Utility (VEU) installiert und deinstalliert. Dieses Dienstprogramm empfängt Signale über eine Konfigurationsdatei von der NWSD. Erstellt ein Benutzer beispielsweise eine Leitungsbeschreibung unter der NWSD für einen bestimmten Virtual Ethernet-Port, dann installiert das VEU den entsprechenden VE-Port. Durch Warmstart des Windows-Servers wird die Adresse des VE-Ports konfiguriert.

Die folgenden Virtual Ethernet-Komponenten verwenden den aufgelisteten Treiber:

- Virtual Ethernet-Adapter: qvndvemp.sys
- Virtual Ethernet-Datentransport: qvndvedt.sys
- Virtual Ethernet-Installationsdienstprogramm: qvndveu.exe

Fehler bei Virtual Ethernet beheben

Wenn die Kommunikation zwischen VE-Ports nicht funktioniert, müssen Sie zur Fehlerbehebung zwei allgemeine Tasks ausführen.

1. Sie müssen den Status der VE-Ports feststellen.
2. Sie müssen die festgestellten Ergebnisse den folgenden Fehlerbehebungsmaßnahmen zuordnen.

Status der VE-Ports feststellen

So stellen Sie den Status der VE-Ports fest:

- Verwenden Sie die iSeries-Konsole um festzustellen, ob eine Leitungsbeschreibung für den VE-Port unter der NWSD erstellt wurde.
- Verwenden Sie die Windows-Konsole, um den Ordner **Netzwerk- und DFÜ-Verbindungen** zu öffnen, und prüfen Sie, ob das Symbol für den VE-Port vorhanden ist.

Portstatus den Fehlerbehebungsmaßnahmen zuordnen

So ordnen Sie die Ergebnisse aus der Überprüfung des VE-Portstatus den folgenden Fehlerbehebungsmaßnahmen zu:

- „Sowohl Leitungsbeschreibung als auch Symbol sind vorhanden“.
- „Leitungsbeschreibung ist vorhanden und Symbol fehlt“ auf Seite 246.
- „Leitungsbeschreibung fehlt und Symbol ist vorhanden“ auf Seite 247.
- „Sowohl Leitungsbeschreibung als auch Symbol fehlen“ auf Seite 247.

Bei jeder Fehlerbehebungsmaßnahme müssen Sie zuerst die i5/OS-Seite und dann die Windows-Seite prüfen. Zur Überprüfung der Windows-Seite müssen Sie m"glicherweise das Ereignisprotokoll und den Geräte-Manager öffnen.

- Klicken Sie zum Öffnen des Ereignisprotokolls im Windows-Menü **Start** auf **Programme, Verwaltung und Ereignisanzeige**.
- Klicken Sie zum Öffnen des Geräte-Managers im Windows-Menü **Start** auf **Einstellungen, Systemsteuerung, Verwaltung, Computerverwaltung** und dann auf **Geräte-Manager**.

Sowohl Leitungsbeschreibung als auch Symbol sind vorhanden

i5/OS-Seite überprüfen

Prüfen Sie die Leitungsbeschreibung. Befindet sich die Leitungsbeschreibung im Status FEHLER, führen Sie die folgenden Schritte durch:

1. Erfassen Sie PAL-Einträge und VLOGs.
2. Fordern Sie Unterstützung an.
3. Überprüfen Sie die Windows-Seite.

Befindet sich die Leitungsbeschreibung im Status ANHÄNGEN ANSTEHEND, ANHÄNGEN oder RCYPND (WIEDERHERSTELLUNG ANSTEHEND), überprüfen Sie stattdessen die Windows-Seite.

Windows-Seite überprüfen

Öffnen Sie das Fenster **Netzwerk- und DFÜ-Verbindungen** und prüfen Sie das VE-Symbol.

- Wenn das VE-Symbol funktionsfähig zu sein scheint und die Leitungsbeschreibung sich im Status ANHÄNGEN befindet, prüfen Sie, ob die IP-Adressen korrekt konfiguriert sind. Bleibt der Fehler bestehen, fordern Sie Unterstützung an.
- Wenn das VE-Symbol funktionsfähig zu sein scheint und die Leitungsbeschreibung sich im Status ANHÄNGEN ANSTEHEND oder RCYPND (WIEDERHERSTELLUNG ANSTEHEND) befindet, prüfen Sie, ob Einträge im PAL vorhanden sind, und fordern Sie Unterstützung an.
- Ist das VE-Symbol mit einem roten X markiert (Kabel ist ausgesteckt), öffnen Sie das Ereignisprotokoll, und suchen Sie nach Einträgen für den Treiber qvndvemp.sys.
 - Wenn Sie Einträge für qvndvemp.sys finden, notieren Sie diese, und fordern Sie Unterstützung an. Möglicherweise ist die Treiberinitialisierung fehlgeschlagen, und ein IOP-Speicherauszug ist erforderlich, um den Fehler zu bestimmen.
 - Wenn Sie keine Einträge für qvndvemp.sys finden, fordern Sie Unterstützung an, und melden Sie den Status der Leitungsbeschreibung. Der Fehler hängt möglicherweise mit dem Lizenzprogramm i5/OS zusammen.

Leitungsbeschreibung ist vorhanden und Symbol fehlt

i5/OS-Seite überprüfen

Prüfen Sie die Leitungsbeschreibung. Befindet sich die Leitungsbeschreibung im Status FEHLER, führen Sie die folgenden Schritte durch:

1. Erfassen Sie PAL-Einträge und VLOGs.
2. Fordern Sie Unterstützung an.
3. Überprüfen Sie die Windows-Seite.

Befindet sich die Leitungsbeschreibung im Status ANHÄNGEN ANSTEHEND, ANHÄNGEN oder RCYPND (WIEDERHERSTELLUNG ANSTEHEND), überprüfen Sie stattdessen die Windows-Seite.

Windows-Seite überprüfen

Öffnen Sie den **Geräte-Manager**, klicken Sie auf **Netzwerkadapter**, um die installierten Adapter aufzulisten, und suchen Sie den Eintrag für den VE-Port.

- Wenn neben dem VE-Port ein Ausrufezeichen (!) steht, führen Sie die folgenden Schritte aus:
 1. Öffnen Sie das Ereignisprotokoll, suchen Sie die Einträge für den Treiber qvndvemp.sys, und notieren Sie diese.
 2. Fordern Sie Unterstützung an. Der Treiber wurde nicht initialisiert, weshalb Unterstützung beim Feststellen der Ursache erforderlich ist.
- Wenn der VE-Port mit einem roten X markiert ist, führen Sie die folgenden Schritte durch:
 1. Klicken Sie mit der rechten Maustaste auf den VE-Port, und wählen Sie **Aktivieren** aus.
 2. Öffnen Sie das Fenster **Netzwerk- und DFÜ-Verbindungen**, und suchen Sie das VE-Symbol.
 3. Fehlt das Symbol für den VE-Port oder bleibt es grau, öffnen Sie das **Ereignisprotokoll**.
 4. Suchen Sie nach Einträgen für den Treiber qvndvemp.sys, notieren Sie die Einträge, die Sie finden, und fordern Sie Unterstützung an. Der VE-Port wurde nicht geladen oder nicht gestartet.

Leitungsbeschreibung fehlt und Symbol ist vorhanden

i5/OS-Seite überprüfen

Vergewissern Sie sich, dass keine Leitungsbeschreibung für den VE-Port unter der NWSD vorhanden ist, und prüfen Sie die Windows-Seite.

Windows-Seite überprüfen

Öffnen Sie das Fenster **Netzwerk- und DFÜ-Verbindungen**, und prüfen Sie das VE-Symbol. Wurde der VE-Port vom Installations-VEU nicht entfernt, führen Sie einen Warmstart für den integrierten Server durch, um diese Bedingung zu beseitigen. Bleibt der Fehler bestehen, führen Sie die folgenden Schritte durch:

1. Verwenden Sie das VEU, um den VE-Port mit dem folgenden Befehl manuell zu entfernen:

```
qvndveu -a -R -x [port_id]
```

Dabei ist die [port_id] entweder eine Dezimalzahl (0-9), die dem zu entfernenden Port entspricht, oder ein p für Punkt-zu-Punkt (Virtual Ethernet-Punkt-zu-Punkt).

2. Ist das Symbol für den VE-Port nach der Befehlsausführung nicht mehr vorhanden, ist der Prozess beendet. Konnte das VEU den VE-Port jedoch nicht deinstallieren und entfernen, fahren Sie mit den restlichen Schritten fort.
3. Suchen Sie die VEU-Protokolldatei (D:\as400nt\qvndveu.log).
4. Öffnen Sie das **Ereignisprotokoll**, suchen Sie die Einträge für den Treiber qvndvemp.sys, und notieren Sie diese.
5. Fordern Sie Unterstützung an. Vergewissern Sie sich, dass Sie Folgendes zur Hand haben:
 - Alle Einträge, die Sie für qvndvemp.sys notiert haben.
 - Die VEU-Protokolldatei.

Sowohl Leitungsbeschreibung als auch Symbol fehlen

i5/OS-Seite überprüfen

In der NWSD muss eine Leitungsbeschreibung für einen zu installierenden VE-Port vorhanden sein. Anhand der Anweisungen im Abschnitt „Virtual Ethernet-Netzwerke konfigurieren“ auf Seite 121 können Sie eine Leitungsbeschreibung erstellen.

Anmerkung:

Zum Hinzufügen einer Leitungsbeschreibung muss die NWSD abgehängt werden. Sobald Sie eine Leitungsbeschreibung erstellt und einen Warmstart für den integrierten Windows-Server durchgeführt haben, erstellt das Installations-VEU automatisch den VE-Port unter Windows.

Besteht weiterhin ein Fehler mit einem VE-Port, nachdem Sie erfolgreich eine Leitungsbeschreibung erstellt und einen Warmstart für den integrierten Windows-Server durchgeführt haben, kehren Sie zu diesem Abschnitt mit den Fehlerbehebungsmaßnahmen zurück, und folgen Sie den Anweisungen für die neue Fehlersituation.

Windows-Seite überprüfen

Wenn keine i5/OS-Leitungsbeschreibung vorhanden ist, sollte kein VE-Port unter Windows aufgelistet sein. Installieren Sie die Leitungsbeschreibung anhand der Anweisungen im Abschnitt „Virtual Ethernet-Netzwerke konfigurieren“ auf Seite 121, und starten Sie den integrierten Server erneut. Prüfen Sie, ob der Fehler hierdurch behoben werden konnte.

Fehler bei externen Netzwerken

Bei Fehlern im externen Netzwerk eines integrierten Servers haben Sie die folgenden Möglichkeiten:

- Überprüfen Sie das Ereignisprotokoll des integrierten Windows-Servers auf Übertragungsfehler oder Fehler bei Einheitentreibern. Sie können hierzu die **Ereignisanzeige** von Windows verwenden. Ereignisprotokolle für externe Adapter, die von den Modellen 2890, 2892 und 4812 des integrierten xSeries-Servers unterstützt werden, enthalten im Feld "Quelle" des Ereignisprotokolls möglicherweise eine der folgenden Angaben: IBMTRP, PCNET, ALTND5, E100B oder E1000. Wenn Sie keinen Text in den Ereignisprotokollen für den IBMTRP Token-Ring-Dienst finden, müssen Sie Änderungen in der Windows-Registrierung vornehmen.

Anmerkung:


Falls Sie die Vorgehensweise zum Ändern der Windows-Registrierung nicht kennen, wenden Sie sich an den zuständigen Ansprechpartner.

Wenn Sie wissen, wie der Text in den Ereignisprotokollen sichtbar gemacht wird, führen Sie die folgenden Schritte durch:

1. Rufen Sie das Windows-Menü **Start** auf, und klicken Sie auf **Ausführen**.
 2. Geben Sie `regedit` ein.
 3. Suchen Sie im Registrierungseditor nach der Angabe
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\IBMTRP`.
 4. Wählen Sie **EventMessageFile** aus.
 5. Wählen Sie im Menü **Bearbeiten** des Registrierungseditors **Ändern** aus.
 6. Geben Sie `%SystemRoot%\System32\netevent.dll;%SystemRoot%\System32\ibmsgnet.dll` ein.
 7. Schließen Sie den Registrierungseditor, und starten Sie den integrierten Server erneut.
- Vergewissern Sie sich bei Ethernet-Adaptoren, dass ein Treiber mit **iSeries** oder **AMD PCNET Family Ethernet Adapter (PCI)** als Namensteil aufgelistet ist und den Status **Gestartet** hat.
 1. Klicken Sie auf **Start, Verwaltung, Computerverwaltung, Systemprogramme, Geräte-Manager und Netzwerkadapter**.
 2. Vergewissern Sie sich, dass ein Treiber mit **iSeries** oder **AMD PCNET Family Ethernet Adapter (PCI)** als Namensteil aufgelistet ist und den Status **Gestartet** hat.
 - Vergewissern Sie sich bei Token-Ring-Netzwerken (ebenfalls unter **Geräte-Manager**, dass der **IBM High-Speed 100/16/4 Token-Ring PCI Adapter** oder **IBM PCI Token-Ring Adapter** gestartet ist.


Anmerkung:

Die Starteinstellung sollte **Aktiviert** sein.

- Vergewissern Sie sich bei Token-Ring-Netzwerken, dass die Einstellung für die Datenrate des Netzwerks für Ihr Netzwerk geeignet ist.
- Vergewissern Sie sich bei Ethernet-Netzwerken, dass die Einstellungen für die Verbindungsgeschwindigkeit und für Duplex für Ihren Switch oder Hub geeignet sind. Wenn Ihr Modell 4812 oder 5701 nur Verbindungen mit maximal 100 Millionen Bit pro Sekunde herstellen kann, müssen Sie die Spezifikationen des Switches überprüfen, um die Übereinstimmung mit dem Standard IEEE 802.3ab zu gewährleisten. Windows-LAN-Treiber für 4812- oder 5701-GB-Ethernet-Ports unterliegen möglicherweise bei Verbindungen zu bestimmten älteren Switchmodellen, die diesem Standard nicht entsprechen, einer Einschränkung auf 100 Millionen Bit pro Sekunde.
- Der 10/100 Mbit/s-Ethernet-Port auf dem integrierten xSeries-Server 2892 unterstützt keine direkten Verbindungen zu bestimmten 10 Mbit/s-Hubs und -Routern, die nicht mit einer Funktion für die **Automatische Polarität** ausgestattet sind. Wenn Ihr 10/100-Port auf einem Modell 2892 mit einem 10 Mbit/s-Hub oder -Router überhaupt nicht funktioniert, prüfen Sie die Angaben zur Unterstützung der **automatischen Polarität** in den Spezifikationen. Prüfen Sie außerdem, ob der 10/100-Port des Modells 2892 mit anderen Einheiten funktioniert.
- Wenn das Problem weiterhin besteht, überprüfen Sie die Datenbank mit technischen Informationen auf der Webseite [@server IBM iSeries Support](#) . Wird dort keine Lösung angeboten, wenden Sie sich an die technische Unterstützung.

LAN-Treiber auf dem integrierten Windows-Server manuell aktualisieren

Bei Windows 2000 Server und Windows Server 2003 werden die LAN-Treiber, die den LAN-Adaptoren und -Ports entsprechen, im Allgemeinen automatisch installiert. Unter besonderen Umständen können Sie einen LAN-Treiber aber auch manuell installieren oder aktualisieren.

Soll ein LAN-Treiber für einen Adapter (außer Virtual Ethernet) auf einem extern angeschlossenen Netfinity- oder xSeries-Server manuell installiert oder aktualisiert werden, rufen Sie die Webseite IBM Personal Computing Support  auf, und wählen Sie dort **Servers** und dann **Device Driver File Matrix** aus.

So installieren oder aktualisieren Sie manuell einen LAN-Treiber für einen Adapter oder Port auf einem integrierten xSeries-Server oder für Virtual Ethernet:

1. „Installation oder Aktualisierung des LAN-Treibers beginnen“.
2. „Zu installierenden oder zu aktualisierenden Adapter auswählen“.
3. „Installation oder Aktualisierung des LAN-Treibers abschließen“.

Installation oder Aktualisierung des LAN-Treibers beginnen

So beginnen Sie die manuelle Installation oder Aktualisierung des LAN-Treibers oder -Ports auf einem integrierten xSeries-Server oder für Virtual Ethernet.

1. Klicken Sie im Windows-Menü auf **Start, Einstellungen und Systemsteuerung**.
2. Doppelklicken Sie auf **System**.
3. Wählen Sie im Fenster **Systemeigenschaften** die Indexzunge **Hardware** aus.
4. Ist der neue LAN-Treiber nicht digital signiert oder sind Sie sich nicht sicher, ob der LAN-Treiber digital signiert ist, vergewissern Sie sich, dass die Treibersignierungsrichtlinien auf "Ignorieren" gesetzt sind.
 - a. Klicken Sie im Fenster **Systemeigenschaften** auf **Treibersignierung**.
 - b. Notieren Sie die aktuelle Einstellung, und klicken Sie anschließend auf **Ignorieren** und dann auf **OK**.
5. Klicken Sie auf **Geräte-Manager**.
6. „Zu installierenden oder zu aktualisierenden Adapter auswählen“.

Zu installierenden oder zu aktualisierenden Adapter auswählen

Nachdem Sie die Schritte zum Beginnen der Installation oder Aktualisierung für den LAN-Treiber oder -Port auf einem integrierten xSeries-Server oder für Virtual Ethernet durchgeführt haben (siehe „Installation oder Aktualisierung des LAN-Treibers beginnen“), müssen Sie den Adapter auswählen.

So wählen Sie den Adapter aus, der installiert oder aktualisiert werden soll:

1. Klicken Sie im Fenster **Geräte-Manager** auf **Netzwerkadapter**.
2. Klicken Sie unter **Netzwerkadapter** mit der rechten Maustaste auf den Adapter, der aktualisiert werden soll, und wählen Sie **Eigenschaften** aus.
3. Klicken Sie im Fenster **Eigenschaften** für den Adapter auf die Indexzunge **Treiber**.
4. Klicken Sie auf **Treiber aktualisieren** oder **Treiber installieren** (nur eine Option wird angezeigt).
5. Klicken Sie im Dialogfenster **Assistent zum Aktualisieren von Gerätetreibern** auf **Weiter**.
6. „Installation oder Aktualisierung des LAN-Treibers abschließen“.

Installation oder Aktualisierung des LAN-Treibers abschließen

Vergewissern Sie sich, dass Sie die beiden ersten Aufgaben, die für eine manuelle Installation oder Aktualisierung des LAN-Treibers oder -Ports auf einem integrierten xSeries-Server oder für Virtual Ethernet erforderlich sind, durchgeführt haben:

- „Installation oder Aktualisierung des LAN-Treibers beginnen“.

- „Zu installierenden oder zu aktualisierenden Adapter auswählen“ auf Seite 249.

Wählen Sie eine der folgenden Vorgehensweisen aus, die Ihrer Situation am besten entspricht, um den LAN-Treiber oder -Port zu installieren oder zu aktualisieren.

- Sie arbeiten mit Windows 2000 Server oder wurden angewiesen, den LAN-Treiber aus einem bestimmten Ordner für Windows Server 2003 zu installieren.
- Sie arbeiten mit Windows Server 2003 und wurden nicht angewiesen, den LAN-Treiber aus einem bestimmten Ordner zu installieren.

Bei Verwendung von Windows 2000 Server oder bei Anweisung, den LAN-Treiber aus einem bestimmten Ordner für Windows Server 2003 zu installieren

So schließen Sie die Installation oder Aktualisierung des LAN-Treibers ab:

1. Wählen Sie **Treiber für das Gerät in einer Liste anzeigen und den entsprechenden Treiber selbst auswählen** aus, und klicken Sie auf **Weiter**.
2. Klicken Sie auf **Datenträger**, um das Dialogfenster **Installation von Datenträger** zu öffnen, und geben Sie die Position des Treibers an.
 - Falls Sie angewiesen wurden, den Treiber von einem bestimmten Laufwerk und Ordner zu installieren, klicken Sie auf **Durchsuchen**, um die Position anzugeben, und klicken Sie dann auf **Öffnen**.
 - Klicken Sie andernfalls auf **Durchsuchen**, um die Position des Treibers, der dem Adapter entspricht, der installiert oder aktualisiert werden soll, auf dem Systemlaufwerk (normalerweise C:) anzugeben. Gehen Sie anhand der folgenden Liste vor, um den Ordner zu lokalisieren, in dem sich der Treiber für die bestimmte Hardware befindet:
 - \wsv\ibm für Hardwaretyp 2744
 - \wsv\alt für Hardwaretypen 2743 und 2760
 - \wsv für Virtual Ethernet
 - \wsv\amd für Hardwaretyp 2838 in Windows 2000
 - \windows\inf für Hardwaretypen 2723 und 2838 unter Windows Server 2003
 - \wsv\it1 für Hardwaretyp 2892 unter Windows 2000
 - \wsv für Hardwaretyp 2892 unter Windows Server 2003
 - \wsv\alt für Hardwaretypen 4812, 5700 und 5701 unter Windows 2000
 - \wsv\itg für Hardwaretypen 4812, 5700 und 5701 unter Windows Server 2003
3. Klicken Sie auf **OK**.
4. Ist der entsprechende Treiber im Dialogfeld **Assistent zum Aktualisieren von Gerätetreibern** nicht bereits hervorgehoben, wählen Sie ihn in der Liste aus und klicken Sie auf **Weiter**.
5. Klicken Sie nochmals auf **Weiter**.
6. Wird nach Abschluss der Treiberaktualisierung der Rückkehrcode 22 angezeigt, ist der Adapter möglicherweise inaktiviert. Um den Adapter in diesem Fall zu aktivieren, klicken Sie im Fenster **Geräte-Manager** mit der rechten Maustaste auf den inaktivierten Adapter und wählen Sie **Aktivieren** aus.
7. Sollen weitere Adapter installiert oder aktualisiert werden, finden Sie unter „Zu installierenden oder zu aktualisierenden Adapter auswählen“ auf Seite 249 weitere Informationen.

Anmerkung:

Wird von Windows eine Anmerkung ausgegeben, dass nach einer Treiberaktualisierung ein Neustart durchgeführt werden muss, verzögern Sie ihn, bis alle Adapter aktualisiert sind.

8. Haben Sie die Treibersignierungsrichtlinie geändert, als Sie mit der Installation oder Aktualisierung begonnen haben (siehe „Installation oder Aktualisierung des LAN-Treibers beginnen“ auf Seite 249), dann stellen Sie die Originalrichtlinie wieder her.

Bei Verwendung von Windows Server 2003 und ohne Anweisung, den LAN-Treiber aus einem bestimmten Ordner zu installieren

So schließen Sie die Installation oder Aktualisierung des LAN-Treibers ab:

1. Wählen Sie **Nach einem passenden Treiber für das Gerät suchen** aus, und klicken Sie auf **Weiter**.
2. Klicken Sie auf **Weiter**, um kompatible Hardware anzuzeigen.
3. Nehmen Sie die Auswahl für alle **Anderen Quellen für die Suche** zurück, und klicken Sie auf **Weiter** und anschließend nochmal auf **Weiter**.
4. Wird nach Abschluss der Treiberaktualisierung der Rückkehrcode 22 angezeigt, ist der Adapter m"licherweise inaktiviert. Um den Adapter in diesem Fall zu aktivieren, klicken Sie im Fenster **Geräte-Manager** mit der rechten Maustaste auf den inaktivierten Adapter und wählen Sie **Aktivieren** aus.
5. Sollen weitere Adapter installiert oder aktualisiert werden, finden Sie unter „Zu installierenden oder zu aktualisierenden Adapter auswählen“ auf Seite 249 weitere Informationen.

Anmerkung:

Wird von Windows ein Anmerkung ausgegeben, dass nach einer Treiberaktualisierung ein Neustart durchgeführt werden muss, verz"gern Sie ihn, bis alle Adapter aktualisiert sind.

6. Haben Sie die Treibersignierungsrichtlinie geändert, als Sie mit der Treiberinstallation oder -aktualisierung begonnen haben (siehe „Installation oder Aktualisierung des LAN-Treibers beginnen“ auf Seite 249), dann stellen Sie die Originalrichtlinie wieder her.

IP-Adressenkonflikte bei Virtual Ethernet-Punkt-zu-Punkt

IBM iSeries Integrated Server Support verwendet IP-Adressen im Bereich von 192.168.x.y für das Punkt-zu-Punkt-Ethernet-Netzwerk des integrierten Servers. Die tatsächlichen Adressen werden standardmäßig vom i5/OS-Befehl INSWNTSVR (Windows-Server installieren) ausgewählt. Details und Beispiele finden Sie unter „IP-Adressen für Virtual Ethernet-Punkt-zu-Punkt zuordnen“ auf Seite 252. Abhängig vom Netzwerk kann es zu Konflikten mit Adressen kommen, die bereits in Gebrauch sind. Um potenzielle Konflikte zu vermeiden, können Sie den Parameter VRTPTPPORT für einen integrierten xSeries-Server oder den xSeries-Server verwenden, der über einen integrierten xSeries-Adapter angeschlossen ist.

Müssen die Adressen wegen eines Konflikts geändert werden, muss sichergestellt werden, dass das Virtual Ethernet-Punkt-zu-Punkt ein eigenes Teilnetz unter i5/OS belegt. Die verwendete Teilnetzmaske ist 255.255.255.0. Um zu gewährleisten, dass das Virtual Ethernet-Punkt-zu-Punkt sein eigenes Teilnetz verwendet, sollten IP-Adressen im Format a.b.x.y benutzt werden, wobei a.b.x für beide Seiten des Virtual Ethernet-Punkt-zu-Punkt denselben Wert aufweist. Außerdem muss geprüft werden, dass der Wert für a.b.x im Netzwerk eindeutig ist.

So ändern Sie die Adressen im Virtual Ethernet-Punkt-zu-Punkt aufgrund eines Konflikts:

1. Geben Sie an der i5/OS-Konsole den Befehl DSPNWSN WSD(name) OPTION (*PORTS) ein. Notieren Sie die angeschlossene Leitung für die Portnummer *VRTETHPTP, die auch als Leitungsbeschreibung bezeichnet wird.
2. Verwenden Sie den Befehl CFGTCP (TCP/IP konfigurieren) und geben Sie Auswahl 1 ein, um die TCP-Schnittstellen anzuzeigen. Notieren Sie die IP-Adresse und die Teilnetzmaske aus Schritt 1, die der Leitungsbeschreibung zugeordnet sind.

Anmerkung:

Eine IP-Adresse, die an der Windows-Konsole für das Virtual Ethernet-Punkt-zu-Punkt eingegeben wurde, überschreibt die in der NWS-Beschreibung eingestellten Werte *VRTETHPTP für den Parameter TCPPRTCFG.

1. Klicken Sie auf **Start** —> **Einstellungen** —> **Systemsteuerung** und dann auf **Netzwerk- und DFÜ-Verbindungen**.
2. Klicken Sie mit der rechten Maustaste auf die korrekte **LAN-Verbindung** für das Virtual Ethernet-Punkt-zu-Punkt und wählen Sie im Menü die Option **Eigenschaften** aus.

3. Wählen Sie aus der Liste der installierten Protokolle **TCP/IP-Protokoll** aus und klicken Sie auf die Schaltfläche **Eigenschaften**, um die TCP/IP-Eigenschaften anzuzeigen.
4. Ändern Sie die IP-Adresse für den neuen Wert, den Sie ausgewählt haben.
5. Klicken Sie auf **OK** und anschließend auf **Schließen**, um die Anwendung zu beenden.
6. Beenden Sie den integrierten Windows-Server, ohne ihn erneut zu starten.
7. Hängen Sie die NWS-D unter i5/OS ab.
8. Führen Sie den Befehl RMVTCPIFC (TCP/IP-Schnittstelle entfernen) mit der IP-Adresse aus, die Sie in Schritt 2 notiert haben.
9. Führen Sie den Befehl ADDTCPIFC (TCP/IP-Schnittstelle hinzufügen) aus, um die neue Schnittstelle hinzuzufügen. Verwenden Sie die IP-Adresse, die Sie für die i5/OS-Seite des Virtual Ethernet-Punkt-zu-Punkt ausgewählt haben. Sie müssen außerdem die Teilnetzmaske und die Leitungsbeschreibung eingeben, die Sie in den Schritten 1 und 2 notiert haben.
10. Geben Sie in der i5/OS-Befehlszeile den Befehl CHGNWS NWSD(name) ein, und drücken Sie F4.
 - a. Blättern Sie vor zu dem Abschnitt mit der Bezeichnung TCP/IP-Port-Konfiguration.
 - b. Ändern Sie die IP-Adresse im Feld Internet-Adresse für den Port *VRTETHPTP in den Wert, den Sie in Schritt 3 verwendet haben. Drücken Sie die Eingabetaste, damit die Änderung wirksam wird.
 - c. Hängen Sie die NWS-D an.

Anmerkung:

Wenn Sie mehrere Server installieren, sollten Sie zur Vermeidung zukünftiger Konflikte die IP-Adressen für das Virtual Ethernet-Punkt-zu-Punkt selbst zuordnen (siehe „IP-Adressen für Virtual Ethernet-Punkt-zu-Punkt zuordnen“), statt sie vom Befehl INSWNTSVR generieren zu lassen. Der Parameter Virtual Ethernet-PTP-Port erlaubt Ihnen die Eingabe von IP-Adressen, von denen bekannt ist, dass sie im System eindeutig sind.

IP-Adressen für Virtual Ethernet-Punkt-zu-Punkt zuordnen

Der Befehl INSWNTSVR (Windows-Server installieren) ordnet dem Virtual Ethernet-PTP standardmäßig IP-Adressen im Format 192.168.x.y zu. Um potenzielle Konflikte zu vermeiden, können Sie jedoch mit Hilfe des Parameters VRTPTPPORT in diesem Befehl IP-Adressen zuordnen, von denen Sie wissen, dass sie im System eindeutig sind.

Wenn Sie die Adressenzuordnung von dem Befehl durchführen lassen und dann einen Konflikt feststellen, haben Sie die Möglichkeit, die IP-Adressen zu ändern. Für IXS und integrierte Server mit IXA-Anschluss ordnet der Befehl x einen Wert zu, der auf der Ressourcennummer des integrierten xSeries-Servers beruht. Der Befehl sucht nach einem Wertepaar y und y+1 (beginnend mit y=1) in Adressen, die unter dem betreffenden i5/OS nicht in Gebrauch sind. Der Befehl ordnet die niedrigere Nummer des Paares der i5/OS-Seite des Virtual Ethernet-PTP und die höhere Nummer der Windows-Server-Seite zu.



Beispiel: Angenommen, Sie haben einen integrierten xSeries-Server 2892 mit dem Ressourcenamen LIN03. Nach Ausführung des Befehls INSWNTSVR (Windows-Server installieren) erhalten Sie möglicherweise die folgenden Adressen für das Virtual Ethernet-PTP:

192.168.3.1 (i5/OS-Seite)
 192.168.3.2 (Windows-Server-Seite)

Im Falle eines Konflikts auf einem von Ihnen installierten Server stellen Sie sicher, dass ein bestimmter Substitutionswert (z. B. 192.168.17) in Ihrem Netzwerk nicht benutzt wird, und ändern Sie die IP-Adressen in diesen Wert.

192.168.17.1 (i5/OS-Seite)
 192.168.17.2 (Windows-Server-Seite)

Beachten Sie, dass eine IP-Adresse, die an der Windows-Konsole für das Virtual Ethernet-PTP eingegeben wurde, den Wert in der NWS-Beschreibung für die TCPPTPCFG-Parameter des Ports *VRTETHPTP überschreibt.

Wenn das Problem weiterhin besteht, überprüfen Sie die Datenbank mit technischen Informationen auf der Webseite  **server** IBM iSeries Support  . Wird dort keine Lösung angeboten, wenden Sie sich an die technische Unterstützung. Bleibt das Problem bestehen, wenden Sie sich an den IBM Kundendienst.

Fehler bei TCP/IP über Virtual Ethernet

Prüfen Sie, ob die TCP/IP-Konfiguration für das Virtual Ethernet-Punkt-zu-Punkt korrekt ist. Wenn es sich um eine neue oder geänderte TCP/IP-Konfiguration unter i5/OS handelt, gehen Sie folgendermaßen vor, um zu prüfen, ob die TCP/IP-Konfiguration unter Windows korrekt ist.

1. Klicken Sie auf **Start** → **Systemsteuerung** → **Netzwerkverbindungen** oder **Start** → **Einstellungen** → **Netzwerk- und DFÜ-Verbindungen**.
2. Klicken Sie mit der rechten Maustaste auf **Netzwerkverbindungen** oder **Netzwerk- und DFÜ-Verbindungen**; es erscheint ein Popup-Menü, in dem Sie **Öffnen** auswählen.
3. Klicken Sie doppelt auf **IBM iSeries Virtual Ethernet Punkt-zu-Punkt-Verbindung**.
4. Klicken Sie auf die Schaltfläche **Eigenschaften**.
5. Wählen Sie das Internet Protocol (TCP/IP) aus.
6. Klicken Sie auf die Schaltfläche **Eigenschaften**. Wenn **Folgende IP-Adresse verwenden** ausgewählt ist und die IP-Adresse der i5/OS-Konsole erscheint, müssen Sie keine weiteren Schritte ausführen. Wenn "IP-Adresse beziehen" ausgewählt ist, fahren Sie mit dem nächsten Schritt fort.
7. Wählen Sie das Optionsfeld **Folgende IP-Adresse verwenden** aus.
8. Geben Sie in einer i5/OS-Befehlszeile den folgenden Befehl ein, wobei "nwsd" der Name der NWSD Ihres Servers ist, und drücken Sie die Eingabetaste: `DSPNWSD NWSD(nwsd) OPTION(*TCPIP)`
 - Suchen Sie im Dialogfeld DSPNWSD nach dem Port namens *VRTETHPTP. Dort werden die Werte für die IP-Adresse und die Teilnetzmaske für das Virtual Ethernet-PTP angezeigt.
 - Geben Sie an der Konsole des integrierten Servers die Werte für die IP-Adresse und Teilnetzmaske des Virtual Ethernet-PTP ein, die im Befehl DSPNWSD angezeigt wurden.
9. Klicken Sie auf OK.
10. Klicken Sie auf OK.
11. Klicken Sie auf Schließen.

Informationen darüber, wie die TCP/IP-Konfiguration in i5/OS und Windows geprüft wird, finden Sie unter „Virtual Ethernet-Punkt-zu-Punkt-Netzwerke anzeigen und ändern“ auf Seite 123.

Das von allen aktiven Servern verwendete Virtual Ethernet-PTP, muss ein eigenes IP-Teilnetz benutzen. Weitere Informationen über Voraussetzungen für Teilnetze oder das Ändern der TCP/IP-Konfiguration finden Sie unter „IP-Adressenkonflikte bei Virtual Ethernet-Punkt-zu-Punkt“ auf Seite 251.

Prüfen Sie, ob die iSeries Virtual Ethernet-Adapter richtig konfiguriert und betriebsfähig sind.

Die Vorgehensweise bei der Fehlerbehebung für Virtual Ethernet-Adapter wird in den folgenden Abschnitten beschrieben.

- „Virtual Ethernet-Fehler bei Servern mit iSCSI-Anschluss“ auf Seite 242.
- „Virtual Ethernet-Fehler bei IXS und Servern mit IXA-Anschluss“ auf Seite 244

Informationen darüber, wie geprüft wird, ob eine Leitungsbeschreibung richtig für einen Virtual Ethernet-Adapter konfiguriert ist, finden Sie unter Kapitel 6, „Virtual Ethernet- und externe Netzwerke verwalten“, auf Seite 121.

| Vergewissern Sie sich, dass keine Firewall eingreift.

- | Wenn eine Firewall aktiv ist (z. B. eine Software-Firewall unter Windows), dann muss diese so konfiguriert sein, dass sie den erforderlichen Datenverkehr zulässt.
- | • Für die IP-Adresse der IBM iSeries Virtual Ethernet-PTP-Verbindung: Lassen Sie dynamische TCP-Ports zu, um Fehler bei den Verwaltungsanwendungen der integrierten Server zu verhindern. Verwenden Sie keine NAT (Network Address Translation).
- | • Für die IP-Adresse einer IBM iSeries Virtual Ethernet-Verbindung: Lassen Sie Protokolle und Ports zu, die von Ihren Anwendungen benötigt werden.
- | • Informationen über die IP-Adresse einer iSCSI-HBA-Verbindung finden Sie unter „Firewall konfigurieren“ auf Seite 142.

Fehler beim Zugriff auf Freigaben von Windows Server 2003 mit dem Dateisystem QNTC

Wenn das i5/OS-Dateisystem QNTC nicht für den Zugriff auf Freigaben auf einem Server mit Windows Server 2003 und installiertem Active Directory verwendet werden kann (z. B. bei einem Domänencontroller), müssen Sie möglicherweise einige zusätzliche Konfigurationsschritte ausführen. Weitere Informationen hierzu finden Sie in „Kerberos für Windows Server 2003 Active Directory Server aktivieren“ auf Seite 115.

IFS-Zugriffsfehler

Wenn Sie versuchen, von einem integrierten Windows-Server aus über iSeries NetServer auf das i5/OS Integrated File System (IFS) zuzugreifen, kann der Zugriff unter folgenden Bedingungen fehlschlagen:

- Wenn Sie einen UNC-Namen (Universal Naming Convention) mit einer eingebetteten IP-Adresse verwenden und
- | • Wenn es zwischen dem integrierten Windows-Server und i5/OS sowohl Virtual Ethernet-PTP- als auch externe LAN-Pfade gibt.

Ändern Sie entweder den UNC-Namen so, dass stattdessen der Name von iSeries NetServer verwendet wird, oder inaktivieren Sie den externen LAN-Pfad, und wiederholen Sie anschließend die fehlgeschlagene Operation.

Fehler beim Sichern von Dateien des integrierten Windows-Servers

Treten Fehler beim Sichern von Dateien des integrierten Servers auf Dateiebene auf, prüfen Sie das Windows-Ereignisprotokoll und die i5/OS-Nachrichtenwarteschlange QSYSOPR auf Nachrichten.

- Gehen Sie folgendermaßen vor, wenn beim Sichern von Dateien ein Sitzungsinitialisierungsfehler (CPDB050) oder ein Sitzungsübertragungsfehler (CPDB055) ausgegeben wird:
 1. Vergewissern Sie sich, dass sich i5/OS NetServer in derselben Domäne wie der integrierte Server befindet (siehe „Zugehörigkeit von iSeries NetServer und integriertem Windows-Server zur selben Domäne sicherstellen“ auf Seite 207), dessen Dateien gesichert werden sollen.
 2. Vergewissern Sie sich, dass Sie die Schritte unter „Freigaben auf integrierten Windows-Servern erstellen“ auf Seite 207 und „Teildateien zur Datei QAZLCSAVL hinzufügen“ auf Seite 207 ausgeführt haben.
 3. Vergewissern Sie sich, dass das Subsystem QSERVER aktiv ist.
 4. Vergewissern Sie sich, dass TCP/IP aktiv ist:
 - a. Verwenden Sie Auswahl 1 des Befehls CFGTCP.
 - b. Drücken Sie F11, um den Schnittstellenstatus anzuzeigen.
 - c. Geben Sie eine 9 neben dem entsprechenden Netzwerkservice ein, um die TCP/IP-Schnittstelle zu starten.
 - d. Aktualisieren Sie die Anzeige mit F5. Der betreffende TCP/IP-Service müsste jetzt aktiv sein.
 5. Versuchen Sie anschließend nochmals, die Dateien zu sichern.

- Wird eine Fehlermeldung ausgegeben, die auf einen Fehler beim Austausch von Sicherheitsinformationen (CPDB053) oder auf einen Fehler beim Anmelden am Server (NTA02AE) hinweist, gehen Sie folgendermaßen vor:
 1. Vergewissern Sie sich, dass Sie auf dem integrierten Server als Mitglied in der Gruppe der Administratoren registriert sind.
 2. Vergewissern Sie sich, dass Sie auf dem integrierten Server dasselbe Kennwort wie unter i5/OS haben.
 3. Versuchen Sie anschließend nochmals, die Dateien zu sichern.
- Wird eine Fehlermeldung ausgegeben, die auf ein Problem bei der Verarbeitung der Freigabeteildatei hinweist (CPDB058), vergewissern Sie sich, dass die Datei QAZLCSAVL korrekt definiert ist:
 1. Prüfen Sie, ob Sie die Schritte unter „Freigaben auf integrierten Windows-Servern erstellen“ auf Seite 207 ausgeführt haben.
 2. Prüfen Sie, ob Sie ebenfalls die Schritte unter „Teildateien zur Datei QAZLCSAVL hinzufügen“ auf Seite 207 ausgeführt haben. In dieser Datei muss außerdem die Freigabe aufgelistet sein, die im Befehl SAV (Sichern) angegeben war.
- Wird eine Fehlermeldung ausgegeben, die auf einen Fehler bei der Kommunikation mit NTSAV hinweist (NTA02A3), prüfen Sie, ob der Dienst "Remote Procedure Call" aktiv ist:
 1. Klicken Sie in der Taskleiste des integrierten Servers auf **Start** —> **Programme** —> **Verwaltung**.
 2. Doppelklicken Sie auf **Dienste**.
 3. Prüfen Sie, ob der Dienst "Remote Command" aktiv ist.
- Bei der Ausführung des Befehls SAV können die folgenden Fehler auftreten:
 - CPFA09C Keine Berechtigung für Objekt
 - CPD3730 Verzeichnis /qntc/(server)/(share)/System Volume Information kann nicht gesichert werden

Diese Fehler weisen darauf hin, dass das Verzeichnis **System Volume Information** nicht gesichert wurde. Dies ist ein verdecktes Systemverzeichnis, auf das nur mit dem Windows-Systemaccount zugegriffen werden kann. Wird diese Nachricht ignoriert, werden das Verzeichnis und sein Inhalt nicht gesichert. (Es enthält temporäre Protokolldateien, die bei der Verschlüsselung von Dateien verwendet werden.) Sie können dem Benutzer, der den Befehl SAV für dieses Verzeichnis ausführt, auch weitere Berechtigungen erteilen. Zur Erteilung der Berechtigungen müssen Sie das Verzeichnis sichtbar machen. (Verdecken Sie keine Dateien, die schon verdeckt sind, und verdecken Sie keine geschützten Betriebssystemdateien.) Im Hilfetext von Windows 2000 Server oder Windows Server 2003 finden Sie weitere Informationen zum Konfigurieren von Ordnerberechtigungen.

Sie sehen evtl. auch die Fehlermeldung CPFA09C, wenn Sie eine Dateisicherung als QSECOFR durchführen, unabhängig davon, ob QSECOFR auf dem Server registriert ist oder nicht. Verwenden Sie ein anderes registriertes Benutzerprofil, das über eine Sicherungsberechtigung auf dem integrierten Server verfügt.

Nicht lesbare Nachrichten in der Servernachrichtenwarteschlange

Nachrichten im Windows-Ereignisprotokoll werden nicht korrekt angezeigt, wenn die CCSID (ID des codierten Zeichensatzes) der Nachrichtenwarteschlange auf *HEX (65535) gesetzt ist. Befinden sich in der Servernachrichtenwarteschlange (angegeben durch den Parameter MSGQ der NWSID) nicht lesbare Nachrichten, gehen Sie folgendermaßen vor:

1. Geben Sie an der i5/OS-Konsole den Befehl CHGMSGQ ein, um die CCSID der Servernachrichtenwarteschlange in einen anderen Wert als *HEX (65535) zu ändern, z. B. *MSG.
 Beispiel: Lautet der Name der Nachrichtenwarteschlange MYSVRQ in der Bibliothek MYLIB, dann können Sie mit dem folgenden Befehl unter i5/OS die CCSID der Nachrichtenwarteschlange ändern: CHGMSGQ MSGQ(MYLIB/MYSVRQ) CCSID(*MSG)

2. Wenn das Problem weiterhin besteht, überprüfen Sie die Datenbank mit technischen Informationen auf der Webseite  **server** IBM iSeries Support  . Wird dort keine Lösung angeboten, wenden Sie sich an die technische Unterstützung.

Fehler beim Erstellen eines Windows-Systemspeicherauszugs



Der integrierte Windows-Server ist so konfiguriert, dass bei Auftreten eines STOP-Fehlers oder Blue-Screen-Fehlers automatisch ein Systemspeicherauszug erstellt wird, wenn auf dem Systemlaufwerk ausreichend freier Speicherplatz vorhanden ist. Wird kein Systemspeicherauszug erstellt, gehen Sie folgendermaßen vor:

1. Wählen Sie **Start, Programme und Verwaltung**.
2. Klicken Sie auf **Computerverwaltung**.
3. Klicken Sie im **Vorgangsmenü** auf **Eigenschaften**.
4. Wählen Sie die Indexzunge **Erweitert** aus.
5. Klicken Sie auf die Schaltfläche **Starten und Wiederherstellen**.
6. Aktivieren Sie das Markierungsfeld **Debuginformationen speichern in**. Der Standardpfad der Datei "memory.dmp", die beim Auftreten eines Blue-Screen-Fehlers erstellt wird, lautet %SystemRoot%. Unter Windows 2000 Server handelt es sich dabei um das Verzeichnis C:\WINNT und bei Windows Server 2003 um das Verzeichnis C:\WINDOWS.

Andere Fehler, die dazu führen, dass kein Systemspeicherauszug erstellt wird:

- Für die Auslagerungsdatei ist eine unzureichende Größe angegeben. Die aktuelle Größe der Auslagerungsdatei muss so gewählt werden, dass sie den gesamten physischen RAM aufnehmen kann, zuzüglich 12 MB. So können Sie die Größe des physischen RAM auf der Maschine prüfen:
 1. Wählen Sie **Start, Einstellungen und Systemsteuerung** aus.
 2. Doppelklicken Sie auf **System**. Der auf dem System vorhandene physische RAM ist auf der Seite **Allgemein** unter **Computer** angegeben.

So können Sie die Größe der Auslagerungsdatei prüfen oder ändern:

1. Wählen Sie die Indexzunge **Erweitert** aus, und klicken Sie im Abschnitt **Virtueller Arbeitsspeicher** auf die Schaltfläche **Systemleistungsoptionen**. Im Fenster wird unter **Virtueller Arbeitsspeicher** die Größe der Auslagerungsdatei angezeigt.
 2. Muss die Größe der Auslagerungsdatei geändert werden, klicken Sie auf die Schaltfläche **Ändern**.
- Die Auslagerungsdatei befindet sich nicht auf dem Systemlaufwerk. Ein Systemspeicherauszug wird nur erstellt, wenn sich die Auslagerungsdatei auf dem Systemlaufwerk befindet. Das Systemlaufwerk ist das Laufwerk C:. So können Sie diese Einstellung prüfen oder ändern:
 1. Wählen Sie die Indexzunge **Erweitert** aus und klicken Sie im Abschnitt **Virtueller Arbeitsspeicher** auf die Schaltfläche **Systemleistungsoptionen**.
 - Auf dem als Pfad für die Datei memory.dmp angegebenen Laufwerk ist nicht genügend freier Speicherplatz verfügbar. Der Standardpfad für die Datei memory.dmp ist das Systemlaufwerk, Sie können den Pfad aber in ein anderes Laufwerk ändern. Prüfen Sie, ob auf dem Systemlaufwerk oder dem Alternativlaufwerk genügend freier Speicherplatz verfügbar ist. Der erforderliche freie Speicherplatz muss der Größe des physischen RAM zuzüglich 12 MB entsprechen.
 - Wenn das Problem weiterhin besteht, überprüfen Sie die Datenbank mit technischen Informationen auf der Webseite  **server** IBM iSeries Support  . Wird dort keine Lösung angeboten, wenden Sie sich an die technische Unterstützung.

Integrierten Windows-Server erneut installieren

Wenn auf einem integrierten Windows-Server Fehler auftreten, können Sie den Verlust von Anwendungen und Benutzerdaten unter Umständen verhindern, indem Sie den integrierten Windows-Server erneut installieren. Versuchen Sie, sich anzumelden oder mit DOS zu starten, indem Sie das Boot-Menü des NT-Ladeprogramms (NTLDR) benutzen. Dies ist nur unter FAT möglich. Anschließend können Sie den Windows-Server neu installieren. Dadurch wird das System auf den ursprünglich installierten Basiscode des Windows-Servers zurückgesetzt. Anschließend müssen Sie alle Service-Packs von Microsoft anwenden, die Sie zuvor installiert hatten. Wiederholen Sie außerdem die Installation des neuesten Service Packs von IBM iSeries Integrated Server Support.

So führen Sie die Neuinstallation des Windows-Servers aus:

1. Stoppen Sie den integrierten Server. Weitere Informationen hierzu finden Sie in „Integrierten Server starten und stoppen“ auf Seite 157.
2. Wählen Sie im Boot-Menü aus, ob PC-DOS oder der Windows-Server gestartet wird, abhängig davon, welche Aktion ausgeführt werden kann.
3. Wenn Sie den Windows-Server ausgewählt haben, öffnen Sie ein MS-DOS-Fenster.
4.
 - Geben Sie für Windows 2000 ein `winnt /s:D:\i386 /u:D:\unattend.txt` ein.
 - Geben Sie für Windows Server 2003 ein `winnt /b /t:C: /s:D:\i386 /u:D:\unattend.txt` ein.
5. Geben Sie im DOS-Fenster Folgendes ein:

```
D:
cd \i386
winnt /s:D:\i386 /u:D:\unattend.txt
```
6. Drücken Sie die Eingabetaste.

Anmerkung:

Die Netzwerklaufwerke sind unter Umständen so stark beschädigt, dass Sie sich nicht am integrierten Windows-Server anmelden oder mit DOS starten können. Versuchen Sie in einem solchen Fall, alle vordefinierten und benutzerdefinierten Speicherbereiche aus verwendbaren Sicherungen zurückzuspeichern. Entsprechende Anweisungen finden Sie unter „Vordefinierte Plattenlaufwerke für integrierte Windows-Server sichern“ auf Seite 201 und „Benutzerdefinierte Plattenlaufwerke für einen integrierten Windows-Server sichern“ auf Seite 202.

Windows 2000 Server und Windows Server 2003 verfügen über die Windows-Wiederherstellungskonsole. Hierbei handelt es sich um eine Befehlszeilenkonsole, die begrenzten Zugriff auf das System zulässt, damit Aufgaben zur Verwaltung oder Reparatur des Systems ausgeführt werden können. Zusätzliche Informationen finden Sie in der Dokumentation von Windows 2000 Server oder Windows Server 2003.

Möglicherweise müssen Sie die erneute Installation auch komplett neu durchführen, indem Sie die Prozedur unter „Installation über die i5/OS-Konsole starten“ auf Seite 100 ausführen.

Service­daten des integrierten Windows-Servers erfassen

Wenn Sie Service­daten für die Benutzerunterstützung bereitstellen müssen, sehen Sie zuerst in den i5/OS-Protokollen (siehe „Nachrichten und Jobprotokolle prüfen“ auf Seite 219) sowie im Windows-Ereignisprotokoll nach. Sie können auch eine Kopie der Windows-Ereignisprotokolle unter i5/OS erstellen (siehe „Nachrichtenprotokollierung“ auf Seite 161) und Windows-Speicherauszüge für die ferne Fehlerbehebung erstellen. Die folgenden Themen unterstützen Sie bei der Erstellung von Hauptspeicheraus­zügen, um weitere Diagnoseinformationen zu erfassen:

1. „Hauptspeicheraus­zug für einen integrierten Windows-Server unter i5/OS erstellen“ auf Seite 258.
2. Unter „NWSD-Speicheraus­zugstool unter i5/OS verwenden“ auf Seite 258 ist beschrieben, an welchen Stellen des Hauptspeicheraus­zugs die Konfigurations- und Protokolldateien angegeben sind, die Sie zuerst zur Fehleranalyse heranziehen sollten.

Hauptspeicherauszug für einen integrierten Windows-Server unter i5/OS erstellen

Sie können eine Windows-Hauptspeicherauszugsdatei unter i5/OS erstellen, die Ihnen bei der Behebung von Fehlern auf dem integrierten Server hilft. Wenn Sie den Windows-Server auf der iSeries installieren, wird der Speicherauszug standardmäßig in das Systemlaufwerk gestellt:

- %SystemRoot%\Memory.Dmp (Windows Server 2003)
- %SystemRoot%\Memory.Dmp (Windows 2000 Server)

Anmerkung:

Wenn Sie unter Windows einen vollständigen Hauptspeicherauszug fehlerfrei erstellen möchten, muss sich die Auslagerungsdatei auf dem Systemlaufwerk befinden und mindestens dieselbe Größe wie der Hauptspeicher plus 12 Megabyte aufweisen. Der Hauptspeichereinhalte wird bei der Erstellung des Speicherauszugs in die Auslagerungsdatei geschrieben. Dies stellt den ersten Schritt im Hauptspeicherauszugsprozess dar. Im zweiten Schritt werden die Daten von der Auslagerungsdatei in die tatsächliche Speicherauszugsdatei geschrieben. Dieser Schritt findet beim Booten des Systems nach dem Speicherauszug statt. Die Kapazität an freiem Speicherplatz auf dem Laufwerk, das die Hauptspeicherauszugsdatei (memory.dmp ist der Standardwert) enthält, muss mindestens der des installierten Hauptspeichers entsprechen.

Der Hauptspeicherauszug ist standardmäßig aktiviert, wenn das Systemlaufwerk über genügend Platz für die Auslagerungsdatei verfügt. So können Sie überprüfen, ob die Unterstützung für den Hauptspeicherauszug aktiviert ist oder ob die Datei memory.dmp auf ein anderes Laufwerk geschrieben werden kann:

1. Klicken Sie auf **Start, Einstellungen und Systemsteuerung**.
2. Öffnen Sie die Anwendung **System**.
 - Klicken Sie auf die Indexzunge **Erweitert** und dann auf die Schaltfläche **Starten und Wiederherstellung**.
3. Klicken Sie auf das Markierungsfeld **Debug-Informationen speichern in**.
4. Ändern Sie gegebenenfalls die Pfadangabe der Speicherauszugsdatei.
5. Wenn das System die Datei jedes Mal überschreiben soll, wenn ein Kernel-STOP-Fehler auftritt, klicken Sie auf das Markierungsfeld **Vorhandene Dateien überschreiben**.
6. Wählen Sie anhand der Größe der Auslagerungsdatei und des auf dem Systemlaufwerk verfügbaren freien Speicherbereichs die gewünschte Art des Hauptspeicherauszugs aus (kompakter Hauptspeicherauszug, Kernel-Hauptspeicherauszug oder vollständiger Hauptspeicherauszug).
7. Klicken Sie auf **OK**.

NWSD-Speicherauszugstool unter i5/OS verwenden

Mit dem NWSD-Speicherauszugstool (QFPDMPLS) können Sie Speicherauszüge der verschiedenen Konfigurations- und Protokolldateien erstellen, die mit dem integrierten Windows-Server verwendet werden. Hierzu benötigen Sie die Sonderberechtigung *ALLOBJ.

Führen Sie dazu folgende Schritte aus:

1. Hängen Sie die NWSD ab (siehe „Integrierten Server starten und stoppen“ auf Seite 157).
2. Geben Sie in der i5/OS-Befehlszeile Folgendes ein:

```
CALL QFPDMPLS PARM(nwsdname)
```

(Hierbei ist "nwsdname" der Name der NWS-Beschreibung.)

Das Programm erstellt die Datenbankdatei QGPL/QFPNWSDMP mit mehreren Teildateien. Der Name einer Datenbankteildatei besteht aus dem Namen der NWSD gefolgt von zwei Ziffern (01-99). Beispiel: Bei einer NWSD namens MYSERVER lautet der Name der ersten Teildatei MYSERVER01.

3. Rufen Sie die Teildatei auf, um den Inhalt der verschiedenen Dateien anzuzeigen, die Ihrer Serverbeschreibung zugeordnet sind. Unterschiedliche Dateien sind für die Fehleranalyse wichtig, abhängig von dem Installationsschritt, der das Problem verursacht.
4. Anhand der folgenden Tabelle können Sie die Bedeutung einer Datei für die verschiedenen Installationsschritte erkennen. Ist eine Datei mit einer 1 markiert, beachten Sie diese Datei bei der Fehleranalyse zuerst, dann die mit 2 und anschließend die mit 3 markierte Datei. Dateien, die nicht markiert sind, haben für die Installation keine Bedeutung, sie können jedoch später von Bedeutung sein. Einige Teildateien werden erst in der Phase nach der Installation erstellt.

Anmerkung:

Sie können Dateien auf dem Systemlaufwerk nicht mit QFPDMPLS abrufen, wenn das Laufwerk in NTFS konvertiert wird.

Möglicherweise sind nicht alle nachfolgend aufgelisteten Dateien auf Ihrem Server vorhanden. Wenn eine bestimmte Datei nicht gefunden wird, wird diese nicht über die API QFPDMPLS abgerufen, und die zugehörige Datenbankteildatei wird nicht erstellt.

NWSD-Konfigurations- und Protokolldateien

Teildateiname	Datentyp	Dateiname	Windows-Verzeichnis	Installation	Nach der Installation
nwsdname01	Txt	CONFIG.SYS	C:\	3	3
nwsdname02	Txt	AUTOEXEC.BAT	C:\	2	2
nwsdname03	Txt	BOOT.INI	C:\		
nwsdname04	Txt	HOSTS	C:\ oder D:\		3
nwsdname05	Txt	QVNI.CFG	C:\ oder D:\		
nwsdname06	Txt	QVNACFG.TXT	C:\ oder D:\		
nwsdname07	Txt	QVNADAEM.LOG	C:\ oder D:\		
nwsdname08	Txt	DUMPFIL.C01	C:\		
nwsdname09	Bin	DUMPFIL.C01	C:\		
nwsdname10	Txt	DUMPFIL.C02	C:\		
nwsdname11	Bin	DUMPFIL.C02	C:\		
nwsdname12	Txt	UNATTEND.TXT	D:\	1	
nwsdname13	Txt	INSWNTSV.LNG	D:\	2	
nwsdname14	Txt	INSWNTSV.VER	D:\	2	
nwsdname15	Txt	QVNADAEM.LOG	D:\		
nwsdname16	Txt	QVNARCMD.LOG	D:\		
nwsdname17	Txt	QVNDT400.LOG	D:\		
nwsdname18	Txt	QVNDVSTP.LOG	D:\		
nwsdname19	Txt	QVNDVSCD.LOG	D:\		
nwsdname20	Txt	QVNDVSDD.LOG	D:\		
nwsdname21	Txt	EVENTSYS.TXT	D:\		
nwsdname22	Txt	EVENTSEC.TXT	D:\		
nwsdname23	Txt	EVENTAPP.TXT	D:\		
nwsdname24	Txt	PERFDATA.TSV	D:\		
nwsdname25	Txt	REGSERV.TXT	D:\		
nwsdname26	Txt	REGIBM.TXT	D:\		
nwsdname27	Txt	REGIBMCO.TXT	D:\		
nwsdname28	Txt	DUMPFIL.D01	D:\		
nwsdname29	Bin	DUMPFIL.D01	D:\		
nwsdname30	Txt	DUMPFIL.D02	D:\		
nwsdname31	Bin	DUMPFIL.D02	D:\		
nwsdname32	Txt	HOSTS	%SystemRoot%\SYSTEM32\DRIVERS\ETC		3
nwsdname33	Txt	LMHOSTS	%SystemRoot%\SYSTEM32\DRIVERS\ETC		3
nwsdname34	Bin	MEMORY.DMP	C:\WINNT		

Teildateiname	Datentyp	Dateiname	Windows-Verzeichnis	Installation	Nach der Installation
nwsdname35	Txt	VRMFLOG.TXT	E:\PROGRA~1\IBM\AS400NT\SERVICE\VRM		
nwsdname36	Txt	PTFLOG.TXT	E:\PROGRA~1\IBM\AS400NT\SERVICE\PTF		
nwsdname37	Txt	PTFUNIN.TXT	E:\PROGRA~1\IBM\AS400NT\SERVICE\PTF		
nwsdname38	Txt	A4EXCEPT.LOG	D:\		
nwsdname39	Txt	DUMPPFILE.E01	E:\		
nwsdname40	Bin	DUMPPFILE.E01	E:\		
nwsdname41	Txt	DUMPPFILE.E02	E:\		
nwsdname42	Bin	DUMPPFILE.E02	E:\		
nwsdname43	Txt	CMDLINES.TXT	D:\I386\%OEM\$	2	
nwsdname44	Txt	QVNABKUP.LOG	D:\AS400NT		
nwsdname45	Txt	QVNADAEM.LOG	D:\AS400NT		
nwsdname46	Txt	QCONVGRP.LOG	D:\AS400NT		
nwsdname47	Txt	SETUPACT.LOG	C:\WINNT	1	
nwsdname48	Txt	SETUPAPILOG	C:\WINNT	1	
nwsdname49	Txt	SETUPERR.LOG	C:\WINNT	1	
nwsdname50	Txt	SETUPLOG.TXT	C:\WINNT	1	
nwsdname51	Txt	VRMFLOG.TXT	D:\AS400NT		
nwsdname52	Txt	PTFLOG.TXT	D:\AS400NT		
nwsdname53	Txt	PTFUNIN.TXT	D:\AS400NT		
nwsdname54	Txt	VRMLOG.TXT	%SystemRoot%\AS400WSV\SERVICE\VRM		
nwsdname55	Txt	PTFLOG.TXT	%SystemRoot%\AS400WSV\SERVICE\SERVPACK		
nwsdname56	Txt	PTFUNIN.TXT	%SystemRoot%\AS400WSV\SERVICE\SERVPACK		
nwsdname57	Txt	QVNDVEU.LOG	D:\AS400NT		
nwsdname58	Txt	SERVICE.LOG	D:\AS400NT		
nwsdname59	Txt	LVDELOEM.LOG	D:\AS400NT		
nwsdname60	Txt	INVOKINF.LOG	D:\AS400NT		
nwsdname61	Txt	LVMMASTER.LOG	D:\AS400NT		
nwsdname62	Txt	QITDINST.LOG	D:\AS400NT		
nwsdname63	Txt	QVNDVIMR.LOG	D:\AS400NT		
nwsdname64	Txt	QVNDVIMC.LOG	D:\AS400NT		
nwsdname65	Txt	QVNSDMR.LOG	D:\AS400NT		
nwsdname66	Txt	QVNSDMC.LOG	D:\AS400NT		
nwsdname67	Txt	QVNILMGR.LOG	D:\AS400NT		

Kapitel 15. Konfigurationsdateien für NWS-Beschreibung (NWSD)

Hier wird erläutert, wie Sie Ihre integrierten Windows-Server durch die Erstellung von eigenen Konfigurationsdateien anpassen können. So könnten Sie beispielsweise die Bildschirmauflösung ändern oder die Installation des IPX-Protokolls unterdrücken. Gehen Sie dazu folgendermaßen vor:

1. Erstellen Sie eine NWSD-Konfigurationsdatei. Weitere Informationen finden Sie unter „NWS-Beschreibungen“ auf Seite 73.
2. Geben Sie diese Datei mit Hilfe des Parameters Konfigurationsdatei beim Installieren eines Servers an, oder erstellen oder ändern Sie eine NWS-Beschreibung.

Bei jedem Start des Netzwerkserver verwendet i5/OS die Konfigurationsdatei, um die angegebene Datei des integrierten Servers auf Laufwerk C oder D des Servers zu ändern.

Wenn der Befehl INSWNTSVR (Windows-Server installieren) den integrierten Netzwerkserver aktiviert, generiert er eine Windows-Setup-Script-Datei für die nichtüberwachte Installation (UNATTEND.TXT). Durch Angabe der Konfigurationsdatei im Befehl INSWNTSVR kann diese Datei während der Installation benutzt werden, um die Datei UNATTEND.TXT zu ändern.

Achtung: Bei Änderungen der Konfigurationsdateien muss besonders sorgfältig gearbeitet werden. Es dürfen beispielsweise keine Einheitentreiber aus der Datei UNATTEND.TXT entfernt werden. Auch der OEM-Abschnitt bzw. der Abschnitt zur Installation von TCP darf nicht geändert werden. Änderungen dieser Abschnitte könnten dazu führen, dass der Server möglicherweise nicht mehr gestartet werden kann. Wenn Sie eine Konfigurationsdatei zum Ändern eines installierten Servers erstellen, sollten Sie immer zuerst eine Sicherungskopie von allen Dateien erstellen, die geändert werden sollen.

- Mit Hilfe des Befehls WRKNWSSTG (Mit NWS-Speicherbereichen arbeiten) können Sie abfragen, wie das Systemlaufwerk formatiert ist.
- Bevor eine Konfigurationsdatei erstellt wird, lesen Sie die Informationen unter „Format der NWSD-Konfigurationsdatei“. In diesem Abschnitt wird erklärt, wie die einzelnen Eintragsarten verwendet werden.
- Außerdem sollten Sie die Informationen im Abschnitt „Substitutionsvariablen für Schlüsselwortwerte verwenden“ auf Seite 274 lesen, um herauszufinden, welche Variablen verfügbar sind und wie Sie eine eigene Liste erstellen können.
- Unter Umständen empfiehlt sich in diesem Zusammenhang auch die Lektüre des Abschnitts „Beispiel: NWSD-Konfigurationsdatei“ auf Seite 263.
- Danach können Sie eine eigene Konfigurationsdatei erstellen (siehe hierzu „NWSD-Konfigurationsdatei erstellen“ auf Seite 262).

Treten nach dem Erstellen einer Konfigurationsdatei Fehler beim Starten des Servers auf, lesen Sie den Abschnitt „Fehler in der NWSD-Konfigurationsdatei“ auf Seite 231.

Format der NWSD-Konfigurationsdatei

Eine NWSD-Konfigurationsdatei besteht aus mehreren Vorkommen von **Eintragsarten**, die jeweils unterschiedliche Funktionen beinhalten. Die Eintragsarten sind:

„Zeilen aus einer bestehenden Datei eines integrierten Servers mit der Eintragsart CLEARCONFIG entfernen“ auf Seite 264

Verwenden Sie diese Eintragsart, wenn Sie alle Zeilen aus der Datei des integrierten Servers entfernen möchten.

„Datei eines integrierten Servers mit Eintragsart ADDCONFIG ändern“ auf Seite 264

Verwenden Sie diese Eintragsart, um Zeilen in der Datei des integrierten Servers hinzuzufügen, zu ersetzen oder zu entfernen.

„Datei des integrierten Windows-Servers mit Eintragsart UPDATECONFIG ändern“ auf Seite 270

Verwenden Sie diese Eintragsart, um Zeichenfolgen in Zeilen der Datei des integrierten Servers hinzuzufügen oder zu entfernen.

„Konfigurationsstandardwerte mit der Eintragsart SETDEFAULTS festlegen“ auf Seite 271

Verwenden Sie diese Eintragsart, um Standardwerte für bestimmte Schlüsselwörter einzurichten. In i5/OS werden Standardwerte nur bei der Verarbeitung von ADDCONFIG- und UPDATECONFIG-Einträgen in der aktuellen Teildatei verwendet.

Das Vorkommen einer Eintragsart wird als **Eintrag** bezeichnet. Jeder Eintrag enthält eine Reihe von Schlüsselwörtern, auf die ein Gleichheitszeichen (=) und Werte für die Schlüsselwörter folgen.

Formatrichtlinien

- Die Satzlänge der physischen Quellendatei muss 92 Byte betragen.
- Eine Zeile kann nur einen Eintrag enthalten, aber ein Eintrag kann sich über mehrere Zeilen erstrecken.
- Zwischen Eintragsart und Schlüsselwort, vor und nach dem Gleichheitszeichen und nach den Kommas kann ein Leerzeichen gesetzt werden.
- Sie können Leerzeilen zwischen Einträgen und zwischen Schlüsselwörtern setzen.

Schlüsselwörter

- Sie können Eintragungsschlüsselwörter in beliebiger Reihenfolge anordnen.
- Setzen Sie nach jedem Schlüsselwortwert ein Komma, außer nach dem letzten im Eintrag.
- Schließen Sie die Schlüsselwortwerte in einfache Anführungszeichen ein, wenn diese Kommas, Leerstellen, Sterne, Gleichheitszeichen oder einfache Anführungszeichen enthalten.
- Wenn Sie Schlüsselwörter verwenden, die einfache Anführungszeichen enthalten, verwenden Sie als Anführungszeichen innerhalb des Werts zwei einfache Anführungszeichen.
- Zeichenfolgen für Schlüsselwortwerte dürfen maximal 1024 Zeichen lang sein.
- Schlüsselwortwerte können sich zwar über mehrere Zeilen erstrecken, aber der betreffende Wert muss in einfache Anführungszeichen eingeschlossen werden. Der Wert umfasst führende und folgende Leerzeichen in jeder Zeile.

Kommentare

- Beginnen Sie einen Kommentar mit einem Stern (*).
- Sie können einen Kommentar in eine separate Zeile stellen oder in eine Zeile mit anderem Text, der nicht zum Kommentar gehört.

NWSD-Konfigurationsdatei erstellen

Bevor Sie eine Konfigurationsdatei erstellen, lesen Sie die Informationen unter „Format der NWSD-Konfigurationsdatei“ auf Seite 261 und „Substitutionsvariablen für Schlüsselwortwerte verwenden“ auf Seite 274. Unter Umständen empfiehlt sich in diesem Zusammenhang auch die Lektüre des Abschnitts „Beispiel: NWSD-Konfigurationsdatei“ auf Seite 263.

So erstellen Sie eine NWSD-Konfigurationsdatei:

1. Erstellen Sie eine physische Quellendatei.
 - a. Geben Sie in der i5/OS-Befehlszeile CRTSRCPF ein, und drücken Sie F4.
 - b. Geben Sie einen Namen für die Datei an, einen beliebigen beschreibenden Text sowie einen Teildateinamen und drücken Sie die Eingabetaste, um die Datei zu erstellen.

2. Verwenden Sie einen verfügbaren Editor, um der Datei syntaktisch korrekte Einträge hinzuzufügen, die der NWS-Beschreibung entsprechen. Weitere Informationen finden Sie unter „Format der NWS-D-Konfigurationsdatei“ auf Seite 261. So können Sie beispielsweise den Befehl WRKMBRPDM (Mit Teildateien arbeiten (mit PDM)) verwenden:
 - a. Geben Sie in der i5/OS-Befehlszeile WRKMBRPDM file(*Dateiname*) mbr(*Teildateiname*) ein und drücken Sie die Eingabetaste.
 - b. Geben Sie eine 2 neben der Datei ein, die editiert werden soll.

Beispiel: NWS-D-Konfigurationsdatei

Diese Beispielkonfigurationsdatei führt folgende Funktionen aus:

- Sie legt den Standarddateipfad fest.
- Sie löscht die Zeitzone und verwendet eine Konfigurationsvariable, um sie wieder hinzuzufügen.
- Sie legt die Standardsuchwerte fest, die bewirken, dass Anzeigekonfigurationszeilen vor dem Abschnitt mit Benutzerdaten hinzugefügt werden.
- Sie fügt Zeilen hinzu, die die Anzeige konfigurieren.

```

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

```

Zeilen aus einer bestehenden Datei eines integrierten Servers mit der Eintragsart CLEARCONFIG entfernen

Mit der Eintragsart CLEARCONFIG können Sie alle Zeilen aus der vorhandenen Datei eines integrierten Servers entfernen.

Achtung: Nach dem Entfernen aller Zeilen aus der Datei des integrierten Servers können Sie den Netzwerkserver möglicherweise nicht mehr anhängen. Bei Problemen können Sie im Abschnitt „Fehler in der NWSD-Konfigurationsdatei“ auf Seite 231 nachlesen.

Erstellen Sie zum Löschen der Datei eines integrierten Servers eine NWSD-Konfigurationsdatei, die die Eintragsart CLEARCONFIG wie folgt enthält:

```
CLEARCONFIG
LINECOMMENT      = '<"REM "|<Anmerkung>>',          (optional)
TARGETDIR        = '<BOOT|Pfad>',                  (optional)
TARGETFILE       = '<Dateiname>'                  (erforderlich)
```

Unter den folgenden Schlüsselwortlinks erhalten Sie eine detaillierte Erläuterung der CLEARCONFIG-Schlüsselwörter. Sie können auch wieder zum Abschnitt „Format der NWSD-Konfigurationsdatei“ auf Seite 261 zurückkehren oder mit dem Abschnitt „Datei eines integrierten Servers mit Eintragsart ADDCONFIG ändern“ fortfahren.

- „Schlüsselwort LINECOMMENT“ auf Seite 267
- „Schlüsselwort TARGETDIR“
- „Schlüsselwort TARGETFILE“

Schlüsselwort TARGETDIR

Verwenden Sie das Schlüsselwort TARGETDIR, um den Pfad für die Datei des integrierten Servers anzugeben, deren Inhalt gelöscht werden soll.

Anmerkung:

Bei Änderung einer Datei verwendet i5/OS nur das erste Verzeichnis für die Datei. OS/400 ignoriert alle weiteren Einträge, die ein anderes Zielverzeichnis angeben.

Schlüsselwort TARGETFILE

Verwenden Sie das Schlüsselwort TARGETFILE, um die Datei des integrierten Servers anzugeben, deren Inhalt gelöscht werden soll.

Datei eines integrierten Servers mit Eintragsart ADDCONFIG ändern

Mit der Eintragsart ADDCONFIG können Sie die Datei eines integrierten Windows-Servers ändern, indem Sie

- eine Zeile am Dateianfang oder -ende hinzufügen.
- eine neue Zeile vor oder nach einer Zeile hinzufügen, die eine spezifische Zeichenfolge enthält.
- eine Zeile in einer Datei löschen.
- das erste, letzte oder alle Vorkommen einer Zeile in der Datei ersetzen.
- angeben, in welches Verzeichnis die Datei gestellt werden soll.

Erstellen Sie zum Ändern der Datei eines integrierten Servers eine NWSD-Konfigurationsdatei, die die Eintragsart ADDCONFIG wie folgt enthält:

```
ADDCONFIG
VAR           = '<Variablenname>',           (bedingt erforderlich)
ADDSTR        = '<Zu verarbeitende Zeile>',   (optional)
ADDWHEN       = '<ALWAYS|NEVER|<Ausdruck>>', (optional)
DELETEWHEN   = '<NEVER|ALWAYS|<Ausdruck>>', (optional)
LINECOMMENT   = '<"REM " |<Anmerkung>>',     (optional)
LOCATION        = '<END|BEGIN>',              (optional)
FILESEARCHPOS = '<AFTER|BEFORE>',           (optional)
FILESEARCHSTR = '<Suchbegriff>',            (bedingt erforderlich)
FILESEARCHSTROCC = '<LAST|FIRST>',          (optional)
REPLACEOCC    = '<LAST|FIRST|ALL>',         (optional)
TARGETDIR     = '<BOOT|Pfad>',              (optional)
TARGETFILE    = '<CONFIG.SYS|<Dateiname>>', (optional)
UNIQUE        = '<NO|YES>'                  (optional)
```

Unter den folgenden Schlüsselwortlinks erhalten Sie eine detaillierte Erläuterung der ADDCONFIG-Schlüsselwörter. Sie können auch wieder zum Abschnitt „Format der NWSD-Konfigurationsdatei“ auf Seite 261 zurückkehren oder mit dem Abschnitt „Datei des integrierten Windows-Servers mit Eintragsart UPDATECONFIG ändern“ auf Seite 270 fortfahren.

- „Schlüsselwort VAR“
- „Schlüsselwort ADDSTR“
- „Schlüsselwort ADDWHEN“ auf Seite 266
- „Schlüsselwort DELETEWHEN“ auf Seite 267
- „Schlüsselwort LINECOMMENT“ auf Seite 267
- „Schlüsselwort LOCATION“ auf Seite 267
- „Schlüsselwort FILESEARCHPOS (Eintragsart ADDCONFIG)“ auf Seite 268
- „Schlüsselwort FILESEARCHSTR“ auf Seite 268
- „Schlüsselwort FILESEARCHSTROCC“ auf Seite 268
- „Schlüsselwort REPLACEOCC“ auf Seite 268
- „Schlüsselwort TARGETDIR“ auf Seite 269
- „Schlüsselwort TARGETFILE“ auf Seite 269
- „Schlüsselwort UNIQUE“ auf Seite 269

Schlüsselwort VAR

Das Schlüsselwort VAR gibt den Wert links vom Gleichheitszeichen an, der die Zeile identifiziert, die der Datei hinzugefügt oder aus ihr gelöscht werden soll. Beispiel:

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

Wenn REPLACEOCC nicht angegeben wird, benötigt i5/OS das Schlüsselwort.

Schlüsselwort ADDSTR

Verwenden Sie das Schlüsselwort ADDSTR zum Angeben der Zeichenfolge, die der Datei des integrierten Windows-Servers hinzugefügt werden soll. Beispiel:

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

Schlüsselwort ADDWHEN

Verwenden Sie das Schlüsselwort ADDWHEN, um anzugeben, wann i5/OS der Datei des integrierten Windows-Servers während der Verarbeitung eine neue Zeile oder Zeichenfolge hinzufügen soll.

Sie können Folgendes angeben:

- ALWAYS, wenn Sie möchten, dass i5/OS die Zeile oder Zeichenfolge bei jeder Verarbeitung der Konfigurationsdatei hinzufügt. (Der Standardwert ist ALWAYS, es sei denn, Sie haben einen anderen Standardwert durch Angabe des Eintrags SETDEFAULTS in der Teildatei definiert.)
- NEVER, wenn Sie möchten, dass i5/OS die Zeile oder Zeichenfolge nie hinzufügt.
- Einen Ausdruck, der i5/OS anweist, die Zeile oder Zeichenfolge hinzuzufügen, wenn die angegebene Bedingung wahr ist. Ausdrücke setzen sich aus Operatoren (siehe „Ausdrucksoperatoren ADDWHEN und DELETEWHEN“) zusammen und müssen entweder gleich TRUE oder FALSE sein.

Anmerkung:

Wenn Sie nicht möchten, dass i5/OS einen Ausdruck (wie beispielsweise einen Ausdruck, der einen Stern (*) enthält) als mathematische Operation interpretiert, setzen Sie den betreffenden Ausdruck in Anführungszeichen. Beispiel: Zum Hinzufügen einer Zeile, wenn die NWSD-Art *WINDOWSNT ist, müssten Sie Folgendes angeben:

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

Ausdrucksoperatoren ADDWHEN und DELETEWHEN

Sie können für Ausdrücke die folgenden Operatoren verwenden:

Operator	Beschreibung
==	Gibt TRUE zurück, wenn die Operanden gleichwertig sind, FALSE, wenn dies nicht der Fall ist.
!=	Gibt FALSE zurück, wenn die Operanden gleichwertig sind, TRUE, wenn dies nicht der Fall ist.
>	Gibt TRUE zurück, wenn der Operand auf der linken Seite größer als der Operand auf der rechten Seite ist, FALSE, wenn dies nicht der Fall ist. Wenn es sich bei den Operanden um Zeichenfolgen handelt, werden die ASCII-Werte verglichen.
<	Gibt TRUE zurück, wenn der Operand auf der linken Seite kleiner als der Operand auf der rechten Seite ist, FALSE, wenn dies nicht der Fall ist. Wenn es sich bei den Operanden um Zeichenfolgen handelt, werden die ASCII-Werte verglichen.
>=	Gibt TRUE zurück, wenn der Operand auf der linken Seite gleich oder größer als der Operand auf der rechten Seite ist, FALSE, wenn dies nicht der Fall ist. Wenn es sich bei den Operanden um Zeichenfolgen handelt, werden die ASCII-Werte verglichen.
<=	Gibt TRUE zurück, wenn der Operand auf der linken Seite gleich oder kleiner als der Operand auf der rechten Seite ist, FALSE, wenn dies nicht der Fall ist. Wenn es sich bei den Operanden um Zeichenfolgen handelt, werden die ASCII-Werte verglichen.
&&	Logisches AND. Gibt TRUE zurück, wenn beide Operanden einen Wert ungleich Null haben. Die Operanden müssen ganze Zahlen sein.
	Logisches OR. Gibt TRUE zurück, wenn einer der beiden Operanden einen Wert ungleich Null hat. Die Operanden müssen ganze Zahlen sein.
+	Wenn beide Operanden ganze Zahlen sind, ist das Ergebnis die Summe aus beiden ganzen Zahlen. Handelt es sich bei beiden Operanden um Zeichenfolgen, ist das Ergebnis eine Verkettung der beiden Zeichenfolgen.
-	Subtrahiert ganze Zahlen.
*	Multipliziert ganze Zahlen.
/	Dividiert ganze Zahlen.
()	Runde Klammern erzwingen eine Auswertungsreihenfolge.
!	Logisches NOT. Gibt TRUE zurück, wenn der Wert eines einzelnen Operanden 0 ist, FALSE, wenn dies nicht der Fall ist.
ALWAYS	Gibt immer TRUE zurück.

Operator	Beschreibung
NEVER	Gibt immer FALSE zurück.

Schlüsselwort DELETEWHEN

Verwenden Sie DELETEWHEN, um anzugeben, wann i5/OS während der Verarbeitung eine Zeile oder Zeichenfolge aus der Datei löschen soll. Sie können Folgendes angeben:

- ALWAYS, wenn Sie möchten, dass i5/OS die Zeile oder Zeichenfolge bei jeder Verarbeitung der Konfigurationsdatei löscht.
- NEVER, wenn Sie möchten, dass i5/OS die Zeile oder Zeichenfolge nie löscht. (Der Standardwert ist NEVER, es sei denn, Sie haben einen anderen Standardwert durch Angabe des Eintrags SETDEFAULTS in der Teildatei definiert.)
- Einen Ausdruck, der i5/OS anweist, die Zeile oder Zeichenfolge zu löschen, wenn die angegebene Bedingung wahr ist. Ausdrücke setzen sich aus Operatoren (siehe „Ausdrucksoperatoren ADDWHEN und DELETEWHEN“ auf Seite 266) zusammen und müssen entweder gleich TRUE oder FALSE sein.

Anmerkung:

Wenn Sie nicht möchten, dass i5/OS einen Ausdruck (wie beispielsweise einen Ausdruck, der einen Stern (*) enthält) als mathematische Operation interpretiert, setzen Sie den betreffenden Ausdruck in Anführungszeichen. Beispiel: Geben Sie zum Löschen einer Zeile, wenn die NWS-Datei *WINDOWSNT ist, Folgendes an:

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

Schlüsselwort LINECOMMENT

LINECOMMENT gibt die Präfixzeichenfolge zum Identifizieren von Kommentaren in einer Datei an. Verwenden Sie den Standardwert, wenn LINECOMMENT den Wert REM zur Identifizierung von Kommentaren verwenden soll. Sie können auch einen anderen Wert angeben. Um beispielsweise Kommentare mit Hilfe eines Semikolons zu identifizieren, verwenden Sie LINECOMMENT = ';' im **ersten** Eintrag, der auf diese Datei verweist. (i5/OS ignoriert das Schlüsselwort LINECOMMENT in allen anderen Einträgen.)

Schlüsselwort LOCATION

LOCATION gibt die Position innerhalb der Datei an, an der die neue Zeile hinzugefügt werden soll. Der Standardwert END weist i5/OS an, die Zeile am Ende der Datei hinzuzufügen. Wenn Sie möchten, dass i5/OS die Zeile am Anfang der Datei hinzufügt, geben Sie BEGIN an.

Schlüsselwort LINESEARCHPOS

Verwenden Sie LINESEARCHPOS, um anzugeben, ob die im Schlüsselwort ADDSTR mit dem Wert AFTER (dem Standardwert) angegebene Zeichenfolge nach oder vor dem Zeilensuchbegriff hinzugefügt werden soll.

Schlüsselwort LINESEARCHSTR

Gibt den Suchbegriff an, nach dem Zeilen durchsucht werden sollen.

Anmerkung:

Nur die Seite rechts vom Gleichheitszeichen wird nach dem mit LINESEARCHSTR angegebenen Wert durchsucht.

Schlüsselwort LINELOCATION

Verwenden Sie LINELOCATION, um anzugeben, an welcher Position die mit dem Schlüsselwortwert ADDSTR angegebene Zeichenfolge in der Zeile hinzugefügt werden soll.

Verwenden Sie den Standardwert END, wenn i5/OS die Zeichenfolge am Ende der Zeile hinzufügen soll. Wenn Sie möchten, dass i5/OS die Zeichenfolge am Anfang der Zeile hinzufügt, geben Sie BEGIN an.

Schlüsselwort FILESEARCHPOS (Eintragsart ADDCONFIG)

Geben Sie an, wo eine Zeile in Bezug auf den Dateisuchbegriff zu suchen ist. Sie können Folgendes angeben:

- AFTER, wenn Sie möchten, dass i5/OS die Zeile nach der Zeile hinzufügt, die den Dateisuchbegriff enthält. (Der Standardwert ist AFTER, es sei denn, Sie haben einen anderen Standardwert durch Angabe des Eintrags SETDEFAULTS in der Teildatei definiert.)
- BEFORE, wenn Sie möchten, dass i5/OS die Zeile vor der Zeile hinzufügt, die den Dateisuchbegriff enthält.

Schlüsselwort FILESEARCHSTR

Verwenden Sie FILESEARCHSTR mit dem Schlüsselwort REPLACEOCC, um die zu ersetzende Zeile anzugeben. Sie müssen die gesamte Zeile als Wert angeben.

Wenn Sie eine neue Zeile hinzufügen, kann FILESEARCHSTR ein beliebiger Teil einer zu suchenden Zeile sein.

Es gibt keinen Standardwert, es sei denn, Sie haben einen Standardwert durch Angabe des Eintrags SETDEFAULTS in der Teildatei definiert.

Schlüsselwort FILESEARCHSTROCC

Gibt an, bei welchem Vorkommen einer mehrmals in einer Datei vorkommenden Zeichenfolge die neue Zeile positioniert werden soll.

Der Standardwert LAST gibt das letzte Vorkommen des Suchbegriffs an. Wenn i5/OS das erste Vorkommen des Suchbegriffs verwenden soll, geben Sie FIRST an.

Schlüsselwort REPLACEOCC

Gibt an, welches Vorkommen einer Zeile ersetzt werden soll.

- Verwenden Sie LAST, wenn i5/OS das letzte Vorkommen von FILESEARCHSTR ersetzen soll.
- Verwenden Sie ALL, wenn i5/OS alle Vorkommen von FILESEARCHSTR ersetzen soll.
- Verwenden Sie FIRST, wenn i5/OS das erste Vorkommen von FILESEARCHSTR ersetzen soll.

Verwenden Sie FILESEARCHSTR, um die gesamte Zeile anzugeben, die ersetzt werden soll.

i5/OS löscht die Zeile, die der Angabe bei FILESEARCHSTR entspricht, und fügt die mit VAR angegebene Variable sowie die mit ADDSTR angegebene Zeichenfolge der Datei an dieser Position hinzu.

Anmerkung:

REPLACEOCC hat Vorrang vor LOCATION und FILESEARCHPOS. Kann i5/OS den Wert FILESEARCHSTR, der mit einem Schlüsselwort REPLACEOCC angegeben wurde, nicht finden, wird keine Zeile ersetzt, sondern eine neue Zeile auf der Basis des im Schlüsselwort LOCATION angegebenen Werts hinzugefügt.

Schlüsselwort TARGETDIR

Verwenden Sie TARGETDIR, um den Pfad für die zu ändernde Datei des integrierten Servers anzugeben.

Sofern Sie nicht zuerst den Standardwert mit dem Eintrag SETDEFAULTS ändern, müssen Sie den Pfad für die Datei UNATTEND.TXT oder Ihre eigene Datei des integrierten Servers angeben. (Standardmäßig wird das Schlüsselwort BOOT verwendet, das i5/OS anweist, die Datei im Stammverzeichnis von Laufwerk C zu ändern.)

Anmerkungen:

1. Die Unterstützung für NWSD-Konfigurationsdateien besteht nur für vordefinierte Plattenlaufwerke, die als FAT formatiert wurden. Auf Speicherbereiche, die in NTFS konvertiert wurden, haben Konfigurationsdateien keinen Zugriff. Weitere Informationen finden Sie unter „Vordefinierte Plattenlaufwerke für integrierte Windows-Server“ auf Seite 171.
2. Bei Änderung einer Datei verwendet i5/OS nur das erste Verzeichnis für die Datei. OS/400 ignoriert alle weiteren Einträge, die ein anderes Zielverzeichnis angeben.

Schlüsselwort TARGETFILE

Das Schlüsselwort TARGETFILE gibt die zu ändernde Datei des integrierten Servers an. Der Wert UNATTEND.TXT weist i5/OS an, die Setup-Script-Datei für eine unüberwachte Installation des integrierten Servers zu ändern.

Sofern Sie nicht zunächst den Standardwert mit dem Eintrag SETDEFAULTS ändern, müssen Sie den Pfad für die Datei UNATTEND.TXT oder Ihre eigene Datei des integrierten Servers angeben. (Der Standardwert für dieses Schlüsselwort ist CONFIG.SYS.)

Schlüsselwort UNIQUE

Geben Sie YES an, wenn Sie nur ein Vorkommen einer Zeile in der Datei zulassen möchten.

Der Standardwert NO gibt an, dass mehrere Vorkommen zulässig sind.

Schlüsselwort VAROCC

Verwenden Sie VAROCC, um anzugeben, welches Vorkommen der Variablen geändert werden soll.

Wenn das letzte Vorkommen der Variablen geändert werden soll, können Sie den Standardwert verwenden. Andernfalls geben Sie FIRST an, um das erste Vorkommen der Variablen zu ändern.

Schlüsselwort VARVALUE

Verwenden Sie VARVALUE, wenn Sie eine Zeile nur dann ändern möchten, wenn sie diesen speziellen Wert für die anzugebende Variable enthält.

Sie können die Zeichenfolge ganz oder teilweise auf der rechten Seite eines zu ändernden Ausdrucks angeben.

Datei des integrierten Windows-Servers mit Eintragsart UPDATECONFIG ändern

Mit der Eintragsart UPDATECONFIG können Sie eine Datei des integrierten Servers ändern, indem Sie

- Zeichenfolgen in Zeilen der Datei hinzufügen.
- neue Zeichenfolgen vor oder nach einer angegebenen Zeichenfolge hinzufügen.
- Zeichenfolgen aus Zeilen in der Datei löschen.
- angeben, in welchem Pfad die Datei gestellt werden soll.

Erstellen Sie zum Ändern der Datei eines integrierten Servers eine NWSD-Konfigurationsdatei, die die Eintragsart UPDATECONFIG wie folgt enthält:

```
UPDATECONFIG
VAR           = '<Variablenname>',           (erforderlich)
ADDSTR        = '<Zu verarbeitende Zeile>',   (erforderlich)
ADDWHEN       = '<ALWAYS|NEVER|<Ausdruck>>', (optional)
DELETEWHEN    = '<NEVER|ALWAYS|<Ausdruck>>', (optional)
LINECOMMENT   = '<"REM "|<Anmerkung>>',      (optional)
LINELOCATION    = '<END|BEGIN>',              (optional)
LINESEARCHPOS = '<AFTER|BEFORE>',           (optional)
LINESEARCHSTR = '<Zeichenfolge einer Zeile>', (optional)
FILESEARCHPOS = '<AFTER|BEFORE>',           (optional)
FILESEARCHSTR = '<Suchbegriff>',            (optional)
FILESEARCHSTROCC = '<LAST|FIRST>',          (optional)
TARGETDIR     = '<BOOT|<Pfad>>',            (optional)
TARGETFILE    = '<CONFIG.SYS|<Dateiname>>', (optional)
VAROCC        = '<LAST|FIRST>',            (optional)
VARVALUE      = '<Variablenwert>'          (optional)
```

Unter den folgenden Schlüsselwortlinks erhalten Sie eine detaillierte Erläuterung der UPDATECONFIG-Schlüsselwörter. Sie können auch wieder zum Abschnitt „Format der NWSD-Konfigurationsdatei“ auf Seite 261 zurückkehren oder mit dem Abschnitt „Konfigurationsstandardwerte mit der Eintragsart SETDEFAULTS festlegen“ auf Seite 271 fortfahren.

- „Schlüsselwort VAR“ auf Seite 265
- „Schlüsselwort ADDSTR“ auf Seite 265
- „Schlüsselwort ADDWHEN“ auf Seite 266
- „Schlüsselwort DELETEWHEN“ auf Seite 267
- „Schlüsselwort LINECOMMENT“ auf Seite 267
- „Schlüsselwort LINELOCATION“ auf Seite 267
- „Schlüsselwort LINESEARCHPOS“ auf Seite 267
- „Schlüsselwort LINESEARCHSTR“ auf Seite 267
- „Schlüsselwort FILESEARCHPOS (Eintragsart UPDATECONFIG)“ auf Seite 271
- „Schlüsselwort FILESEARCHSTR (Eintragsart UPDATECONFIG)“ auf Seite 271
- „Schlüsselwort FILESEARCHSTROCC (Eintragsart UPDATECONFIG)“ auf Seite 271
- „Schlüsselwort TARGETDIR“ auf Seite 269
- „Schlüsselwort TARGETFILE“ auf Seite 269
- „Schlüsselwort VAROCC“ auf Seite 269
- „Schlüsselwort VARVALUE“ auf Seite 269

Schlüsselwort FILESEARCHPOS (Eintragsart UPDATECONFIG)

Mit FILESEARCHPOS können Sie angeben, welches Vorkommen der Variable i5/OS in Bezug auf eine Zeile suchen soll, die den Suchbegriff enthält. Verwenden Sie den Wert

- AFTER, wenn Sie möchten, dass i5/OS das erste Vorkommen der Variablen in oder nach der Zeile sucht, die den Suchbegriff enthält. (Der Standardwert ist AFTER, es sei denn, Sie haben einen anderen Standardwert durch Angabe des Eintrags SETDEFAULTS in der Teildatei definiert.)
- BEFORE, wenn Sie möchten, dass i5/OS das erste Vorkommen der Variablen in oder vor der Zeile sucht, die den Suchbegriff enthält.

Anmerkung:

Wenn i5/OS den Suchbegriff nicht findet, wird die zu ändernde Zeile anhand des Schlüsselworts VAROCC festgelegt.

Schlüsselwort FILESEARCHSTR (Eintragsart UPDATECONFIG)

Mit dem Schlüsselwort FILESEARCHSTR können Sie einen Suchbegriff für i5/OS bereitstellen, der zum Suchen des Vorkommens einer zu ersetzenden Variablen benutzt werden soll.

Es gibt keinen Standardwert, es sei denn, Sie haben einen Standardwert durch Angabe des Eintrags SETDEFAULTS in der Teildatei definiert.

Schlüsselwort FILESEARCHSTROCC (Eintragsart UPDATECONFIG)

Verwenden Sie FILESEARCHSTROCC, um anzugeben, welches Vorkommen einer mehrmals in einer Datei vorhandenen Zeichenfolge nach den zu ändernden Zeilen durchsucht werden soll.

Verwenden Sie LAST, wenn i5/OS das letzte Vorkommen des Suchbegriffs verwenden soll. Wenn i5/OS das erste Vorkommen des Suchbegriffs verwenden soll, geben Sie FIRST an.

Konfigurationsstandardwerte mit der Eintragsart SETDEFAULTS festlegen

Sie können die Standardwerte für bestimmte Schlüsselwörter in den Eintragsarten ADDCONFIG und UPDATECONFIG mit Hilfe von SETDEFAULTS einstellen. Sie können Standardwerte für Folgendes festlegen:

- Zeilen hinzufügen und löschen
- Zeilen suchen
- Namen der zu ändernden Datei und des zu ändernden Pfades angeben

Zum Einstellen der Standardwerte erstellen Sie eine NWSD-Konfigurationsdatei, die die Eintragsart SETDEFAULTS wie folgt enthält:

```
SETDEFAULTS
ADDWHEN      = '<ALWAYS|NEVER|<Ausdruck>>',      (optional)
DELETEWHEN  = '<NEVER|ALWAYS|<Ausdruck>>',      (optional)
FILESEARCHPOS = '<AFTER|BEFORE>',                (optional)
FILESEARCHSTR = '<Suchbegriff>',                 (optional)
TARGETDIR   = '<Pfad>',                          (optional)
TARGETFILE   = '<Dateiname>'                     (optional)
```

Unter den folgenden Schlüsselwortlinks erhalten Sie eine detaillierte Erläuterung der SETDEFAULTS-Schlüsselwörter.

- „ADDWHEN“
- „DELETEWHEN“
- „Schlüsselwort FILESEARCHPOS (Eintragsart SETDEFAULTS)“ auf Seite 273
- „Schlüsselwort FILESEARCHSTR (Eintragsart SETDEFAULTS)“ auf Seite 273
- „TARGETDIR“ auf Seite 273
- „TARGETFILE“ auf Seite 273

ADDWHEN

Verwenden Sie ADDWHEN mit der Eintragsart SETDEFAULTS zum Einstellen des Standardwerts für das Schlüsselwort ADDWHEN in den Eintragsarten ADDCONFIG und UPDATECONFIG.

Geben Sie im Standardwert an, wann i5/OS der Datei während der Verarbeitung die neue Zeile oder Zeichenfolge hinzufügen soll. Sie können Folgendes angeben:

- ALWAYS, wenn Sie möchten, dass i5/OS die Zeile oder Zeichenfolge bei jeder Verarbeitung der Konfigurationsdatei hinzufügt. (Der Standardwert ist ALWAYS, es sei denn, Sie haben einen anderen Standardwert definiert.)
- NEVER, wenn Sie möchten, dass i5/OS die Zeile oder Zeichenfolge nie hinzufügt.
- Einen Ausdruck, der i5/OS anweist, die Zeile oder Zeichenfolge hinzuzufügen, wenn die angegebene Bedingung wahr ist. Ausdrücke setzen sich aus Operanden (siehe „Ausdrucksoperatoren ADDWHEN und DELETEWHEN“ auf Seite 266) zusammen und müssen entweder gleich TRUE oder FALSE sein.

Anmerkung:

Wenn Sie nicht möchten, dass i5/OS einen Ausdruck (wie beispielsweise einen Ausdruck, der einen Stern (*) enthält) als mathematische Operation interpretiert, setzen Sie den betreffenden Ausdruck in Anführungszeichen. Beispiel: Zum Hinzufügen einer Zeile, wenn die NWSD-Art *WINDOWSNT ist, müssten Sie Folgendes angeben:

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

DELETEWHEN

Verwenden Sie DELETEWHEN mit der Eintragsart SETDEFAULTS zum Einstellen des Standardwerts für das Schlüsselwort DELETEWHEN in den Eintragsarten ADDCONFIG und UPDATECONFIG.

Geben Sie an, wenn i5/OS während der Verarbeitung eine Zeile oder Zeichenfolge aus der Datei löschen soll.

Sie können Folgendes angeben:

- ALWAYS, wenn Sie möchten, dass i5/OS die Zeile oder Zeichenfolge bei jeder Verarbeitung der Konfigurationsdatei löscht.
- NEVER, wenn Sie möchten, dass i5/OS die Zeile oder Zeichenfolge nie löscht. (Der Standardwert ist NEVER, es sei denn, Sie haben einen anderen Standardwert definiert.)
- Einen Ausdruck, der i5/OS anweist, die Zeile oder Zeichenfolge zu löschen, wenn die angegebene Bedingung wahr ist. Ausdrücke setzen sich aus Operanden (siehe „Ausdrucksoperatoren ADDWHEN und DELETEWHEN“ auf Seite 266) zusammen und müssen entweder gleich TRUE oder FALSE sein.

Anmerkung:

Wenn Sie nicht möchten, dass i5/OS einen Ausdruck (wie beispielsweise einen Ausdruck, der einen Stern (*) enthält) als mathematische Operation interpretiert, setzen Sie den betreffenden Ausdruck in Anführungszeichen. Beispiel: Geben Sie zum Löschen einer Zeile, wenn die NWSD-Art *WINDOWSNT ist, Folgendes an:

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

Schlüsselwort FILESEARCHPOS (Eintragsart SETDEFAULTS)

Verwenden Sie FILESEARCHPOS mit der Eintragsart SETDEFAULTS zum Einstellen des Standardwerts für das Schlüsselwort FILESEARCHPOS in den Eintragsarten ADDCONFIG und UPDATECONFIG.

Geben Sie an, wo eine Zeile in Bezug auf den Dateisuchbegriff zu suchen ist. Sie können Folgendes angeben:

- AFTER, wenn Sie möchten, dass die Zeile nach der Zeile gesucht wird, die den Dateisuchbegriff enthält. (Der Standardwert ist AFTER, es sei denn, Sie haben einen anderen Standardwert definiert.)
- BEFORE, wenn Sie möchten, dass i5/OS die Zeile vor der Zeile hinzufügt, die den Dateisuchbegriff enthält.

Schlüsselwort FILESEARCHSTR (Eintragsart SETDEFAULTS)

Verwenden Sie FILESEARCHSTR mit der Eintragsart SETDEFAULTS zum Einstellen des Standardwerts für das Schlüsselwort FILESEARCHSTR in den Eintragsarten ADDCONFIG und UPDATECONFIG.

Der im Schlüsselwort FILESEARCHSTR angegebene Wert kann ein beliebiger Teil der zu suchenden Zeile sein.

TARGETDIR

Verwenden Sie TARGETDIR mit der Eintragsart SETDEFAULTS zum Festlegen des Standardwerts für das Schlüsselwort TARGETDIR in den Eintragsarten ADDCONFIG und UPDATECONFIG.

Das Verzeichnis, das die zu verarbeitende Datei enthält, wird in einem Pfad angegeben.

Beispiel: Zum Festlegen des TARGETDIR-Standardwerts für eine Datei auf Laufwerk D könnten Sie Folgendes angeben:

```
SETDEFAULTS TARGETDIR = 'D:\'
```

TARGETFILE

Verwenden Sie TARGETFILE mit der Eintragsart SETDEFAULTS zum Festlegen des Standardwerts für das Schlüsselwort TARGETFILE in den Eintragsarten ADDCONFIG und UPDATECONFIG.

Ein Name gibt die zu verarbeitende Datei an.

Beispiel: Zum Festlegen des TARGETFILE-Standardwerts für Datei UNATTEND.TXT auf Laufwerk D könnten Sie Folgendes angeben:

```
SETDEFAULTS  
  TARGETDIR = 'D:\',  
  TARGETFILE = 'UNATTEND.TXT'
```

Substitutionsvariablen für Schlüsselwortwerte verwenden

Für Schlüsselwortwerte können Substitutionsvariablen verwendet werden. Die NWSD-Konfigurationsdatei ersetzt die korrekten Werte für die Variablen. Die Substitutionsvariablen werden anhand der in der NWS-Beschreibung (NWSD) gespeicherten Werte oder der in der NWS-Beschreibung festgestellten Hardware konfiguriert.

i5/OS stellt die folgenden Variablen bereit:

Substitutionsvariable	Beschreibung
%FPAIPADDRPP%	TCP/IP-Adresse (NWSD-Port *VRTETHPTP) *
%FPAIPADDR01%	TCP/IP-Adresse (NWSD-Port 1) *
%FPAIPADDR02%	TCP/IP-Adresse (NWSD-Port 2) *
%FPAIPADDR03%	TCP/IP-Adresse (NWSD-Port 3) *
%FPASUBNETPP%	TCP/IP-Teilnetzadresse (NWSD-Port *VRTETHPTP) *
%FPASUBNET01%	TCP/IP-Teilnetzadresse (NWSD-Port 1) *
%FPASUBNET02%	TCP/IP-Teilnetzadresse (NWSD-Port 2) *
%FPASUBNET03%	TCP/IP-Teilnetzadresse (NWSD-Port 3) *
%FPATCPHOSTNAME%	TCP/IP-Hostname
%FPATCPDOMAIN%	TCP/IP-Domänenname
%FPATCPDNSS%	TCP/IP-DNS, durch Komma getrennt
%FPATCPDNS01%	TCP/IP-Domain Name-Server 1
%FPATCPDNS02%	TCP/IP-Domain Name-Server 2
%FPATCPDNS03%	TCP/IP-Domain Name-Server 3
%FPANWSDTYPE%	Art der NWSD, die angehängt wird
%FPANWSDNAME%	Name der NWSD, die angehängt wird
%FPACARDTYPE%	Ressourcenart der NWSD, die angehängt wird (z. B. 2890, 2892, 4812, 2689, iSCSI)
%FPAINSMEM%	Größe des festgestellten installierten Hauptspeichers
%FPAUSEMEM%	Größe des nutzbaren installierten Hauptspeichers
%FPACODEPAGE%	ASCII-Codepage zum Umsetzen von EBCDIC
%FPALANGVERS%	i5/OS-Sprachversion, die in der NWSD benutzt wird
%FPASYSDRIVE%	Laufwerksbuchstabe, der für das Systemlaufwerk verwendet wird (C, E, wenn der Server mit V4R4 oder einer früheren Version installiert wurde)
%FPA_CARET%	Winkelzeichen (^)
%FPA_L_BRACKET%	Linke eckige Klammer (l)
%FPA_R_BRACKET%	Rechte eckige Klammer (r)
%FPA_PERCENT%	Prozentzeichen (%) HINWEIS: Da das Prozentzeichen als Begrenzer für Substitutionsvariablen verwendet wird, sollte diese Substitutionsvariable nur benutzt werden, wenn die Zeichenfolge ein Prozentzeichen enthält, das NICHT als Begrenzer für Substitutionsvariable interpretiert werden soll.
%FPABOOTDRIVE%	Immer Laufwerk E für den integrierten xSeries-Server
%FPACFGFILE%	Name der NWSD-Konfigurationsdatei, die verarbeitet wird
%FPACFGLIB%	Bibliothek, die die NWSD-Konfigurationsdatei enthält, die verarbeitet wird

Substitutionsvariable	Beschreibung
%FPACFGMBR%	Name der Teildatei der NWS-D-Konfigurationsdatei, die verarbeitet wird
* Diese Werte werden aus der NWS-Beschreibung (NWS-D) abgerufen	

Durch Erstellen einer Datei in QUSRSYS und Benennen der Datei mit dem gleichen Namen wie die NWS-D, gefolgt vom Suffix 'VA', können Sie zusätzliche Substitutionsvariablen konfigurieren. Sie müssen die Datei als physische Quellendatei mit einer Mindestsatzlänge von 16 und einer maximalen Satzlänge von 271 erstellen.

Geben Sie in der i5/OS-Befehlszeile beispielsweise Folgendes ein:

```
CRTSRCPF FILE(QUSRSYS/nwsdnameVA) RCDLEN(271) MBR(nwsdname) MAXMBRS(1) TEXT('Konfigurationsdateivariablen')
```

Die Teildatei 'nwsdname' enthält Daten in festen Spalten in folgendem Format:

- Ein Variablenname in Spalte 1-15 mit Leerzeichen aufgefüllt und
- Ein Wert, der in Spalte 16 beginnt.

Beispiel:

Spalten:

```
12345678901234567890123456789012345678901234567890...
```

```
myaddr          9.5.9.1
```

Hierbei wird %myaddr% der Liste der verfügbaren Substitutionsvariablen hinzugefügt und hat den Wert "9.5.9.1".

Kapitel 16. Referenzinformationen

Die folgenden iSeries Handbücher und IBM Redbooks (PDF-Format), Websites sowie Information Center-Themen enthalten Informationen zur Windows-Umgebung auf der iSeries. Sie können alle PDFs anzeigen oder drucken.

Handbücher

- iSeries Performance Capabilities Reference 
- Sicherung und Wiederherstellung 
- Anweisungen zur Hardwareinstallation. Weitere Informationen finden Sie unter „iSeries-Features installieren“ topic.

Redbooks (www.redbooks.ibm.com)

Microsoft Windows Server 2003 Integration with iSeries, SG24-6959 

| IBM xSeries and BladeCenter Server Management, SG24-6495 

Websites

- | • Neueste Informationen zu Produkten und Services: IBM iSeries Integrated xSeries solutions 
| (www.ibm.com/servers/eserver/series/integratedxseries)
- iSeries Performance Management 
(www.ibm.com/eserver/series/perfmgmt)
- IXA install read me first 
(www.ibm.com/servers/eserver/series/integratedxseries/ixareadme)
- | • iSCSI install read me first 
| (www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme)
- IXS install read me first 
(www.ibm.com/servers/eserver/series/integratedxseries/ixsreadme)
- | • Troubleshooting 
| (www.ibm.com/servers/eserver/series/integratedxseries/troubleshooting.html).

Anhang. Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. An Stelle der IBM Produkte, Programme oder Services können auch andere ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb von Fremdprodukten, Fremdprogrammen und Fremdservices liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

| IBM Europe
| Director of Licensing
| 92066 Paris La Defense Cedex
| France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen oder in Technical News Letters (TNLs) bekannt gegeben. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt; die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

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

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

- | Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials
- | erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der IBM Internationalen Nutzungs-
- | bedingungen für Programmpakete, der IBM Lizenzvereinbarung für Maschinencode oder einer äquivalen-
- | ten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht von IBM dar, unterliegen Änderungen oder können zurückgenommen werden, und repräsentieren nur die Ziele von IBM.

Wird dieses Buch als Softcopy (Book) angezeigt, erscheinen keine Fotografien oder Farbabbildungen.

Marken

Folgende Namen sind in gewissen Ländern Marken der International Business Machines Corporation:

AIX
AS/400
BladeCenter
DB2
IBM
iSeries Netfinity
NetServer
OS/400
i5/OS
PAL
Redbooks
ServerGuide
Virtualization Engine xSeries

Pentium ist in gewissen Ländern (oder Regionen) eine Marke oder eingetragene Marke der Intel Corporation.

- | Linux ist in gewissen Ländern eine Marke von Linus Torvalds.

Microsoft, Windows, Windows NT und das Windows-Logo sind in gewissen Ländern Marken der Microsoft Corporation.

Andere Namen von Unternehmen, Produkten und Services können Marken oder Servicemarken anderer Unternehmen sein.

Bedingungen

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

Persönliche Nutzung: Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM weder weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Kommerzielle Nutzung: Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Abgesehen von den hier gewährten Berechtigungen erhalten Sie keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum.

IBM behält sich das Recht vor, die in diesem Dokument gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Vorschriften, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Veröffentlichungen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf "as-is"-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit oder die Freiheit der Rechte Dritter zur Verfügung gestellt.

IBM