



Systemy IBM - iSeries

Prostředí Windows na serveru iSeries







Systemy IBM - iSeries

Prostředí Windows na serveru iSeries

**Poznámka**

Než začnete používat tyto informace a produkt, který podporují, si nezapomeňte přečíst informace uvedené v tématu “Poznámky”, na stránce 251.

**Desáté vydání (únor 2006)**

Toto vydání se týká verze 5, vydání 4, modifikace 0 operačního systému i5/OS (číslo produktu 5722–SS1) a všech následujících vydání a modifikací, dokud nebude v nových vydáních uvedeno jinak. Tato verze nepracuje na všech modelech počítačů RISC (reduced instruction set computer), ani na modelech CISC.

© Copyright International Business Machines Corporation 1998, 2006. Všechna práva vyhrazena.

# Obsah

<b>Kapitola 1. Prostředí Windows na serveru iSeries . . . . .</b>	<b>1</b>	Konfigurace zabezpečeného připojení . . . . .	45
<b>Kapitola 2. Co je nového ve verzi V5R4 . . . . .</b>	<b>3</b>	Paměť certifikátů . . . . .	45
<b>Kapitola 3. Tisk souborů ve formátu PDF . . . . .</b>	<b>5</b>	Koncepce vysoké dostupnosti . . . . .	46
<b>Kapitola 4. Koncepce . . . . .</b>	<b>7</b>	Koncepce zabezpečení . . . . .	46
Přehled integrovaných serverů . . . . .	7	Zabezpečení pro systémy IXS a systémy připojené pomocí adaptéru IXA . . . . .	46
Výhody . . . . .	8	Zabezpečení u systémů připojených pomocí iSCSI . . . . .	47
Terminologie . . . . .	9	Koncepce týkající se uživatelů a skupin . . . . .	49
Koncepce týkající se hardwaru . . . . .	13	Typy uživatelských konfigurací . . . . .	51
Seryery IXS a servery připojené pomocí adaptéru IXA . . . . .	14	Šablony pro zápis uživatelů . . . . .	52
Seryery připojené pomocí iSCSI . . . . .	16	Posouzení hesla . . . . .	53
Přehled serverů připojených pomocí iSCSI . . . . .	18	<b>Kapitola 5. Instalace a konfigurace prostředí Windows na serveru iSeries . . . . .</b>	<b>55</b>
Základní podpora jednoho serveru . . . . .	18	Hardwarové požadavky . . . . .	55
Podpora více serverů . . . . .	20	Softwarové požadavky . . . . .	57
Rozšířená podpora sítě iSCSI . . . . .	20	Příprava na instalaci integrovaných Windows serverů . . . . .	58
Zavádění systému bez disku přes iSCSI . . . . .	22	Požadavky na velikost společné oblasti vyhrazené pro operační systém . . . . .	59
Konzole Windows . . . . .	23	Synchronizace času . . . . .	60
Pokyny . . . . .	24	Konfigurace i5/OS TCP/IP u integrovaných Windows serverů . . . . .	60
Výkon . . . . .	24	Produkt iSeries Access for Windows na integrovaných Windows serverech . . . . .	61
Paměťové prostory a vyhrazené disky na serveru iSeries . . . . .	25	Povolení serveru iSeries NetServer . . . . .	61
Rovnováha paměťových prostorů . . . . .	25	Vytvoření uživatelského profilu 'guest' pro iSeries NetServer . . . . .	61
Výkon serverů připojených pomocí iSCSI . . . . .	26	Instalace licencovaného programu IBM i5/OS Integrated Server Support . . . . .	62
Virtuální síť Ethernet . . . . .	27	Plán instalace Windows serveru . . . . .	62
Koncepce v oblasti sítí . . . . .	27	Plán instalace hardwaru iSCSI . . . . .	63
Připojení servisního procesoru . . . . .	28	Plán zaváděcího režimu pro hostovaný systém . . . . .	63
Síť iSCSI . . . . .	28	Vytvoření konfigurace servisního procesoru a konfigurace vzdáleného systému . . . . .	63
Dvoubodová virtuální síť Ethernet . . . . .	30	Plán připojení servisního procesoru . . . . .	65
Virtuální síť Ethernet . . . . .	31	Konfigurace metody zjišťování servisního procesoru na serveru iSeries . . . . .	65
Externí síť . . . . .	35	Popisy síťového serveru . . . . .	65
Koncepce týkající se softwaru . . . . .	35	Pracovní formulář pro parametry instalace i5/OS . . . . .	65
Seryery IXS (Integrated xSeries Server) a servery xSeries připojené pomocí adaptéru IXA (Integrated xSeries Adapter) . . . . .	35	Porovnání systémů souborů FAT, FAT32 a NTFS . . . . .	84
Popis síťového serveru . . . . .	38	Rada: Vyhledejte jména prostředků, máte-li více integrovaných serverů . . . . .	85
Jméno hardwarového prostředku . . . . .	38	Podporované jazykové verze . . . . .	85
Paměťové prostory síťového serveru . . . . .	38	Instalace serverů Windows 2000 Server nebo Windows Server 2003 . . . . .	86
Popisy linek virtuální sítě Ethernet . . . . .	39	Příprava hardwaru iSCSI na instalaci Windows . . . . .	87
Rozhraní TCP/IP . . . . .	39	Inicializace zabezpečení servisního procesoru . . . . .	87
Systémová sběrnice a datové toky typu HSL . . . . .	39	Vytvoření a spuštění adaptéru NWSH . . . . .	87
Seryery xSeries a IBM BladeCenter připojené pomocí iSCSI . . . . .	39	Spuštění instalace z konzole i5/OS . . . . .	87
Adaptéry hostitele síťového serveru . . . . .	41	Pokračování instalace z konzole integrovaného Windows serveru . . . . .	91
Konfigurace vzdáleného systému . . . . .	41	Dokončení instalace serveru . . . . .	91
Konfigurace servisního procesoru . . . . .	41	Přechod na vyšší verzi licencovaného programu IBM iSeries Integration for Windows Server . . . . .	92
Popis síťového serveru . . . . .	42		
Paměťové prostory síťového serveru . . . . .	43		
Datové toky . . . . .	43		
Seryery xSeries a BladeCenter připojené pomocí iSCSI se zabezpečením . . . . .	43		
Konfigurace vzdáleného systému . . . . .	45		
Konfigurace servisního procesoru . . . . .	45		

Přechod na vyšší verzi licencovaného produktu IBM i5/OS Integrated Server Support na straně integrovaného serveru. . . . .	94	Změna vlastností objektu NWSH . . . . .	115
Migrace z hardwaru 285x nebo 661x na hardware integrovaného serveru IXS 2890 . . . . .	95	Spuštění objektu NWSH . . . . .	115
Migrace na servery připojené pomocí iSCSI . . . . .	95	Zastavení objektu NWSH . . . . .	115
Klastrová služba Windows . . . . .	95	Výmaz objektu NWSH . . . . .	116
Instalace klastrové služby Windows . . . . .	96	Správa konfigurací síťových serverů ve vzdáleném systému . . . . .	116
Instalace klastrové služby Windows na nový integrovaný Windows server. . . . .	96	Vytvoření objektu konfigurace vzdáleného systému	116
Instalace klastrové služby Windows na stávající server . . . . .	96	Vytvoření objektu NWSH na základě jiného objektu. . . . .	117
Příprava Windows před instalací klastrové služby Windows . . . . .	97	Zobrazení vlastností konfigurace vzdáleného systému . . . . .	117
Instalace klastrové služby Windows do operačního systému Windows . . . . .	98	Změna vlastností konfigurace vzdáleného systému	117
Instalace klastrové služby Windows na Windows 2000 Server. . . . .	99	Zobrazení stavu vzdáleného systému . . . . .	118
Instalace klastrové služby Windows na Windows Server 2003. . . . .	99	Výmaz objektu konfigurace vzdáleného systému	118
Použití služby Kerberos se serverem Windows Server 2003 Active Directory Server . . . . .	100	Správa konfigurací síťových serverů se servisními procesory . . . . .	118
Instalace ovladačů videozařízení ATI Radeon 7000M pro Windows 2000 na serveru IXS 2892-002 nebo 4812-001 . . . . .	101	Vytvoření objektu konfigurace servisního procesoru . . . . .	119
Přizpůsobení akcelerace hardwaru u serveru Windows Server 2003 na serveru IXS 2892-002 nebo 4812-001 . . . . .	102	Vytvoření objektu konfigurace servisního procesoru na základě jiného objektu . . . . .	119
Odpovědi na chybové zprávy během instalace . . . . .	102	Zobrazení vlastností konfigurace servisního procesoru . . . . .	119
Nastavení integrovaného Windows serveru na automatické logické zapnutí s TCP/IP . . . . .	102	Změna vlastností konfigurace servisního procesoru	120
Opravy kódu . . . . .	103	Inicializace servisního procesoru . . . . .	120
Typy oprav kódu . . . . .	104	Výmaz objektu konfigurace servisního procesoru	121
Synchronizace úrovně softwaru pro integraci z konzole integrovaného Windows serveru . . . . .	104	Správa konfigurací síťových serverů se zabezpečeným připojením. . . . .	121
Synchronizace úrovně softwaru pro integraci prostřednictvím produktu iSeries Navigator . . . . .	105	Vytvoření objektu konfigurace zabezpečeného připojení . . . . .	121
Synchronizace úrovně softwaru pro integraci prostřednictvím vzdáleného příkazu . . . . .	105	Vytvoření objektu konfigurace zabezpečeného připojení na základě jiného objektu . . . . .	122
<b>Kapitola 6. Správa virtuálních sítí Ethernet a externích sítí. . . . .</b>	<b>107</b>	Zobrazení vlastností konfigurace zabezpečeného připojení . . . . .	122
Konfigurace hodnot IP adresa, brána a MTU . . . . .	107	Změna vlastností konfigurace zabezpečeného připojení . . . . .	122
Konfigurace virtuálních sítí Ethernet . . . . .	107	Výmaz objektu konfigurace zabezpečeného připojení . . . . .	123
Konfigurace virtuálních sítí Ethernet mezi logickými částmi . . . . .	108	Konfigurace zabezpečení mezi operačním systémem i5/OS a hostovanými systémy. . . . .	123
Prozkoumání dvoubodových virtuálních sítí Ethernet . . . . .	109	Konfigurace protokolu CHAP . . . . .	123
Externí sítě . . . . .	110	Konfigurace IPSec . . . . .	124
Instalace ovladačů zařízení síťových adaptérů a přidání informací o adrese adaptéru do integrovaného Windows serveru . . . . .	110	Konfigurace zabezpečení SSL servisního procesoru	125
Odstranění síťových adaptérů . . . . .	111	Automatická inicializace zabezpečení SSL . . . . .	125
<b>Kapitola 7. Administrace připojení k serverům připojeným pomocí iSCSI . . . . .</b>	<b>113</b>	Manuální inicializace zabezpečení SSL . . . . .	126
Práce s objekty konfigurace iSCSI . . . . .	113	Heslo servisního procesoru . . . . .	126
Správa objektů NWSH . . . . .	113	Konfigurace firewallu . . . . .	126
Vytvoření objektu NWSH . . . . .	113	Správa adaptérů iSCSI HBA . . . . .	127
Vytvoření objektu NWSH na základě jiného objektu. . . . .	114	Výměna adaptérů v lokálním hostitelském systému iSCSI za chodu . . . . .	128
Zobrazení vlastností objektu NWSH . . . . .	114	Správa využití adaptérů iSCSI HBA . . . . .	128
		Sdílení adaptéru iSCSI HBA několika hostovanými servery. . . . .	128
		Rozložení zatížení na několik adaptérů iSCSI HBA	129
		Použití několika adaptérů iSCSI HBA za účelem redundance . . . . .	130
		Správa alokací iSCSI HBA na straně Windows sítě iSCSI . . . . .	131
		Posouzení velikosti maximální přenosové jednotky (MTU). . . . .	131

Konfigurace virtuální sítě Ethernet na maximální výkon v sítích iSCSI, které podporují rámce větší než 1500 bajtů . . . . .	132
Konfigurace virtuální sítě Ethernet pro sítě iSCSI, které mají maximální velikost rámce menší než 1500 bajtů . . . . .	132
Konfigurace virtuální sítě Ethernet, která podporuje neobvyklé aplikace nevyužívající TCP a nevyjednávající MTU. . . . .	132
Integrovaný server DHC . . . . .	133
Zjišťování vzdálených serverů a jejich správa . . . . .	134
Instalace a konfigurace produktu IBM Director . . . . .	134
Zjišťování vzdálených serverů a servisních procesorů . . . . .	135
Konfigurace zjišťování servisních procesorů . . . . .	135
Dynamické IP adresování (DHCP) . . . . .	137
Metody zjišťování servisních procesorů . . . . .	137
Protokol SLP (Service Location Protocol) s využitím výběrového adresování . . . . .	137
Zjišťování podle IP adresy . . . . .	138
Zjišťování podle jména . . . . .	138
Použití webového rozhraní modulu Management Module a adaptéru RSA II . . . . .	139

## **Kapitola 8. Administrace integrovaných Windows serverů . . . . . 141**

Spuštění a zastavení integrovaného serveru . . . . .	141
Spuštění a zastavení integrovaného Windows serveru pomocí produktu iSeries Navigator . . . . .	141
Spuštění a zastavení integrovaného Windows serveru v prostředí znakově orientovaného rozhraní. . . . .	142
Ukončení práce integrovaného Windows serveru z konzole Windows serveru . . . . .	142
Bezpečné ukončení práce systému iSeries, když jsou přítomny integrované Windows servery . . . . .	142
Připojení k virtuální sériové konzoli serveru IXS 4812 . . . . .	143
Prohlížení a změna informací o konfiguraci integrovaného Windows serveru . . . . .	144
Protokolování zpráv . . . . .	144
Vzdálené spuštění příkazů integrovaného Windows serveru . . . . .	145
Pokyny pro spuštění vzdálených příkazů . . . . .	146
Příkaz SBMNWSCMD a podpora zálohování na úrovni souborů pro protokol Kerberos v5 a mapování EIM . . . . .	147
Výměna hardwaru serveru za chodu . . . . .	148

## **Kapitola 9. Správa systému pro ukládání dat . . . . . 151**

Správa systému pro ukládání dat operačního systému i5/OS . . . . .	151
Diskové jednotky pro integrované Windows servery . . . . .	152
Předdefinované diskové jednotky pro integrované Windows servery. . . . .	154
Administrace diskových jednotek integrovaného Windows serveru v systému i5/OS . . . . .	155
Přístup k integrovanému systému souborů operačního systému i5/OS z integrovaného serveru . . . . .	155
Získání informací o diskových jednotkách integrovaného serveru . . . . .	156

Přidání diskových jednotek na integrované Windows servery . . . . .	156
Vytvoření diskové jednotky integrovaného serveru . . . . .	156
Propojení diskové jednotky s integrovaným serverem . . . . .	157
Formátování diskových jednotek integrovaného Windows serveru. . . . .	158
Kopírování diskové jednotky . . . . .	158
Rozbalení diskové jednotky . . . . .	159
Rozbalení systémové jednotky. . . . .	160
Odpojení diskových jednotek integrovaného Windows serveru. . . . .	160
Výmaz diskových jednotek integrovaného Windows serveru. . . . .	160
Použití programu Windows Disk Management s integrovanými Windows servery . . . . .	161

## **Kapitola 10. Sdílení zařízení . . . . . 163**

Určení popisu zařízení a jmen hardwarových prostředků pro zařízení iSeries . . . . .	163
Použití optických jednotek serveru iSeries s integrovanými Windows servery . . . . .	163
Použití páskových jednotek serveru iSeries s integrovanými Windows servery . . . . .	164
Instalace ovladačů páskových jednotek . . . . .	165
Formátování pásy v i5/OS pro použití s integrovanými Windows servery . . . . .	165
Alokace páskové jednotky serveru iSeries pro integrovaný Windows server . . . . .	165
Předání řízení páskové jednotky z integrovaného Windows serveru zpět na server iSeries . . . . .	166
Podporované páskové jednotky iSeries . . . . .	167
Identifikace páskových jednotek iSeries pro aplikace . . . . .	167
Přenos řízení páskových a optických jednotek iSeries mezi integrovanými Windows servery . . . . .	167
Tisk z integrovaného Windows serveru na tiskárnách serveru iSeries . . . . .	168

## **Kapitola 11. Administrace uživatelů integrovaných Windows serverů v operačním systému i5/OS . . . . . 169**

Zápis jednoho uživatele operačního systému i5/OS do prostředí Windows pomocí produktu iSeries Navigator . . . . .	169
Zápis skupiny uživatelů operačního systému i5/OS do prostředí Windows pomocí produktu iSeries Navigator . . . . .	170
Zápis uživatelů operačního systému i5/OS do prostředí Windows pomocí znakově orientovaného rozhraní . . . . .	170
Vytvoření šablony uživatele . . . . .	170
Zadání domovského adresáře do šablony. . . . .	171
Změna atributu LCLPMDMGT v uživatelském profilu . . . . .	172
Mapování EIM . . . . .	172
Vyřazení uživatelů zapsaných v prostředí Windows . . . . .	174
Vyřazení skupin zapsaných v prostředí Windows . . . . .	174
Uživatel QAS400NT . . . . .	175
Jak zabránit zápisu a přenesení uživatelského profilu na integrovaný Windows server . . . . .	177

## **Kapitola 12. Zálohování a obnova integrovaných Windows serverů . . . . . 179**

Zálohování NWSD a dalších objektů přiřazených k integrovanému Windows serveru . . . . .	179	Další protokoly a zprávy pro servery připojené pomocí iSCSI. . . . .	199
Zálohování NWSD integrovaného Windows serveru	180	Problémy s integrovaným Windows serverem v systému iSeries . . . . .	200
Zálohování NWSH integrovaného Windows serveru připojeného pomocí iSCSI . . . . .	180	Chyby typu STOP nebo "modrá obrazovka". . . . .	201
Zálohování objektů iSCSI NWSCFG a ověřovací seznamy . . . . .	180	Plná systémová jednotka integrovaného serveru . . . . .	201
Zálohování předdefinovaných diskových jednotek pro integrované Windows servery . . . . .	181	Problémy s optickou jednotkou . . . . .	202
Zálohování uživatelem definovaných diskových jednotek u integrovaného Windows serveru. . . . .	181	Uzamknutá optická jednotka při selhání serveru	202
Ukládání a obnova informací o zápisu uživatelů . . . . .	182	Problémy s páskami. . . . .	202
Které objekty by se měly ukládat a kde jsou v systému i5/OS umístěny . . . . .	183	Kontrola, zda byl zaveden ovladač páskové jednotky . . . . .	203
Zálohování jednotlivých souborů a adresářů integrovaného Windows serveru . . . . .	184	Problémy se spuštěním integrovaného Windows serveru. . . . .	204
Omezení při zálohování na úrovni souborů . . . . .	184	Problémy týkající se výměny za chodu mezi servery	205
Přípravné kroky administrátora . . . . .	185	Problémy sdílení hardwaru hostovaného systému . . . . .	206
Vytvoření sdílených položek na integrovaných Windows serverech . . . . .	186	Několik NWSD definovaných na stejném hardwaru hostovaného systému . . . . .	206
Přidání členů do souboru QAZLCSAVL . . . . .	186	Speciální pokyny týkající se systémů připojených pomocí iSCSI. . . . .	206
Zajištění stejné domény pro server iSeries NetServer a integrovaný Windows server . . . . .	187	Chyby v konfiguračním souboru NWSD . . . . .	207
Ukládání souborů . . . . .	187	Oprava konfiguračního souboru NWSD . . . . .	208
Příklady: Jak adresovat součásti integrovaného Windows serveru. . . . .	187	Resetování parametru konfiguračního souboru NWSD. . . . .	208
Program Windows Backup . . . . .	188	Použití předchozí verze souboru integrovaného serveru. . . . .	208
Obnova NWSD a diskových jednotek integrovaného Windows serveru. . . . .	188	DASD na serverech připojených pomocí IXA nebo iSCSI . . . . .	208
Obnova předdefinovaných diskových jednotek pro integrované Windows servery . . . . .	189	Problémy při zápisu uživatelů a skupin . . . . .	208
Obnova uživatelsky definovaných diskových jednotek pro integrované Windows servery . . . . .	190	Problémy s oprávněním k zápisu uživatelů . . . . .	209
Obnova NWSD u integrovaného Windows serveru	190	Problémy s heslem . . . . .	210
Obnova objektů NWSH integrovaných Windows serverů pro servery připojené pomocí iSCSI . . . . .	191	Program typu snap-in IBM iSeries Integrated Server Support . . . . .	211
Obnova objektů NWSCFG integrovaných Windows serverů pro servery připojené pomocí iSCSI. . . . .	191	Problémy se servery připojenými pomocí iSCSI . . . . .	212
Obnova souborů integrovaného Windows serveru . . . . .	192	Síťová analýza cesty pro zavedení systému a cesty k paměťovým prostorům . . . . .	214
		Správa certifikátů cest . . . . .	214
		Odstraňování problémů s produktem IBM Director	215
		Problémy zjišťování . . . . .	215
		Problémy s připojeními typu SSL. . . . .	216
		Problémy virtuální sítě Ethernet se servery připojenými pomocí iSCSI . . . . .	218
		Problémy virtuální sítě Ethernet se servery připojenými pomocí IXS a IXA . . . . .	220
		Existuje popis linky i ikona . . . . .	221
		Existuje popis linky, ale chybí ikona . . . . .	221
		Popis linky chybí, ale ikona existuje . . . . .	222
		Chybí popis linky i ikona . . . . .	222
		Problémy s externími sítěmi . . . . .	223
		Manuální aktualizace ovladačů LAN na integrovaném Windows serveru. . . . .	223
		Zahájení instalace nebo aktualizace ovladače LAN	224
		Výběr adaptéru, který se bude instalovat nebo aktualizovat . . . . .	224
		Dokončení instalace nebo aktualizace ovladače LAN . . . . .	224
		Konflikty IP adres ve dvoubodové virtuální síti Ethernet . . . . .	226
		Přidělování IP adres ve dvoubodové virtuální síti Ethernet . . . . .	227
		Problémy s TCP/IP nad virtuální sítí Ethernet . . . . .	227

### **Kapitola 13. Odinstalování operačního systému Windows serveru z hardwaru integrovaného serveru . . . . . 193**

Výmaz NWSD integrovaného Windows serveru . . . . .	193
Výmaz popisů linek integrovaného Windows serveru . . . . .	194
Výmaz rozhraní TCP/IP asociovaných s integrovaným Windows serverem . . . . .	194
Výmaz popisů řadičů integrovaného Windows serveru	195
Výmaz popisů zařízení asociovaných s integrovaným Windows serverem . . . . .	195
Výmaz konfigurací síťového serveru asociovaných s integrovaným Windows serverem sítě iSCSI . . . . .	195
Výmaz produktu IBM i5/OS Integrated Server Support, volba 29 operačního systému i5/OS (5722–SS1) . . . . .	195

### **Kapitola 14. Odstraňování problémů s integrovanými Windows servery . . . 197**

Kontrola zpráv a protokolů úloh . . . . .	197
Monitorovací úloha . . . . .	199



Problémy s přístupem ke sdíleným položkám serveru Windows Server 2003 ze systému souborů QNTC . . . . .	228
Problémy s přístupem u IFS . . . . .	228
Problémy s ukládáním souborů integrovaného Windows serveru. . . . .	228
Nečitelné zprávy ve frontě zpráv serveru. . . . .	229
Problémy se získáním výpisu paměti systému Windows . . . . .	230
Přinstalování integrovaného Windows serveru. . . . .	230
Shromáždění údajů pro servis u integrovaného Windows serveru. . . . .	231
Vytvoření výpisu paměti integrovaného Windows serveru v operačním systému i5/OS . . . . .	231
Použití nástroje operačního systému i5/OS pro výpis paměti popisu síťového serveru (NWSO). . . . .	232

## **Kapitola 15. Konfigurační soubory popisu síťového serveru. . . . . 235**

Formát konfiguračního souboru NWSO . . . . .	235
Vytvoření konfiguračního souboru NWSO . . . . .	236
Příklad: Konfigurační soubor NWSO . . . . .	236
Odstranění řádků z existujícího souboru integrovaného serveru pomocí typu záznamu CLEARCONFIG . . . . .	237
Klíčové slovo TARGETDIR . . . . .	237
Klíčové slovo TARGETFILE . . . . .	238
Změna souboru integrovaného serveru pomocí typu záznamu ADDCONFIG. . . . .	238
Klíčové slovo VAR . . . . .	239
Klíčové slovo ADDSTR . . . . .	239
Klíčové slovo ADDWHEN. . . . .	239
Operátory ve výrazech používané u klíčových slov ADDWHEN a DELETEWHEN . . . . .	239
Klíčové slovo DELETEWHEN . . . . .	240
Klíčové slovo LINECOMMENT . . . . .	240
Klíčové slovo LOCATION. . . . .	240
Klíčové slovo LINESEARCHPOS . . . . .	240
Klíčové slovo LINESEARCHSTR . . . . .	240
Klíčové slovo LINELOCATION . . . . .	240

Klíčové slovo FILESEARCHPOS (typ záznamu ADDCONFIG) . . . . .	241
Klíčové slovo FILESEARCHSTR. . . . .	241
Klíčové slovo FILESEARCHSTROCC . . . . .	241
Klíčové slovo REPLACEOCC. . . . .	241
Klíčové slovo TARGETDIR . . . . .	241
Klíčové slovo TARGETFILE . . . . .	242
Klíčové slovo UNIQUE. . . . .	242
Klíčové slovo VAROCC . . . . .	242
Klíčové slovo VARVALUE . . . . .	242

Změna souboru integrovaného Windows serveru pomocí typu záznamu UPDATECONFIG . . . . .	242
Klíčové slovo FILESEARCHPOS (typ záznamu UPDATECONFIG) . . . . .	243
Klíčové slovo FILESEARCHSTR (typ záznamu UPDATECONFIG) . . . . .	243
Klíčové slovo FILESEARCHSTROCC (typ záznamu UPDATECONFIG) . . . . .	243

Nastavení konfiguračních předvoleb pomocí typu záznamu SETDEFAULTS . . . . .	244
ADDWHEN . . . . .	244
DELETEWHEN . . . . .	244
Klíčové slovo FILESEARCHPOS (typ záznamu SETDEFAULTS) . . . . .	245
Klíčové slovo FILESEARCHSTR (typ záznamu SETDEFAULTS) . . . . .	245
TARGETDIR. . . . .	245
TARGETFILE . . . . .	245

Použití substitučních proměnných pro hodnoty klíčových slov. . . . .	246
---	-----

## **Kapitola 16. Související informace . . 249**

### **Dodatek. Poznámky. . . . . 251**

Ochranné známky . . . . .	252
Ustanovení a podmínky . . . . .	253



---

# Kapitola 1. Prostředí Windows na serveru iSeries

Prostředí Windows na serveru iSeries je spíše koncepce, než jenom jednotlivé součásti hardwaru nebo softwaru. Je to způsob, jakým server iSeries a osobní počítače (PC) spolupracují, a zároveň způsob, jakým server iSeries osobní počítače spravuje, a tím usnadňuje jejich administraci.

První součástí prostředí Windows na serveru iSeries je hardware PC, který je nutné do iSeries dodat. To je možné v zásadě udělat trojím způsobem.

- Pomocí adaptéru IXA (*Integrated xSeries Adapter*) může server iSeries ovládat servery IBM xSeries. IBM nazývá svou řadu PC *serverů xSeries*.
- Pomocí adaptéru *iSCSI HBA* (iSCSI Host Bus Adapter) se může server iSeries připojit k síti Ethernet a řídit servery IBM xSeries nebo IBM BladeCenter.
- Server IXS (*Integrated xSeries Server*) je přídavná karta iSeries, která obsahuje paměť RAM a procesor Intel. Můžeme na ni pohlížet jako na PC, který byl transplantován do rámu serveru iSeries.

Druhou součástí je volba 29 operačního systému IBM i5/OS (5722–SS1), která je nainstalovaná na serveru iSeries a umožňuje mu ovládat PC. Tyto PC se pak nazývají integrované Windows servery.

A nakonec je nutné instalovat software pro Microsoft Windows 2000 Server nebo Windows Server 2003.

Tento dokument je rozdělen do následujících témat:

## **Kapitola 2, “Co je nového ve verzi V5R4”, na stránce 3**

Toto téma uvádí změny a zlepšení v tomto vydání.

## **Kapitola 3, “Tisk souborů ve formátu PDF”, na stránce 5**

Zde najdete informace o tom, jak vytisknout tento dokument ve formátu PDF.

## **Kapitola 4, “Koncepce”, na stránce 7**

V rámci tohoto tématu se seznámíte s tím, jak je řešeno prostředí Windows na serveru iSeries.

## **Kapitola 5, “Instalace a konfigurace prostředí Windows na serveru iSeries”, na stránce 55**

Toto téma uvádí pokyny pro instalaci nového integrovaného Windows serveru z pracovního média.

## **Kapitola 6, “Správa virtuálních sítí Ethernet a externích sítí”, na stránce 107**

Zde se dozvíte, jak používat tři různé typy sítí, které mají integrované servery k dispozici.

## **Kapitola 7, “Administrace připojení k serverům připojeným pomocí iSCSI”, na stránce 113**

Konfigurace serveru iSeries pro připojení k serverům xSeries nebo IBM BladeCenter pomocí iSCSI.

## **Kapitola 8, “Administrace integrovaných Windows serverů”, na stránce 141**

Toto téma obsahuje informace o spuštění a ukončení serveru, o provádění vzdálených integrovaných příkazů serveru, prohlížení a změně konfiguračních informací a o monitorování protokolů zpráv a chyb.

## **Kapitola 9, “Správa systému pro ukládání dat”, na stránce 151**

Zde najdete informace o pevných discích integrovaného Windows serveru.

## **Kapitola 10, “Sdílení zařízení”, na stránce 163**

Toto téma uvádí informace o používání zařízení iSeries na integrovaných serverech.

**Kapitola 11, “Administrace uživatelů integrovaných Windows serverů v operačním systému i5/OS”, na stránce 169**

Zde se dozvíte o integraci uživatelů i5/OS do prostředí Windows.

**Kapitola 12, “Zálohování a obnova integrovaných Windows serverů”, na stránce 179**

Toto téma popisuje, jak zálohovat soubory integrovaného serveru na pásková média nebo na pevné disky serveru iSeries.

**Kapitola 13, “Odinstalování operačního systému Windows serveru z hardwaru integrovaného serveru”, na stránce 193**

Zde zjistíte vše, co musíte vědět, abyste mohli odstranit software integrovaného Windows serveru ze systému.

**Kapitola 14, “Odstraňování problémů s integrovanými Windows servery”, na stránce 197**

Zde najdete odpovědi na běžné otázky.

**Kapitola 15, “Konfigurační soubory popisu síťového serveru”, na stránce 235**

Toto téma popisuje, jak lze integrované servery uživatelsky přizpůsobit prostřednictvím vytvoření vlastních konfiguračních souborů.

**Kapitola 16, “Související informace”, na stránce 249**

---

## Kapitola 2. Co je nového ve verzi V5R4

Ve verzi V5R4 má prostředí Windows na serveru iSeries několik nových funkcí:



- Byla přidána podpora integrace systémů xSeries a IBM BladeCenter do serveru iSeries, která je poskytována prostřednictvím adaptérů iSCSI HBA. Tato technologie integrace serverů doplňuje stávající technologie serveru IXS (Integrated xSeries Server) a adaptéru IXA (Integrated xSeries Adapter). Jsou podporovány servery připojené pomocí škálovatelné sítě typu Gigabit Ethernet za použití protokolu iSCSI i adaptéry jak na serveru iSeries, tak na serveru xSeries. Více informací o způsobu využití technologie iSCSI při integraci systémů IBM xSeries a BladeCenter do serveru iSeries najdete v tématu Kapitola 4, “Koncepce”, na stránce 7. Informace o tom, jak řídit a konfigurovat servery připojené pomocí protokolu iSCSI, uvádí Kapitola 7, “Administrace připojení k serverům připojeným pomocí iSCSI”, na stránce 113 a Kapitola 8, “Administrace integrovaných Windows serverů”, na stránce 141.
- Produkt IBM iSeries Integration for Windows Server (5722-WSV) byl nově sbalen pod názvem i5/OS Integrated Server Support (5722-SS1 volba 29).

**Poznámka:** Pokud přecházíte na verzi V5R4 z předchozího vydání operačního systému i5/OS, bude produkt 5722-WSV automaticky odstraněn a na jeho místo bude nainstalován produkt 5722-SS1 volba 29.

- Došlo ke zvýšení kapacity paměti pro Windows servery připojené pomocí protokolu iSCSI. Windows serveru připojenému pomocí protokolu SCSI je možné přiřadit až 64 diskových jednotek (paměťových prostorů síťového serveru), což umožňuje více než 60 TB diskového prostoru na jeden server.
- Byla přidána podpora rozšířené velikosti diskové jednotky (paměťový prostor síťového serveru). Další informace najdete v tématu “Rozbalení diskové jednotky” na stránce 159.
- Byla přidána podpora produktu Windows Server 2003 Volume Shadow Copy Service, který mohou využívat zálohovací aplikace, které pracují v operačním systému Windows. Data aplikací, které podporují produkt Volume Shadow Copy Service, mohou být zálohována bez zastavení aplikace, což zvyšuje dostupnost aplikací. Další informace najdete v tématu Kapitola 12, “Zálohování a obnova integrovaných Windows serverů”, na stránce 179.
- Byla přidána další podpora grafického rozhraní iSeries Navigator, včetně podpory řídicích serverů připojených pomocí iSCSI, řídicích integrovaných serverů Linux a AIX a konfigurace portů virtuální sítě Ethernet pro integrované servery.
- Byla zrušena podpora serverů 200 MHz a 333 MHz IBM Integrated PC Server for AS/400 (IPCS) a IBM Integrated Netfinity Server for AS/400 (INS). Nepodporované typy hardwarových prostředků IPCS a INS jsou 6617 a 2850 s kódem označení 2854, 2857, 2865, 2866, 6617 a 6618. Jelikož servery IPCS a INS byly jediné typy integrovaných serverů, které poskytovaly podporu hostitelské sítě typu LAN (sdílením adaptérů typu LAN mezi operačními systémy i5/OS a Windows), byla funkce hostitelské sítě typu LAN rovněž odstraněna.
- Z tohoto dokumentu byly odstraněny informace, které se v předchozích vydáních vztahovaly k serverům Windows NT 4.0 (které nejsou dále podporovány, jak tomu bylo ve verzi V5R3), hardwaru IPCS nebo INS (typ 6617 a 2850), sdíleným síťovým adaptérům (hostitelská síť typu LAN) a pokyny pro servery instalované před verzí V4R5. Informace vztahující se k této problematice naleznete pod heslem Prostředí Windows v tématu iSeries v aplikaci iSeries Information Center verze V5R3.

### Jak poznat, co je nové nebo co se změnilo

Pro snazší vyhledání provedených technických změn byly v dokumentu použity níže uvedené symboly:

- Symbol  označuje začátek nových nebo změněných informací.
- Symbol  označuje konec nových nebo změněných informací.

Chcete-li získat další informace o tom, co je v tomto vydání nové nebo co se změnilo, prostudujte si Sdělení pro uživatele.



---

## Kapitola 3. Tisk souborů ve formátu PDF

Chcete-li si prohlédnout nebo stáhnout PDF verzi tohoto dokumentu, vyberte téma Prostředí Windows na serveru iSeries (asi 4,2 MB).


Prohlížet nebo vytisknout si můžete také PDF verze souvisejících publikací nebo Červených knih Redbooks, jejichž seznam je uveden v tématu Kapitola 16, “Související informace”, na stránce 249.

### Ukládání souborů ve formátu PDF

Chcete-li uložit soubor ve formátu PDF na pracovní stanici za účelem prohlížení nebo tisku, postupujte takto:

1. V prohlížeči klepněte pravým tlačítkem na soubor PDF (na výše uvedený odkaz).
2. Pokud používáte Internet Explorer, klepněte na **Uložit cíl jako...** Pokud používáte Netscape Communicator, klepněte na **Save Link As...**
3. Vyhledejte adresář, do něhož chcete soubor uložit.
4. Klepněte na **Uložit (Save)**.

### Jak stáhnout produkt Adobe Reader

- | K prohlížení nebo tisku souborů ve formátu PDF potřebujete produkt Adobe Reader. Jeho bezplatnou kopii si můžete
- | stáhnout z webových stránek Adobe ([www.adobe.com/products/acrobat/readstep.html](http://www.adobe.com/products/acrobat/readstep.html))  .





## Kapitola 4. Koncepce

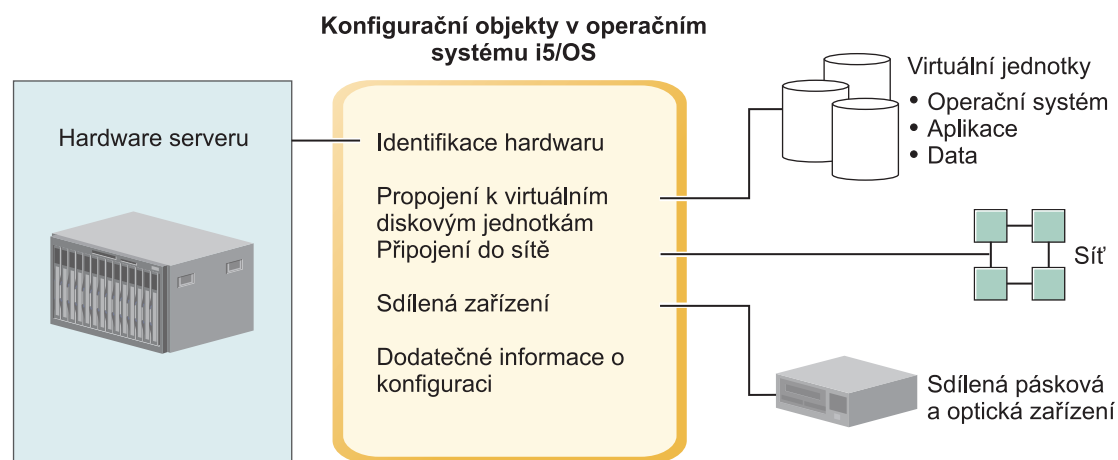
V tomto dokumentu se termín *integrováný Windows server* (nebo jenom *integrováný server*) vztahuje k instanci serveru Microsoft Windows 2000 Server či Windows Server 2003, která je spuštěna na serveru IXS (Integrated xSeries Server), na serveru xSeries připojenému k serveru iSeries pomocí adaptéru IXA (Integrated xSeries Adapter), nebo na serveru xSeries či IBM BladeCenter připojenému k serveru iSeries pomocí adaptéru iSCSI HBA. Stejně, jako se termín PC často používá pro software operačního systému Windows firmy Microsoft provozovaný na mikroprocesoru Intel a asociovaném hardwaru, představuje termín integrováný Windows server kombinaci hardwaru a softwaru, která tvoří celý produkt.

Prostudujte si tato témata zabývající se konceptem:

- “Přehled integrovaných serverů”
- “Výhody” na stránce 8
- “Terminologie” na stránce 9
- “Koncepce týkající se hardwaru” na stránce 13
- “Pokyny” na stránce 24
- “Výkon” na stránce 24
- “Koncepce v oblasti sítí” na stránce 27
- “Koncepce týkající se softwaru” na stránce 35
- “Koncepce vysoké dostupnosti” na stránce 46
- “Koncepce zabezpečení” na stránce 46
- “Koncepce týkající se uživatelů a skupin” na stránce 49

### Přehled integrovaných serverů

Integrovaný server sestává z několika hardwarových a softwarových součástí.



RZAHQ507-1

Obrázek 1. Přehled integrovaných serverů

Termín **hardware serveru** znamená fyzický hardware (například procesor a paměť), na kterém je integrováný server provozován. Pro integrované servery můžete použít několik typů hardwaru serveru dle potřeby. Hardware serveru může mít formu karty, která se vloží do serveru iSeries, do externího serveru IBM xSeries, který je připojen k serveru iSeries přes adaptér IXA (Integrated xSeries Adapter), nebo do externího serveru IBM xSeries či serveru IBM BladeCenter,

l který je připojen k serveru iSeries přes adaptér iSCSI HBA. Integrovaný server může také používat páskové a optické jednotky, které jsou připojeny k hostitelské logické části s operačním systémem i5/OS. Další informace o typech hardwaru, které lze použít pro integrované servery, najdete v tématu “Koncepte týkající se hardwaru” na stránce 13.

l Každý integrovaný server má alespoň jedno připojení do sítě. Jsou podporována jak připojení do fyzické sítě přes síťové adaptéry, tak připojení do virtuální sítě Ethernet na serveru iSeries. Další informace o typech připojení do sítě, které lze použít pro integrované servery, najdete v tématu “Koncepte v oblasti sítí” na stránce 27.

l Každý integrovaný server používá **virtuální diskové jednotky**, které obsahují operační systém serveru, aplikace a data. Tyto virtuální diskové jednotky jsou alokovány z diskové paměti operačního systému i5/OS. Integrovaný server zachází s těmito jednotkami jako s fyzickými diskovými jednotkami serveru. Integrovaný server nemá ve skutečnosti žádné vlastní fyzické diskové jednotky. Další informace o virtuálních diskových jednotkách najdete v tématu “Koncepte týkající se softwaru” na stránce 35.

l **Sdílená zařízení** zahrnují všechny podporované typy páskových a optických jednotek, ke kterým může integrovaný server přistupovat tak, jako by se jednalo o lokální zařízení integrovaného serveru. Podle předvoleného nastavení jsou všechny páskové a optické jednotky serveru iSeries integrovanému serveru automaticky přístupné. Můžete vybrat, ke kterým z těchto jednotek serveru iSeries, povolíte integrovanému serveru přístup.

l **Objekty konfigurace v systému i5/OS** popisují jednotlivé integrované servery. Objekty konfigurace v systému i5/OS identifikují hardware, na kterém se integrovaný server provozuje, virtuální diskové jednotky, které integrovaný server používá, připojení virtuální sítě Ethernet, které integrovaný server používá, a mnoho dalších atributů serveru. Další informace o objektech konfigurace operačního systému i5/OS, které popisují integrovaný server, najdete v tématu “Koncepte týkající se softwaru” na stránce 35.

---

## Výhody

Prostředí Windows na serveru iSeries zajišťuje většinu funkcí vyplývajících z použití serveru Microsoft Windows a serverů na bázi PC, a oproti jiným počítačovým systémům poskytuje následující výhody.

### Úspora prostoru

- Je méně hardwarových součástí a vyžadují méně fyzického prostoru.

### Vyšší dostupnost a lepší ochrana dat

- Integrovaný Windows server používá diskovou paměť serveru iSeries, která je obecně spolehlivější než pevné disky PC serverů.
- Při zálohování integrovaného Windows serveru máte přístup k rychlejším páskovým jednotkám serveru iSeries.
- Celý Windows server můžete zálohovat jako součást zálohování serveru iSeries. Obnova serveru po selhání pak bude mnohem snazší a rychlejší než obvyklá obnova na úrovni souborů ve Windows.
- Integrované servery implicitně využívají prvotřídních schémat ochrany dat, které nabízí operační systém i5/OS, například RAID a zrcadlení jednotek.
- Obvyklé konfigurace integrovaných serverů mají paměťový prostor rozložený na více diskových jednotkách serveru iSeries, než by bylo možné konfigurovat v instalacích samostatného (neintegrovaného) Windows serveru. Tím je často zajištěna vyšší kapacita I/O operací na disku v době provozní špičky, protože žádný server není omezen na několik málo vyhrazených jednotek.
- Integrovaným serverům můžete přidat další diskovou paměť a nemusíte přitom server vypínat.
- Je možné získat přístup k datům DB2 UDB for iSeries, a to pomocí zdokonaleného ovladače zařízení ODBC, který používá produkt iSeries Access. Tento ovladač zařízení podporuje aplikace typu “server-to-server” mezi integrovanými servery a operačním systémem i5/OS.
- Integrovaný server můžete používat jako druhou vrstvu v třívrstvé aplikaci klient/server.
- Použití virtuálních sítí nevyžaduje žádný další hardware pro síť LAN a zajišťuje komunikaci mezi logickými částmi serveru iSeries, servery IXS (Integrated xSeries Server), adaptéry IXA (Integrated xSeries Adapter) a adaptéry iSCSI HBA.

### **Zjednodušená administrace**

- V operačním systému i5/OS lze snáze spravovat uživatelské parametry, jako jsou například hesla. Můžete vytvořit uživatele a skupiny a zapsat je z operačního systému i5/OS na integrované servery. To usnadňuje aktualizaci hesel a dalších uživatelských informací z operačního systému i5/OS.
- Počítačový systém se stává mnohem jednodušší díky integraci funkcí pro administraci uživatelů, zabezpečení dat, správu serveru a plánů zálohování a obnovy v prostředí operačních systémů i5/OS a Microsoft Windows. Data integrovaného serveru můžete ukládat na stejná média jako ostatní data systému i5/OS a můžete obnovovat jednotlivé soubory i objekty i5/OS.

### **Vzdálená správa a analýza problémů**

- Do operačního systému i5/OS se lze přihlásit ze vzdáleného systému a integrovaný server vypnout nebo restartovat.
- Zrcadlení informací protokolu událostí integrovaného serveru do operačního systému i5/OS umožňuje provádět analýzu chyb systému Microsoft Windows ve vzdáleném systému.

### **| Server xSeries připojený pomocí adaptéru IXA (Integrated xSeries Adapter) nebo iSCSI HBA**

- Při konfiguraci standardního plného serveru xSeries máte podstatně větší flexibilitu než při konfiguraci serveru IXS, tj. xSeries na kartě.
- Standardní modely xSeries jsou vydávány častěji, což znamená, že můžete získat nejnovější procesory Intel i další hardware.
- Pro standardní plné servery xSeries je k dispozici více karet s komponentou PCI než pro servery IXS.

### **| Server IBM BladeCenter připojený pomocí adaptéru iSCSI HBA**

- | • Balení serveru IBM BladeCenter s vysokou hustotou.
- | • Nové modely serveru IBM BladeCenter jsou vydávány častěji než server IXS.

### **Vícenásobné servery**

- Služba Microsoft Cluster Service umožňuje zapojit několik serverů do klastrů. Klastry serverů zajišťují vysokou dostupnost a snadnou správu dat a programů prováděných v rámci klastru.
- Bez použití hardwaru sítě LAN mají servery a logické části spuštěné na stejném serveru iSeries vysoce výkonnou, zabezpečenou komunikaci ve virtuální síti.
- Na jediném serveru iSeries můžete spustit několik integrovaných serverů. Je to nejen vyhovující a efektivní, ale dává vám to i možnost snadno se přepnout na jiný server, který je nastavený a v provozu, pokud dojde k selhání hardwaru.
- Je-li na serveru iSeries nainstalováno několik integrovaných serverů, můžete definovat jejich role v doméně Windows tak, aby se zjednodušil zápis a přístup uživatelů. Například můžete nastavit jeden z těchto serverů jako řadič domény. Pak stačí jen zapsat uživatele do řadiče domény a uživatelé se budou moci přihlašovat z libovolného počítače se systémem Microsoft Windows v této doméně.
- Optické a páskové jednotky serveru iSeries mohou být sdíleny integrovanými servery na serveru iSeries.

### **| Podpora výměny za chodu**

- | • Integrace serverů a virtualizace paměti poskytují inovační možnosti, které zvyšují spolehlivost a obnovitelnost prostředí Windows serverů.
- | • Selže-li hardware Windows serveru, můžete snadno a rychle přepnout konfiguraci serveru na jiný připravený volný server xSeries nebo IBM BladeCenter, aniž by bylo nutné server iSeries restartovat. Tím lze snížit celkový počet PC serverů, který je nutný pro zajištění zvýšené dostupnosti.
- | • Podpora výměny za chodu zvyšuje také flexibilitu, protože umožňuje chránit několik provozních serverů pomocí jediného volného serveru.

---

## **Terminologie**

Níže uvedené termíny se týkají prostředí Windows na serveru iSeries. Další termíny a definice týkající se serveru iSeries najdete ve slovníčku v rámci aplikace Information Center.

| **Řadič BMC (Baseboard Management Controller)** Základní servisní procesor s nižší výkonností používaný k řízení systémů xSeries.

| **Certifikát** Standardní formát pro spojování identity s veřejným klíčem, který je podepsaný vydavatelem certifikátů a platí v zadaném období. Identita v certifikátu (nazývaná také "předmět" certifikátu) informuje o tom, komu a za jakým účelem byl certifikát vydán. Může mít celou řadu syntaxí, obvykle obsahuje rozlišovací jméno s atributy, jako jsou CN=společné jméno, O=organizace, OU=organizační jednotka. Veřejný klíč je součástí dvojice soukromý/veřejný klíč, obvykle té, která byla vytvořena pro použití s šifrovacím systémem veřejných klíčů RSA. Odpovídající soukromý klíč naopak není částí certifikátu a neměl by být zobrazován.

| **Vydavatel certifikátů** Dvojice soukromý klíč/certifikát, která může podepisovat ostatní certifikáty za účelem autentizace, může například určit, zda byl certifikát opravdu vydán uvedeným vydavatelem certifikátů. Vydavatele certifikátů může buď vlastnit jiná organizace (tzv. třetí strana), která ověřuje informace o identitě a vydává digitálně podepsané certifikáty, nebo může být tento vydavatel certifikátů lokální a soukromý. Digitálně podepsaný certifikát již nelze změnit, aniž by byla tato změna odhalena.

| **Protokol CHAP (Challenge Handshake Authentication Protocol)** Autentizační protokol, který zahrnuje šifrovací klíč známý jak straně, která autentizaci provádí, tak straně, jejíž autentizace je prováděna. Klíč je během přenosu chráněn před nasloucháním.

| **Konfigurace síťového serveru se zabezpečeným připojením** Objekt konfigurace v operačním systému i5/OS, pomocí kterého se konfiguruje hodnoty související se zabezpečením, které řídí způsob síťového zabezpečení dat sítě SCSI s adaptérem iSCSI HBA a virtuální sítě Ethernet. Příslušný typ objektu v operačním systému i5/OS je \*NWSCFG s podtypem \*CNNSEC. Pro tento objekt se také používá kratší termín **konfigurace zabezpečeného připojení**.

| **ID krytu** Sériové číslo, typ a model krytu (skříně), který obsahuje servisní procesor. U standardního serveru xSeries mají server, servisní procesor a server xSeries společný identifikátor krytu. ID krytu u serveru IBM BladeCenter označuje řídicí modul Management Module, který obsahuje jím řízené servery IBM BladeCenter.

**Mapování EIM (Enterprise Identity Mapping)** Mechanismus pro mapování/asociaci osoby nebo entity ke správným uživatelským identitám v rámci různých registrů několika operačních systémů. Funkce Administrace uživatelů integruje zápis uživatelů s mapováním EIM tím, že podporuje automatické vytváření zdrojových asociací EIM ve Windows. Zapsané uživatelské profily i5/OS též umožňují, aby uživatelské profily ve Windows byly jiné než uživatelské profily i5/OS, pokud administrátor ručně definoval zdrojové asociace EIM ve Windows.

**Identifikátor EIM** Představuje skutečnou osobu nebo entitu v mapování EIM. Když vytváříte identifikátor EIM, přiřazujete mu uživatelskou identitu dané osoby.

**Asociace identity v mapování EIM** Prostředí jediného přihlášení je umožněno asociací identity uživatele s identifikátorem EIM v registru. Existují tři typy asociace: zdrojová, cílová a administrační. Zápis uživatele se integruje s EIM, když je definována cílová asociace v operačním systému i5/OS a zdrojová ve Windows. Asociace se definují buď automaticky pomocí atributu uživatelského profilu EIMASSOC, nebo ručně pomocí produktu iSeries Navigator. Cílové asociace se používají především k zajištění existujících dat. Zdrojové asociace se používají především pro účely autentizace.

| **external network** Síť, k níž přistupují integrované servery přes fyzický síťový hardware. Viz také **Virtuální síť**.

| **Adaptér HBA (Host Bus Adapter)** Karta, která se připojuje ke sběrnici hostitelského systému. Například adaptér sítě Ethernet nebo adaptér sítě iSCSI.

| **Výměna za chodu** Výměna za chodu umožňuje mít připravenou rezervní sadu hardwaru serveru (například nečinný server IXS) jako zálohu pro jeden nebo více aktivních serverů. Selže-li hardware jednoho z aktivních serverů, lze tento server rychle přepnout z vadného hardwaru na připravený záložní hardware serveru a spustit jej znovu. Tím se významně sníží prostoje serverů, které obvykle selhání hardwaru serveru provázejí. Další informace najdete v tématu "Výměna hardwaru serveru za chodu" na stránce 148.

| **IBM Director** Aplikace, která zajišťuje zjišťování, řízení napájení a správu vzdálených serverů xSeries a IBM BladeCenter. Aplikace IBM Director je přístupná z produktu Virtualization Engine Standard Edition. V kontextu serverů iSeries připojených pomocí iSCSI se jedná o hostitelskou část aplikace IBM Director, která je spuštěna v logické části s operačním systémem i5/OS, která je hostitelem serverů připojených pomocí iSCSI.

**IBM i5/OS Integrated Server Support** Rozšíření operačního systému i5/OS na serveru iSeries, které umožňuje spolupráci tohoto serveru s integrovanými Windows a Linux servery. Jedna komponenta tohoto produktu je také spuštěna na integrovaném serveru.

**Integrovaný Windows server** Nazývá se také *integrováný server*. Instance serveru Windows 2000 Server či Windows Server 2003, která je spuštěna na serveru IXS, na serveru xSeries připojeném pomocí adaptéru IXA nebo na serveru xSeries či IBM BladeCenter připojeném pomocí adaptéru iSCSI HBA.

**Integrated xSeries Server (IXS)** (server IXS) PC (počítač na bázi procesoru Intel) na rozšiřující kartě PCI, která se instaluje do serveru iSeries.

**Integrated xSeries Adapter (IXA)** Rozšiřující karta PCI, která se instaluje do vybraných modelů serverů IBM eServer xSeries a zajišťuje vysokorychlostní propojení se serverem iSeries.

- | **Zabezpečení IPSec (Internet Protocol Security)** Šifruje přenosy v síti iSCSI.
- | **Výběrové vysílání IP** Přenos IP datagramu do sady systémů, které tvoří jednu skupinu výběrového vysílání.
- | **IPSec** Viz Zabezpečení IPSec.
- | **IQN** Viz Kvalifikované jméno iSCSI.
- | **iSCSI** Internetová síť SCSI. Zapouzdření protokolu SCSI v paketech TCP/IP. Poskytuje řešení vzájemné spolupráce, které využívá existující internetovou infrastrukturu, internetové prostředky správy a omezení vzdálenosti adres.
- | **Připojení iSCSI** Jedná se o připojení TCP. Komunikace mezi iniciátorem a cílem prochází přes jedno nebo více připojení TCP.
- | **Adaptér iniciátoru iSCSI** Adaptér HBA, který iniciuje požadavky iSCSI. Iniciátor iSCSI vydá příkazy SCSI, kterými požaduje služby od komponent a logických jednotek serveru známého pod názvem **cílový**. Iniciátorem iSCSI je adaptér iSCSI HBA na serveru xSeries nebo BladeCenter.
- | **Kvalifikované jméno iSCSI (IQN)** Jednoznačné jméno, které označuje cílový adaptér iSCSI nebo adaptér iniciátoru iSCSI podle definice standardu iSCSI (RFC 3722).
- | **Cílový adaptér iSCSI** Adaptér HBA, který obsluhuje požadavky iniciátoru iSCSI. Cílový adaptér iSCSI slouží jako řadič paměti, který je hostitelem logických jednotek (LUN). V kontextu serverů iSeries připojených pomocí iSCSI je cílovým adaptérem iSCSI adaptér iSCSI HBA pro server iSeries.
- | **Kerberos** Síťový bezpečnostní protokol vytvořený v ústavu MIT. Poskytuje nástroje pro autentizaci a kvalitní šifrování v síti a pomáhá zabezpečit informační systémy celého podniku. Produkt iSeries Navigator zajišťuje přihlášení autentizované protokolem Kerberos. Administrace uživatelů podporuje prostředí s jedním přihlášením tím, že v operačním systému i5/OS dovoluje definovat hesla uživatelských profilů s hodnotou \*NONE a zapsaným uživatelům ve Windows dovoluje nastavit jejich hesla. Tato podpora je poskytována, když je atribut zapsaného uživatelského profilu zadán jako LCLPWDMGT(\*NO).
- | **Lokální rozhraní** Lokální rozhraní reprezentuje parametry konfigurace, které popisují cílový adaptér iSCSI umístěný na serveru iSeries.
- | **Protokol MAC** Viz MAC (Media Access Control).
- | **Management Module** Servisní procesor s vysokou účinností, který ovládá skříň serveru IBM BladeCenter a jednotlivé servery v této skříni.
- | **MAC (Media Access Control)** Protokol v síti LAN, který určuje přístup jednotlivých zařízení k přenosovému médium v daném čase.
- | **Služba MSCS (Microsoft Windows Cluster Service)** Služba v systému Microsoft Windows, která propojuje jednotlivé servery, aby mohly plnit společné úkoly.
- | **Konfigurace síťového serveru (NWSCFG)** Objekt konfigurace v operačním systému i5/OS, který popisuje atributy použité vzdáleným integrovaným serverem připojeným pomocí iSCSI. Mezi tyto atributy patří vzdálený systém (\*RMTSYS), servisní procesor ve vzdáleném systému (\*SRVPRC) a hodnoty zabezpečení konfigurace použité pro komunikaci se serverem (\*CNNSEC). Typ příslušného objektu v operačním systému i5/OS je \*NWSCFG.
- | **network server description (NWSD)** Objekt konfigurace v operačním systému i5/OS, který popisuje integrovaný server. Typ příslušného objektu v operačním systému i5/OS je \*NWSD.
- | **Adaptér NWSH (Network Server Host Adapter)** Objekt konfigurace v operačním systému i5/OS, který obsahuje informace o konfiguraci zařízení s adaptérem iSCSI HBA na serveru iSeries. Typ příslušného objektu v operačním systému i5/OS je \*NWSH.

**Paměťový prostor síťového serveru (NWSSTG)** Disková paměť operačního systému i5/OS přidělená integrovanému serveru.

| **NWSH** Viz Adaptér NWSH.

**Dvoubodová virtuální síť Ethernet** Virtuální síť Ethernet konfigurovaná mezi serverem iSeries a integrovaným Windows serverem během jeho instalace. Takové spojení se používá pro komunikaci mezi iSeries a integrovaným serverem.

| **Vzdálené rozhraní** Vzdálené rozhraní reprezentuje parametry konfigurace, které popisují adaptér iniciátoru iSCSI umístěný na serveru xSeries nebo IBM BladeCenter. Vzdálené rozhraní zahrnuje parametry pro funkce adaptéru jak v síti SCSI, tak i v síti LAN.

| **ID vzdáleného systému** Sériové číslo, typ a model serveru xSeries nebo serveru IBM BladeCenter. U standardního serveru xSeries sdílí servisní procesor se serverem xSeries společný identifikátor. U serveru IBM BladeCenter tento identifikátor označuje server v rámci skříně.

| **Konfigurace síťového serveru ve vzdáleném systému** Objekt konfigurace v operačním systému i5/OS, pomocí kterého se konfiguruje atributy specifické pro určitý server xSeries nebo IBM BladeCenter. Obsahuje informace potřebné k identifikaci a zavedení vzdáleného systému a informace o adaptérech iniciátoru iSCSI, které vzdálený systém používá. Příslušný typ objektu v operačním systému i5/OS je \*NWSCFG s podtypem \*RMTSYS. Pro tento objekt se také používá kratší termín **konfigurace vzdáleného systému**.

| **Adaptér RSA (Remote Supervisor Adapter)** Servisní procesor s vysokou účinností, který řídí systémy xSeries.

| **Servisní procesor** Procesor, který je oddělený od hlavního procesoru systému. Servisní procesor řídí napájení systému a provádí další administrační a diagnostické funkce. Se systémy xSeries a IBM BladeCenter můžete použít několik různých typů servisních procesorů. Viz **Adaptér RSA, Řadič BMC a Management Module**.

| **Konfigurace síťového serveru se servisním procesorem** Objekt konfigurace v operačním systému i5/OS, který uchovává sadu parametrů, které se vztahují k servisnímu procesoru ve vzdáleném systému. V případě serverů IBM BladeCenter je objektem konfigurace kryt serveru IBM BladeCenter. Příslušný typ objektu v operačním systému i5/OS je \*NWSCFG s podtypem SRVPRC. Pro tento objekt se také používá kratší termín **konfigurace servisního procesoru**.

| **Cesta paměťovým prostorům** Cesta k paměťovým prostorům definuje adaptér NWSH, který mohou paměťové prostory používat, a pravidlo zabezpečení IP, které má zabezpečit datové přenosy.

| **Cílový uzel** Objekt firmwaru sítě iSCSI na serveru iSeries, který spravuje relace a připojení sítě iSCSI.

| **Unicast** Přenos dat do jednoho místa určení.

**virtual network** Síť Ethernet emulovaná na serveru iSeries, která umožňuje vytvářet sítě mezi logickými částmi s operačním systémem i5/OS, logickými částmi s operačním systémem Linux a integrovanými Windows servery.

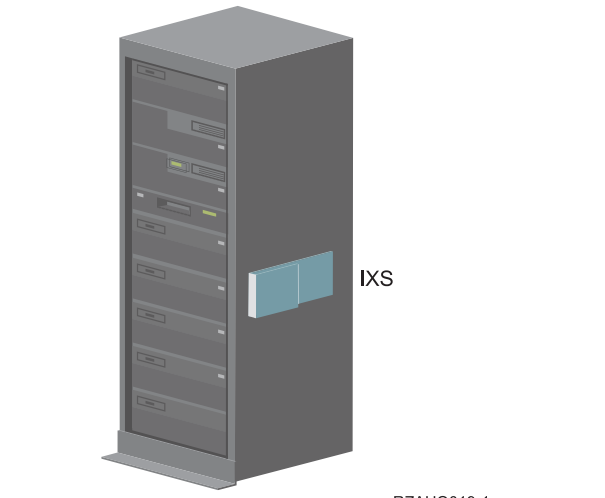
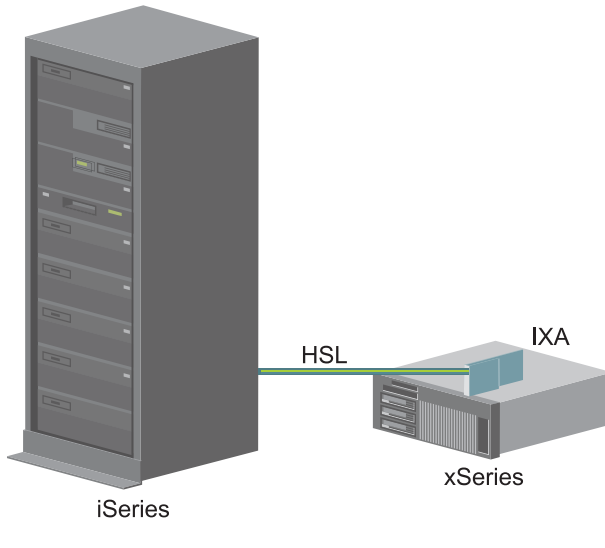
**Windows server** Microsoft Windows 2000 Server nebo Windows Server 2003

| **Služba VSCS (Volume Shadow Copy Service) na serveru Windows Server 2003** Podpora, která umožňuje zálohování dat aplikace bez ukončení této aplikace. Tato služba zvyšuje dostupnost aplikací.

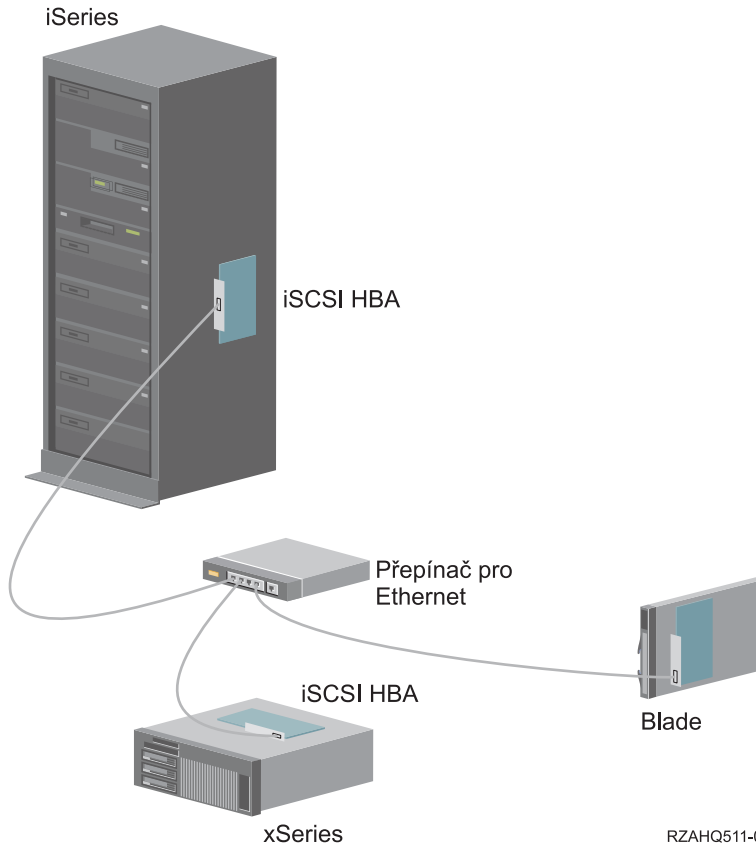


## Koncepce týkající se hardwaru

- | Servery iSeries podporují několik konfigurací hardwaru, které dovolují integraci serverů IBM xSeries a BladeCenter.
- | Níže uvedená tabulka uvádí základní rozdíly mezi serverem IXS (Integrated xSeries Server), serverem xSeries
- | připojeným pomocí IXA (Integrated xSeries Adapter) a serverem připojeným pomocí iSCSI.

Porovnání serverů IXS a serverů xSeries připojených pomocí adaptérů IXA a iSCSI HBA	
 <p>iSeries</p> <p>IXS</p> <p>RZAHQ019-1</p>	<p>Server IXS je PC Server bez disku s procesorem a pamětí, které jsou nainstalovány na serveru iSeries.</p>
 <p>iSeries</p> <p>HSL</p> <p>IXA</p> <p>xSeries</p> <p>RZAHQ020-1</p>	<p>Adaptér IXA je adaptér sběrnice typu HSL (high-speed link) zapojený do podporovaného serveru xSeries. Server xSeries se jeví jako rozšiřující jednotka připojená pomocí linky HSL k serveru iSeries.</p>

## Porovnání serverů IXS a serverů xSeries připojených pomocí adaptérů IXA a iSCSI HBA



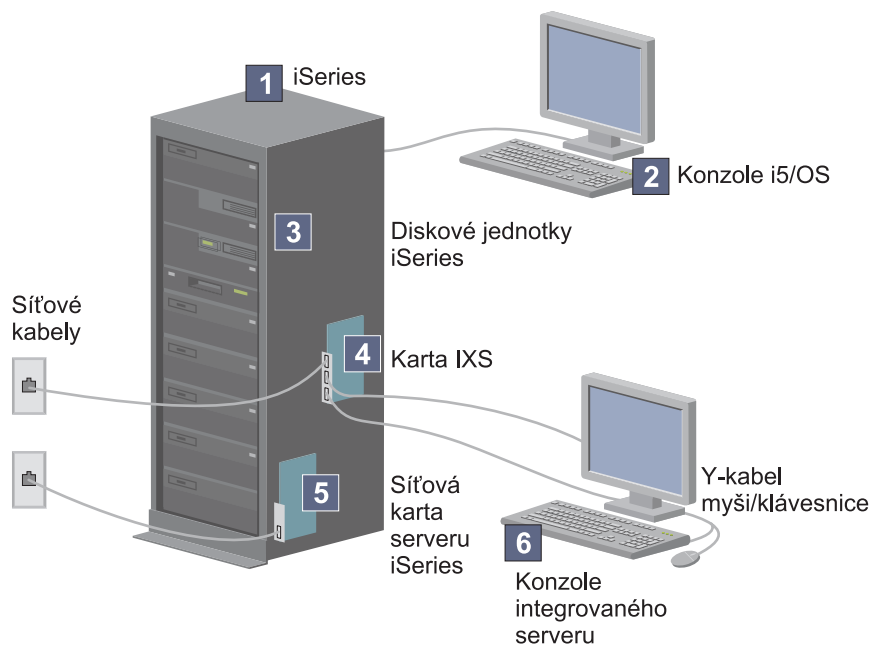
Technologie iSCSI připojuje jak servery xSeries bez disků, tak servery IBM BladeCenter k systémům iSeries prostřednictvím sítě Ethernet, které jsou nízkorozpočtové a rozšiřitelné. Adaptéry iSCSI HBA jsou na serveru iSeries v každém zúčastněném serveru xSeries a IBM BladeCenter.

## Servery IXS a servery připojené pomocí adaptéru IXA

### Typická instalace serveru IXS

Níže uvedený obrázek znázorňuje typickou instalaci serveru IXS.





RZAHQ025-0

Obrázek 2. Typická instalace serveru IXS

1. Potřebujete kompatibilní server iSeries. (Informace o kompatibilitě najdete v tématu “Hardwarové požadavky” na stránce 55.)
2. Konzole i5/OS, z níž se připojujete k serveru iSeries v prostředí produktu iSeries Navigator nebo ve znakovém rozhraní, je zde zobrazena proto, aby byl vidět rozdíl mezi touto konzolí a konzolí integrovaného serveru.
3. Integrovaný server nemusí mít vlastní diskovou jednotku. Operační systém i5/OS emuluje prostor na jednotce pevného disku, které může integrovaný server používat na pevných discích serveru iSeries.
4. Karta IXS je procesor typu Intel s vlastní pamětí RAM a je nasazená na desku PCI a zapojená do rozšiřujícího slotu serveru iSeries. Karta IXS fyzicky zabírá dva sloty.
5. Typický server iSeries má síťovou kartu.
6. Konzole integrovaného serveru vám umožňuje komunikovat s integrovaným serverem. Konzole integrovaného serveru se může skládat z monitoru, klávesnice a myši, které jsou přímo připojeny ke kartě IXS. Další informace o typech konzolí integrovaného serveru najdete v tématu “Konzole Windows” na stránce 23.

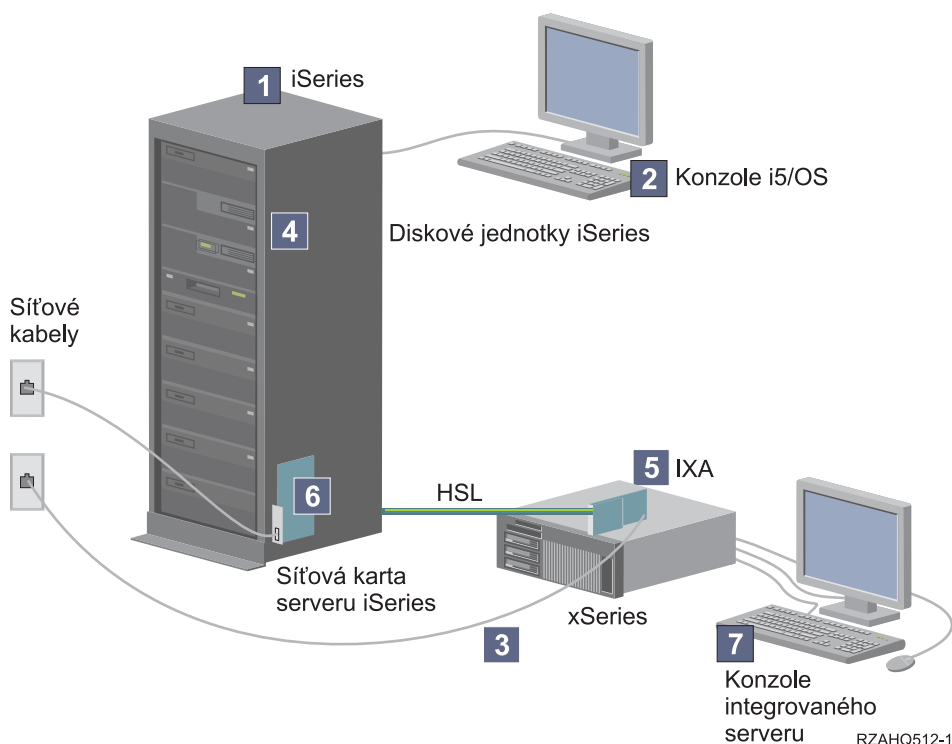
**Poznámka:** V závislosti na typu karty IXS existují různé způsoby zajišťování propojitelnosti sítě. Některé typy procesorů IXS mohou “převzít” sousední sloty PCI, čímž umožní procesoru IXS kontrolu nad síťovou kartou iSeries (viz “Hardwarové požadavky” na stránce 55, kde naleznete informace o tom, které síťové karty jsou podporovány). Tímto způsobem můžete nainstalovat až tři síťové karty. Jiné typy karet IXS mají integrované síťové řadiče a nepodporují síťové karty v sousedních slotech.

#### Typická instalace serveru připojeného pomocí adaptéru IXA

Integrované servery připojené pomocí adaptéru IXA jsou standardní modely serverů xSeries, které obsahují procesory, paměť, rozšiřující karty, ale žádné disky. Veškerý diskový prostor se nachází na serveru iSeries a je spravován stejně jako u modelů IXS.

Postup při instalaci integrovaného Windows serveru připojeného pomocí adaptéru IXA je téměř identický jako pro integrovaný server IXS. Hlavní rozdíl mezi nimi spočívá v tom, že aktualizované možnosti nových serverů xSeries jsou rychleji dávány k dispozici, protože se tyto servery vydávají častěji než servery IXS. Servery xSeries připojené pomocí adaptéru IXA mají navíc vlastní rozšiřující sloty, jejich rozšiřitelnost je tedy mnohem vyšší než u serverů IXS.

l Níže uvedený obrázek znázorňuje typickou instalaci serveru připojeného pomocí IXA.



Obrázek 3. Typická instalace serveru připojeného pomocí adaptéru IXA

1. Potřebujete kompatibilní server iSeries. (Informace o kompatibilitě najdete v tématu “Hardwarové požadavky” na stránce 55.)
2. Konzole i5/OS, z níž se připojujete k serveru iSeries v prostředí produktu iSeries Navigator nebo ve znakovém rozhraní, je zde zobrazena proto, aby byl vidět rozdíl mezi touto konzolí a konzolí integrovaného serveru.
3. Typický server xSeries má alespoň jeden řadič integrované sítě. K většině serverů xSeries lze přidat další síťové karty a zvýšit tak jejich propojitelnost v síti. Informace o kompatibilitě síťových karet pro server xSeries najdete na webové stránce Integrated xSeries solutions.
4. Server xSeries připojený pomocí adaptéru IXA nemá vlastní diskovou jednotku. Operační systém i5/OS emuluje prostor na jednotce pevného disku, které může integrovaný server používat na pevných discích serveru iSeries.
5. Karta IXA se zapojuje do zvláštního slotu serveru xSeries a je připojena k serveru iSeries kabely typu HSL.
6. Typický server iSeries má síťovou kartu.
7. Konzole integrovaného serveru vám umožňuje komunikovat se serverem xSeries připojeným pomocí adaptéru IXA. Konzole integrovaného serveru se může skládat z monitoru, klávesnice a myši, které jsou přímo připojeny k serveru xSeries. Další informace o typech konzolí integrovaného serveru najdete v tématu “Konzole Windows” na stránce 23.

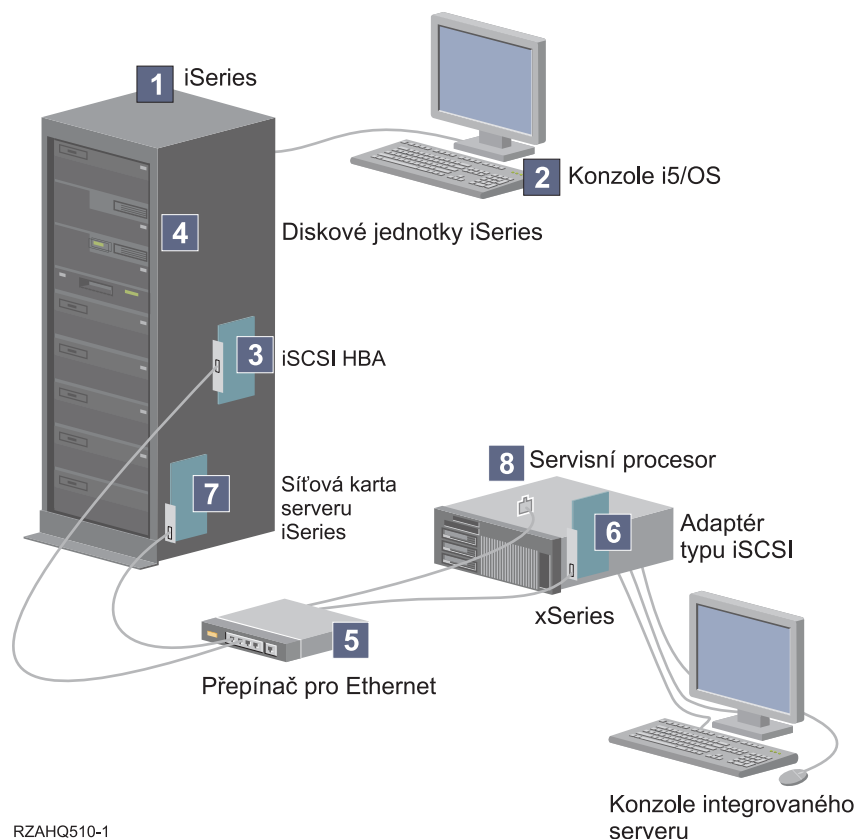
## l Servery připojené pomocí iSCSI

### l Typická instalace serverů IBM xSeries a BladeCenter

l Servery připojené pomocí iSCSI jsou standardní modely serverů xSeries nebo IBM BladeCenter, které mají procesory, paměť a rozšiřující karty, ale nemají disky. Veškerý diskový prostor je umístěn na serveru iSeries a je spravován stejně jako u IXS a modelů IXA.

Instalační procedura integrovaných Windows serverů připojených pomocí iSCSI vyžaduje hardware, který musí být instalován a konfigurován na serveru iSeries a na serverech xSeries a IBM BladeCenter. Tak jako u serverů připojených pomocí adaptéru IXA, mají také servery xSeries připojené pomocí iSCSI HBA vlastní rozšiřující sloty. Je tedy možné instalovat další doplňky a rozšířit tak možnosti serveru.


Níže uvedený obrázek znázorňuje typickou instalaci s adaptérem iSCSI HBA:



RZAHQ510-1

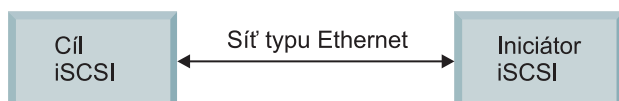
Obrázek 4. Typická instalace serveru připojeného pomocí iSCSI nebo serveru IBM BladeCenter

1. Potřebujete kompatibilní server iSeries. Informace o kompatibilitě najdete v tématu “Hardwarové požadavky” na stránce 55.
2. Konzole i5/OS, z níž se připojujete k serveru iSeries v prostředí produktu iSeries Navigator nebo ve znakovém rozhraní, je zde zobrazena proto, aby byl vidět rozdíl mezi touto konzolí a konzolí integrovaného serveru.
3. V závislosti na typu fyzické sítě jsou k dispozici adaptéry iSCSI HBA z mědi nebo optických vláken. Adaptér iSCSI slouží jako cílové zařízení a připojuje se k síti Ethernet pomocí standardních kabelů Ethernet.
4. Integrovaný server nemusí mít vlastní diskovou jednotku. Operační systém i5/OS emuluje prostor na pevném disku, které může používat na jednotce pevného disku serveru iSeries. Přístup k těmto jednotkám a dalším paměťovým zařízením serveru iSeries zajišťuje adaptér iSCSI HBA.
5. Síťové kabely iSCSI HBA jsou připojeny k standardnímu přepínači typu Gigabit Ethernet.
6. Pro server xSeries je vyžadován další adaptér iSCSI HBA. Tento adaptér zajišťuje připojení k adaptéru iSCSI HBA pro server iSeries. Tento adaptér je ze serveru xSeries vidět jako paměťový adaptér, kde se nacházejí disky v rámci celé sítě.
7. Typický server iSeries má síťovou kartu. Při zjišťování a správě vzdálených serverů xSeries a IBM BladeCenter vyžaduje IBM Director připojení serveru iSeries do sítě LAN.
8. Servisní procesor dovoluje serveru iSeries zjišťovat a spravovat vzdálený systém. Servisním procesorem může být adaptér RSA II, řadič BMC nebo Management Module serverů IBM BladeCenter. RSA II, BMC a Management Module jsou připojeny k serveru iSeries přes síť Ethernet.

| Další informace o hardwaru najdete na webových stránkách IBM iSeries Integrated xSeries solutions   
| ([www.ibm.com/servers/eserver/series/integratedxseries](http://www.ibm.com/servers/eserver/series/integratedxseries))

## | **Přehled serverů připojených pomocí iSCSI**

| Základní síť iSCSI se skládá z cílového adaptéru iSCSI (adaptéru iSCSI HBA instalovaného na serveru iSeries)  
| a adaptéru iniciátoru iSCSI (adaptéru iSCSI HBA, který je instalován na serveru xSeries nebo IBM BladeCenter).  
| Cílové zařízení i zařízení iniciátoru je připojeno přes síť Ethernet LAN. Adaptér iSCSI HBA pro server iSeries zajišťuje  
| paměťová zařízení a zařízení s vyjímatelnými médii pro síť iSCSI. Obrázek 5 znázorňuje základní síť iSCSI.



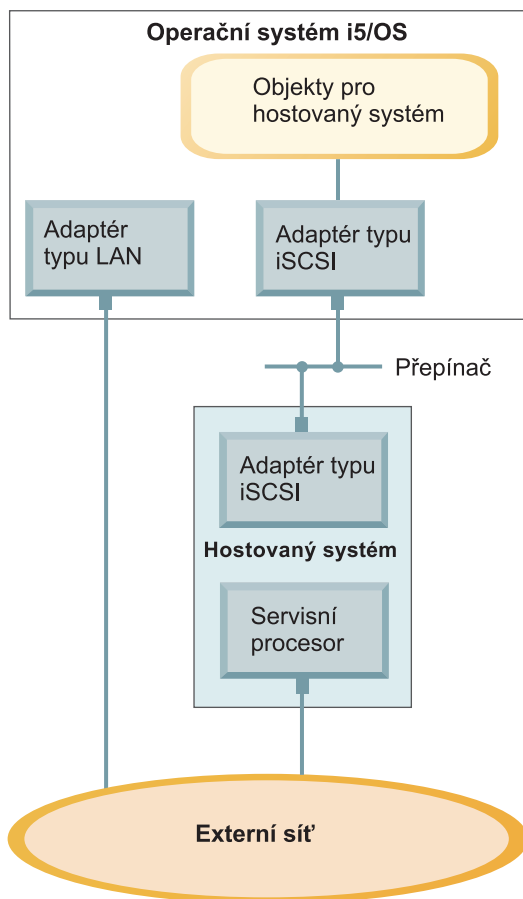
RZAHQ509-0

| *Obrázek 5. Základní koncepce sítě iSCSI*

| Cílový adaptér a adaptér iniciátoru iSCSI musejí být konfigurovány pomocí příkazů vydaných na serveru iSeries. Síť  
| iSCSI je používána pouze pro provoz iSCSI HBA.

## | **Základní podpora jednoho serveru**

| Chcete-li servery xSeries a IBM BladeCenter připojit prostřednictvím iSCSI k serveru iSeries, nebo chcete-li je  
| prostřednictvím iSCSI hostovat v tomto operačním systému, musí být jak v systému iSeries, tak v hostovaném  
| systému nainstalován potřebný hardware. Hardwarem potřebným na obou koncích je adaptér iSCSI HBA nebo adaptér  
| iSCSI. Tyto dva adaptéry jsou připojeny přes přepínač typu Ethernet pomocí standardních kabelů Ethernet.  
| Nejjednodušší způsob fyzického připojení mezi hostovaným systémem a serverem iSeries znázorňuje Obrázek 6  
| na stránce 19.



RZAHQ501-1

Obrázek 6. Jeden server připojený pomocí iSCSI

Server xSeries nebo IBM BladeCenter (hostovaný systém) má nainstalován adaptér iniciátoru iSCSI HBA. Tento adaptér má rozhraní sítě Ethernet a je připojen k cílovému adaptéru iSCSI HBA instalovanému na serveru iSeries přes přepínač typu Ethernet. Hostovaným systémem je server bez disku. Hostitelem nebo poskytovatelem virtuálních disků a virtuálních zařízení s vyjímatelnými médii je adaptér iSCSI HBA pro server iSeries. Příkazy SCSI pro přístup k těmto zařízením jsou zabaleny v rámci TCP/IP a jsou z hostovaného systému do adaptéru iSCSI HBA pro server iSeries přenášeny přes síť Ethernet. Tento režim komunikace je znám pod názvem Internet SCSI nebo iSCSI.

Servery připojené pomocí iSCSI jsou konfigurovány v objektech operačního systému i5/OS. Další informace o těchto objektech najdete v tématu "Koncepte týkající se softwaru" na stránce 35.

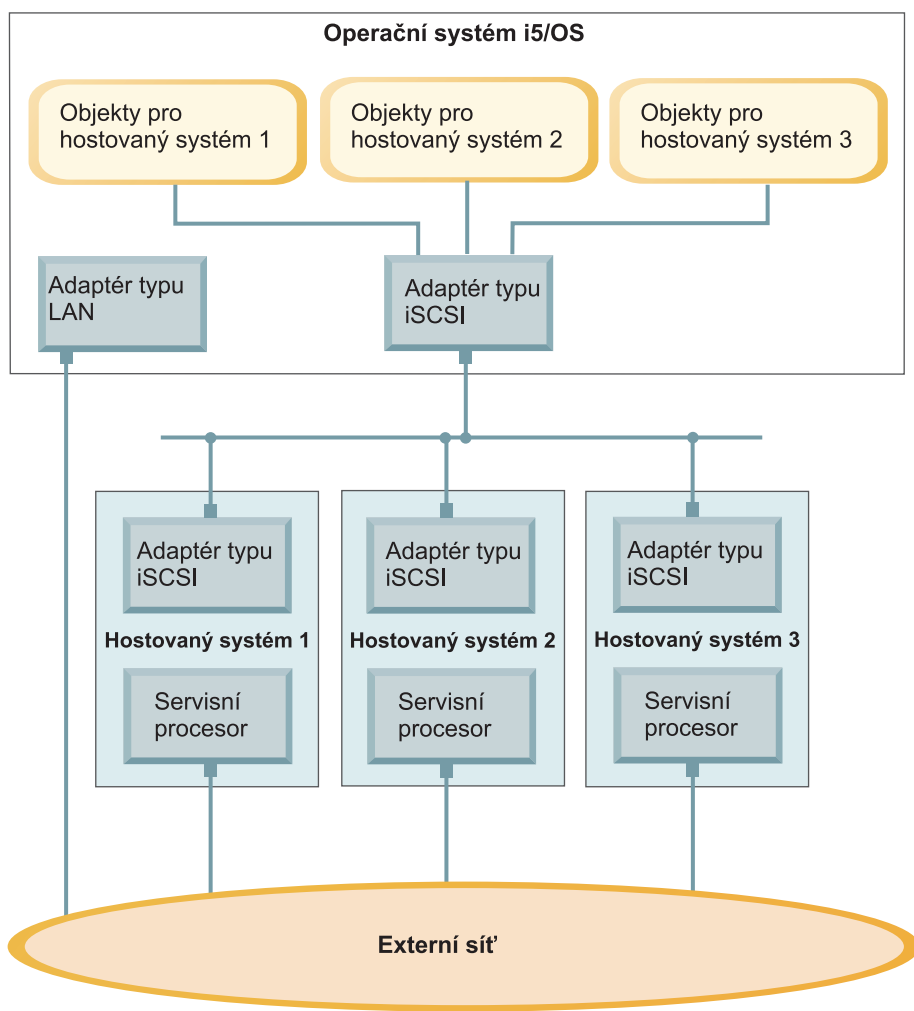
Operační systém i5/OS může vyhledávat a spravovat vzdálené systémy odesláním příkazů servisnímu procesoru ke vzdálenému systému přes síť Ethernet. Tyto funkce jsou prováděny pomocí produktu IBM Director, který musí být instalován a spuštěn ve všech logických částech, které jsou připojeny k adaptérům iSCSI HBA. Další informace najdete v tématu "Zjišťování vzdálených serverů a jejich správa" na stránce 134.

Obrázek 6 znázorňuje dvě odlišené sítě. Síť iSCSI používá izolovaný přepínač. Připojení servisního procesoru je realizováno přes externí síť (sdílenou síť). Dvě odlišené sítě však nejsou vyžadovány. Připojení servisního procesoru by například mohlo používat stejný izolovaný přepínač jako síť iSCSI. Toto připojení představuje jeden ze způsobů zabezpečeného připojení servisního procesoru. Adaptér sítě LAN v operačním systému i5/OS by pak ale nebyl dostupný dalším aplikacím v externí síti.

Oba typy sítí by měly být zabezpečeny. Další informace o zabezpečení serverů připojených pomocí iSCSI najdete v tématu "Koncepte zabezpečení" na stránce 46.

## Podpora více serverů

Jediný adaptér iSCSI HBA pro server iSeries může být hostitelem několika serverů xSeries a IBM BladeCenter. Toto pojetí znázorňuje Obrázek 7.



RZAHQ502-3

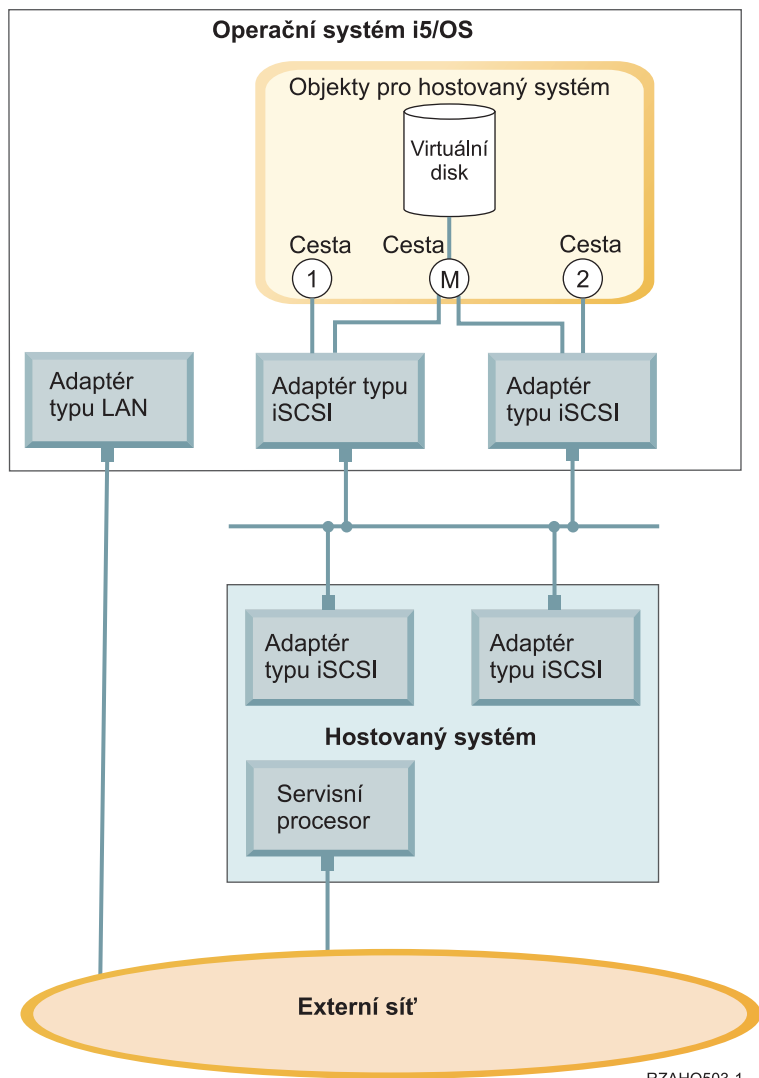
Obrázek 7. Několik serverů připojených pomocí iSCSI

Každý hostovaný systém vyžaduje, aby byl na serveru instalován alespoň jeden adaptér iSCSI HBA. Každý adaptér iSCSI HBA v hostovaném systému je připojen k adaptéru iSCSI HBA pro server iSeries přes síť Ethernet. Tato síť může být fyzicky zabezpečená nebo izolovaná, pokud bude model zabezpečení implementován fyzicky. V operačním systému i5/OS bude každý z hostovaných nebo vzdálených systémů reprezentován sadou objektů. Tyto objekty jsou podrobněji popsány v tématu “Koncepte týkající se softwaru” na stránce 35.

Každý hostovaný systém musí mít nainstalovaný servisní procesor pro vzdálené zjišťování a správu napájení. Několik servisních procesorů může být připojeno k jednomu adaptéru sítě LAN serveru iSeries přes externí síť.

## Rozšířená podpora sítě iSCSI

Jeden adaptér iSCSI HBA pro server iSeries může podporovat několik serverů nebo hostovaných systémů. Každý hostovaný systém může být také připojen k několika adaptérům iSCSI HBA pro server iSeries. Obrázek 8 na stránce 21 znázorňuje hostovaný systém, který je připojen k více než jednomu adaptéru iSCSI HBA pro server iSeries.



RZAHQ503-1

Obrázek 8. Rozšířená konfigurace

Obrázek 8 znázorňuje několik adaptérů iSCSI HBA nainstalovaných v hostovaném systému.

### Definice cesty

Je-li hostovaný systém připojen k adaptéru iSCSI HBA pro server iSeries, je definována cesta mezi hostovaným systémem a adaptérem iSCSI HBA pro server iSeries.

Obrázek 8 znázorňuje několik odlišných cest. Jsou označeny 1, 2 a M.

O virtuálním zařízení, jehož hostitelem je server iSeries, se říká, že se nachází mimo dosah cesty. Konfigurovaný virtuální disk (například jednotka C:), jehož hostitelem je operační systém i5/OS přes adaptér iSCSI HBA pro server iSeries nebo adaptér NWSH, je mimo dosah tohoto adaptéru NWSH.

Obrázek 8 ukazuje, že každá z cest 1 a 2 je definována pro samostatný adaptér iSCSI HBA pro server iSeries. Zařízení definovaná v cestě 1 se mohou nacházet pouze mimo dosah adaptéru iSCSI, kde je cesta definována. Podobně zařízení definovaná v cestě 2 se mohou nacházet pouze mimo dosah adaptéru iSCSI, kde je cesta definována. O libovolných zařízeních, která jsou definována mimo dosah cest 1 a 2, se říká, že se nacházejí výhradně mimo dosah svých specifických adaptérů iSCSI HBA.

## Úvod do vícenásobných cest

Hostovaný systém může mít rezervní cesty pro přístup k virtuálním diskům, jejichž hostitelem je operační systém i5/OS. Nejsložitější je případ rezervní cesty na každém konci. K danému virtuálnímu disku lze přistupovat z hostovaného systému pomocí libovolného ze dvou adaptérů iSCSI HBA instalovaných v hostovaném systému a nacházejících se na serveru iSeries, který používá libovolný z obou adaptérů iSCSI HBA pro server iSeries. To je známo pod názvem vícenásobná cesta.

Obrázek 8 na stránce 21 znázorňuje vícenásobnou cestu definovanou jako M. K virtuálním diskům nacházejícím se mimo dosah vícenásobné cesty lze přistupovat pomocí obou adaptérů iSCSI HBA, které jsou instalovány na serveru iSeries. Vícenásobná cesta je definována jako skupina adaptérů iSCSI HBA pro server iSeries, která má přístup k cestě M nebo ji může používat. Lze definovat pouze jednu vícenásobnou cestu na hostovaný systém. Tato skupina může obsahovat i více adaptérů iSCSI HBA pro server iSeries.

**Poznámka:** Zařízení s vyjímatelnými médii nemohou být ve vícenásobné cestě definována.

## Vyhrazená šířka pásma

V některých případech nejsou rezervní cesty vyžadovány, ale virtuální disky, které vyžadují vyšší výkon, mohou potřebovat vyhrazenou cestu.


Obrázek 8 na stránce 21 znázorňuje konfiguraci hostovaného systému, ve které lze definovat virtuální disky mimo dosah cesty 1 a 2, a nikoli mimo dosah cesty M. Tímto způsobem může být určitým virtuálním diskům vyhrazena šířka pásma adaptéru iSCSI.

## Zavádění systému bez disku přes iSCS

Všechny samostatné servery připojené pomocí iSCSI a servery IBM BladeCenter jsou bez disku a vyžadují jako zaváděcí zařízení adaptér iSCSI HBA na serveru xSeries nebo na serveru IBM BladeCenter.

Jak konfigurace vzdáleného systému i5/OS, tak adaptér iSCSI HBA vzdáleného serveru musejí být konfigurovány dříve, než začnete nový integrovaný Windows server instalovat nebo používat. Další informace najdete v tématu “Konfigurace vzdáleného systému” na stránce 41.

Adaptér iSCSI HBA musí být konfigurován během procesu zavádění systému na serveru xSeries nebo IBM BladeCenter pomocí obslužného programu CTRL-Q tohoto adaptéru. Doporučuje se, aby byl konfigurován jako součást výchozího nastavení serveru. V adaptéru iSCSI HBA na hostovaném serveru musí být konfigurována minimální sada parametrů. Tyto parametry se musejí shodovat s odpovídajícími parametry konfigurovanými v objektu konfigurace vzdáleného systému. Parametry se liší v závislosti na vybraném režimu zavádění.

Podrobnější informace o tom, jak konfigurovat hostovaný systém adaptéru iSCSI HBA jako zaváděcí zařízení iSCSI, najdete na webové stránce iSCSI install read me first . Podrobnosti o způsobu konfigurace sady parametrů v objektu konfigurace vzdáleného systému najdete v tématu “Změna vlastností konfigurace vzdáleného systému” na stránce 117.

## Povolení zaváděcího zařízení hostovaného serveru

Adaptér iSCSI HBA instalovaný na serveru xSeries nebo IBM BladeCenter funguje během procesu zavádění systému jako zaváděcí zařízení na základě konfigurovaných parametrů.

Pokud má server xSeries pouze jeden adaptér iSCSI HBA, musí být tento adaptér konfigurován jako zaváděcí zařízení. Zavádění systému pomocí iSCSI je v předvoleném nastavení povoleno na všech adaptérech iSCSI HBA, musíte ale konfigurovat další informace.

Pokud má server xSeries několik nainstalovaných adaptérů iSCSI HBA, stačí, aby byl jako zaváděcí zařízení konfigurován pouze jeden z nich.



l Adaptér iSCSI HBA serveru IBM BladeCenter má adaptér s duálním portem. Stačí, aby byl jako zaváděcí zařízení konfigurován pouze jeden port.

### l **Režimy a parametry zavádění systému**

l Řešení iSeries iSCSI podporuje různé režimy zavádění systému. V závislosti na vybraném režimu zavádění systému musejí být v hostitelském systému adaptéru iSCSI HBA konfigurovány různé zaváděcí parametry.

l Tyto parametry jsou konfigurovány pomocí obslužného programu CTRL-Q tohoto adaptéru. Zaváděcí zařízení je nutné vybrat a konfigurovat při první instalaci serveru. Doporučuje se, aby požadované parametry byly konfigurovány jako součást tohoto procesu výchozího nastavení.

### l **Integrovaný server DHCP**

l Při konfiguraci serveru připojeného pomocí iSCSI pro použití předvoleného zaváděcího režimu nebo zaváděcího režimu DHCP používá tento server integrovaný server DHCP. Integrovaný server DHCP není server pro obecné účely. Je určen výhradně pro instalaci zaváděcích parametrů do adaptéru iSCSI HBA na hostovaném serveru. Tento server je automaticky konfigurován při logickém zapnutí objektu NWSD s parametry, které poskytuje konfigurace vzdáleného systému. Další informace najdete v tématu “Integrovaný server DHC” na stránce 133.

## **Konzole Windows**

S integrovaným serverem komunikujete pomocí konzole Windows. Podle hardwarové a softwarové konfigurace můžete používat monitor, klávesnici a myš, které jsou připojeny jednou z níže uvedených metod:

### l **Přímo připojený monitor, klávesnice a myš**

l Můžete používat monitor, klávesnici a myš, které jsou přímo připojeny ke kartě IXS, serveru xSeries připojenému pomocí adaptéru IXA nebo k serveru xSeries nebo BladeCenter připojenému pomocí iSCSI, a tvoří tak konzoli integrovaného serveru. Prostřednictvím těchto zařízení komunikujete s integrovaným serverem, přesně jako na standardním PC.

l Servery připojené pomocí iSCSI vyžadují některá předinstalační nastavení hardwaru. Tato nastavení jsou prováděna pomocí přímo připojeného monitoru, klávesnice a myši.


### **Aplikace pro vzdálené zobrazení pracovní plochy GUI**

l Chcete-li zobrazit pracovní plochu grafického uživatelského rozhraní (GUI) na vzdálené pracovní stanici, můžete použít aplikace, jako jsou například Microsoft Terminal Services, Remote Desktop nebo aplikace třetích stran. Většina administračních úloh, které jsou běžně prováděny na konzoli přímo připojené k serveru, může být prováděna na vzdálené pracovní ploše. Informace o tom, jak konfigurovat a používat vzdálenou pracovní plochu pro konzoli serveru, najdete v dokumentaci služby Microsoft Terminal Services nebo v dokumentaci dalších aplikací třetích stran.

### **Virtuální sériová konzole**

Operační systém i5/OS poskytuje možnost připojení k virtuální konzoli pro server IXS 4812. Tato možnost je podobná podpoře virtuální sériové konzole v operačním systému i5/OS, která je poskytována logickými částmi se systémem iSeries. Poskytuje konzoli v textovém režimu pro server IXS 4812 a je možné ji využít pro různé administrační úlohy, které nevyžadují přístup na pracovní plochu uživatelského grafického rozhraní (GUI). Informace o tom, jak vytvořit relaci s virtuální sériovou konzolí pro server IXS 4812, najdete v tématu “Připojení k virtuální sériové konzoli serveru IXS 4812” na stránce 143.

Virtuální sériová konzole je v současné době podporována pouze serverem Windows Server 2003. Je možné ji použít k monitorování chyb serveru nebo k obnovení komunikace se sítí LAN. Toto připojení konzole lze použít před konfigurací TCP/IP na serveru. Informace o úlohách, které je možné provádět pomocí virtuální

sériové konzole, najdete v dokumentu Microsoft Emergency Management Services  (www.microsoft.com/whdc/system/platform/server/default.mspx). Pamatujte si, že:

- Operační systém i5/OS provádí většinu konfigurace pro virtuální sériovou konzoli automaticky, takže některé z konfiguračních úloh uvedených v dokumentaci Microsoft nejsou pro virtuální sériovou konzoli operačního systému i5/OS nutné.

- Implementace iSeries nevyžaduje žádný dodatečný hardware, jako například modemy, koncentrátory nebo kabely, které jsou zmiňovány v dokumentaci firmy Microsoft.

## Přesměrování grafické konzole adaptéru RSA II

U serverů xSeries vybavených adaptérem RSA II poskytuje adaptér RSA II také úplné hardwarové přesměrování grafické konzole, to znamená, že přístup ke vzdálenému serveru a jeho řízení můžete provádět z lokální pracovní plochy.

---

## Pokyny

I když je integrovaný Windows server hodně podobný Windows serveru na bázi PC, existuje několik rozdílů, které byste měli vzít v úvahu:

- Nemusí být k dispozici disketová jednotka. To znamená, že nemůžete použít spouštěcí disketu ani opravnou disketu pro stav nouze. Můžete ale využít diskový prostor na serveru iSeries a zálohovat soubory nebo celý obraz disku.
- Páskové a diskové jednotky iSeries jsou k dispozici.
- Pro komunikaci TCP/IP se serverem iSeries nebo jinými integrovanými servery nejsou při vytváření virtuálních sítí potřebné adaptéry, kabely, rozbočovače ani přepínače pro síť LAN.
- Instalace operačního systému Microsoft Windows s prostředím Windows na server iSeries se liší od typické instalace PC serveru. Nejprve nainstalujte produkt IBM i5/OS Integrated Server Support, potom nainstalujte operační systém Microsoft Windows. Velkou část informací o konfiguraci zadáte v rámci příkazu INSWNTSVR (Instalace Windows serveru) operačního systému i5/OS, takže některé z panelů typické instalace se nezobrazí. Tento příkaz zahrnuje ještě další parametry, specifické pro integraci serveru s operačním systémem i5/OS, například synchronizace data a času.
- Na straně správy serverů v systému i5/OS je integrovaný Windows server reprezentován popisem síťového serveru (NWS) a síťová rozhraní jsou reprezentována popisy linek. Server můžete v operačním systému i5/OS restartovat logickým vypnutím a zapnutím objektu NWS.
- V operačním systému i5/OS můžete provádět mnoho úloh administrace uživatelů, například vytváření uživatelů Windows.
- Protože operační systém i5/OS spravuje paměť jinak než PC server (viz “Správa systému pro ukládání dat operačního systému i5/OS” na stránce 151), nejsou některé techniky potřebné pro administraci paměti na PC serveru pro integrované servery nutné.

---


## Výkon

Servery připojené pomocí IXS, IXA a iSCSI mají vlastní paměť a jeden nebo více procesorů, ale používají sdílený prostor na pevných discích serveru iSeries prostřednictvím virtuálních (simulovaných) diskových jednotek. Diskové jednotky jsou alokovány do Windows vytvořením objektu paměťového prostoru na serveru iSeries. Hlavní rozdíl mezi integrovanými servery a samostatnými servery spočívá v tom, že samostatné servery používají vyhrazené diskové jednotky a integrované servery používají paměťové prostory serveru iSeries jako virtuální disky. Integrované servery iSeries zahrnují také volitelné funkce, jako jsou například ovladače systému Windows pro sdílení páskových jednotek, jednotek CD a DVD serveru iSeries spolu s vysokorychlostními adaptéry virtuální sítě Ethernet.

Použití paměťových prostorů (virtuálních jednotek) serveru iSeries zajišťuje vyšší výkonnost, která obvykle nebývá k dispozici v prostředí samostatných serverů bez značných investic do systému pro ukládání dat a zvýšených nákladů na údržbu. Znamená to však některá omezení. Při plánování a konfiguraci integrovaných serverů byste měli vzít tato omezení v úvahu. Následující informace zdůrazňují některé faktory, které ovlivňují výkon.

Informace související s výkonem najdete v níže uvedených tématech:

- “Paměťové prostory a vyhrazené disky na serveru iSeries” na stránce 25
- “Rovnováha paměťových prostorů” na stránce 25
- “Výkon serverů připojených pomocí iSCSI” na stránce 26
- “Virtuální síť Ethernet” na stránce 27

- | • IBM iSeries Integrated xSeries solutions   
| ([www.ibm.com/servers/eserver/series/integratedxseries](http://www.ibm.com/servers/eserver/series/integratedxseries))
- | • iSeries Performance Management   
| ([www.ibm.com/eserver/series/perfmgmt](http://www.ibm.com/eserver/series/perfmgmt))
- | • Kapitola 17 v publikaci iSeries Performance Capabilities Reference 

## | Paměťové prostory a vyhrazené disky na serveru iSeries

| Při intenzivní práci procesoru a paměti na integrovaném serveru jsou charakteristiky výkonu ekvivalentní jako u samostatného serveru s vyhrazenými disky. Protože diskové jednotky integrovaného serveru jsou alokovány mimo systém pro ukládání dat serveru iSeries, závisí výkon disků na serveru iSeries.

### | Vyšší disková kapacita díky sdíleným diskům serveru iSeries

| U většiny samostatných serverů je vyhrazeno jen několik disků pro každý server. U aplikací s malým průměrným zatížením disků je výkon postačující. Někdy však může být výkon určitého serveru omezen kapacitou takto malého počtu vyhrazených disků.

| Je-li tato skupina serverů integrována se serverem iSeries, jsou virtuální disky rozmístěny na několika pevných discích serveru iSeries. Celkové průměrné zatížení disků nemusí být o mnoho větší než u skupiny serverů s vyhrazenými disky. Ale v případě, že jednotlivý server potřebuje dočasně vyšší diskovou kapacitu, může ji získat prostřednictvím větší sady disků na serveru iSeries.

| U serverů s vyhrazenými disky je doba odezvy disků relativně stabilní. Můžete například využít předvídatelnou dobu odezvy a konfigurovat produkt Windows Performance Monitor tak, aby při překročení obvyklých prahových hodnot doby odezvy vydával výstrahy a indikoval výjimečný stav, který může vyžadovat vaši pozornost.

| V případě integrovaného serveru jsou paměť, CPU a diskový prostor serveru iSeries sdíleny mezi aplikacemi integrovaného serveru a serveru iSeries. Je obvyklé, že se odezva disků ve Windows pohybuje v širším rozmezí. V případě, že o stejný disk soupeří I/O operace z několika integrovaných serverů nebo jiné operace serveru iSeries, může dojít ke kratším prodávám. Některé aplikace na serveru iSeries, které jsou náročné na disky (například SAV a RST), mohou po určité období snížit výkon disků pozorovaný na Windows serveru. Je tedy obtížnější stanovit prahovou hodnotu pro kratší časová období.

### | Při vyhodnocování nedostatku paměťového prostoru vezměte v úvahu celou skupinu disků

| Paměťový prostor serveru iSeries se ve Windows jeví jako jedna disková jednotka. Překročil-li průměrná délka fronty na fyzickém disku (v produktu Windows Performance Monitor) hodnotu 2, nemusí být výkon serveru omezen. Za předpokladu, že byly vyloučeny problémy se stránkováním paměti, ukazuje hodnota délky fronty 2 nebo 100% využití disku ve Windows jen na nedostatek paměťového prostoru, provádí-li operace pouze jeden fyzický disk. Na serveru iSeries je obvykle více disků v rámci ASP, které pracují paralelně. Obvykle by dvojnásobný počet disků v ASP mohl ukazovat na nedostatek diskového prostoru. Měli byste vzít také v úvahu průměrné délky front všech serverů, které ASP používají.

## | Rovnováha paměťových prostorů

| Při vytváření paměťového prostoru jsou data rozložena po discích v uživatelsky definované společné oblasti paměti (ASP) nebo v nezávislé společné oblasti paměti (IASP). Disky ve společné oblasti mohou být konfigurovány jako nechráněné, chráněné pomocí RAID-5 nebo zrcadlení. Nechráněné disky neposkytují žádnou ochranu proti selhání. Disky chráněné pomocí RAID udržují sady parit, které v případě selhání disku v sadě parit umožňují nápravu (ale za cenu výkonu). Zrcadlení poskytuje ochranu proti selhání disku s mnohem vyšším výkonem než parita. Integrovaný server těží z výhod výkonné architektury paměti serveru iSeries bez ohledu na to, jak jsou konfigurována ASP a IASP.

| Server iSeries poskytuje funkce, které umožňují udržovat efektivní rozložení dat na discích. Příkladem je operace STRDSKRGZ (Spuštění reorganizace disků), která vyrovnává využití diskové paměti. Dalším příkladem je operace

l “Přidání jednotek do ASP a vyvážení dat”, která je k dispozici po přiřazení prostředků pevného disku k ASP.  
l Paměťový prostor lze na integrovaných serverech přemístit nebo vyvážit na discích pouze tehdy, je-li propojený server logicky vypnut.

l Umístění dat přiřazených k paměťovému prostoru je obvykle automaticky spravováno serverem iSeries. Není nutné konfigurovat rozptýlené svazky ani softwarové pole RAID pro disky ve Windows. Konfigurace těchto funkcí ve Windows by mohlo naopak zpomalit dobře fungující diskové operace. I když je paměťový prostor rozložen na discích serveru iSeries v malých oblastech, provádějte i nadále defragmentaci asociovaného disku ve Windows, aby byly v systému souborů zachovány efektivní datové struktury.

l Můžete monitorovat, jak server iSeries plní požadavky integrovaného serveru na disky; použijte příkazy WRKDSKSTS (Práce se stavem disku), WRKNWSSTG (Práce s pamětí síťového serveru) a WRKNWSSTS (Práce se stavem síťového serveru). Při dalších úvahách o výkonu si pamatujte, že integrované servery jsou servery Microsoft Windows. Můžete tedy použít produkt Microsoft Windows Performance Monitor stejně jako u libovolného jiného serveru. Informace o použití produktu Performance Monitor najdete v dokumentaci operačního systému Microsoft Windows.

## l **Výkon serverů připojených pomocí iSCSI**

l U serverů připojených pomocí iSCSI existuje několik voleb konfigurace, které umožňují dosáhnout vyššího výkonu podle potřeby. Některé volby vyžadují odlišné konfigurace cílových disků nebo svazků na integrovaných serverech.

### l **Konfigurace disků ve Windows**

l U integrovaných serverů připojených pomocí iSCSI jsou virtuální diskové jednotky optimalizovány:

- l • pro 1 diskovou oblast na virtuální jednotku,
- l • pro paměťové prostory o velikosti 1 GB nebo větší,
- l • pro systém souborů NTFS naformátovaný s velikostí klastrů 4 kB nebo větší.

l Tyto pokyny umožňují serveru iSeries efektivně spravovat paměťové prostory a současně zvyšovat výkon disků. Tyto pokyny také ovlivňují servery IXS a servery připojené pomocí adaptéru IXA, ale v mnohem menším rozsahu.

l Chcete-li zvýšit velikost paměťového prostoru pomocí CL příkazu CHGNWSSTG (Změna paměťového prostoru síťového serveru), nezapomeňte zvýšit velikost logických částí disku ve Windows pomocí příkazu DISKPART na serveru Windows Server 2003.

l **Poznámka:** Přidáním paměťového prostoru k serveru můžete dosáhnout vyššího výkonu než přidáním další logické části disku do tohoto nového prostoru.

### l **Společné oblasti paměti na serveru iSeries**

l U serverů připojených pomocí iSCSI jsou operace s paměťovými prostory prováděny prostřednictvím společné oblasti paměti serveru iSeries. Tato paměť funguje u diskových operací v podstatě jako paměť cache, takže velikost paměti může ovlivnit výkon disků ve Windows. Tyto I/O operace nemohou být přímou příčinou chybného stránkování v základní společné oblasti. Ale protože je společná oblast sdílena s dalšími aplikacemi na serveru i5/OS, mohou diskové operace ve Windows způsobit chybné stránkování v jiných aplikacích, nebo mohou jiné aplikace vyvolat stránkování diskových operací v síti iSCSI. Ve výjimečných případech můžete zmírnit potíže s pamětí tím, že upravíte velikosti společných oblastí nebo přiřadíte aplikace k jiným společným oblastem paměti.

l Servery IXS a servery připojené pomocí adaptéru IXA neprovádějí diskové operace prostřednictvím základní společné oblasti paměti. Používají vyhrazenou paměť ze společné oblasti počítače (ID systémové společné oblasti je 1). Diskové operace tedy nesdílejí paměť s ostatními aplikacemi.

### l **Konfigurace výkonu iSCSI**

l Pokud u integrovaných serverů připojených pomocí iSCSI dosahuje jedna síť své maximální kapacity, můžete přidat další kanály pomocí dalších adaptérů iSCSI HBA na serveru xSeries i na serveru iSeries (za předpokladu, že síť, která je navzájem propojuje, má dostupnou šířku pásma).

l Provoz iSCSI a síťový provoz můžete rozložit mezi samostatné kanály několika způsoby:

- l • Vyhraďte jeden kanál pro operace SCSI a druhý pro operace virtuální sítě Ethernet.
- l • Použijte dva cílové paměťové prostory. Každý cíl by měl být propojen s cestami k samostatnému adaptéru HBA. Další informace najdete v tématu “Správa adaptérů iSCSI HBA” na stránce 127.
  - l – Ve Windows nastavte aplikace tak, aby používaly obě jednotky (pokud je to možné), nebo vyhraďte tyto jednotky pro různé aplikace tak, aby byl celkový objem diskových operací rozložen mezi obě jednotky.
  - l – Nakonfigurujte tyto dva disky v rámci sady dynamických svazků ve Windows s daty rozptýlenými po těchto dvou discích. Až budou aplikace svazek používat, budou diskové operace automaticky vyvažovány mezi disky v sadě svazků.

## l Virtuální síť Ethernet

l Virtuální síť Ethernet standardně používá k propojení hostitelské logické části serveru iSeries s jednotlivými integrovanými Windows servery dvoubodové připojení. Toto dvoubodové připojení se používá především pro administrativní operace, které jsou součástí integrovaného prostředí.

l Náklady na využití CPU serveru iSeries a náklady na využití procesoru ve Windows při použití dvoubodového připojení jsou podobné jako při použití hardwarového síťového adaptéru. Toto připojení má vysokou rychlost, ale celková šířka pásma je vždy sdílena s diskovými, páskovými a dalšími operacemi na serveru IXS a adaptérech IXA. Použijete-li internetovou síť SCSI (iSCSI), můžete oddělit operace virtuální sítě Ethernet pomocí jiného kanálu iSCSI HBA.

l Při použití virtuální sítě Ethernet k propojení mezi dvěma nebo více integrovanými servery se přepínají přenosy mezi servery pomocí CPU serveru iSeries dokonce i tehdy, není-li iSeries koncovým bodem tohoto přenosu. U většiny připojení není toto využití význačné. Očekáváte-li však trvalé vysoké zatížení sítě ve všech připojeních virtuální sítě Ethernet mezi integrovanými servery, můžete se pokusit vyvážit náklady na použití vnitřního přepínače Virtual Ethernet a na externí síťové adaptéry na integrovaných serverech.

---

## Koncepce v oblasti sítí

l Hostované systémy zahrnují několik různých typů připojení do sítě.

l Níže uvedené typy připojení mají pouze systémy připojené pomocí iSCSI.

- l • **“Připojení servisního procesoru” na stránce 28**

l Toto fyzické připojení umožňuje hostitelské logické části s operačním systémem i5/OS komunikaci se servisním procesorem hostovaného systému.
- l • **“Síť iSCSI” na stránce 28**

l Tato fyzická síť připojuje adaptéry iSCSI v hostitelské logické části s operačním systémem i5/OS k adaptérům iSCSI v hostovaném systému.

Všechny typy integrovaných Windows serverů mohou mít následující typy připojení.

- l • **Virtuální síť Ethernet**

l Jedná se o simulované připojení typu Ethernet, které nevyžaduje žádné další síťové karty ani kabely. Existují dva typy virtuální sítě Ethernet.

- l – **“Dvoubodová virtuální síť Ethernet” na stránce 30**

l Toto připojení zajišťuje obecnou komunikaci mezi hostovaným systémem a hostitelským operačním systémem i5/OS.

- l – **“Virtuální síť Ethernet” na stránce 31**

l Tyto sítě jsou vytvořeny mezi hostovanými systémy, logickými částmi s operačním systémem i5/OS a ostatními logickými částmi, například s operačním systémem Linux.



- **“Externí síť” na stránce 35**

Tyto síť jsou normální síť Windows, používají je všechny servery. Byly vytvořeny prostřednictvím fyzických síťových karet řízených hostovaným systémem.

## **Připojení servisního procesoru**

**Poznámka:** Tato část se týká pouze systémů připojených pomocí iSCSI.

Toto fyzické připojení je požadováno, aby hostitelský operační systém i5/OS mohl komunikovat se servisním procesorem hostovaného systému. Toto připojení může sestávat z jednoduché komutované síť nebo ze složitější směrované síť. Prostředí Windows na serveru iSeries spravuje stav hostovaného systému pomocí produktu IBM Director přes toto připojení.

Na jednom konci tohoto připojení je adaptér nebo adaptéry síť LAN řízené operačním systémem i5/OS. Tento adaptér LAN je nadále k dispozici pro další použití. IP adresa a další atributy tohoto adaptéru jsou řízeny pomocí standardních metod konfigurace operačního systému i5/OS. Prostředí Windows na serveru iSeries tento adaptér nekonfiguruje. Může automaticky zjišťovat servisní procesor pomocí produktu IBM Director a jednoho nebo více rozhraní TCP operačního systému i5/OS, která jsou již konfigurována.

Na druhém konci připojení je servisní procesor. Servisní procesor má vlastní port síť Ethernet a zásobník TCP/IP. Tento zásobník TCP/IP je aktivní, kdykoli je napájecí kabel serveru zapojen do zásuvky, dokonce i tehdy, když není server zapnutý. U některých modelů serveru xSeries může být jeden port síť Ethernet sdílen systémem Windows a určitým typem servisního procesoru, který je znám pod názvem řadič BMC (Baseboard Management Controller). V tomto případě poskytuje stejný fyzický port v hostovaném systému připojení servisního procesoru i externí připojení do síť.

### **Server DHCP pro servisní procesor**

Nastavení IP adresy servisního procesoru může vyžadovat externí server DHCP v síti poskytující připojení servisního procesoru. Server DHCP by měl být aktivní před zapojením napájecího kabelu hostovaného systému do zásuvky. (Tento server DHCP se liší od serveru DHCP, který je zabudován na straně síť iSCSI s operačním systémem i5/OS a pomáhá se zaváděním iSCSI hostovaného operačního systému.) Další informace najdete v tématu “Dynamické IP adresování (DHCP)” na stránce 137.

### **Výběrové vysílání IP**

Prostředí Windows na serveru iSeries nabízí několik voleb pro zjišťování servisního procesoru. Povšimněte si, že volby, které umožňují většinu automatizace, vyžadují, aby síť podporovala výběrové vysílání IP. V předvoleném nastavení nepodporují některé síť a přepínače výběrové vysílání IP. Další informace najdete v tématu “Metody zjišťování servisních procesorů” na stránce 137.

### **Výkon a Maximální přenosová jednotka (MTU)**

Pro připojení servisního procesoru neexistuje žádný požadavek na vysokorychlostní síť ani na velikost MTU.

### **Zabezpečení**

Možnosti zabezpečení hardwaru servisního procesoru mohou ovlivnit vaše rozhodnutí, zda chcete připojení servisního procesoru poskytovat pomocí izolované, nebo sdílené síť. Další informace najdete v tématu “Konfigurace zabezpečení SSL servisního procesoru” na stránce 125.

## **Síť iSCSI**

Tato fyzická síť spojuje adaptéry Ethernet síť iSCSI v hostitelském systému i5/OS s adaptéry Ethernet síť iSCSI v hostovaném systému. Obvykle se jedná o jednoduchý přepínač typu Gigabit Ethernet. Tímto připojením procházejí dva typy přenosů: přenosy přes paměťové prostory (SCSI) a přenosy přes virtuální síť Ethernet (LAN).

Na jedné straně síť je adaptér iSCSI nebo adaptéry řízené operačním systémem i5/OS. Každý adaptér má dvě IP adresy: jednu pro SCSI a jednu pro LAN. Konfigurace IP adres a dalších atributů adaptéru se provádí v objektu popisu zařízení v operačním systému i5/OS. Další informace najdete v tématu “Adaptéry hostitele síťového serveru” na stránce 41

na stránce 41. Každý adaptér iSCSI řízený operačním systémem i5/OS potřebuje vlastní objekt. Každý adaptér iSCSI obsahuje zásobník TCP/IP, který je implementován v hardwaru nezávisle na normálním zásobníku TCP/IP operačního systému i5/OS. Až adaptér hostitele síťového serveru logicky zapnete, bude adaptér iSCSI řízený operačním systémem i5/OS používat konfigurované hodnoty. Pokud chcete použít jiné hodnoty, musíte změnit konfiguraci a adaptér hostitele serveru znovu logicky zapnout. Zásobník TCP/IP operačního systému i5/OS nerozpoznává IP adresy konfigurované pro adaptéry iSCSI.

Na druhé straně sítě je adaptér iSCSI nebo adaptéry pro hostovaný systém. Konfigurace IP adres a dalších atributů těchto adaptérů se provádí v objektu operačního systému i5/OS, který je také znám pod názvem konfigurace vzdáleného systému. Další informace najdete v tématu “Konfigurace vzdáleného systému” na stránce 41. Tato konfigurace se liší od objektu adaptéru síťového serveru v i5/OS v několika ohledech:

- Port pro adaptér iSCSI v hostovaném systému můžete konfigurovat s jednou nebo dvěma IP adresami: SCSI, LAN nebo obojí. Mezi konfigurovanými adaptéry musí být alespoň jedna IP adresa sítě SCSI a jedna IP adresa sítě LAN.
- Při každé konfiguraci IP adresy pro adaptér iSCSI v hostovaném systému musíte také konfigurovat adresu MAC příslušného adaptéru. Každý adaptér má označení, které uvádí jeho adresy MAC. Při konfiguraci adres MAC postupujte opatrně, abyste ji provedli správně.
- Konfiguraci všech adaptérů iSCSI pro hostovaný systém proveďte ve stejném objektu konfigurace vzdáleného systému v i5/OS. Až bude integrovaný server logicky zapnut, tento produkt automaticky zajistí, aby adaptéry iSCSI v hostovaném systému používaly hodnoty uvedené v konfiguraci vzdáleného systému v i5/OS. Pokud chcete použít jiné hodnoty, musíte konfiguraci změnit a server znovu logicky zapnout.
- Provoz v síti SCSI používá hardwarový zásobník TCP/IP adaptéru iSCSI, ale provoz v síti LAN používá zásobník TCP/IP systému Windows. V důsledku toho nejsou zásobníku TCP/IP ve Windows známy IP adresy v síti SCSI, ale jsou mu známy IP adresy v síti LAN.

#### **Poznámky:**

1. V objektech konfigurace operačního systému i5/OS jsou informace o síťových rozhraních označeny jako lokální nebo vzdálené. Tyto termíny jsou relativní vzhledem k operačnímu systému i5/OS. Informace o lokálních rozhraních se vztahují k i5/OS. Informace o vzdálených rozhraních se vztahují k hostovanému operačnímu systému Windows.
2. Konfigurace adaptéru hostitele síťového serveru a konfigurace vzdáleného systému definují informace o IP adresách pro opačné strany sítě iSCSI. Jsou-li propojeny jednoduchou komutovanou sítí, platí následující pravidla:
  - Internetové adresy SCSI v těchto dvou objektech, které jsou propojeny přepínačem, musejí být ve stejné podsíti. Například u IP adres ve tvaru a.b.x.y a masek podsítě 255.255.255.0 musí být hodnota a.b.x stejná pro oba objekty.
  - Internetové adresy sítě LAN v těchto dvou objektech, které jsou propojeny přepínačem, musejí být ve stejné podsíti.
  - V objektu NWSH mohou být prvky brány libovolně nepřirazené IP adresy v kterékoli podsíti, pokud v síti není brána.
  - V konfiguraci vzdáleného systému by prvky brány měly být prázdné, pokud v síti není brána.

#### **DHCP a přenos DHCP**

Zaváděcí informace můžete do hostovaného systému doručit několika způsoby. Předvolená metoda dodání informací o IP adrese a paměťovém prostoru pro zavedení operačního systému Windows používá integrovaný server DHCP (Dynamic Host Configuration Protocol) na straně sítě iSCSI s operačním systémem i5/OS. IP adresy mohou být považovány za statické dokonce i s použitím DHCP, protože server DHCP přiřazuje jednotlivé IP adresy k adresám MAC. Další informace najdete v tématu “Zavádění systému bez disku přes iSCSI” na stránce 22.

Integrovaný server DHCP může koexistovat s libovolnými servery DHCP, které také mohou být v síti iSCSI.

Pokud jsou v síti iSCSI mezi serverem iSeries a hostovaným systémem směrovače a metodou dodání zaváděcích informací je DHCP, pak je v síti požadován vhodně konfigurovaný agent přenosu DHCP, známý pod názvem agent přenosu BOOTP.

### **l Výkon a Maximální přenosová jednotka (MTU)**

l Pro síť iSCSI je žádoucí větší šířka pásma a nižší latence. Virtuální síť Ethernet může využívat až 9000bajtové rámce typu 'jumbo', podporuje-li síť větší MTU. Zvyšuje se tak výkon virtuální sítě Ethernet.

### **l Správa využití adaptérů iSCSI v systému i5/OS**

l Cesty konfigurované v popisu síťového serveru kontrolují, které přenosy přes paměťové prostory, pokud existují, a které přenosy přes virtuální síť Ethernet, pokud existují, mohou procházet adaptérem iSCSI v systému i5/OS. Další informace najdete v tématu "Správa využití adaptérů iSCSI HBA" na stránce 128.

l Několik hostovaných systémů může používat adaptér iSCSI v operačním systému i5/OS simultánně, pokud několik popisů síťového serveru používá stejný objekt NWSH.

### **l Správa využití adaptérů iSCSI v hostovaném systému**

l Adaptér iSCSI můžete v hostovaném systému konfigurovat s IP adresou sítě SCSI, IP adresou sítě LAN nebo s oběma druhy IP adres. Přítomnost IP adresy sítě SCSI umožňuje přenosy v rámci paměťových prostorů, přítomnost IP adresy sítě LAN umožňuje přenosy přes virtuální síť Ethernet. Každý adaptér virtuální sítě Ethernet ve Windows je obvykle automaticky přiřazen k fyzickému adaptéru sítě iSCSI. Na kartě rozšířených vlastností adaptéru virtuální sítě Ethernet není žádná volba, která by umožňovala vybrat určitý fyzický adaptér iSCSI. Další informace najdete v tématu "Správa alokací iSCSI HBA na straně Windows sítě iSCSI" na stránce 131.

l IBM nepodporuje použití adaptéru iSCSI jako obecného externího připojení do sítě. Další informace o externím připojení do sítě najdete v tématu "Externí síť" na stránce 35.

### **l Další posouzení**

- Síť iSCSI používá pouze IP verze 4.
- Formát rámců je Ethernet verze 2.
- Síť iSCSI nepodporuje převod síťové adresy (NAT).

### **l Zabezpečení**

l Přenosy v rámci paměťových prostorů a přenosy přes virtuální síť Ethernet můžete zabezpečit několika způsoby. Další informace najdete v tématu "Koncepte zabezpečení" na stránce 46.

## **Dvoubodová virtuální síť Ethernet**

l Operační systém i5/OS potřebuje se svými integrovanými Windows servery komunikovat. Tato komunikace se uskutečňuje přes dvoubodovou virtuální síť Ethernet. Při instalaci integrovaného serveru je vytvořena speciální virtuální síť mezi ním a řídicí logickou částí operačního systému i5/OS. Tato virtuální dvoubodová (point-to-point) síť má pouze dva koncové body, integrovaný server a server iSeries, a je na serveru iSeries emulována (stejně jako virtuální síť Ethernet) a nepotřebuje žádné další fyzické síťové adaptéry ani kabely. V operačním systému i5/OS je konfigurována jako popis linky Ethernet s hodnotou čísla portu \*VRTETHPTP.

l Při spuštění příkazu INSWNTSVR (Instalace Windows serveru), se nakonfiguruje i dvoubodová virtuální síť Ethernet.

Možná se ptáte, čím se dvoubodová virtuální síť Ethernet liší od klasické virtuální sítě Ethernet. Odpověď zní:

Dvoubodová virtuální síť Ethernet je konfigurována odlišně a může mít pouze dva koncové body, server iSeries a integrovaný server. Dvoubodová virtuální síť Ethernet podporuje pouze protokol TCP/IP a v předvoleném nastavení používá vyhrazené IP adresy v soukromých doménách, takže tyto adresy neprocházejí branami ani směrovači.

l U serverů xSeries připojených pomocí IXS (Integrated xSeries Server) a IXA (Integrated xSeries Adapter) mají tyto adresy tvar 192.168.xxx.yyy, kde xxx a yyy mohou být 1 až 2 číslice. Například server IXS, který je definován s číslem hardwarového prostředku LIN03, bude mít IP adresu 192.168.3.yyy.

l U hardwaru iSCSI mají tyto adresy tvar 192.168.xxx.yyy, kde xxx může být v rozmezí od 100 do 254, a výsledkem je jedinečná síť třídy C. V našem příkladě dostane strana dvoubodové sítě operačního systému i5/OS IP adresu 192.168.100.1 a strana Windows má 192.168.100.2. Když budete pro stejný hardwarový prostředek definovat další popisy linky, bude se yyy zvyšovat.



Můžete povolit, aby příkaz INSWNTSVR přiřadil IP adresy automaticky nebo je můžete konfigurovat manuálně, abyste předešli kolizím TCP/IP adres s jinými hostiteli v systému.

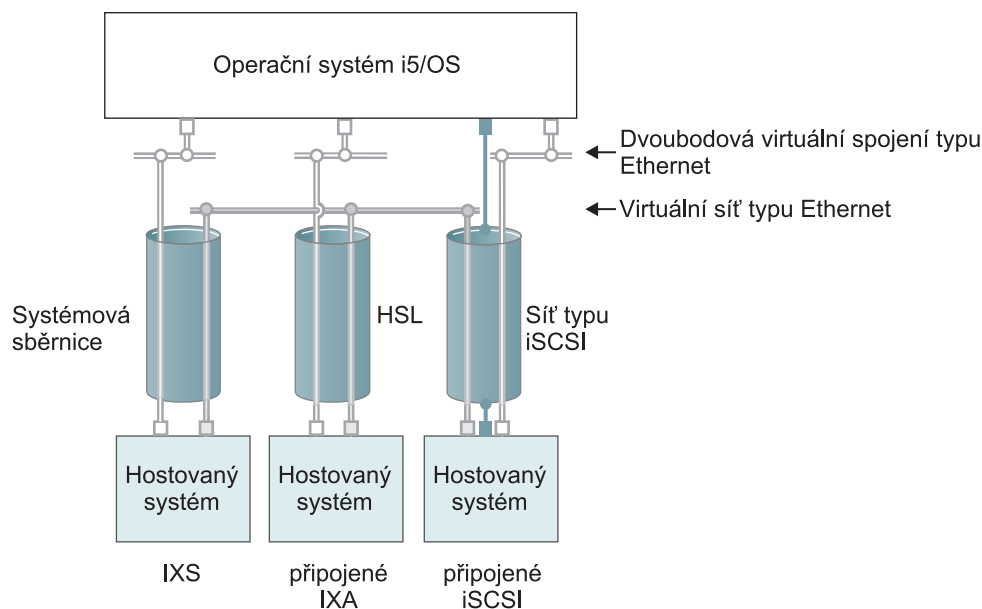
## Virtuální síť Ethernet

Virtuální síť Ethernet jsou flexibilní a lze je konfigurovat mnoha různými způsoby.

### Virtuální síť Ethernet s nejméně jednou logickou částí

Postup při vytváření virtuálních sítí Ethernet je vysvětlen v tématu “Konfigurace virtuálních sítí Ethernet” na stránce 107.

|  
|



□ nebo □ IP adresa na virtuálním adaptéru

■ Lokální IP adresa na adaptéru typu iSCSI

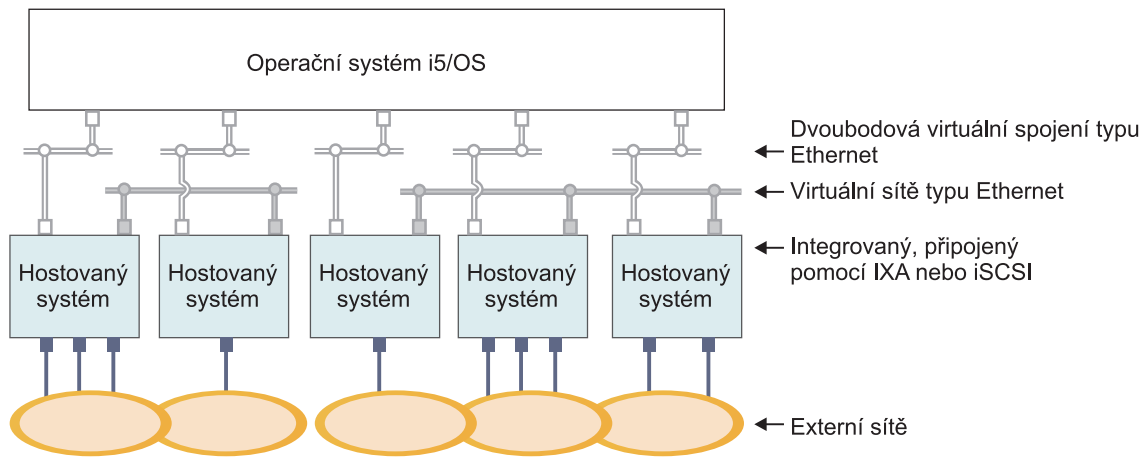
RZAHQ500-5

Obrázek 9. Tunely systémové sběrnice, linka HSL a síť iSCSI

Systémy připojené pomocí serverů IXS, adaptérů IXA a iSCSI HBA mohou být účastníky virtuálních sítí Ethernet a mohou spolu navzájem komunikovat.

- U serverů IXS prochází provoz virtuální sítě Ethernet přes systémové sběrnice serveru iSeries.
- U hostovaných systémů připojených pomocí adaptéru IXA prochází provoz virtuální sítě Ethernet přes kabely typu HSL.
- U hostovaných systémů připojených pomocí iSCSI prochází provoz virtuální sítě Ethernet tunely prostřednictvím fyzické sítě iSCSI. Virtuální síť Ethernet je v přítomnosti sítě iSCSI potřebná z několika důvodů:
  - Virtuální síť Ethernet může pracovat s další podporou virtuálních sítí Ethernet na serveru iSeries.
  - Virtuální síť Ethernet může poskytovat několik samostatných virtuálních sítí prostřednictvím jednotlivých adaptérů iSCSI HBA dokonce i tehdy, když přepínače v síti iSCSI nepodporují standard IEEE 802.1Q VLAN.
  - Je-li povoleno zabezpečení IPSec, je provoz v síti iSCSI šifrován. Virtuální síť Ethernet můžete považovat za vysoce výkonnou síť VPN (Virtual Private Network). Virtuální Ethernet se zabezpečením IPSec může zajistit ochranu celé virtuální sítě, na rozdíl od typických sítí VPN, které mají jen dva koncové body.

**Poznámka:** Každé rozhraní iSCSI HBA může mít dvě IP adresy, jednu pro funkce ukládání a jednu pro funkce sítě LAN. Tyto IP adresy jsou používány jako tunel do virtuální sítě Ethernet. Rozhraní TCP/IP operačního systému i5/OS tyto IP adresy nerozpoznává. U adaptérů iSCSI HBA jsou tunely virtuální sítě Ethernet vytvářeny prostřednictvím fyzické sítě s adaptéry iSCSI HBA ve fyzických koncových bodech.



■ nebo □ IP adresa na virtuálním adaptéru

■ IP adresa na externím adaptéru nebo portu

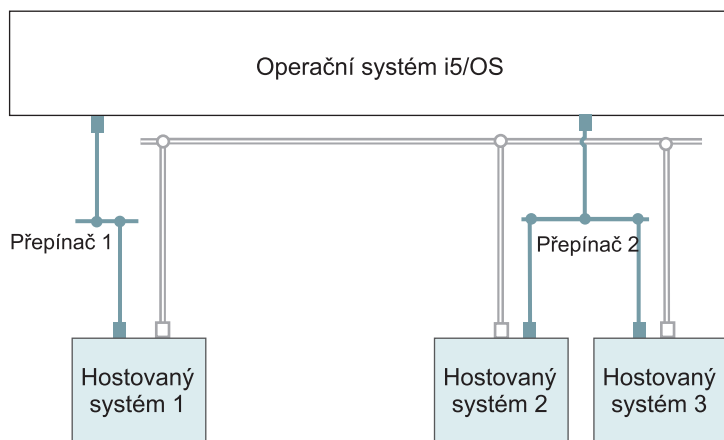
RZAHQ015-8

Obrázek 10. Dvě samostatné skupiny integrovaných Windows serverů na stejném serveru iSeries. Každá skupina má vlastní virtuální síť Ethernet.

Obrázek 10 vás seznámí s tím, jak fungují virtuální sítě na serveru iSeries. Je tu pět samostatných integrovaných Windows serverů. Všechny jsou připojeny k jediné řídicí logické části s operačním systémem i5/OS přes dvoubodové virtuální sítě Ethernet (označené bílou barvou). Modré čtverečky pod integrovanými servery představují fyzické síťové karty, které jednotlivým serverům umožňují vytvořit externí připojení do sítě. Obláčky, k nimž jsou připojeny, představují externí síť. Dále jsou tu dvě samostatné virtuální sítě Ethernet (označené zeleně). Každý integrovaný server se může současně účastnit až čtyř virtuálních sítí Ethernet.

Tento typ připojení je vyžadován při konfiguraci skupiny integrovaných serverů pro spojování do klastrů.

Stejně jako dvoubodové virtuální sítě Ethernet jsou i virtuální sítě Ethernet konfigurovány prostřednictvím popisů linek Ethernet. Integrovaný server je připojen k virtuální síti Ethernet, pokud je jeho popis (objekt NWSD) v operačním systému i5/OS konfigurován tak, že číslo portu v popisu linky Ethernet má hodnotu v rozmezí \*VRTETH0 až \*VRTETH9. Integrované servery, jejichž objekty NWSD jsou konfigurovány se stejnými hodnotami čísla portu, jsou připojeny do stejné virtuální sítě Ethernet. Při instalaci nového integrovaného serveru může příkaz INSWNTSVR (Instalace Windows serveru) automaticky vytvořit požadované popisy linek a přiřadit jim IP adresy. Na obrázku nejsou vidět popisy linek na straně operačního systému i5/OS. Na rozdíl od použití virtuální sítě Ethernet byste měli adresu TCP/IP konfigurovat na straně operačního systému i5/OS v popisu linky pro virtuální síť Ethernet.



□ IP adresa na virtuálním adaptéru

■ Lokální IP adresa na adaptéru typu iSCSI

RZAHQ513-2

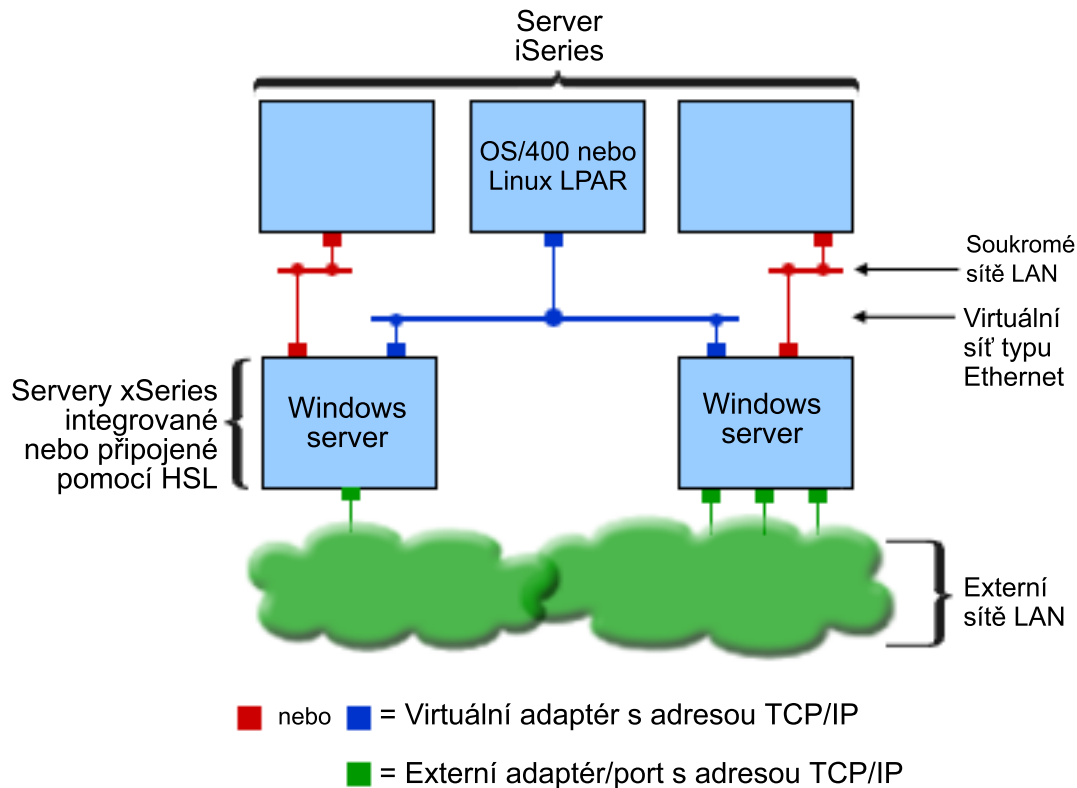
Obrázek 11. Virtuální síť Ethernet tunelovaná prostřednictvím sítě iSCSI

Virtuální síť Ethernet tunelovaná prostřednictvím sítě iSCSI má zvláštní charakteristiky, které znázorňuje Obrázek 11.

- Hostovaný systém 1 může komunikovat s hostovaným systémem 2 a s hostovaným systémem 3, i když jsou použity samostatné sítě iSCSI (samostatné fyzické přepínače).
- Komunikace virtuální sítě Ethernet mezi hostovaným systémem 2 a hostovaným systémem 3 vyžaduje systém iSeries, i když jsou oba tyto hostované systémy připojeny ke stejnému fyzickému přepínači.
- Ve fyzické síti iSCSI je pro komunikaci přes virtuální síť Ethernet v každém hostovaném systému zahrnuta dvojice IP adres sítě LAN. Dvojice pro hostovaný systém 2 a dvojice pro hostovaný systém 3 mají své IP adresy spolu na straně operačního systému i5/OS.

#### Virtuální síť Ethernet s více než jednou logickou částí

Postup při vytváření virtuálních sítí Ethernet je vysvětlen v tématu “Konfigurace virtuálních sítí Ethernet mezi logickými částmi” na stránce 108.



RZAHQ016-4

Obrázek 12. Jednoduchá virtuální síť Ethernet mezi logickými částmi.

Při rozdělení serveru iSeries na logické části byly na serveru iSeries vytvořeny tři samostatné virtuální logické části s operačním systémem i5/OS. Na obrázku jsou znázorněny tři virtuální sítě: dvě dvoubodové virtuální sítě Ethernet (označené šedou a bílou barvou) a jedna virtuální síť Ethernet (modrá). Každý integrovaný server má dvoubodovou virtuální síť Ethernet pro komunikaci se svou řídicí logickou částí. V tomto případě má virtuální síť Ethernet tři účastníky: dva integrované servery, z nichž každý je řízen jinou logickou částí s operačním systémem i5/OS, a třetí logickou část s operačním systémem i5/OS nebo jiným. Takové prostředí se nazývá síť Ethernet mezi logickými částmi.

U serverů bez konzole HMC (Hardware Management Console) existuje spojení mezi logickými částmi, které používají stejné číslo sítě, a integrované servery jsou připojeny pouze tehdy, jsou-li připojeny jejich řídicí logické části s operačním systémem i5/OS. Síťová čísla 0-9 se vztahují k integrovaným serverům. Je-li například logická část s operačním systémem i5/OS konfigurována na spojení mezi logickými částmi v sítích 1 a 5, pak integrované servery řízené touto logickou částí se mohou účastnit komunikace mezi logickými částmi na portech \*VRTETH1 a \*VRTETH5. Postup, kterým se to provede, je v online nápovědě produktu iSeries Navigator. Přehled najdete také v tématu Koncepte logických částí systému.

U serverů s konzolí HMC existuje spojení mezi logickými částmi nebo integrovanými servery, které používají stejný ID virtuální sítě LAN. Zúčastněné integrované servery nepodporují ID virtuální sítě LAN přímo. Místo toho potřebuje každý účastnický integrovaný server popis linky Ethernet, který spojuje hodnotu portu, například \*VRTETH1 s virtuálním adaptérem, který má ID virtuální LAN. Virtuální adaptér vytvoříte pomocí konzole HMC. Další informace najdete v tématech Partitioning with an eServer i5 a Configuring a virtual Ethernet adapter for i5/OS v aplikaci IBM Systems Hardware Information Center. Pokud provádíte migraci virtuální sítě Ethernet mezi logickými částmi ze serveru bez konzole HMC na server s konzolí HMC, musíte pomocí konzole HMC vytvořit virtuální adaptéry Ethernet a další popisy linek Ethernet, abyste mohli provést odpovídající přiřazení. Pamatujte si, že v rámci téže logické části spolu mohou Windows servery stále komunikovat pouze pomocí stejného čísla portu virtuální sítě Ethernet.

## Externí síť

Integrovaný Windows server může být součástí externích sítí stejně jako normální PC server. To je možné udělat různým způsobem. Na integrovaném serveru připojeném pomocí adaptéru IXA nebo iSCSI jsou k dispozici rozšiřující sloty pro sběrnice PCI, můžete tedy použít libovolný integrovaný síťový adaptér nebo nainstalovat síťovou kartu jako u osobního počítače. Server IXS je prakticky PC server na kartě, která je instalována ve slotu PCI na serveru iSeries. Nemá žádné rozšiřující sloty PCI. Některé servery IXS mohou ovládat iSeries PCI slot sousedící s místem, kde je instalovaný, a tak "převzít" síťový adaptér iSeries. Kromě toho obsahují modely 2892 a 4812 serveru IXS integrovaný síťový adaptér Ethernet.

Postup, jak fyzicky instalovat síťové karty pro servery IXS a xSeries a jak je konfigurovat pro použití s integrovanými servery, najdete v tématu "Externí síť" na stránce 110.

---

## Koncepce týkající se softwaru

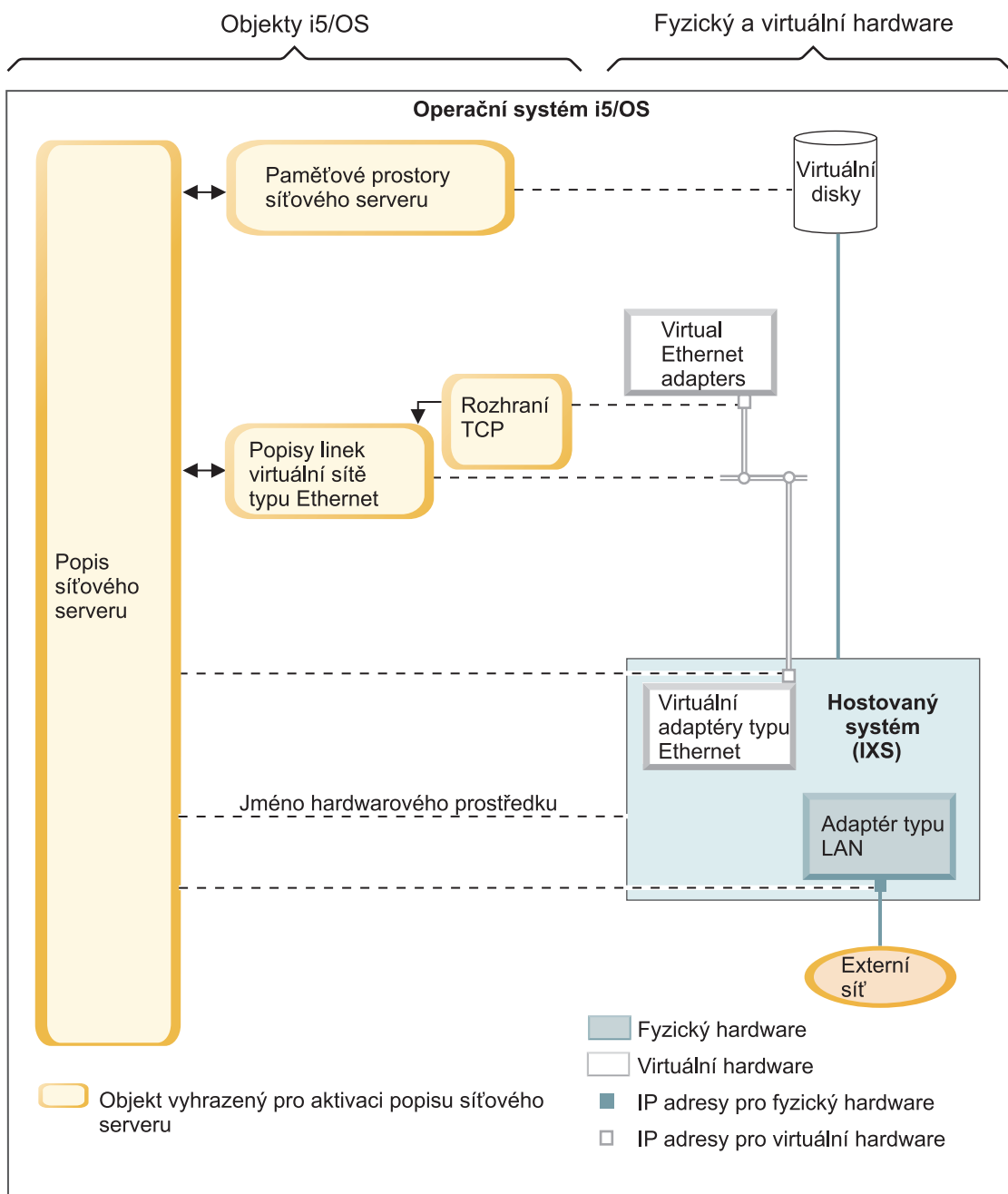
Operační systém i5/OS pomáhá definovat, konfigurovat a spravovat integrované servery bez ohledu na typ jejich hardwaru. Popis objektů operačního systému i5/OS, které se používají pro různé konfigurace hardwaru, najdete v níže uvedených schématech. Popis podporovaných konfigurací hardwaru najdete v tématu "Koncepce týkající se hardwaru" na stránce 13.

Informace o konfiguraci operačního systému i5/OS najdete v těchto publikacích.

- "Servery IXS (Integrated xSeries Server) a servery xSeries připojené pomocí adaptéru IXA (Integrated xSeries Adapter)"
- "Servery xSeries a IBM BladeCenter připojené pomocí iSCSI" na stránce 39
- "Servery xSeries a BladeCenter připojené pomocí iSCSI se zabezpečením" na stránce 43

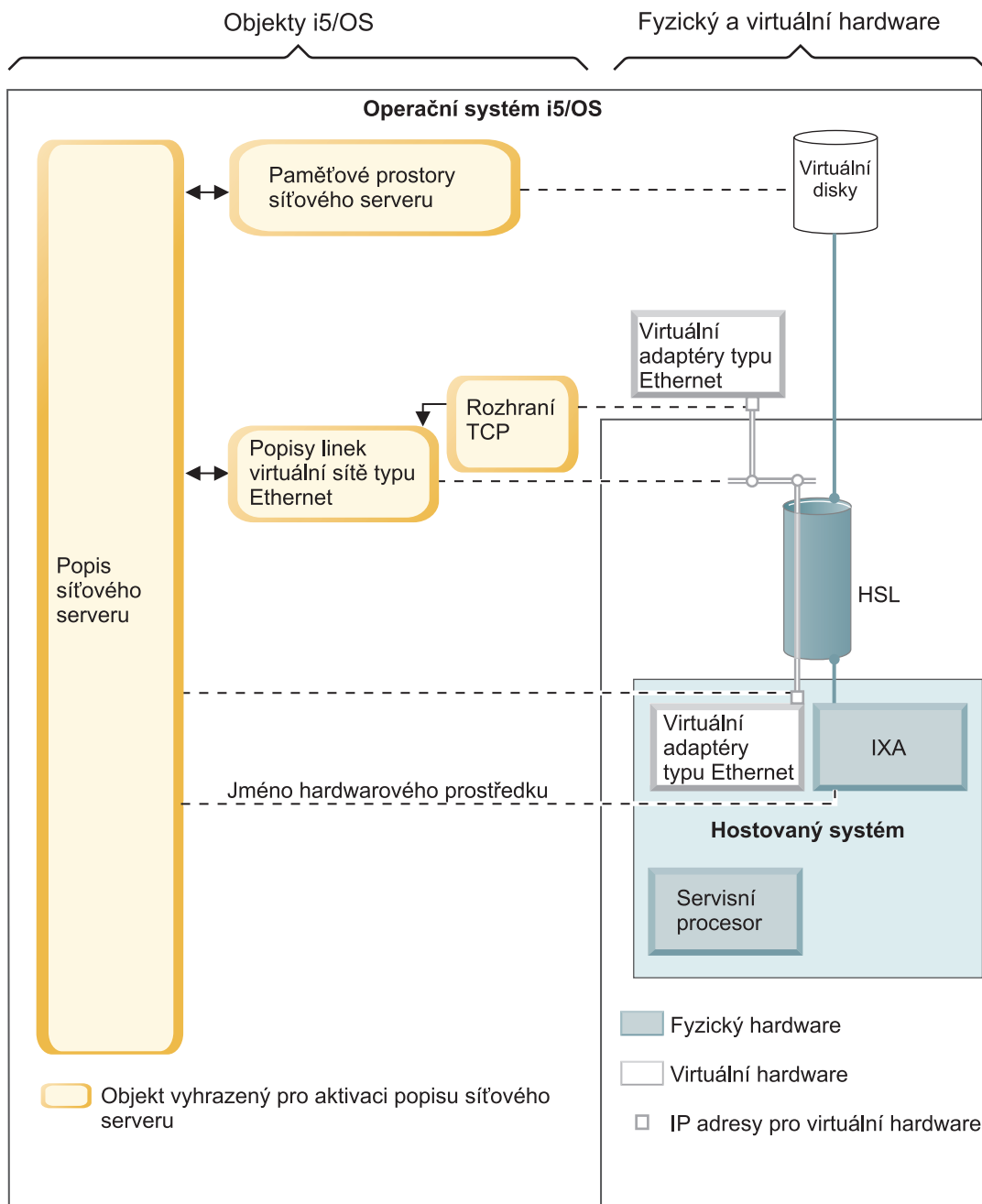
## Servery IXS (Integrated xSeries Server) a servery xSeries připojené pomocí adaptéru IXA (Integrated xSeries Adapter)

Operační systém i5/OS reprezentuje servery IXS a servery xSeries připojené pomocí adaptéru IXA podobným způsobem.



RZAHQ508-3

Obrázek 13. Objekty konfigurace serveru IXS v systému i5/OS



RZAHQ504-2

Obrázek 14. Objekty konfigurace IXA v systému i5/OS

Obrázek 14 znázorňuje klíčové objekty operačního systému i5/OS a také hardwarové komponenty, které jsou použity pro servery IXS a servery xSeries připojené pomocí adaptéru IXA.

Objekty, které znázorňuje Obrázek 13 na stránce 36 a Obrázek 14, jsou popsány v těchto tématech:

- “Popis síťového serveru” na stránce 38
- “Jméno hardwarového prostředku” na stránce 38
- “Paměťové prostory síťového serveru” na stránce 38
- “Popisy linek virtuální sítě Ethernet” na stránce 39
- “Rozhraní TCP/IP” na stránce 39

- “Systémová sběrnice a datové toky typu HSL” na stránce 39

## Popis síťového serveru

Popis síťového serveru (objekt NWSD), který znázorňuje Obrázek 13 na stránce 36 a Obrázek 14 na stránce 37, je klíčovým objektem konfigurace operačního systému i5/OS pro všechny typy integrovaných serverů. Objekt NWSD sdružuje všechny ostatní objekty operačního systému i5/OS, které se vztahují k integrovanému serveru. Obsahuje například odkaz na hardware, na kterém je server spuštěn, propojení s diskovými jednotkami, které server používá, odkazy na síťové porty, které server používá, a mnoho dalších atributů serveru. Objekt NWSD a několik dalších objektů operačního systému i5/OS, které server potřebuje, můžete vytvořit pomocí příkazu INSWNTSVR (Instalace Windows serveru) v systému i5/OS.

Popis hodnot, které objekt NWSD obsahuje, najdete v příkazu CRTNWSD (Vytvoření popisu síťového serveru) operačního systému i5/OS.

U integrovaného serveru je hardware serveru IXS a serveru xSeries připojeného pomocí adaptéru IXA řízen operačním systémem i5/OS.

- Integrovaný server se spouští logickým zapnutím objektu NWSD pro tento server. Zahájí se tak proces zavádění operačního systému Windows.
- Činnost integrovaného serveru se ukončuje logickým vypnutím objektu NWSD pro tento server. Zahájí se tak proces ukončení operačního systému Windows.
- Při provádění úloh spuštění a ukončení činnosti u serveru IXS komunikuje operační systém i5/OS přímo s hardwarem serveru IXS.
- Při zahájení úloh spuštění a ukončení práce u serveru xSeries připojeného pomocí adaptéru IXA komunikuje operační systém i5/OS přes sběrnici typu HSL s adaptérem IXA, který je instalován na serveru xSeries. Při provádění úloh spuštění a ukončení práce komunikuje adaptér IXA se servisním procesorem (SP) systému xSeries.

**Poznámka:** Protože adaptér IXA zajišťuje fyzické připojení k servisnímu procesoru serveru xSeries, není při konfiguraci charakteristiky servisního procesoru serveru xSeries potřebný žádný objekt operačního systému i5/OS.

## Jméno hardwarového prostředku

U serverů IXS a serverů xSeries připojených pomocí adaptéru IXA je hardware serveru identifikován v operačním systému i5/OS pomocí jména hardwarového prostředku (například LIN23). Odkaz na jméno hardwarového prostředku pro server IXS a server xSeries připojený pomocí adaptéru IXA je uložen v objektu NWSD. Viz Obrázek 13 na stránce 36 a Obrázek 14 na stránce 37.

**Poznámka:** Protože je hardware, na kterém je provozován server IXS a server xSeries připojený pomocí adaptéru IXA, definován jménem hardwarového prostředku v objektu NWSD, je snadné tento hardware přepnout. To je výhodné v případech selhání hardwaru serveru IXS nebo serveru xSeries připojeného pomocí adaptéru IXA, protože lze integrovaný server přepnout "za chodu" z vadného hardwaru na kompatibilní rezervní hardware a spustit jej na tomto hardwaru. Další informace o možnosti výměny za chodu najdete v tématu “Výměna hardwaru serveru za chodu” na stránce 148.

## Paměťové prostory síťového serveru

Paměťový prostor síťového serveru (objekt NWSSTG) představuje virtuální diskovou jednotku, kterou tento server používá. Další informace najdete v tématu Obrázek 13 na stránce 36 a Obrázek 14 na stránce 37. Velikost virtuálních diskových jednotek se může pohybovat v rozmezí od 1 MB do 1000 GB. K serveru lze připojit až 64 virtuálních diskových jednotek v závislosti na konfiguraci serveru, takže kapacita paměťového prostoru integrovaného serveru se pohybuje v rozmezí od několika GB do mnoha TB. Virtuální diskové jednotky jsou nejprve vytvořeny jako samostatné objekty a potom se propojí s integrovaným serverem přes objekt NWSD integrovaného serveru, který je používá.

Každý server má alespoň dvě virtuální diskové jednotky, automaticky vytvořené příkazem INSWNTSVR, ale může mít i uživatelsky definované diskové jednotky.

- Systémová jednotka (obvykle jednotka C:) obsahuje operační systém Windows serveru (například Windows Server 2003).



- Instalační jednotka (obvykle jednotka D:) obsahuje kopii instalačních médií Windows serveru a také část kódu produktu i5/OS Integrated Server Support (produkt 5722-SS1 volba 29), který je spuštěn na Windows serveru. Instalační jednotka je používána během procesu instalace Windows a je také používána při každém spuštění serveru, protože serveru předává informace o konfiguraci z operačního systému i5/OS.
- Další uživatelsky definované jednotky jsou obvykle používány pro aplikace a data serveru.

Skutečná disková paměť pro virtuální diskové jednotky je alokována z integrovaného systému souborů (IFS) operačního systému i5/OS. Virtuální diskové jednotky mohou být alokovány z předvolené společné systémové diskové oblasti (známé pod názvem společná oblast paměti neboli systémové ASP), v uživatelsky definované společné diskové oblasti nebo v nezávislé společné diskové oblasti (IASP).

Další informace o virtuálních diskových jednotkách najdete v tématu Kapitola 9, “Správa systému pro ukládání dat”, na stránce 151.

#### **Poznámky:**

1. Protože virtuální diskové jednotky jsou objekty IFS operačního systému i5/OS, lze celý obraz virtuálních diskových jednotek zálohovat a obnovit pomocí příkazů SAV (Uložení) a RST (Obnova) operačního systému i5/OS. Soubory na virtuálních diskových jednotkách lze v operačním systému i5/OS zálohovat jednotlivě pomocí zálohování na úrovni souborů systému souborů QNTC (Network Client) v IFS nebo pomocí nativního zálohovacího programu ve Windows. Další informace uvádí Kapitola 12, “Zálohování a obnova integrovaných Windows serverů”, na stránce 179.
2. I když jsou paměťové prostory alokovány mimo IFS, paměťové operace prostřednictvím IFS se neprovádějí, dokud je integrovaný server logicky zapnut. To znamená, že nejsou povoleny operace, jako je zápis do žurnálu.

#### **Popisy linek virtuální sítě Ethernet**

Popis linky virtuální sítě Ethernet se používá na serveru iSeries při konfiguraci virtuální sítě Ethernet, jejíž součástí je integrovaný server. Další informace najdete v tématu Obrázek 13 na stránce 36 a v tématu Obrázek 14 na stránce 37. Popis linky se používá v konfiguraci integrovaného serveru, která definuje komunikaci integrovaného serveru s operačním systémem i5/OS přes dvoubodovou virtuální síť Ethernet. Popis linky se také používá v konfiguraci integrovaného serveru, která má definovat komunikaci integrovaného serveru nebo jiných logických částí přes virtuální síť Ethernet uvnitř logické části nebo mezi logickými částmi. Další informace o virtuálních sítích Ethernet najdete v tématu “Koncepce v oblasti sítí” na stránce 27.

**Poznámka:** Popisy linek (LIND) se nepoužívají pro žádné fyzické síťové adaptéry, které by mohly integrovaný server mít. Fyzické adaptéry jsou konfigurovány z prostředí Windows pomocí obvyklých metod konfigurace síťových adaptérů ve Windows.

#### **Rozhraní TCP/IP**

Rozhraní TCP/IP se používá v dvoubodové virtuální síti Ethernet k nastavení adresy TCP/IP na straně operačního systému i5/OS. Viz Obrázek 13 na stránce 36 a Obrázek 14 na stránce 37.

**Poznámka:** Adresa TCP/IP na straně Windows v dvoubodové virtuální síti Ethernet se nastavuje prostřednictvím parametru TCPPORTCFG (Konfigurace portu TCP/IP) v objektu NWSD.

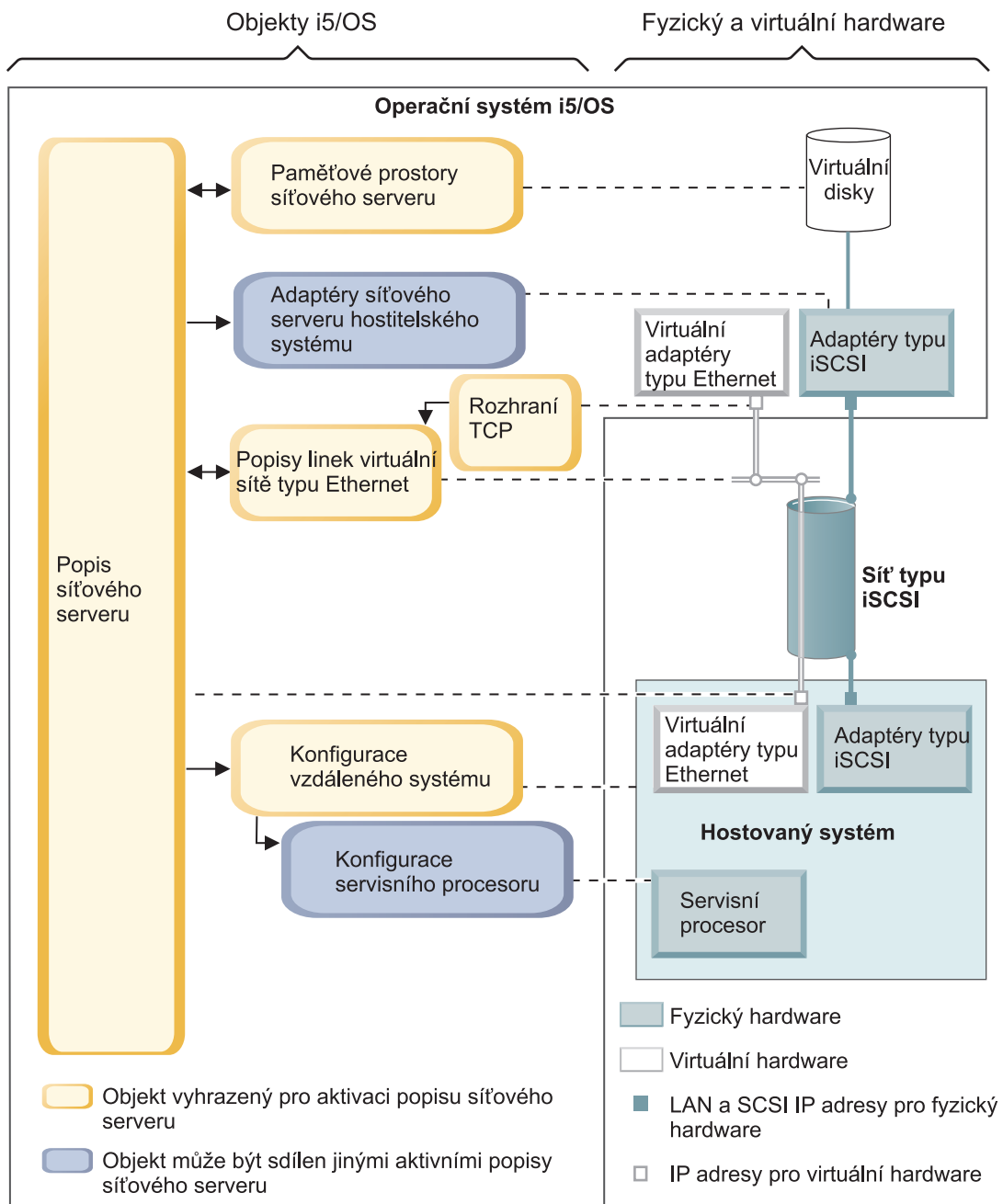
#### **Systémová sběrnice a datové toky typu HSL**

Data diskových jednotek SCSI a virtuální sítě Ethernet procházejí mezi operačním systémem i5/OS a integrovaným serverem přes systémovou sběrnici serveru iSeries (u serveru IXS), nebo přes připojení typu HSL mezi I/O věží a systémem iSeries (u adaptéru IXA). Další informace najdete v tématu Obrázek 13 na stránce 36 a v tématu Obrázek 14 na stránce 37. V podstatě jsou diskové jednotky SCSI a protokoly virtuální sítě Ethernet zapouzdřeny uvnitř normálních protokolů pro přenos dat pomocí systémové sběrnice nebo linky HSL serveru iSeries.

#### **Servery xSeries a IBM BladeCenter připojené pomocí iSCSI**

Operační systém i5/OS popisuje servery xSeries a IBM BladeCenter připojené pomocí iSCSI podobně, jako popisuje servery IXS a servery xSeries připojené pomocí adaptéru IXA. Technologie iSCSI však vyžaduje další objekty a informace o konfiguraci v operačním systému i5/OS, které nebyly vyžadovány u serverů IXS a serverů xSeries.

připojených pomocí adaptéru IXA. Protože servery připojené pomocí iSCSI jsou připojeny k systému iSeries přes síť Ethernet (nikoli připojením systémové sběrnice nebo linky HSL, které se používá u IXS a IXA), jsou požadovány další informace o konfiguraci, aby bylo možné server xSeries nebo IBM BladeCenter identifikovat v síti a komunikovat s ním. Protože servery připojené pomocí iSCSI mohou navíc existovat v síti Ethernet spolu s dalšími systémy, může být předmětem zájmu zabezpečení komunikace a datových toků mezi operačním systémem i5/OS a servery připojenými pomocí iSCSI. Následující obrázek znázorňuje, jak jsou servery připojené pomocí iSCSI popisovány operačním systémem i5/OS.



RZAHQ505-1

Obrázek 15. Objekty konfigurace iSCSI v operačním systému i5/OS bez zabezpečení sítě

Obrázek 15 znázorňuje klíčové objekty operačního systému i5/OS a klíčové hardwarové komponenty používané pro servery xSeries a IBM BladeCenter připojené pomocí iSCSI v případě, že se nepoužívá zabezpečení sítě.

| Objekty, které znázorňuje Obrázek 15 na stránce 40, jsou popsány v těchto tématech:

- | • “Adaptéry hostitele síťového serveru”
- | • “Konfigurace vzdáleného systému”
- | • “Konfigurace servisního procesoru”
- | • “Popis síťového serveru” na stránce 42
- | • “Paměťové prostory síťového serveru” na stránce 43
- | • “Datové toky” na stránce 43
- | • “Popisy linek virtuální sítě Ethernet” na stránce 39
- | • “Rozhraní TCP/IP” na stránce 39

| Informace o objektech i5/OS použitých pro servery xSeries a IBM BladeCenter připojené pomocí iSCSI se zabezpečením sítě znázorňuje Obrázek 16 na stránce 44.

### | **Adaptéry hostitele síťového serveru**

| Objekt s popisem zařízení NWSH, který znázorňuje Obrázek 15 na stránce 40, reprezentuje adaptér iSCSI HBA používaný v připojení iSCSI na straně serveru iSeries:

- | • Identifikuje jméno hardwarového prostředku serveru iSeries (například LIN33) pro adaptér iSCSI HBA.
- | • Definuje způsob, jakým jsou protokolovány chyby komunikací, a obsahuje informace o obnově komunikace.
- | • Definuje internetovou adresu, porty apod. pro rozhraní sítí SCSI a LAN na adaptéru iSCSI HBA.

| Server iSeries může mít několik adaptérů iSCSI HBA, s každým z nich je asociován objekt NWSH.

- | • Každý objekt NWSH může být sdílen několika integrovanými servery. V konfiguracích, kde šířka pásma není důležitá, vede tato možnost k řešení s nižšími náklady.
- | • Každý integrovaný server může používat několik objektů NWSH. Umožňuje to vytvořit několik cest k datům v síti SCSI a ve virtuální síti Ethernet mezi serverem iSeries a systémy xSeries nebo IBM BladeCenter, které mohou poskytovat větší šířku pásma a redundanci připojení.

### | **Konfigurace vzdáleného systému**

| Objekt konfigurace síťového serveru ve vzdáleném systému (NWSCFG typu RMTSYS) (viz Obrázek 15 na stránce 40) reprezentuje server xSeries nebo IBM BladeCenter připojený pomocí iSCSI:

- | • Identifikuje hardware serveru podle sériového čísla, typu a modelu.
- | • Obsahuje informace o konfiguraci adaptérů iSCSI HBA používaných serverem xSeries nebo IBM BladeCenter.
- | • Obsahuje hodnoty požadované pro zavedení systému serveru (například určení, ze kterého adaptéru iSCSI má být systém zaveden).
- | • Obsahuje odkaz na objekt NWSCFG servisního procesoru (viz níže) používaný k řízení serveru xSeries nebo IBM BladeCenter.
- | • Konfigurace vzdáleného systému může volitelně obsahovat hodnoty používané pro zabezpečení procesu zavádění systému.

| Server xSeries a IBM BladeCenter mohou mít několik adaptérů iSCSI HBA. Umožňuje to vytvořit několik cest k datům v síti SCSI a ve virtuální síti Ethernet mezi serverem iSeries a systémy xSeries nebo IBM BladeCenter, které mohou poskytovat větší šířku pásma a možnost rezervních připojení.

| Objekt konfigurace vzdáleného systému pro integrovaný server je vyhledáván pomocí parametru v objektu NWSD.

### | **Konfigurace servisního procesoru**

| Objekt konfigurace síťového serveru se servisním procesorem (objekt NWSCFG typu SRVPRC) (viz Obrázek 15 na stránce 40) reprezentuje servisní procesor serveru xSeries nebo Management Module serveru IBM BladeCenter:

- | • Identifikuje servisní procesor podle sériového čísla, typu a modelu.
- | • Definuje, jak lze servisní procesor nebo Management Module vyhledat v síti Ethernet pomocí internetové adresy nebo jména hostitele.

- Objekt servisního procesoru může volitelně obsahovat hodnoty určené pro zabezpečení procesu zavádění systému i5/OS při komunikaci se servisním procesorem.

**Poznámka:** U serverů xSeries připojených pomocí iSCSI je mezi objektem servisního procesoru a konfigurací vzdáleného systému relace typu 1:1, protože každý servisní procesor řídí pouze jeden server xSeries. U serverů IBM BladeCenter připojených pomocí iSCSI však může být mezi objektem servisního procesoru a konfigurací vzdáleného systému relace typu 1:N, protože každý Management Module může řídit libovolný ze serverů IBM BladeCenter, které jsou obsaženy ve skříni IBM BladeCenter. Proto by u serverů IBM BladeCenter připojených pomocí iSCSI mělo být obvyklé, aby několik konfigurací vzdáleného systému sdílelo stejný objekt servisního procesoru (nebo na něj odkazovalo).

## Popis síťového serveru

Objekt NWSD (popis síťového serveru), který znázorňuje Obrázek 15 na stránce 40, je v podstatě stejný jako ten, který popisuje Obrázek 14 na stránce 37, kromě následujících výjimek:

- Obsahuje odkaz na objekt konfigurace vzdáleného systému místo na jméno hardwarového prostředku serveru iSeries.
- Na rozdíl od serveru připojeného pomocí adaptéru IXA, který spravuje všechny datové toky sítě SCSI a virtuální sítě Ethernet pomocí jedné karty IXA v systému xSeries, u řešení se serverem připojeným pomocí SCSI mohou mít jak server iSeries, tak server xSeries několik adaptéru iSCSI HBA. To umožňuje vytvořit několik cest k datům v síti SCSI a ve virtuální síti Ethernet mezi serverem iSeries a systémy xSeries nebo IBM BladeCenter, které mohou poskytovat větší šířku pásma a možnost rezervních připojení.
- Můžete definovat jednu nebo více cest k paměťovým prostorům. Tyto cesty k paměťovým prostorům odkazují na objekty NWSH přiřazené adaptéru iSCSI HBA, které jsou používány integrovanými servery. Pro každou virtuální diskovou jednotku můžete zvolit, která cesta bude pro datové toky v síti SCSI použita. Přiřazením virtuálních diskových jednotek k různým cestám k paměťovým prostorům můžete rozložit celkové zatížení datových toků v síti SCSI na serveru na adaptéry iSCSI HBA v dané cestě a získat tak větší šířku pásma.
- Můžete definovat skupinu několika cest, která bude podmnožinou konfigurovaných cest k paměťovým prostorům. Potom můžete přiřadit virtuální diskovou jednotku této skupině cest, a nikoli pouze určité cestě. Použití skupiny několika cest pro virtuální diskovou jednotku má tu výhodu, že zatížení toku dat v síti SCSI pro tuto virtuální diskovou jednotku bude v případě, že selže adaptér iSCSI HBA pro jeden z objektů NWSH ve vícenásobné cestě nebo připojení tohoto adaptéru iSCSI HBA do sítě, automaticky přeměrováno na jeden z ostatních adaptéru iSCSI HBA, který je konfigurován ve vícenásobné cestě. Tím je zajištěna redundance připojení a zvýšena dostupnost.
- Můžete definovat jednu nebo více cest k virtuální síti Ethernet. Tyto cesty také odkazují na objekty NWSH, které používá integrovaný server. Pro každý port virtuální sítě Ethernet, který bude používat integrovaný server, můžete vybrat objekt NWSH. Přiřazením různých portů virtuální sítě Ethernet různým objektům NWSH můžete rozložit celkové zatížení datových toků virtuální sítě Ethernet na serveru na adaptéry iSCSI HBA v cestě k virtuální síti Ethernet a získat tak větší šířku pásma.
- Stejně jako u serverů IXS a serverů připojených pomocí adaptéru IXA je hardware serveru xSeries nebo IBM BladeCenter řízen operačním systémem i5/OS.
  - Spuštění serveru připojeného pomocí iSCSI a jeho ukončení se provádí stejně jako u serveru IXS nebo serveru připojeného pomocí adaptéru IXA (viz Obrázek 14 na stránce 37) logickým zapnutím a vypnutím objektu NWSD pro tento server.
  - U serverů xSeries a IBM BladeCenter připojených pomocí iSCSI komunikuje operační systém i5/OS při spuštění a ukončování úloh přes síť Ethernet se servisním procesorem (SP) systému xSeries nebo přes Management Module systému IBM BladeCenter pro server IBM BladeCenter.

Hlavní rozdíl mezi konfiguracemi IXS/IXA a iSCSI při řízení napájení hardwaru serveru spočívá v tom, že u serverů IXS a serverů připojených pomocí adaptéru IXA je hardware serveru identifikován jménem hardwarového prostředku na serveru iSeries, kdežto u serverů připojených pomocí iSCSI je hardware serveru identifikován objektem konfigurace vzdáleného systému.

**Poznámka:** Protože server xSeries nebo IBM BladeCenter, na němž je provozován server připojený pomocí iSCSI, je definován pomocí jména konfigurace vzdáleného systému v objektu NWSD, je snadné tento hardware, na kterém je spuštěn integrovaný server připojený pomocí iSCSI, přepnout. Výměnu serveru

xSeries nebo serveru IBM BladeCenter, na němž je zaveden existující objekt NWSA, lze za chodu provést změnu jména konfigurace vzdáleného systému. Další informace najdete v tématu “Výměna hardwaru serveru za chodu” na stránce 148.

### **Paměťové prostory síťového serveru**

Objekty paměťového prostoru síťového serveru (NWSSTG), které znázorňuje Obrázek 15 na stránce 40, jsou v podstatě stejné jako ty, které popisuje výše uvedený Obrázek 14 na stránce 37, kromě níže uvedených výjimek:

- Při vytváření propojení virtuální diskové jednotky s objektem NWSA musíte určit, která z cest k paměťovým prostorům objektu NWSA má být pro tuto virtuální diskovou jednotku použita pro datové toky SCSI.
- Můžete vybrat určitou cestu k paměťovým prostorům, skupinu více cest nebo můžete používat předvolenou cestu.

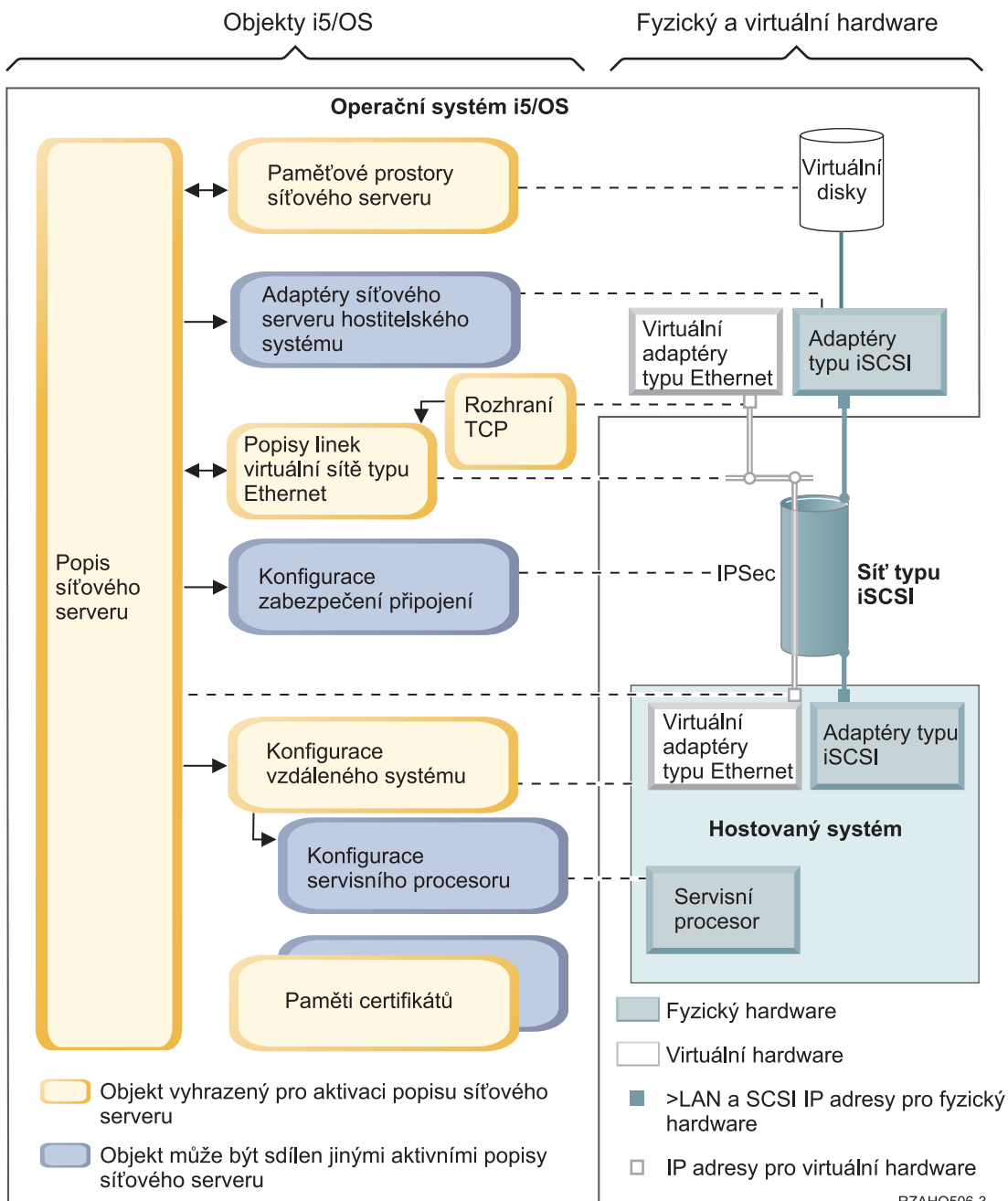
Další informace najdete v tématu “Paměťové prostory síťového serveru” na stránce 38.

### **Datové toky**

Obrázek 15 na stránce 40 znázorňuje, jak data diskové jednotky SCSI a virtuální sítě Ethernet procházejí mezi operačním systémem i5/OS a integrovaným serverem připojeným pomocí iSCSI přes síť Ethernet. V podstatě jsou protokoly diskových jednotek SCSI a protokoly virtuální sítě Ethernet zapouzdřeny a tunelovány uvnitř normálních síťových protokolů typu Ethernet.

### **Servery xSeries a BladeCenter připojené pomocí iSCSI se zabezpečením**

Protože servery připojené pomocí iSCSI mohou sdílet síť s jinými systémy, můžete síť iSCSI a připojení servisních procesorů do sítě zabezpečit. Následující obrázek znázorňuje objekty, které operační systém i5/OS používá při konfiguraci zabezpečení pro servery připojené pomocí iSCSI.



RZAHQ506-3

Obrázek 16. Objekty konfigurace iSCSI v systému i5/OS se zabezpečením sítě

Obrázek 16 znázorňuje klíčové objekty operačního systému i5/OS a také klíčové hardwarové komponenty používané pro servery xSeries a IBM BladeCenter připojené pomocí iSCSI, je-li použito zabezpečení sítě.

Níže uvedené části popisují objekty, které ukazuje Obrázek 16:

- “Konfigurace vzdáleného systému” na stránce 45
- “Konfigurace servisního procesoru” na stránce 45
- “Konfigurace zabezpečeného připojení” na stránce 45
- “Paměť certifikátů” na stránce 45
- “Popis síťového serveru” na stránce 42
- “Paměťové prostory síťového serveru” na stránce 43



- “Datové toky” na stránce 43
- “Popisy linek virtuální sítě Ethernet” na stránce 39
- “Rozhraní TCP/IP” na stránce 39

## Konfigurace vzdáleného systému

Objekt konfigurace síťového serveru ve vzdáleném systému (objekt NWSCFG typu RMTSYS), který znázorňuje Obrázek 16 na stránce 44, je stejný jako objekt, který je popsán v tématu “Konfigurace vzdáleného systému” na stránce 41 (Obrázek 15 na stránce 40), s tou výjimkou, že obsahuje hodnoty konfigurace protokolu CHAP (Challenge Handshake Authentication Protocol) používané k ověřování identity vzdáleného systému při prvním přístupu k paměťovým prostorům.

## Konfigurace servisního procesoru

Objekt konfigurace síťového serveru se servisním procesorem (objekt NWSCFG typu SRVPRC), který znázorňuje Obrázek 16 na stránce 44, je stejný jako objekt, který je popsán v tématu “Konfigurace servisního procesoru” na stránce 41 (Obrázek 15 na stránce 40), s následujícími výjimkami:

- Obsahuje jméno uživatele a heslo servisního procesoru používané pro přihlášení k servisnímu procesoru.
- Obsahuje informace požadované pro správu volitelných certifikátů SSL používaných pro zabezpečení komunikací servisního procesoru v systému i5/OS.

## Konfigurace zabezpečeného připojení

Objekt konfigurace síťového serveru se zabezpečeným připojením (objekt NWSCFG typu CNNSEC), který znázorňuje Obrázek 16 na stránce 44, zabezpečuje toky dat v síti SCSI a ve virtuální síti Ethernet mezi operačním systémem i5/OS a serverem xSeries nebo IBM BladeCenter připojeným pomocí iSCSI:

- Identifikuje sadu pravidel zabezpečení IP (IPSec) používaných pro různá připojení paměti a virtuální sítě Ethernet.
- Můžete rozhodnout, které toky dat budou zabezpečené a které ne. Můžete zabezpečit všechna připojení v rámci paměťových prostorů a připojení přes virtuální síť Ethernet, nebo jen některá z nich, anebo žádná. Můžete například zvolit, že chcete zabezpečit pouze toky dat SCSI nebo jen jedno z připojení přes virtuální síť Ethernet.
- Zadáním odpovídajících pravidel pro parametry cest k paměťovým prostorům a cest k virtuální síti Ethernet v objektu NWSD označíte, které toky dat SCSI a které toky dat virtuální sítě Ethernet budou zabezpečené.
- Používáte-li zabezpečení IPSec, jsou toky dat sítě SCSI a virtuální sítě Ethernet mezi operačním systémem i5/OS a integrovaným serverem připojeným pomocí iSCSI šifrovány a mají další vrstvu zapouzdření (tunelování) v normálních protokolech sítě Ethernet.

## Paměť certifikátů

Certifikáty zabezpečují komunikace mezi operačním systémem i5/OS a hostovaným systémem pro různé funkce. Certifikáty se uchovávají v níže uvedených pamětech certifikátů operačního systému i5/OS:

- **Systémová paměť certifikátů operačního systému i5/OS.** Tato paměť certifikátů je místo, do něhož jsou ukládány certifikáty vydavatele certifikátů z důvěryhodného zdroje, které byly manuálně importovány do servisního procesoru hostovaného systému z externího zdroje. Systémová paměť certifikátů je sdílena mnoha aplikacemi operačního systému i5/OS.
- **Paměť certifikátů, která je asociována s konfigurací servisního procesoru.** Tato paměť certifikátů je vytvářena automaticky. Certifikáty v této paměti certifikátů jsou používány pouze při komunikacích s hostovanými systémy, které používají příslušnou konfiguraci servisního procesoru. Tato paměť certifikátů je sdílená, pokud několik hostovaných systémů (například blade serverů IBM BladeCenter) používá stejnou konfiguraci servisního procesoru. Certifikáty se do této paměti certifikátů ukládají za těchto podmínek:
  - Při generování certifikátu používáte volbu konfigurace servisního procesoru.
  - Synchronizujete certifikát ze servisního procesoru v hostovaném systému s příslušnou konfigurací servisního procesoru.
- **Paměť certifikátů, která je asociována s popisem síťového serveru.** Tato paměť certifikátů je vytvářena a udržována automaticky. Ukládají se do ní certifikáty, které jsou generovány a používány pro interní účely produktem Integrated Server Support operačního systému i5/OS (například certifikáty používané při zápisu uživatelů do hostovaného systému). Certifikáty v této paměti certifikátů slouží pouze ke komunikaci s hostovanými systémy, které používají příslušný popis síťového serveru.



---

## Koncepce vysoké dostupnosti

Integrace a virtualizace paměti serverů iSeries a xSeries umožňuje inovace, které mohou zvýšit spolehlivost a obnovitelnost prostředí Windows serveru. Hostované systémy mohou zajišťovat zvýšenou dostupnost pomocí některé z následujících technologií.

### Výměna hardwaru za chodu

Výměna hardwaru za chodu umožňuje rychle napravit určité typy selhání hardwaru. Pomáhá redukovat prostoje serveru z hodin na minuty. Chcete-li minimalizovat prostoje hostovaných systémů způsobené selháním hardwaru, můžete zvolit jeden ze dvou způsobů výměny hardwaru hostovaných systémů za chodu:

1. Hardware hostovaného systému včetně serverů IXS (Integrated xSeries Server), serverů xSeries připojených pomocí adaptéru IXA (Integrated xSeries Adapter) a serverů xSeries nebo IBM BladeCenter připojených pomocí iSCSI HBA lze vyměňovat za chodu. Selže-li hardware, na kterém je spuštěn hostovaný systém, můžete rychle přepnout obraz disků hostovaného systému na kompatibilní rezervní hardware a hostovaný systém restartovat. Další informace najdete v tématu “Výměna hardwaru serveru za chodu” na stránce 148.
2. U serverů připojených pomocí iSCSI lze cílové adaptéry iSCSI HBA serveru iSeries vyměňovat za chodu. Selže-li adaptér iSCSI HBA používaný hostovaným systémem, můžete hostovaný systém rychle přepnout tak, aby používal rezervní adaptér iSCSI HBA a hostovaný systém restartovat. Další informace najdete v tématu “Výměna adaptérů v lokálním hostitelském systému iSCSI za chodu” na stránce 128.

### Vícenásobné cesty sítě iSCSI

Hostovaný systém může pro přístup k virtuálním diskům, jejichž hostitelem je operační systém i5/OS, používat redundantní datové cesty sítě iSCSI. Stačí definovat skupinu dvou nebo více adaptérů iSCSI HBA a potom zadat, že přístup k danému virtuálnímu disku lze realizovat přes tuto skupinu, a nikoli přes jediný adaptér iSCSI HBA. S touto konfigurací budou data na virtuálním disku přístupná pomocí libovolného adaptéru iSCSI HBA z této skupiny.

Výhodou konfigurace s vícenásobnými cestami je, že když jeden z adaptérů iSCSI HBA ve skupině cest selže, může hostovaný systém bez přerušení pokračovat v přístupu na disky, které jsou konfigurovány na použití této skupiny cest, pomocí libovolného z ostatních adaptérů iSCSI HBA z této skupiny. Další informace najdete v tématu “Rozšířená podpora sítě iSCSI” na stránce 20.

### Služba MSCS (Microsoft Windows Cluster Service)

Hostované servery mohou používat službu MSCS, která zajišťuje přepnutí při selhání aplikací v reálném čase v případě, že hardware nebo software hostovaného systému selže. Uživatelsky vyvolaná přepnutí při selhání mohou být využita, chcete-li server převést do režimu offline, aby mohla být provedena údržba nebo zálohování, zatímco aplikace budou pokračovat v práci na ostatních serverech v klastru. Další informace najdete v tématu “Klastrová služba Windows” na stránce 95.

---

## Koncepce zabezpečení

Postupy, které slouží k implementaci níže uvedených koncepcí zabezpečení, najdete v tématu “Konfigurace zabezpečení mezi operačním systémem i5/OS a hostovanými systémy” na stránce 123. Lze volit mezi několika typy zabezpečení.

- “Zabezpečení pro systémy IXS a systémy připojené pomocí adaptéru IXA”
- “Zabezpečení u systémů připojených pomocí iSCSI” na stránce 47

## Zabezpečení pro systémy IXS a systémy připojené pomocí adaptéru IXA

Toky dat v rámci paměťových prostorů a virtuální sítě Ethernet u systémů IXS a systémů připojených pomocí adaptéru IXA procházejí přes fyzicky zabezpečené systémové sběrnice a kabely typu HSL serveru iSeries.

## **Zabezpečení u systémů připojených pomocí iSCSI**

Technologie iSCSI využívá nízké náklady na vytváření sítí Ethernet a IP a všeobecnou obeznamenost s těmito sítěmi. Flexibilita sítí Ethernet a IP umožňuje systémům připojeným pomocí iSCSI sdílet hardware, rozšiřovat rozsah a zvyšovat šířku pásma přidáváním hardwaru. Tato obeznamenost a flexibilita ale přináší požadavky na náležitě zabezpečení sítí.

Zabezpečení různých typů sítí používaných systémy připojenými pomocí iSCSI ovlivňují různé faktory.

### **Zabezpečené připojení servisního procesoru**

Zabezpečení servisního procesoru může zahrnovat jeden nebo více následujících mechanismů:

- Heslo servisního procesoru.
- Připojení SSL (Secure Sockets Layer).
- Izolace a fyzické zabezpečení sítě.

### **Zabezpečení sítě iSCSI**

Je třeba vzít v úvahu dva typy přenosů v síti iSCSI.

- Zabezpečení paměti může zahrnovat jeden nebo více následujících mechanismů.
    - Protokol CHAP (Challenge Handshake Authentication Protocol).
    - Zabezpečení IPSec (Internet Protocol Security).
    - Ochranné bariéry (firewall).
    - Izolace a fyzické zabezpečení sítě a bezpečnostní brány.
  - Zabezpečení virtuální sítě Ethernet může zahrnovat jeden nebo více následujících mechanismů.
    - Zabezpečení IPSec (Internet Protocol Security).
    - Ochranné bariéry (firewall).
    - Izolace a fyzické zabezpečení sítě a bezpečnostní brány.
    - V případě, že jsou při zápisu uživatele nebo zadání vzdáleného příkazu odesílána přes dvoubodovou virtuální síť Ethernet citlivá data, používají tyto aplikace také připojení SSL mezi operačními systémy i5/OS a Windows.
- Další informace o zápisu uživatele najdete v tématu “Koncepce týkající se uživatelů a skupin” na stránce 49.

### **Heslo servisního procesoru**

Toto heslo je spravováno operačním systémem i5/OS a použije se, když server iSeries zahájí konverzaci se servisním procesorem hostovaného systému. Servisní procesor heslo zkontroluje, aby byla zajištěna autenticita konfigurace operačního systému i5/OS. Nové servisní procesory mají předvolená jména a hesla. Operační systém i5/OS umožňuje změnu hesla.

### **SSL servisního procesoru**

Tento typ zabezpečení SSL můžete povolit pouze tehdy, má-li servisní procesor odpovídající typ hardwaru. Je-li zabezpečení SSL povoleno, zašifruje přenosy v připojení servisního procesoru a zajistí tak autenticitu servisního procesoru. Autentizace se provádí na základě certifikátu od servisního procesoru, který je manuálně nebo automaticky nainstalován v systému i5/OS. Tento certifikát se liší od digitálních certifikátů používaných pro připojení pomocí SSL mezi operačními systémy i5/OS a Windows.

### **Spojení SSL mezi operačními systémy i5/OS a Windows**

Prostředí Windows na serveru iSeries umožňuje funkce zápisu uživatelů a zadávání vzdálených příkazů, které mohou přenášet citlivá data přes dvoubodovou virtuální síť Ethernet. Tyto aplikace automaticky nastavují připojení pomocí SSL, aby byly citlivé síťové přenosy šifrovány a aby bylo na základě automaticky instalovaných digitálních certifikátů zajištěno, že obě strany konverzace jsou autentické. Tyto certifikáty se liší od digitálních certifikátů používaných pro SSL servisního procesoru. Tato funkce zabezpečení je dodávána v předvoleném nastavení a nelze ji konfigurovat. Data souborů, výsledky příkazů a přenosy pro jiné aplikace nejsou tímto připojením SSL chráněny.

### **Protokol CHAP (Challenge Handshake Authentication Protocol)**

Protokol CHAP chrání před možností přístupu neoprávněného systému k paměťovým prostorům pomocí jména iSCSI oprávněného systému. Protokol CHAP nešifruje síťové přenosy, ale omezuje přístup jednotlivých systémů k cestě k paměťovým prostorům v operačním systému i5/OS.

Protokol CHAP zahrnuje konfiguraci šifrovacího klíče, který musí znát jak operační systém i5/OS, tak hostovaný systém. Krátké klíče mohou být odhaleny, je-li vzájemná výměna protokolu CHAP zaznamenána nebezpečným programem, který prohledává síť LAN (LAN sniffer), a analyzována v režimu offline. Klíč CHAP by měl být náhodný a dostatečně dlouhý, aby tento způsob napadení znemožnil. Operační systém i5/OS může klíč generovat. Hostovaný systém používá při přístupu ke všem svým cestám k paměťovým prostorům v operačním systému i5/OS stejný klíč CHAP.

Protokol CHAP není v předvoleném nastavení aktivován, ale doporučuje se.

### **Zabezpečení IPsec (Internet Protocol Security)**

Zabezpečení IPsec šifruje přenosy v rámci paměťových prostorů a přenosy přes virtuální síť Ethernet v síti iSCSI. Související protokol IKE (Internet Key Exchange) zajišťuje, aby komunikující koncové body protokolu IP byly autentické.

Chcete-li zabezpečení IPsec povolit, musejí být splněny dvě podmínky:

1. Jak systém iSeries, tak hostovaný systém musejí mít speciální adaptéry iSCSI HBA s podporou vysokorychlostního IPsec.
2. Musíte konfigurovat předem nasdílený klíč. Operační systém i5/OS může generovat odpovídající předem nasdílené klíče. Pokud je v systému iSeries nebo v hostovaném systému začleněno několik adaptérů iSCSI HBA, můžete různým dvojicím IP adres přiřadit různé předem nasdílené klíče. Všechny ostatní podrobnosti zabezpečení protokolem IPsec a IKE jsou nastaveny automaticky. Podpora zabezpečení IPsec není v rozhraní TCP/IP operačních systémů i5/OS a Windows zahrnuta.

Adaptéry HBA IPsec mají možnost filtrování, která blokuje komunikaci s nenakonfigurovanými IP adresami. Tyto adaptéry provádějí filtrování dokonce i tehdy, není-li šifrování IPsec aktivováno dodáním předem nasdíleného klíče.

Při použití s virtuální sítí Ethernet není zabezpečení IPsec použito přímo na koncové body virtuální sítě Ethernet, ale na adaptéry iSCSI HBA, které tvoří tunel sítí iSCSI. V důsledku toho je konfigurace IPsec na každém z Windows serverů připojených pomocí iSCSI, které navzájem komunikují přes virtuální síť Ethernet, nezávislá na ostatních. Je například možné použít IPsec na serveru, který komunikuje s jinými servery, i když tyto servery používají namísto IPsec fyzické zabezpečení. Vzájemná komunikace serverů nevyžaduje, aby servery používaly stejný předem nasdílený klíč IPsec.

### **Ochranné bariéry (firewall)**

Firewall mezi sdílenou sítí a serverem iSeries chrání server iSeries před nevyžádanými síťovými přenosy. Firewall lze také použít mezi sdílenou sítí a hostovaným systémem; chrání pak hostovaný systém před nevyžádanými síťovými přenosy.

Přenosy v systému připojeném pomocí iSCSI má následující atributy, které se vám mohou hodit při konfiguraci firewallu.

- Adaptéry iSCSI HBA mají statické IP adresy (je tu zaváděcí režim DHCP, ale IP adresy jsou ve skutečnosti předem konfigurovány staticky).
- Porty UDP a TCP jsou deterministické a konfigurovatelné. Každý virtuální adaptér Ethernet v hostovaném systému používá k vytváření tunelů sítí iSCSI jiný port UDP. Pakety virtuální sítě Ethernet jsou zapouzdřeny následujícím způsobem (od vnějšího záhlaví k vnitřnímu):
  - Záhlaví MAC a IP pro adaptér iSCSI HBA používající adresy sítě LAN (ne SCSI).
  - Záhlaví UDP. Informace o volitelném výběru řídicího portu UDP najdete v tématu “Konfigurace firewallu” na stránce 126.
  - Záhlaví MAC a IP pro adaptér virtuální sítě Ethernet.

| Adaptéry HBA zabezpečení IPsec poskytují podobnou funkci jako firewall: blokuji komunikaci s IP adresami, které nejsou konfigurovány, a to i tehdy, není-li zabezpečení IPsec aktivováno dodáním předem nasdíleného klíče.

#### | **Izolace a fyzické zabezpečení sítě**

| Izolace sítě minimalizuje riziko přístupu neoprávněných zařízení k datům a modifikace dat při průchodu sítě.  
| Izolovanou síť můžete vytvořit pomocí vyhrazeného přepínače Ethernet nebo pomocí vyhrazené virtuální sítě VLAN na fyzickém přepínači/síti VLAN. Při konfiguraci přepínače VLAN považujte adaptér iSCSI HBA instalovaný na serveru iSeries za zařízení, které je pro VLAN neznámé.

| Fyzické zabezpečení zahrnuje fyzické bariéry, které omezují přístup k vybavení sítě a k jejím koncovým bodům na určité úrovni (zamčené kryty stojanů, zamčené místnosti, zamčené budovy atd.).

---

## Koncepce týkající se uživatelů a skupin

Jednou z hlavních výhod používání prostředí Windows na serveru iSeries je funkce pro administraci uživatelských profilů i5/OS a Windows. Funkce pro administraci uživatelů umožňuje administrátorům, aby existující uživatelské a skupinové profily i5/OS zapsali do Microsoft Windows. Podrobnější informace o této funkci jsou uvedeny dále v této části.

### **Zápis**

Zápis je proces, kterým jsou uživatelské a skupinové profily i5/OS registrovány pomocí integračního softwaru.

Proces zápisu se provádí automaticky spuštěním události, jako je například spuštění příkazu CHGNWSUSRA, kterým se zapisují uživatelé a skupiny, aktualizace hesla uživatelského profilu nebo atributů uživatele v systému i5/OS pro zapsaného uživatele Windows nebo restart integrovaného serveru. Je-li integrovaný Windows server aktivní, změny se projeví okamžitě. Jestliže je integrovaný server logicky vypnutý, změny se projeví při příštím spuštění serveru.

### **Domény Windows a lokální servery**

Zápis lze provést buď do domény Windows, nebo na lokální server. Doména Windows je sada prostředků (aplikací, počítačů, tiskáren) navzájem propojených v rámci sítě. Uživatel má v celé doméně jediný účet a k získání přístupu ke všem prostředkům mu stačí přihlásit se do domény. Integrovaný server může být členským serverem domény Windows a integrovat uživatelské účty i5/OS do domény Windows.

Zapíšete-li ale uživatele i5/OS na integrovaný server, který není součástí domény, jedná se o **lokální server** a uživatelské účty budou vytvořeny pouze na tomto integrovaném serveru.

**Poznámka:** Při vytváření sítě ve Windows mohou být skupiny lokálních serverů volně sdruženy pomocí pracovních skupin Windows. Jestliže například otevřete složku Místa v síti a klepnete na Okolní počítače, zobrazí se seznam počítačů ve stejné pracovní skupině, ve které se nacházíte.

### **Skupiny uživatelů operačního systému i5/OS v operačním systému Microsoft Windows**

V operačním systému Microsoft Windows jsou jako součást instalace na integrovaný server vytvořeny dvě skupiny uživatelů.

- **AS400\_Users.** Každý uživatel operačního systému i5/OS je při prvním zápisu do prostředí Windows zařazen do skupiny AS400\_Users. Uživatele můžete z této skupiny v prostředí Windows odstranit, ale při příští aktualizaci v systému iSeries bude uživatel do skupiny znovu zařazen. Tato skupina je užitečná, protože umožňuje kontrolovat, které uživatelské profily i5/OS jsou zapsány do prostředí Windows.
- **AS400\_Permanent\_Users.** Uživatele nelze z této skupiny v prostředí Windows odstranit pomocí serveru iSeries. Tato skupina poskytuje uživatelům Windows ochranu před neúmyslným výmazem v důsledku činnosti prováděné v operačním systému i5/OS. I když bude uživatelský profil v operačním systému i5/OS vymazán, tento uživatel

bude nadále existovat v prostředí Windows. Členství v této skupině je řízeno z prostředí Windows na rozdíl od skupiny AS400\_Users. Vymažete-li uživatele z této skupiny, nebude již při aktualizaci operačního systému i5/OS obnoven.

### Použití atributu LCLPWDMGT uživatelského profilu i5/OS

Hesla uživatelských profilů je možné spravovat dvojím způsobem.

- **Tradiční uživatel.** Můžete zvolit, že hesla v operačních systémech i5/OS a Windows budou stejná. Hesla v operačních systémech i5/OS a Windows budou stejná, nastavíte-li v uživatelském profilu i5/OS atribut LCLPWDMGT na hodnotu \*YES. S atributem LCLPWDMGT(\*YES) spravují zapsaní uživatelé Windows svá hesla v operačním systému i5/OS. Atribut LCLPWDMGT se zadává v systému i5/OS pomocí příkazů CRTUSRPRF (Vytvoření uživatelského profilu) nebo CHGUSRPRF (Změna uživatelského profilu).
- **Uživatel Windows.** Můžete zvolit, že správa hesel zapsaných uživatelských profilů Windows bude prováděna v prostředí Windows. Zadáním parametru LCLPWDMGT(\*NO) nastavíte heslo uživatelského profilu i5/OS na hodnotu \*NONE. Toto nastavení umožní zapsaným uživatelům Windows, aby spravovali svá hesla v prostředí Windows, aniž by operační systém i5/OS jejich heslo přepsal.

Další informace najdete v tématu “Typy uživatelských konfigurací” na stránce 51.

### Použití mapování EIM (Enterprise Identity Mapping) v systému i5/OS

- | Podporu mapování EIM v operačním systému i5/OS můžete využít dvěma způsoby. Můžete automaticky vytvořit asociace EIM pomocí funkcí v registru EIM ve Windows. Definováním asociací EIM umožníte operačnímu systému i5/OS, aby podporoval funkci jediného přihlášení pomocí některé z metod autentizace, jako je například Kerberos.
- | Zdrojové asociace EIM ve Windows jsou automaticky vytvářeny a odstraňovány použitím příkazů CRTUSRPRF, CHGUSRPRF a DLTUSRPRF (Vytvoření, Změna a Výmaz uživatelského profilu) operačního systému i5/OS
- | s parametrem EIMASSOC nastaveným na hodnoty \*TARGET, \*TGTSRC a \*ALL.

Asociace EIM můžete definovat manuálně v registru EIM ve Windows. Je-li pro uživatelský profil i5/OS definována cílová asociace EIM v systému i5/OS a zdrojová asociace ve Windows, může být zapsaný uživatelský profil i5/OS definován ve Windows pod odlišným jménem uživatelského profilu.

- | **Poznámka:** Operace SBMNWSCMD, QNTC a zálohování na úrovni souborů fungují pouze s asociacemi EIM pro Kerberos. Uživatelé i5/OS namapované na různá jména uživatelů Windows pomocí registru EIM ve Windows nebudou rozpoznána. Tyto operace se stále pokoušejí používat stejná jména.

Další informace najdete v tématu “Mapování EIM” na stránce 172.

### Zápis existujících uživatelských profilů Windows

Můžete také zapsat uživatele, který již v prostředí Windows existuje. Heslo tohoto uživatele musí být v systému i5/OS stejné, jako má již existující uživatel nebo skupina ve Windows. Další informace najdete v tématu “Posouzení hesla” na stránce 53.

### Šablony pro zápis uživatelů

Oprávnění a vlastnosti, které uživatel obdrží při zápisu, můžete uživatelsky přizpůsobit pomocí šablon pro zápis uživatelů. Další informace najdete v tématu “Šablony pro zápis uživatelů” na stránce 52. Jestliže při zápisu uživatelů nepoužijete šablonu, obdrží uživatelé tato předvolená nastavení:

- Uživatelé se stanou členy skupiny AS400\_Users a buď skupiny Users na lokálním integrovaném Windows serveru, nebo skupiny Domain Users v doméně Windows.
- Operační systém i5/OS sleduje heslo uživatele, datum ukončení platnosti tohoto hesla, popis a stav uživatele (povoleno/zablokováno) v operačním systému i5/OS.

### Zápis skupin i5/OS



- | Doposud byl popisován pouze zápis jednotlivých uživatelských profilů i5/OS do prostředí Windows. Můžete také
- | zapsat celé skupiny i5/OS. Přidáte-li pak uživatele do těchto skupin i5/OS, které byly zapsány do prostředí Windows,
- | automaticky tyto uživatele vytvoříte a zapíšete také v prostředí Windows.

### Zápis do několika domén

Uživatele a skupiny můžete zapsat do několika domén, ale zpravidla to není nutné. Ve většině prostředí Windows vytvářejí vícenásobné domény důvěryhodné vztahy. V takových případech stačí zapsat uživatele do jedné domény, protože díky důvěryhodným vztahům získává automaticky přístup do ostatních domén. Další informace o důvěryhodných vztazích najdete v dokumentaci systému Windows.

### Uložení a obnovení informací o zápisu

Až dokončíte definice zápisů uživatelů a skupin, měli byste je uložit. Informace o zápisech můžete uložit pomocí volby 21 nebo 23 v menu GO SAVE, příkazem SAVSECDTA nebo použitím rozhraní QRSOVO API. Obnova uživatelských profilů se provádí příkazem RSTUSRPRF s parametrem USRPRF(\*ALL) nebo SECDTA(\*PWDGRP).

### Použití parametru PRPDMNUSR

Máte-li několik serverů, které jsou členy téže domény, můžete na každém členském serveru zabránit duplicitnímu zápisu do domény. Použijte příkaz CHGNWD (Změna popisu síťového serveru) nebo příkaz CRTNWS (Vytvoření popisu síťového serveru) s parametrem PRPDMNUSR (Přenesení uživatele domény). Další informace najdete v tématu “Uživatel QAS400NT” na stránce 175.

## Typy uživatelských konfigurací

Je užitečné si představit uživatele integrovaného systému Windows jako příslušníky tří základních typů:

- **Tradiční uživatel (s heslem spravovaným v i5/OS)**

Předvolba zařadí uživatele do tohoto typu. Tento uživatel funguje ve Windows i v systému i5/OS. Heslo v systému i5/OS bude synchronizováno s heslem ve Windows. Pokaždé, když restartujete integrovaný Windows server, bude heslo uživatele znovu nastaveno na heslo systému i5/OS. Změny hesla lze provádět pouze v systému i5/OS. Tento typ uživatele je doporučený pro spouštění zálohování na úrovni souborů a provádění příkazů ve vzdáleném systému Windows. Chcete-li nastavit uživatele Windows na tuto konfiguraci, použijte příkaz WRKUSRPRF s atributem LCLPWDMGT nastaveným na hodnotu \*YES.

- **Uživatel s heslem spravovaným ve Windows**

Tento uživatel provádí většinu své práce ve Windows a téměř nikdy se nepřihlásí do i5/OS. Přihlásí-li se tento uživatel do i5/OS, musí použít metodu autentizace, jako je například Kerberos, aby získal přístup do i5/OS. Tato situace je diskutována v následujícím tématu: Uživatel Windows s konfigurovaným mapováním EIM (Enterprise Identity Mapping).

Pokud je pro uživatele i5/OS atribut uživatelského profilu LCLPWDMGT nastaven na hodnotu \*NO, je heslo uživatelského profilu i5/OS nastaveno na hodnotu \*NONE. Heslo získané při zápisu do i5/OS bude uloženo, dokud nebude úspěšně dokončen zápis do Windows. Až bude uživatel i5/OS zapsán do Windows, může tento uživatel Windows změnit a spravovat své heslo ve Windows, aniž by je operační systém i5/OS přepsal. Použití této metody zajišťuje bezpečnější prostředí, protože se spravuje méně hesel. Informace o tom, jak vytvořit uživatele tohoto typu, najdete v tématu “Změna atributu LCLPWDMGT v uživatelském profilu” na stránce 172.

- **Uživatel Windows s automaticky konfigurovanými asociacemi EIM (Enterprise Identity Mapping)**

Nastavení atributu EIMASSOC uživatelského profilu na hodnotu \*TGT, TGTSRC nebo \*ALL umožňuje integrovanému serveru automaticky definovat zdrojové asociace EIM ve Windows. Použití automatických definic asociací usnadňuje konfiguraci EIM. Informace o tom, jak vytvořit uživatele tohoto typu, najdete v tématu “Mapování EIM” na stránce 172.

- **Uživatel Windows s manuálně konfigurovanými asociacemi EIM**

Uživatel může zvolit, že bude definovat zdrojové asociace EIM ve Windows manuálně. Tuto metodu můžete použít, chcete-li nastavit uživatelský profil i5/OS tak, aby byl do uživatelského profilu Windows zapsán s jiným jménem. Uživatel musí manuálně definovat cílovou asociaci v systému i5/OS pro uživatelský profil i5/OS a také zdrojovou asociaci ve Windows pro stejný identifikátor EIM.

Tabulka 1. Typy uživatelských konfigurací

Typ uživatele	Poskytovaná funkce	Definice uživatelského profilu
<b>Tradiční</b>	<ul style="list-style-type: none"> <li>• Plně funkční operační systém i5/OS i operační systém Windows.</li> <li>• Snadná konfigurace.</li> <li>• Heslo se mění v systému i5/OS.</li> <li>• ID a hesla uživatele v systému i5/OS a ve Windows budou identická.</li> <li>• Doporučuje se pro systémové administrátory, uživatele, kteří i5/OS používají často, a pro systémy, které zálohují a obnovují uživatelské profily v systému i5/OS.</li> </ul>	LCLPWDMGT(*YES) a zdrojové asociace EIM ve Windows nejsou definovány.
<b>Uživatel s heslem spravovaným ve Windows</b>	<ul style="list-style-type: none"> <li>• Heslo lze změnit ve Windows.</li> <li>• Jednoduchá konfigurace.</li> <li>• Administrace hesel ve Windows zvyšuje zabezpečení konfigurace, protože heslo systému i5/OS je *NONE.</li> <li>• Přihlášení do i5/OS vyžaduje metodu autentizace, jakou poskytuje například produkt iSeries Navigator tím, že podporuje přihlášení do i5/OS pomocí protokolu Kerberos.</li> </ul>	LCLPWDMGT(*NO)
<b>Uživatel Windows s automaticky konfigurovanými asociacemi EIM</b>	Automatické vytvoření zdrojových asociací ve Windows usnadňuje nastavení a konfiguraci aplikací, které podporují protokol Kerberos.	Například: EIMASSOC(*CHG *TARGET *ADD *CRTEIMID)
<b>Uživatel Windows s manuálně konfigurovanými asociacemi EIM (Enterprise Identity Mapping)</b>	Umožňuje uživateli definovat asociace EIM pro zapsané uživatelské profily i5/OS tak, aby uživatelské profily byly ve Windows odlišné.	Chcete-li manuálně definovat cílové asociace EIM v systému i5/OS a zdrojové asociace ve Windows, použijte produkt iSeries Navigator.

## Šablony pro zápis uživatelů

Šablona pro zápis uživatelů je nástroj, který usnadňuje zápis uživatelů i5/OS do prostředí Windows. Namísto manuální konfigurace mnoha nových uživatelů (všech se stejným nastavením) můžete k zápisu uživatelů použít šablonu a uživatele nakonfigurovat automaticky. Každá šablona je vlastně uživatelský profil ve Windows, který definuje práva uživatele, jako například členství ve skupině, cesty k adresářům a zásobníky organizační jednotky.

Při zápisu uživatelů a skupin v systému i5/OS do prostředí Windows můžete uživatelskou šablonu použít jako základ pro nové uživatele Windows. Příklad: Můžete vytvořit uživatelskou šablonu a nazvat ji USRTEMP. Šablona USRTEMP bude být členem skupin NTG1 a NTG2 Windows serverů. V operačním systému i5/OS budete mít skupinu se jménem MGMT. Můžete se rozhodnout, že chcete skupinu MGMT a její členy zapsat na Windows server. Během procesu zápisu jako uživatelskou šablonu uvedete USRTEMP. V průběhu zápisu automaticky přidáte všechny členy skupiny MGMT do skupin NTG1 a NTG2.

Uživatelské šablony vám ušetří práci s nastavováním členství ve skupině pro každého uživatele jednotlivě. Také jsou důsledné v nastavení atributů zapsaných uživatelů.

Uživatelská šablona může být členem libovolné skupiny Windows, ať byla tato skupina zapsána v systému i5/OS, nebo ne. Uživatele můžete zapsat i pomocí šablony, která je členem skupiny nezapsané v systému i5/OS. Pokud to však

provedete, stanou se tyto uživatelé také členy této nezapsané skupiny. Operační systém i5/OS nerozpoznává skupiny, které nebyly v systému i5/OS zapsány. To znamená, že členy skupiny můžete odstranit pouze pomocí programu User Manager ve Windows.

Definujete-li zápis nového uživatele pomocí šablony, která má definovanou složku nebo adresář **Cesta** nebo **Připojení**, bude mít nově vytvořený uživatel Windows stejné definice. Definice složky umožní administrátorovi uživatelů využít přesměrování složky a spravovat službu přihlášení na terminálu.

Definujete-li zápis nového uživatele pomocí šablony a tato šablona je uživatelským objektem v zásobníku organizačních jednotek služby Active Directory ve Windows, bude se nově vytvořený objekt uživatele Windows nacházet ve stejné sekci organizačních jednotek. Organizační jednotka představuje metodu, jak poskytnout uživatelům možnost administračního řízení prostředků.

Stávající uživatelské šablony můžete měnit. Takové změny ovlivní pouze ty uživatele, které zapíšete až poté, co jste šablonu změnili.

Šablony jsou používány pouze při vytváření nově zapsaných uživatelů v prostředí Windows. Provádíte-li zápis za účelem synchronizace existujícího uživatele Windows s jeho protějškem v systému i5/OS, systém Windows šablonu ignoruje.

Podrobný postup najdete v tématu “Vytvoření šablony uživatele” na stránce 170.

## Posouzení hesla

1. Zkontrolujte, zda je systémová hodnota QRETSVRSEC v systému i5/OS nastavena na hodnotu 1. K tomu slouží příkaz WRKSYSVAL (Práce se systémovými hodnotami). Pokud by nebyla tato hodnota nastavena, nebudete moci zapisovat uživatele na integrovaný Windows server, dokud se nepřihlásí do i5/OS.

**Poznámka:** Tato systémová hodnota je také vyžadována pro podporu integrovaného serveru připojeného pomocí iSCSI.

2. Chcete-li zapisovat uživatele ve Windows, měli by tyto uživatelé používat v systému i5/OS hesla, která obsahují pouze znaky a jejichž délka je povolena pro hesla ve Windows. Úroveň hesla lze v systému i5/OS nastavit tak, aby délka hesla uživatelského profilu byla v rozmezí buď 1 - 10 znaků, nebo 1 - 128 znaků. Změna úrovně hesla v systémové hodnotě QPWDVLV v systému i5/OS vyžaduje IPL.
3. Úroveň hesla v systému i5/OS o hodnotě 0 a 1 podporuje hesla s délkou 1 - 10 znaků a povoluje omezenou sadu znaků. Je-li úroveň hesla 0 nebo 1, konvertuje i5/OS hesla pro Windows na malá písmena.
4. Úroveň hesla i5/OS o hodnotě 2 a 3 podporuje hesla s délkou 1 - 128 znaků a povoluje více znaků včetně malých a velkých písmen. Na úrovni 2 a 3 systém i5/OS zachovává rozlišování velkých a malých písmen v heslech pro Windows.
5. Skončí-li platnost hesel zapsaných uživatelů v systému i5/OS, skončí také platnost jejich hesel ve Windows. Uživatelé mohou měnit svá hesla ve Windows, ale nesmějí zapomenout, že je třeba je změnit také v systému i5/OS. Změní-li uživatel nejprve heslo v systému i5/OS, změní se automaticky i heslo ve Windows.
6. Je-li systémová hodnota QSECURITY operačního systému i5/OS nastavena na hodnotu 10, nejsou při přihlášení nově vytvořených uživatelů Windows požadována hesla. Všechny ostatní úrovně QSECURITY v systému i5/OS vyžadují, aby objekt uživatele použil při přihlášení heslo. Další informace o úrovních zabezpečení najdete

v publikaci Zabezpečení iSeries - Referenční informace .

7. Používáte-li jiný jazyk než angličtinu, uvědomte si, že použití jiných než invariantních znaků v uživatelských profilech může mít nepředvídatelné následky. Téma Globalizace obsahuje informace o tom, které znaky patří do invariantní znakové sady. Toto tvrzení je však pravdivé jen tehdy, má-li QPWDVLV hodnotu 0 nebo 1. Má-li QPWDVLV hodnotu 2 nebo 3, je možné invariantní znaky bez problému použít.









---

## Kapitola 5. Instalace a konfigurace prostředí Windows na serveru iSeries

Nastavení prostředí Windows na serveru iSeries zahrnuje instalaci hardwaru a dvou samostatných softwarových součástí: produktu IBM i5/OS Integrated Server Support a operačního systému Windows 2000 Server nebo Windows Server 2003 firmy Microsoft.

Při instalaci a konfiguraci prostředí Windows na serveru iSeries postupujte takto:


1. Podívejte se na webovou stránku IBM iSeries Integrated xSeries solutions  (www.ibm.com/servers/eserver/series/integratedxseries). Ujistěte se, že znáte nejnovější zprávy a informace.
2. Vyhledejte si žhavé novinky a nejnovější informace pro instalovaný hardware.
  - 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. Ujistěte se, že máte správný hardware a software. Další informace najdete v tématech:
  - a. “Hardwarové požadavky”.
  - b. “Softwarové požadavky” na stránce 57.
4. U serverů připojených pomocí serveru IXS nebo adaptéru IXA nainstalujte v případě potřeby hardware. Informace naleznete v tématu Instalace komponent systému iSeries. Vyberte svůj model serveru iSeries. Vyberte adaptéry, pro IXS vyberte **PCI Adapter**, pro IXA vyberte **Integrated xSeries Adapter**. Pokud instalujete adaptér iSCSI HBA, budete nasměrováni k nainstalování hardwaru v kroku 6b.
5. Nainstalujte produkt IBM iSeries Integrated Server Support.
  - a. “Příprava na instalaci integrovaných Windows serverů” na stránce 58
  - b. “Instalace licencovaného programu IBM i5/OS Integrated Server Support” na stránce 62
6. Na integrovaný server nainstalujte Microsoft Windows 2000 Server nebo Windows Server 2003.
  - a. “Plán instalace Windows serveru” na stránce 62
  - b. “Instalace serverů Windows 2000 Server nebo Windows Server 2003” na stránce 86
7. Nyní, po dokončení instalace, nakonfigurujte integrovaný Windows server.
  - a. “Opravy kódu” na stránce 103. Tyto opravy kódu opraví případné chyby zjištěné v licencovaném programu od jeho vydání.
  - b. Kapitola 6, “Správa virtuálních sítí Ethernet a externích sítí”, na stránce 107
  - c. “Nastavení integrovaného Windows serveru na automatické logické zapnutí s TCP/IP” na stránce 102


---

### Hardwarové požadavky

K provozování Windows serverů potřebujete tento hardware:

1. Jeden z následujících serverů IXS (Integrated xSeries Server), adaptérů IXA (Integrated xSeries Adapter) nebo iSCSI HBA.

Popis	Kód označení	Typ-model
2.0 GHz Integrated xSeries Server	4811 4812 4813	4812-001
2.0 GHz Integrated xSeries Server	4710	2892-002
2.0 GHz Integrated xSeries Server	4810	2892-002
1.6 GHz Integrated xSeries Server	2792	2892-001
1.6 GHz Integrated xSeries Server	2892	2892-001
1.0 GHz Integrated xSeries Server	2799	2890-003
1.0 GHz Integrated xSeries Server	2899	2890-003
850 MHz Integrated xSeries Server	2791	2890-002
850 MHz Integrated xSeries Server	2891	2890-002
700 MHz Integrated xSeries Server	2790	2890-001
700 MHz Integrated xSeries Server	2890	2890-001
Integrated xSeries Adapter model 100	0092 <sup>2,3</sup>	2689-001
Integrated xSeries Adapter model 200	0092 <sup>2,4</sup>	2689-002
<b>Poznámky:</b>		
1. Adaptér IXA vyžaduje server xSeries. Server xSeries může mít další požadavky, podrobnosti naleznete na webových stránkách Integrated xSeries solutions ( <a href="http://www.ibm.com/servers/eserver/series/integratedxseries">www.ibm.com/servers/eserver/series/integratedxseries</a> )  .		
2. Hardware se objednává prostřednictvím AAS nebo WTAAS jako machine type 1519-100.		
3. Hardware se objednává prostřednictvím AAS nebo WTAAS jako machine type 1519-200.		

**Poznámka:** Pokud máte hardware integrovaného serveru, který není ve výše uvedené tabulce, získáte informace o specifikacích na webových stránkách IBM Integrated xSeries solutions .

Informace o způsobu instalace hardwaru uvádí téma “Instalace funkcí serveru iSeries”. Popis serverů IXS, adaptérů IXA a iSCSI HBA najdete v tématu “Koncepte týkající se hardwaru” na stránce 13.

2. Server iSeries s dostatečným volným diskovým prostorem, včetně 100 MB pro kód softwaru IBM i5/OS Integrated Server Support a 2047 MB, které bude používat systémová jednotka Windows, nebo pro paměťový prostor serveru.
3. Pro servery IXS jeden nebo více schválených portů LAN nebo adaptérů typu PCI:

Popis	Kód označení	Podporovaný hardwarem IXS typu 4812	Podporovaný hardwarem IXS typu 2892	Podporovaný hardwarem IXS typu 2890
iSeries 1000/100/10 Mbps Ethernet Adapter (měděný UTP)	5701		X	
iSeries Gigabit (1000 Mbps) Ethernet Adapter (optické vlákno)	5700		X	
iSeries Gigabit (1000/100/10 Mbps) Ethernet Adapter (měděný UTP)	2760			X

Popis	Kód označení	Podporovaný hardwarem IXS typu 4812	Podporovaný hardwarem IXS typu 2892	Podporovaný hardwarem IXS typu 2890
iSeries Gigabit (1000 Mbps) Ethernet Adapter (optické vlákno)	2743			X
iSeries 2892 10/100 Mbps port Ethernet	2892		X	
IBM iSeries 10/100 Mbps Ethernet Adapter	2838			X
Vysokorychlostní 100/16/4 Mbps adaptér typu Token-ring PCI	2744		X	X
iSeries 4812 1000/100/10 Mbps port Ethernet	4812	X		

4. Monitor kompatibilní se SVGA, myš a klávesnice. IXS má jenom jeden port pro klávesnici a myš, takže budete potřebovat také rozdělovač kabel, abyste mohli klávesnici i myš připojit zároveň. Máte-li několik integrovaných serverů a plánujete provádět administraci v jeden okamžik vždy pouze jednoho z nich, zvažte možnost předávání jedné sady I/O hardwaru mezi integrovanými servery.
5. Alespoň 128 MB RAM nebo v případě, že používáte Windows Server 2003, alespoň 256 MB RAM. Paměť RAM je instalována v integrovaném serveru a musí se objednávat zvlášť.
6. PC s nainstalovaným operačním systémem Microsoft Windows a produktem iSeries Access (který zahrnuje iSeries Navigator).

**Poznámka:** Produkt iSeries Navigator je preferován ve většině prostředí Windows při konfiguračních úlohách serveru iSeries.


Informace o dalších hardwarových požadavcích najdete v tématech:

- “Požadavky na velikost společné oblasti vyhrazené pro operační systém” na stránce 59
- “Koncepce v oblasti sítí” na stránce 27

## Softwarové požadavky

Potřebujete tento software:

1. i5/OS 5722-SS1, verze 5 vydání 4.  
Jak si zkontrolujete úroveň vydání:
    - a. Na příkazový řádek operačního systému i5/OS napište **Go LICPGM** a stiskněte klávesu Enter.
    - b. Do pole pro volbu napište **10** a prohlédněte si nainstalované produkty.
    - c. Vyhleďte **5722SS1**. Vydání zobrazené po straně je vaše verze. (U některých vydání budete možná muset stisknout F11, aby se číslo verze objevilo.)
  2. IBM i5/OS Integrated Server Support (5722-SS1 volba 29) verze V5R4. Další informace najdete v tématu “Instalace licencovaného programu IBM i5/OS Integrated Server Support” na stránce 62.
  3. IBM iSeries Navigator, který je součástí produktu IBM iSeries Access for Windows (5722-XE1).
- Poznámky:**
- a. Při instalaci produktu iSeries Navigator na PC s operačním systémem Windows proveďte úplnou nebo uživatelskou instalaci a vyberte volitelnou komponentu Integrated Server Administration.
  - b. iSeries Navigator je preferován ve většině prostředí Windows při konfiguračních úlohách iSeries.
4. TCP/IP Connectivity Utilities for i5/OS V5R4 (5722-TC1).


5. Pro servery připojené pomocí IXS a IXA potřebujete Microsoft Windows 2000 Server nebo Windows Server 2003. Pro servery připojené pomocí iSCSI potřebujete Windows Server 2003.
6. Veškeré požadované servisní balíky Microsoft Windows. Nejnovější informace o dostupných servisních balících, které IBM otestovala s produktem i5/OS Integrated Server Support, naleznete na webové stránce IBM Integrated xSeries solutions .

Pro servery iSCSI potřebujete rovněž tento software:

1. IBM Director 5.10

**Poznámka:** IBM Director je bezplatná funkce produktu Virtualization Engine (5733-VE2), která má další softwarové požadavky. Informace najdete v tématu Instalace produktu IBM Director v operačním systému i5/OS v rámci aplikace IBM Systems Software Information Center.


2. IBM i5/OS Digital Certificate Manager (5722-SS1 volba 34) V5R4
3. IBM HTTP Server for iSeries (5722-DG1)

Další informace o instalaci nezbytného softwaru najdete v publikaci iSeries Instalace softwaru 

---

## Příprava na instalaci integrovaných Windows serverů

Instalace proběhne hladce, pokud provedete několik přípravných úkolů.

1. Ověřte si, zda máte oprávnění potřebné k provedení instalace. V operačním systému i5/OS musíte mít zvláštní oprávnění \*IOSYSCFG, \*ALLOBJ a \*JOBCTL. K provedení kroku 8 v tomto kontrolním seznamu je vyžadováno zvláštní oprávnění \*SECADM. Informace o zvláštních oprávněních uvádí publikace Zabezpečení iSeries - Referenční informace .
2. Prostudujte si téma “Požadavky na velikost společné oblasti vyhrazené pro operační systém” na stránce 59.
3. Zajistěte, aby byla synchronizace času správně konfigurována. Další informace najdete v tématu “Synchronizace času” na stránce 60.
4. “Konfigurace i5/OS TCP/IP u integrovaných Windows serverů” na stránce 60.
5. Rozhodněte, kolik integrovaných Windows serverů a podsítí pro váš podnik konkrétně potřebujete.

Jestliže instalujete server připojený pomocí iSCSI, bude každý adaptér iSCSI HBA pro server iSeries vyžadovat dvě fixní IP adresy a každý hostovaný systém xSeries nebo IBM BladeCenter bude požadovat minimálně dvě IP adresy pro iSCSI. Další informace týkající se požadavků na IP adresy najdete v tématu “Koncepce v oblasti sítí” na stránce 27.

Pokud vaše organizace používá IP adresy (organizace používající protokol DHCP mohou konfigurovat integrovaný Windows server tak, aby mu IP adresa byla přidělena automaticky, jako každému standardnímu PC serveru), obstarajte si TCP/IP adresy od správce sítě. Jsou to:

- IP adresy pro všechny externí porty typu TCP/IP.
- Masky podsítě.
- Jméno vaší domény nebo pracovní skupiny.
- IP adresa vašeho serveru DNS (Domain Name System), pokud jej máte.
- IP adresa předvolené brány pro síť LAN, pokud ji máte.

Pokud v systému iSeries provozujete TCP/IP, jsou poslední dvě položky z výše uvedeného seznamu do systému již dodány. Při provádění příkazu INSWNTSVR (Instalace Windows serveru) zadejte do těchto parametrů hodnotu \*SYS.




6. Rozhodněte se, zda chcete používat produkt iSeries Access for Windows, který umožňuje použít produkt iSeries Navigator a provozovat ODBC jako službu Windows. Další informace najdete v tématu iSeries NetServer versus iSeries Access for Windows v rámci aplikace Information Center.

7. Aktivujte NetServer a nastavte uživatelský profil 'guest', abyste mohli na vašem integrovaném serveru provádět úlohy údržby. Další informace najdete v tématu "Povolení serveru iSeries NetServer" na stránce 61 a v tématu "Vytvoření uživatelského profilu 'guest' pro iSeries NetServer" na stránce 61.
8. Je-li to možné, vyhněte se během instalace používání fyzických disků CD-ROM. Vyloučíte tím případné zpoždění při dodávce disků CD-ROM na vzdálené pracoviště a náklady s tím spojené, pokud bude nutné provést reinstalaci serveru nebo aplikovat do instalačního zdroje novou verzi servisního balíku Microsoft nebo opravu typu hotfix, která má zabránit virové infekci (článek číslo 828930 v databázi MS Knowledge Base). Uložte obraz instalačního CD, potom pomocí pole Windows source directory zadejte během instalace jméno cesty k tomuto obrazu. Pokud potřebujete pokyny, najdete je v Červené knize Microsoft Windows Server 2003

Integration with iSeries, SG24-6959  .

**Poznámka:**

Obsah instalačního CD může podléhat licencím jednotlivých autorů a distributorů. Za dodržení těchto licencí odpovídáte sami. Tím, že IBM tuto funkci nabízí, nepřebírá žádnou odpovědnost za dodržení ani prosazení případné licenční smlouvy k tomuto CD.

9. Instalaci můžete přizpůsobit tak, že pomocí konfiguračního souboru změňte předvolené hodnoty v souboru skriptů pro neobsluhovanou instalaci Windows (unattend.txt). Další informace najdete v tématu Kapitola 15, "Konfigurační soubory popisu síťového serveru", na stránce 235.
10. Pokud bude server instalován na externí server xSeries pomocí adaptéru IXA (Integrated xSeries Adapter), prostudujte si tyto odkazy:
  - IXA install read me first 
  - Instalace komponent serveru iSeries
11. Pokud bude server instalován na server IXS (Integrated xSeries Server), najdete příslušné informace v tématu IXS install read me first  .
12. Pokud bude server instalován na externím serveru xSeries nebo na serveru IBM BladeCenter pomocí adaptéru iSCSI HBA, musíte připravit server xSeries nebo server IBM BladeCenter. Další informace naleznete v tématu iSCSI install read me first  .
13. Jestliže bude server instalován na externím serveru xSeries nebo na serveru IBM BladeCenter pomocí adaptéru iSCSI HBA, ujistěte se, že je systémová hodnota i5/OS QRETSVRSEC nastavena na 1. To lze provést pomocí příkazu WRKSYSVAL (Práce se systémovými hodnotami).
14. Pokud na serveru iSeries používáte logické části, pamatujte na to, že podporu IBM i5/OS Integrated xSeries Server Support budete muset instalovat pouze v té logické části, kterou budete používat k logickému zapínání serveru. Nevyžaduje se, aby byl licencovaný program instalován do všech logických částí. Jedna logická část může mít například nainstalovaný licencovaný program i5/OS Integrated xSeries Server Support a jeden nebo více integrovaných souborů, zatímco jiná logická část nebude mít nainstalovaný ani licencovaný program i5/OS Integrated xSeries Server Support, ani žádné integrované servery.
15. Když nainstalujete Windows server do operačního systému i5/OS, vytvoří se objekt NWSD (popis síťového serveru), jako například verze Windows a hardwarový prostředek, který se má použít. Pro daný hardwarový prostředek však můžete mít v danou dobu logicky zapnut (spuštěn) pouze jeden popis NWSD.

## Požadavky na velikost společné oblasti vyhrazené pro operační systém

Společná oblast paměti vyhrazená pro operační systém se používá u vysoce sdílených programů počítače a operačního systému. Společná oblast paměti poskytuje diskový prostor pro úlohy, které musí systém zpracovat a které nevyžadují vaši pozornost. Nastavíte-li tyto společné oblasti paměti příliš malé, snížíte výkon systému. QMCHPOOL nemůžete nastavit na méně než 256 KB. Velikost této společné oblasti paměti se zadává v systémové hodnotě QMCHPOOL (Společná oblast paměti počítače). V této společné oblasti se nespouštějí žádné uživatelské úlohy.

Veškerý podporovaný hardware serveru připojený pomocí IXS a IXA vyžaduje minimálně 856 KB paměti. Informace o požadavcích na paměť v případě serveru připojeného pomocí iSCSI najdete v dokumentu iSCSI install read me first



Velikost společné oblasti vyhrazené pro operační systém můžete zobrazit příkazem WRKSYSSTS (Práce se stavem systému). První společná paměťová oblast na obrazovce WRKSYSSTS je společná oblast vyhrazená pro operační systém.

Systémovou hodnotu QPFRADJ můžete změnit tak, aby systém přizpůsoboval velikosti systémových ASP automaticky. Protože však automatické přizpůsobení výkonu může zatížený systém zpomalit, omezíte jeho použití pravděpodobně pouze na jeden z těchto případů:

- Několik prvních dnů po instalaci.
- Zhruba asi hodinu v době, kdy se mění charakter zatížení systému z denního (převážně interaktivní práce) na noční (převážně dávkové zpracování) a naopak.

## Synchronizace času

Chcete-li dosáhnout synchronizace času v operačním systému i5/OS a v prostředí Windows, postupujte takto:

1. V příkazu INSWNTSV (Instalace Windows serveru) nebo CHGNWSD vyberte \*YES pro synchronizaci data a času. Vyberete-li \*YES, proběhne se každých 30 minut synchronizace času mezi operačním systémem i5/OS a integrovaným Windows serverem. Vyberete-li \*NO, bude čas synchronizován jenom při spuštění serveru.
2. Zajistěte, aby na serveru iSeries byl správný čas, datum a časové pásmo. Jakmile jsou tyto hodnoty nastaveny, budou se automaticky aktualizovat každých šest měsíců při úpravě času kvůli úsporám z využití letního času. Systémová hodnota QTIMZON odstraňuje nutnost dvakrát ročně manuálně měnit systémovou hodnotu QUTCOFFSET.
3. Na konzoli Windows klepněte na **Ovládací panely** → **Datum a čas** a klepněte na kartu **Časové pásmo**, kde z rozbalovacího seznamu vyberte časové pásmo.
4. Vyberte zaškrtnuté políčko **Automaticky posunout hodiny při přechodu na letní čas a zpět**. Pak klepněte na OK.

Pokud nastanou problémy se synchronizací času, zkontrolujte, zda je v systémové hodnotě i5/OS nastaveno LOCALE a ujistěte se, že je správně nastavena.

- | **Poznámka:** Synchronizace času by měla být nastavena na \*NO pro Windows servery aktivních domén a pro servery  
| členů domén. Jelikož aktivní adresář Windows má svou vlastní službu synchronizace, způsobilo by  
| nastavení synchronizace času na \*YES konflikt.

## Konfigurace i5/OS TCP/IP u integrovaných Windows serverů

Při instalaci prostředí Windows pro server iSeries můžete hodnoty zadané při konfiguraci TCP/IP v systému i5/OS použít jako předvolené hodnoty pro konfiguraci integrovaného serveru. Pokud chcete tuto možnost využít a konfiguraci TCP/IP jste dosud neprovedli, musíte ji provést ještě před instalací licencovaného programu IBM i5/OS Integrated Server Support. Do operačního systému i5/OS je rovněž nutné dodat adresy brány. Další informace o konfigurování TCP/IP najdete v tématu TCP/IP.

Pokud máte instalovaný produkt iSeries Navigator, můžete jej použít ke konfigurování připojení TCP/IP. Online nápověda produktu iSeries Navigator vám sdělí, jak TCP/IP konfigurovat. Jestliže produkt iSeries Navigator nainstalovaný nemáte, postupujte takto:

1. Na konzoli i5/OS zadejte příkaz CFGTCP a stiskněte klávesu Enter. Objeví se menu Konfigurace TCP/IP.
2. Vyberte volbu 12 Změna informací o doméně TCP/IP () a stiskněte klávesu Enter. Objeví se obrazovka Změna domény TCP/IP (CHGTCPDMN).
3. Zadejte Jméno lokální domény, uvedené v sekci "Pracovní formulář pro parametry instalace i5/OS" na stránce 65.
4. Do pole Server jmen domény zadejte až 3 IP adresy z pomocného programu pro instalaci Windows serveru nebo z tématu "Pracovní formulář pro parametry instalace i5/OS" na stránce 65. Pak stiskněte klávesu Enter.  
IP adresu brány přidáte do operačního systému i5/OS takto:
5. Z menu Konfigurace TCP/IP vyberte volbu 2 Práce se směry TCP/IP. Objeví se obrazovka Práce se směry TCP/IP.



6. Do pole Volba napište 1, čímž přidáte přenosovou cestu TCP/IP. Objeví se obrazovka Přidání směru TCP/IP.
7. Vyplňte odpovídající pole informacemi pro adresu brány.

## Produkt iSeries Access for Windows na integrovaných Windows serverech

Produkt IBM iSeries Access for Windows umožňuje připojit PC k serveru iSeries přes lokální síť (LAN), twinaxiální propojení nebo vzdálenou linku. Vyznačuje se úplnou sadou integrovaných funkcí, které umožňují uživatelům používat prostředky operačního systému i5/OS stejně snadno, jako funkce svých lokálních PC. V prostředí produktu iSeries Access mohou uživatelé a aplikační programátoři rychle zpracovat informace, aplikace a prostředky vztahující se k celé jejich firmě.

Jestliže na integrovaný server nainstalujete produkt iSeries Access for Windows, můžete povolit, aby se ODBC (Open Database Connectivity) spouštěla jako služba Windows. To vám umožní psát aplikace serveru, které volají ovladač zařízení ODBC kvůli získání přístupu k produktu DB2 for iSeries.

Chcete-li povolit spouštění ODBC přes službu Windows, spusíte po instalaci produktu iSeries Access příkaz CWBCFG s parametrem /s.

Jako jediný uživatel přihlášený do Windows máte plnou podporu u všech ostatních funkcí produktu iSeries Access.

Zdroje dalších informací:

- Můžete si přečíst [porovnání produktů iSeries Access for Windows a iSeries NetServer](#).

## Povolení serveru iSeries NetServer

iSeries NetServer umožňuje klientům Windows připojení k cestám sdílených adresářů i5/OS a ke sdíleným výstupním frontám prostřednictvím TCP/IP. Pokud chcete instalovat servisní balíky, musíte být přihlášení k účtu Windows, který odpovídá uživatelskému profilu iSeries se stejným heslem, nebo musíte mít nakonfigurován uživatelský profil 'guest' pro NetServer.

Máte-li v plánu používat iSeries NetServer pouze k provádění úloh údržby, můžete jej nastavit bez produktu iSeries Navigator. V tom případě můžete použít metodu quickstart (snadný začátek), která je popsána v tématu "Konfigurace serveru iSeries pro NetServer". Požadujete-li u serveru iSeries NetServer všechny jeho funkce, je třeba nainstalovat i produkt iSeries Navigator. Tento produkt vyžaduje, abyste na PC, který používáte pro administraci, nainstalovali produkt iSeries Access (viz "Produkt iSeries Access for Windows na integrovaných Windows serverech"). Po instalaci obou verzí musíte nastavit uživatelský profil 'guest'. Další informace najdete v tématu "Vytvoření uživatelského profilu 'guest' pro iSeries NetServer".

## Vytvoření uživatelského profilu 'guest' pro iSeries NetServer


Dříve než budete moci v prostředí Windows na serveru iSeries aplikovat opravy kódu (PTF), musíte být přihlášení k účtu Windows a k uživatelskému profilu iSeries se stejným heslem, nebo musíte mít uživatelský profil typu 'guest' (NetServer) nakonfigurovaný pro iSeries NetServer. K provedení této úlohy potřebujete zvláštní oprávnění \*SECADM.

Máte-li ve svém systému produkt iSeries Navigator, můžete uživatelský profil 'guest' pro iSeries NetServer nastavit pomocí grafického rozhraní a nepotřebujete zvláštní oprávnění ani heslo.

Jestliže produkt iSeries Navigator nainstalovaný nemáte, postupujte při nastavení uživatelského profilu 'guest' pro iSeries NetServer takto:

1. V operačním systému i5/OS vytvořte uživatelský profil bez zvláštních oprávnění a hesla:  
CRTUSRPRF USRPRF(*jméno uživatele*) PASSWORD(\*NONE) SPCAUT(\*NONE)

### Poznámka:

Informace o uživatelských profilech najdete v publikaci iSeries - Referenční informace .

2. Zadejte následující příkaz, kde *jméno uživatele* je jméno uživatelského profilu, který jste vytvořili:  
CALL QZLSCHSG PARM(*jméno uživatele* X'00000000')
3. Chcete-li iSeries NetServer ukončit, zadejte tento příkaz:  
ENDTCPSVR SERVER(\*NETSVR)
4. iSeries NetServer restartujete tímto příkazem:  
STRTCPSVR SERVER(\*NETSVR)

Můžete se znovu vrátit k části “Povolení serveru iSeries NetServer” na stránce 61 nebo “Příprava na instalaci integrovaných Windows serverů” na stránce 58.

---

## Instalace licencovaného programu IBM i5/OS Integrated Server Support

Chcete-li instalovat produkt IBM i5/OS Integrated Server Support, postupujte na serveru iSeries takto:

1. Jestliže přecházíte na produkt IBM iSeries Integration for Windows Server z verze V5R2 nebo V5R3, prostudujte si toto téma: “Přechod na vyšší verzi licencovaného programu IBM iSeries Integration for Windows Server” na stránce 92. Proveďte kroky uvedené v tématu “Příprava na přechod na vyšší verzi” a zase se vraťte sem.
  2. Vložte disk CD s operačním systémem i5/OS, na kterém je software 5722-SS1, volba 29.
  3. Napište GO LICPGM a stiskněte klávesu Enter.
  4. Z menu **Práce s licencovanými programy** vyberte volbu 11 a stiskněte klávesu Enter.
  5. Pomocí klávesy PageDown vyhledejte v seznamu licencovaných programů položku **Integrated Server Support**.
  6. Vedle popisu zadejte do pole **Volba** hodnotu 1.
  7. Stiskněte klávesu Enter.
  8. Zadejte jméno instalační jednotky, do které jste vložili kompaktní disk i5/OS.
  9. Stiskněte klávesu Enter. Systém nainstaluje software pro integraci.
  10. Po instalaci produktu IBM i5/OS Integrated Server Support nainstalujte nejnovější kumulativní balík PTF od IBM. Pamatujte na to, že při instalaci PTF by na serveru iSeries neměli být žádní uživatelé. Pokud váš systém používá logické části, zaveďte PTF do sekundárních logických částí, do kterých instalujete produkt i5/OS Integrated Server Support a nastavte pro ně volbu pro odloženou aplikaci - “apply delay”. Pak je zaveďte do primární části. Další informace uvádí téma **Instalace PTF do systému rozděleného na logické části**.
  11. Při instalaci nejnovějších PTF postupujte takto:
    - a. Na příkazový řádek operačního systému i5/OS napište GO PTF a stiskněte klávesu Enter.
    - b. Aby se balík PTF nainstaloval, napište 8 a stiskněte klávesu Enter.
    - c. Do pole **Device** zadejte jméno optické jednotky.
    - d. U **Automatic IPL** použijte předvolené nastavení \*YES, pokud váš systém nepoužívá logické části. Stiskněte klávesu Enter a nainstalujte všechny PTF. Jestliže jste hodnotu nezměnili na \*NO, systém se automaticky ukončí a restartuje.
- Další informace o PTF najdete pod heslem **Opravy** v tématu **Začínáme se serverem iSeries**.
12. Jestliže přecházíte na produkt IBM iSeries Integration for Windows Server z verze V5R2 nebo V5R3, přejděte na téma “Přechod na vyšší verzi licencovaného programu IBM iSeries Integration for Windows Server” na stránce 92. Proveďte kroky z části “Po přechodu na vyšší verzi i5/OS” a vraťte se zpět.
  13. Pokud přecházíte na produkt i5/OS Integrated Server Support z předchozího vydání, musíte přejít na novou verzi stávajících integrovaných Windows serverů. Další informace najdete v tématu “Přechod na vyšší verzi licencovaného produktu IBM i5/OS Integrated Server Support na straně integrovaného serveru” na stránce 94.

---

## Plán instalace Windows serveru

1. Doporučujeme, abyste z prvního integrovaného Windows serveru v síti udělali řadič domény a pečlivě jej pojmenovali. (Abyste mohli jméno změnit, musíte nejprve změnit jeho roli.) Řadiče domény obsahují hlavní databázi zabezpečení. Kterýkoliv řadič domény může provést změny, které se pak replikují do všech ostatních řadičů domény.

l Pokud instalujete server připojený pomocí iSCSI, měli byste se rovněž podívat na téma “Plán instalace hardwaru iSCSI”.

l Dříve než nainstalujete Windows 2000 Server nebo Windows Server 2003, musíte doplnit a uložit příkaz, který generuje “pomocný program pro instalaci Windows serveru”. Jiná alternativa je, že můžete vyplnit “Pracovní formulář pro parametry instalace i5/OS” na stránce 65.

Pokračování najdete v tématu “Instalace serverů Windows 2000 Server nebo Windows Server 2003” na stránce 86.

## l **Plán instalace hardwaru iSCSI**

l Před zahájením instalace Windows serveru byste měli nakonfigurovat hardware iSCSI.

- l • “Plán zaváděcího režimu pro hostovaný systém”
- l • “Vytvoření konfigurace servisního procesoru a konfigurace vzdáleného systému”
- l • “Plán připojení servisního procesoru” na stránce 65
- l • “Konfigurace metody zjišťování servisního procesoru na serveru iSeries” na stránce 65

## l **Plán zaváděcího režimu pro hostovaný systém**

l Zaváděcí režim určuje, jakým způsobem budou adaptéru iSCSI HBA v hostovaném systému předány informace o IP a paměťovém prostoru požadované při zavádění operačního systému Windows.

### l **Dynamické dodání vzdálenému systému prostřednictvím DHCP**

l Toto je předvolený režim. DHCP server na serveru iSeries automaticky poskytuje informace o konfiguraci prostřednictvím konfigurovaných adaptéru NWSH. Další informace najdete v tématu “Zavádění systému bez disku přes iSCSI” na stránce 22.

- l • V různou dobu může hostovaný systém používat několik NWSH.
- l • Tento režim je možné používat u přepínaných sítí a u směrovaných sítí připojených pomocí relé DHCP.
- l • Je-li povoleno zabezpečení IPSec, bude moci mezi jednotlivými adaptéry iSCSI HBA probíhat provoz DHCP.

### l **Manuální konfigurace ve vzdáleném systému**

- l • Hostovaný systém může používat pouze jeden NWSH.
- l • Toto nastavení funguje u sítí bez relé DHCP.
- l • Je-li povoleno zabezpečení IPSec mezi jednotlivými adaptéry iSCSI HBA, bude provoz DHCP v síti iSCSI zablokován.

## l **Vytvoření konfigurace servisního procesoru a konfigurace vzdáleného systému**

l Před instalací serveru můžete volitelně vytvořit konfiguraci servisního procesoru a konfiguraci vzdáleného systému tak, aby jejich jména mohla být poskytována jako parametry v příkazu INSWNTSVR (Instalace Windows serveru). Tuto proceduru je možné provést před nastavením hardwaru hostovaného systému a je volitelná, neboť tyto objekty lze vytvořit příkazem INSWNTSVR, když zadáte tytéž informace jako parametry. Doporučujeme, abyste v každém případě vytvořili konfiguraci servisního procesoru a konfiguraci vzdáleného systému, pokud platí některá z těchto podmínek:

- l • Dosud jste nikdy neinstalovali server připojený pomocí iSCSI a chcete co možná největší podporu.
- l • Dáváte přednost grafickému rozhraní vždy, kdy je to možné.
- l • Štítky se sériovým číslem vzdáleného systému nebo adaptéru iSCSI HBA budou později hůře přístupné.

l Při vytváření konfigurace servisního procesoru a konfigurace vzdáleného systému postupujte takto:

- l 1. Pokud jste dosud nevytvořili konfiguraci servisního procesoru, která by se měla používat s novým serverem, vytvořte novou konfiguraci nyní. Tento objekt bude možné později změnit.
  - l a. Rozbalte **Administrace integrovaných serverů**.
  - l b. Rozbalte **Připojení iSCSI**.
  - l c. Klepněte pravým tlačítkem myši na **Servisní procesory**.

- d. Vyberte **Nová konfigurace servisního procesoru**.
  - e. Na kartě **Obecné**:
    - Do polí **Jméno** a **Popis** zadejte jméno a popis nové konfigurace.
    - Do pole **Sériové číslo** zadejte sériové číslo krytu, aby bylo možné identifikovat servisní procesor v síti. Tuto hodnotu zjistíte na krytu systému.
    - Vyberte **Oprávnění k objektu**
  - f. Na kartě **Zabezpečení** zadejte **Nepoužívat certifikát (vyžaduje fyzické zabezpečení)**.
  - g. Klepněte na **OK**.
2. Pokud jste dosud nevytvořili konfiguraci vzdáleného systému, vytvořte ji nyní.
- a. Rozbalte **Administrace integrovaných serverů**.
  - b. Rozbalte **Připojení iSCSI**.
  - c. Klepněte pravým tlačítkem myši na **Vzdálené systémy**.
  - d. Vyberte **Nová konfigurace vzdáleného systému**.
  - e. Na kartě **Obecné**:
    - Do polí **Jméno** a **Popis** zadejte jméno a popis nové konfigurace.
    - Pro **konfiguraci servisního procesoru** vyberte stávající nebo novou konfiguraci servisního procesoru z kroku 1.
    - Zadejte odpovídající hodnotu do pole **Identita vzdáleného systému**.

**Poznámka:** Pokud chcete zadat hodnotu identity vzdáleného systému pro blade server IBM BladeCenter, vyberte volbu **Použít následující hodnoty** a zadejte sériové číslo blade serveru IBM BladeCenter. V případě ostatních serverů ponechte vybranou volbu **Použít identitu krytu**.

    - Vyberte **Oprávnění k objektu**.
  - f. Na kartě **Síťová rozhraní** proveďte pro každý port iSCSI HBA, který budete používat v hostovaném systému, tyto kroky:
    - 1) Klepněte na **Přidat...**
    - 2) Na panelu **Vlastnosti síťového rozhraní** zadejte minimálně jednu **adresu adaptéru (MAC)** ze štítku na adaptéru iSCSI HBA. Pokud chcete zjistit, zda máte zadat adresu pro **vzdálené rozhraní SCSI** a **vzdálené rozhraní LAN**, podívejte se na téma “Síť iSCSI” na stránce 28. Jestliže si nejste jisti, zadejte adresu do obou polí. Každá adresa je tvořena 12 hexadecimálními znaky.
      - Pro volbu **Vzdálené rozhraní SCSI** vyhledejte na štítku slovo ‘iSCSI’ a zadejte odpovídající adresu.
      - Pro volbu **Vzdálené rozhraní LAN** vyhledejte na štítku slovo ‘TOE’ a zadejte odpovídající adresu.

**Poznámka:** U adaptéru iSCSI HBA se dvěma porty uvádí tento štítek čtyři adresy. Každý port má jednu iSCSI adresu a jednu TOE adresu.
    - 3) Pro každou adresu adaptéru (MAC), kterou jste uvedli, musíte také zadat internetovou adresu do pole **Internetová adresa** a masku podsítě do pole **Maska podsítě**, přičemž tyto hodnoty musí odpovídat vaší síti iSCSI. Pokud vaše síť iSCSI nemá žádnou bránu, ponechte pole **Brána** prázdné.
    - 4) Na obrazovce **Vlastnosti síťového rozhraní** klepněte na **OK**.
  - g. Na kartě **Parametry zavádění**:
    - Nakonfigurujete režim zavádění systému. Další informace najdete v tématu “Plán zaváděcího režimu pro hostovaný systém” na stránce 63. Ve většině případů se použije předvolená volba **Dynamicky dodávat vzdálenému systému přes DHCP**. Další informace najdete v tématu “Zavádění systému bez disku přes iSCSI” na stránce 22. Zaškrtnuté okénko **Více než jedno rozhraní iSCSI ve vzdáleném systému** ignorujte.
  - h. Na kartě **Autentizace CHAP**:
    - Vyberte volbu **Nepoužívat CHAP**. Další informace najdete v tématu “Zabezpečení u systémů připojených pomocí iSCSI” na stránce 47.
  - i. Chcete-li konfigurovat další informace týkající se daného objektu, nakonfigurujte je nyní.
  - j. Klepněte na **OK**.

## Plán připojení servisního procesoru

Jestliže jste vytvořili novou konfiguraci servisního procesoru, která se má používat s novým serverem, musíte určit, jaké metody jsou u vašeho servisního procesoru podporovány a kterou z nich chcete používat:

- metoda konfigurace
- statické nebo dynamické IP adresování
- metoda zjišťování
- metoda zabezpečení ochrany dat

Uvedené informace budete potřebovat v následujících krocích při přípravě hardwaru a při změně konfigurace servisního procesoru. Chcete-li se rozhodnout, jaké metody budete používat, přečtěte si téma “Připojení servisního procesoru” na stránce 28 a “Konfigurace zjišťování servisních procesorů” na stránce 135, ale zatím neprovádějte žádné konfigurační kroky.

## Konfigurace metody zjišťování servisního procesoru na serveru iSeries

Nakonfigurujte metodu zjišťování servisního procesoru. V tomto okamžiku přeskočte všechny kroky, které musí být provedeny na hostovaném systému, neboť tyto kroky budete provádět později v rámci přípravy hardwaru. Další informace najdete v tématu “Metody zjišťování servisních procesorů” na stránce 137.

## Popisy síťového serveru

Popisy síťového serveru (NWS) představují integrovaný Windows server na serveru iSeries. Příkaz INSWNTSVR (Instalace Windows serveru) automaticky vytvoří popis síťového serveru (NWS) pro každý integrovaný server, který nainstalujete. NWS má zpravidla stejné jméno jako server. Když provedete nějakou akci v NWS, provedete také akci na serveru. logické zapnutí popisu síťového serveru server spustí a logické vypnutí NWS server ukončí.

## Pracovní formulář pro parametry instalace i5/OS

Před instalací serverů Windows 2000 Server nebo Windows Server 2003 vyplňte buď hodnoty v pomocném programu pro instalaci Windows serveru, nebo v tomto pracovním formuláři pro instalaci.

Tento pracovní formulář použijte při instalaci a konfiguraci systému.

Pole	Popis a instrukce	Hodnota
Popis síťového serveru (NWS)	Definuje provozní charakteristiky a komunikační připojení síťového serveru, který ovládá integrovaný Windows server. Další informace najdete v tématu “Popisy síťového serveru”. Použijte takové jméno, které si snadno zapamatujete. Jméno může být až 8 znaků dlouhé. Ve jménu použijte pouze znaky A - Z a 0 - 9 a jako první znak použijte písmeno. Jméno popisu síťového serveru je také jméno počítače a hostitelské jméno TCP/IP integrovaného Windows serveru.	

Pole	Popis a instrukce	Hodnota
Typ instalace (INSTYPE)	<p>Uvádí typ instalace, který se má provést. Vyberte jeden z těchto typů:</p> <p><b>*FULL</b></p> <p>Tento typ je povinný při instalaci na interní server IXS (Integrated xSeries(R) Server) a volitelný při instalaci na externí server xSeries připojený prostřednictvím adaptéru IXA (Integrated xSeries Adapter) nebo iSCSI HBA.</p> <p><b>*BASIC</b></p> <p>Volitelný typ instalace na externě připojený server xSeries připojený pomocí adaptéru IXA nebo iSCSI HBA. U této volby je první část instalačního procesu řízena příkazem INSWNTSVR (Instalace Windows serveru) operačního systému i5/OS. Pak se instalace dokončí instalačním procesem xSeries za použití kompaktního disku ServerGuide.</p>	
Jméno prostředku (RSRCNAME)	<p>Označuje hardware Windows serveru.</p> <p>Pro servery xSeries a IBM BladeCenter připojené pomocí iSCSI uveďte jako jméno prostředku *ISCSI.</p> <p>Pro servery xSeries připojené prostřednictvím serveru IXS a adaptéru IXA uveďte jako jméno prostředku adaptér IOA souborového serveru. Chcete-li zjistit jméno, zadejte na příkazový řádek operačního systému i5/OS příkaz DSPHDWRSC *CMN (Zobrazení hardwarových komunikačních prostředků). Jméno prostředku se objeví jako LINxx, kde xx je číslo.</p> <p>“Rada: Vyhledejte jména prostředků, máte-li více integrovaných serverů” na stránce 85</p>	
Konfigurace portu TCP/IP (TCPPORTCFG)	<p>Zadejte konfigurační hodnoty Windows TCP/IP, které jsou specifické pro každý lokálně řízený port adaptéru. Jinak tento krok přeskočte a použijte předvolenou hodnotu *NONE.</p> <p><b>Poznámka:</b> Pomocí parametru TCPPORTCFG je možné konfigurovat pouze adaptéry, které jsou přímo spravované serverem iSeries a logicky spravované serverem IXS. Adaptéry LAN, které jsou připojeny pomocí IXA nebo iSCSI HBA a jsou spravované serverem xSeries, nelze pomocí tohoto parametru konfigurovat.</p>	<ul style="list-style-type: none"> <li>• Port 1 <ul style="list-style-type: none"> <li>– IP adresa</li> <li>– Maska podsítě</li> <li>– Brána (volitelné)</li> </ul> </li> <li>• Port 2 <ul style="list-style-type: none"> <li>– IP adresa</li> <li>– Maska podsítě</li> <li>– Brána (volitelné)</li> </ul> </li> <li>• Port 3 <ul style="list-style-type: none"> <li>– IP adresa</li> <li>– Maska podsítě</li> <li>– Brána (volitelné)</li> </ul> </li> <li>• Port 4 <ul style="list-style-type: none"> <li>– IP adresa</li> <li>– Maska podsítě</li> <li>– Brána (volitelné)</li> </ul> </li> </ul>



Pole	Popis a instrukce	Hodnota
Port Virtual Ethernet (VRTETHPORT)	<p>Uvádí konfiguraci TCP/IP pro virtuální síť Ethernet, které používá souborový server.</p> <p>Odpovídající port virtuální síť Ethernet je povinný pro instalaci klastrové služby Windows.</p> <p><b>*NONE:</b> Udává, že neexistuje konfigurace portu virtuální síť Ethernet.</p> <p><b>Prvek 1: Port</b></p> <ul style="list-style-type: none"> <li><b>*VRTETHx:</b> Je konfigurován port virtuální síť Ethernet <i>x</i>, kde <i>x</i> nabývá hodnoty 0 až 9.</li> </ul> <p><b>Prvek 2: Internetová adresa Windows</b> Internetová adresa Windows pro port je ve tvaru nnn.nnn.nnn.nnn, kde nnn je číslo desítkové soustavy v rozmezí od 0 do 255.</p> <p><b>Prvek 3: Maska podsítě Windows</b> Maska podsítě pro internetovou adresu Windows je ve tvaru nnn.nnn.nnn.nnn, kde nnn je číslo desítkové soustavy v rozsahu od 0 do 255.</p> <p><b>Prvek 4: Asociovaný port</b> Jméno prostředku, které popisuje port použitý k navázání spojení mezi síťovým Windows serverem a sítí.</p> <ul style="list-style-type: none"> <li><b>*NONE</b> Jméno prostředku asociovaného portu není asociováno s linkou.</li> <li><b>jméno-prostředku</b> Jméno prostředku portu.</li> </ul>	<ul style="list-style-type: none"> <li>Virtuální port 1 <ul style="list-style-type: none"> <li>*VRTETHx</li> <li>IP adresa</li> <li>Maska podsítě</li> <li>Asociovaný port (volitelné)</li> </ul> </li> <li>Virtuální port 2 <ul style="list-style-type: none"> <li>*VRTETHx</li> <li>IP adresa</li> <li>Maska podsítě</li> <li>Asociovaný port (volitelné)</li> </ul> </li> <li>Virtuální port 3 <ul style="list-style-type: none"> <li>*VRTETHx</li> <li>IP adresa</li> <li>Maska podsítě</li> <li>Asociovaný port (volitelné)</li> </ul> </li> <li>Virtuální port 4 <ul style="list-style-type: none"> <li>*VRTETHx</li> <li>IP adresa</li> <li>Maska podsítě</li> <li>Asociovaný port (volitelné)</li> </ul> </li> </ul>
Jméno lokální domény TCP/IP (TCPDMNNAME)	Uvádí jméno lokální domény TCP/IP asociované s integrovaným serverem. Můžete uvést hodnotu *SYS, aby se použila stejná hodnota, kterou používá operační systém i5/OS.	
Server jmen TCP/IP (TCPNAMSVR)	Uvádí internetovou adresu serveru jmen, kterou používá integrovaný server. Můžete zadat až tři internetové adresy nebo můžete zadat hodnotu *SYS, aby se použila stejná hodnota, jakou používá operační systém i5/OS.	
V pracovní skupině (TOWRKGPR)	Uvádí jméno pracovní skupiny Windows serveru, do níž server patří.	
V doméně (TODMN)	Uvádí jméno domény Windows, k níž server náleží.	
Fronta zpráv serveru a knihovna (MSGQ)	Uvádí jméno fronty zpráv a knihovny, ve které bude umístěna. Pokud fronta zpráv ještě neexistuje, vytvoří se příkazem INSWNTSVR. Do fronty zpráv se odesílají protokoly událostí a chyby, které se týkají tohoto serveru. Měli byste uvést jméno fronty zpráv (MSGQ) a knihovnu. Také můžete zadat, aby *JOBLOG odesílal nezávažné chyby do protokolu úlohy monitoru administrace uživatelů a závažné chyby do QSYSOPR. Jestliže zadáte *NONE, nebudou se nezávažné chyby do operačního systému i5/OS posílat a závažné chyby se odešlou do QSYSOPR.	<p>Fronta:</p> <p>Knihovna:</p>



Pole	Popis a instrukce	Hodnota
Protokol událostí (EVTLOG)	<p>Uvádí, zda operační systém i5/OS bude či nebude dostávat z integrovaného Windows serveru zprávy protokolu událostí. Volby jsou: všechny, systémové, zabezpečení, z aplikací nebo žádné:</p> <p><b>*ALL</b> Operační systém i5/OS přijímá všechny zprávy protokolu událostí.</p> <p><b>*NONE</b> Nepřijímají se žádné zprávy protokolu událostí.</p> <p><b>*SYS</b> Operační systém i5/OS přijímá zprávy protokolu systémových událostí.</p> <p><b>*SEC</b> Operační systém i5/OS přijímá všechny zprávy protokolu událostí.</p> <p><b>*APP</b> Operační systém i5/OS přijímá zprávy protokolu událostí aplikací.</p> <p><b>Poznámka:</b> Jestliže necháte integrovaný server odesílat protokol o zabezpečení dat na server iSeries (zadáním *ALL nebo *SEC), nezapomeňte u fronty zpráv nastavit správné zabezpečení.</p>	

Pole	Popis a instrukce	Hodnota
<p>Velikost instalačního zdroje a systémové jednotky a ASP (Auxiliary storage pool)</p> <p>(SVRSTGSIZE)</p> <p>(SVRSTGASP)</p> <p>(STGASPDEV)</p>	<p>Zadejte velikost paměťových prostorů síťového serveru pro instalační zdroj a systémovou jednotku a uveďte, ve kterých ASP (1 - 255) je požadujete. Jméno zařízení ASP je možné zadat pro ASP číslo 33-255, má-li být paměťový prostor vytvořen v nezávislém ASP. Jestliže však použijete jméno, musí být v poli pro číslo ASP ponechána předvolená hodnota 1 nebo hodnota symbolického argumentu *N.</p> <p>Jednotka instalačního zdroje (jednotka D) musí být dostatečně velká, aby pojmla obsah adresáře I386 v obrazu instalačního CD Windows serveru a kód produktu IBM i5/OS Integrated Server Support.</p> <p>Systémová jednotka (jednotka C) musí být dostatečně velká, aby pojmla operační systém Windows serveru. Limit je 1 024 až 1 024 000 MB, v závislosti na možnostech vašich prostředků. Zvažte tyto faktory:</p> <ul style="list-style-type: none"> <li>• Verze Windows serveru (řídte se pokyny týkající se požadavků na operační systém, které uvádí dokumentace Microsoft).</li> <li>• Primární využití (tisk/souborové služby) a počet uživatelů terminálového serveru.</li> <li>• Volný prostor na systémové jednotce.</li> <li>• Požadavky aplikací na prostředky.</li> <li>• Potřeba výpisu paměti v případě havárie.</li> <li>• Paměť instalovaná na serveru</li> </ul> <p>Operační systém i5/OS vytvoří a připojí jednotku jako paměťový prostor síťového serveru formátovaný jako FAT32 nebo NTFS, v závislosti na velikosti.</p> <p>Další informace o těchto jednotkách najdete v tématu “Předdefinované diskové jednotky pro integrované Windows servery” na stránce 154.</p> <p><b>Poznámky:</b></p> <ol style="list-style-type: none"> <li>1. Příkaz INSWNTSVR automaticky nastavuje velikost systémové jednotky na minimální velikost, která je určena částečně na základě takových faktorů, jako jsou verze Windows a instalovaná paměť.</li> <li>2. Při rozhodování o velikosti jednotlivých jednotek ponechte nějaký prostor pro budoucí využití, jako jsou nové aplikace nebo přechody na vyšší verzi Windows serveru. Pokud do parametru SVRSTGSIZE uvedete hodnotu *CALC, pamatujte si, že operační systém i5/OS bude alokovat pouze minimální velikost disku nutnou pro instalaci Windows. Pokud potřebujete další prostor pro aplikace nebo data, měli byste uvážit manuální specifikaci velikosti jednotky.</li> <li>3. Podporu nezávislých ASP (33 - 255) zajišťuje produkt iSeries Navigator. Další informace o práci s nezávislými ASP viz téma Nezávislá ASP. Jak aplikace Information Center, tak produkt iSeries Navigator hovoří o ASP jako o diskových společných oblastech. Chcete-li použít nezávislé ASP, musí být zařízení ASP dostupné předtím, než použijete příkaz INSWNTSVR.</li> </ol>	<p>Jednotka instalačního zdroje:</p> <p>Velikost:</p> <p>ASP:</p> <p>ASPDEV:</p> <p>Systémová jednotka:</p> <p>Velikost:</p> <p>ASP:</p> <p>ASPDEV:</p>

Pole	Popis a instrukce	Hodnota
Režim licence (LICMODE)	<p>Určuje režim licence pro instalaci Microsoft Windows serveru.</p> <p><b>Prvek 1 Typ licence:</b></p> <p><b>*PERSEAT</b> Znamená, že licence klienta byla zakoupena pro každý počítač, který má k serveru přístup.</p> <p><b>*PERSERVER</b> Znamená, že klientské licence byly zakoupeny pro server a povolují určitý počet souběžných připojení k serveru.</p> <p><b>Prvek 2 Klientské licence:</b></p> <p><b>*NONE</b> Znamená, že nejsou instalované žádné klientské licence. *NONE musí být uvedeno, je-li zadáno *PERSEAT.</p> <p><b>počet-klientských-licencí:</b> Uvádí počet klientských licencí zakoupených pro instalovaný server.</p> <p><b>Prvek 3 Windows Terminal Services:</b></p> <p><b>*TSENABLE</b> Ve Windows 2000 nainstaluje produkty Windows Terminal Services a Terminal Services Licensing.</p> <p><b>*PERDEVICE</b> Instaluje a konfiguruje produkt Windows Server 2003 Terminal Services tak, aby od každého připojeného zařízení vyžadoval platnou přístupovou licenci k terminálovému serveru. Má-li klient přístupovou licenci k terminálovému serveru, může mít přístup k více než jednomu terminálovému serveru.</p> <p><b>*PERUSER</b> Instaluje a konfiguruje produkt Windows Server 2003 Terminal Services tak, aby poskytoval jednu přístupovou licenci k terminálovému serveru pro každého aktivního uživatele.</p> <p><b>*NONE</b> Tento server nemá žádné licence, aby fungoval jako terminálový server pro stolní počítače.</p>	<p>Typ licence:</p> <p>Klientské licence:</p> <p>Terminálové služby:</p>
Přenesení uživatele domény (PRPDMNUSR)	<p>Uvádí, zda by tento server měl být použit k přenesení a synchronizaci uživatelů do domény Windows nebo aktivního adresáře.</p> <p><b>*YES</b> Posílat aktualizace uživatelů do domény Windows nebo do aktivního adresáře prostřednictvím tohoto serveru.</p> <p><b>*NO</b> Neposílat aktualizace uživatelů do domény Windows nebo do aktivního adresáře prostřednictvím tohoto serveru.</p>	
Doba do ukončení práce systému (SHUTDTIMO)	<p>Tato hodnota určuje, jak dlouho bude operační systém i5/OS čekat, aby programům umožnil ukončit jejich činnost před vypnutím integrovaného serveru. Tato prodleva může být 2 až 45 minut. Jestliže hodnotu neuvedete, bude nastavena na 15 minut.</p>	Doba do ukončení práce systému:

Pole	Popis a instrukce	Hodnota
Vyhrazené prostředky zařízení (RSTDEVRSC)	<p>Vyhrazuje použití páskových a optických jednotek serveru iSeries vzhledem k integrovanému serveru.</p> <p><b>*NONE</b> Nezamezuje, aby integrovaný server používal páskové či optické jednotky.</p> <p><b>*ALL</b> Zamezuje, aby integrovaný server používal páskové a optické jednotky.</p> <p><b>*ALLTAPE</b> Zamezuje, aby integrovaný server používal všechny páskové jednotky.</p> <p><b>*ALLOPT</b> Zamezuje, aby integrovaný server používal všechny optické jednotky.</p> <p><b>vyhrazené-zařízení</b> (vyhrazené zařízení) Zadejte až 10 zařízení, u nichž nechcete, aby je integrovaný server používal.</p>	
Časové pásmo (Time zone)	(Volitelné) Zaznamená časové pásmo iSeries pro použití ve fázi instalace Windows serveru. Další informace najdete v tématu "Synchronizace času" na stránce 60.	
Dvoubodová virtuální síť Ethernet (VRTPTPPORT)	<p>Mezi operačním systémem i5/OS a Windows serverem existuje lokální síť (viz "Koncepte v oblasti sítí" na stránce 27). Jak na straně operačního systému i5/OS, tak na straně Windows serveru této lokální sítě jsou IP adresy a masky podsítě.</p> <p><b>Poznámka:</b> Předvolba je, že příkaz INSWNTSVR vytvoří tyto adresy automaticky. Adresy jsou ve tvaru 192.168.xx.yy. Pokud váš počítač používá adresy třídy C, je možné, aby se vygenerovaly duplicitní IP adresy.</p> <p>Chcete-li se vyvarovat potenciálních konfliktů, můžete také uvést internetové adresy, o kterých víte, že budou ve vašem systému jedinečné. Používejte adresy ve tvaru a.b.x.y, kde a.b.x má stejnou hodnotu na obou stranách dvoubodové virtuální sítě Ethernet a zajistěte, aby dvoubodová virtuální síť Ethernet obsadila svoji vlastní podsít v operačním systému i5/OS. Z přídatných parametrů příkazu INSWNTSVR použijte parametr Virtuální port typu PTP Ethernet.</p> <p>Maska podsítě je vždy 255.255.255.0.</p>	<p>IP adresa na straně i5/OS:</p> <p>IP adresa na straně Windows serveru:</p>
Konfigurační soubor (CFGFILE)	<p>Během instalace vytvoří a specifikuje uživatelsky přizpůsobený popis síťového serveru (viz Kapitola 15, "Konfigurační soubory popisu síťového serveru", na stránce 235).</p> <p>Předvolba je *NONE. Chcete-li specifikovat konfigurační soubor, který jste vytvořili, nahraďte jméno souboru a knihovny, kde je uložen (*LIBL, *CURLIB nebo jméno knihovny).</p>	

## Instalační pracovní formulář pro dodatečné parametry iSCSI (Internet SCSI)

Pole	Popis a instrukce	Hodnota
Časovač aktivace (ACTTMR)	Udává v sekundách časový interval, po který bude systém čekat na vytvoření připojení k servisnímu procesoru vzdáleného serveru a na zapnutí vzdáleného serveru. Předvolená hodnota je 120. Zadejte hodnotu v rozsahu 30 až 1800 sekund.	Časovač aktivace:
Komunikační fronta zpráv (CMNMSGQ)	Uvádí jméno fronty pro příjem zpráv o stavu komunikace. <b>Kvalifikátor 1:</b> <ul style="list-style-type: none"> <li><b>*SYSOPR</b> Zprávy se budou odesílat do fronty zpráv systémového operátora.</li> <li><b>jméno</b> Zadejte jméno fronty zpráv, která má přijímat zprávy o stavu komunikace.</li> </ul> <b>Kvalifikátor 2:</b> <ul style="list-style-type: none"> <li><b>*LIBL</b> Prohledají se všechny knihovny v seznamu knihoven úlohy, dokud nebude nalezena první shoda.</li> <li><b>*CURLIB</b> Prohledá se aktuální knihovna úlohy. Jestliže nebude pro úlohu specifikována aktuální knihovna, použije se knihovna QGPL.</li> <li><b>jméno-knihovny</b> Zadejte jméno knihovny, která se má použít.</li> </ul>	Fronta zpráv:  Knihovna:
Cesta k paměťovým prostorům (STGPTH)	Uvádí cestu, kterou mohou používat paměťové prostory. Tato informace se skládá z popisu adaptéru NWSH (Network server host adapter). <b>Poznámka:</b> Po instalaci serveru můžete přidávat další cesty k paměťovým prostorům. <b>jméno</b> Zadejte jméno existujícího popisu adaptéru NSWH (Network server host adapter).	Jméno popisu NWSH:

Pole	Popis a instrukce	Hodnota
Cesta k virtuální síti Ethernet (VRTETHPTH)	<p>Uvádí cesty k virtuální síti Ethernet, které mohou používat popisy linek typu Ethernet. Tyto informace se skládají ze dvou částí a zahrnují port virtuální sítě Ethernet a popis adaptéru NWSH (Network server host adapter). Pro tento parametr můžete zadat až pět hodnot. Musíte zadat minimálně jednu cestu k virtuální síti Ethernet, aby mohla být použita jménem popisu linky *VRTETHPTP.</p> <p><b>Poznámka:</b> Po instalaci serveru můžete přidávat k virtuální síti Ethernet další cesty.</p> <p><b>Prvek 1: Port</b></p> <p><b>*VRTETHPTP</b></p> <p>Na síťovém serveru je nakonfigurován virtuální port dvoubodové virtuální sítě Ethernet.</p> <p><b>*VRTETHx</b> Na síťovém serveru je nakonfigurován port x virtuální sítě Ethernet, kde x nabývá hodnoty 0 až 9.</p> <p><b>Prvek 2: Adaptér NWSH</b></p> <p><b>jméno</b> Zadejte jméno existujícího popisu adaptéru NWSH (Network server host adapter). Jméno adaptéru NWSH nemusí být u tohoto popisu NWSH jedinečné pro každý parametr VRTETHPTH.</p>	<p>Cesta k virtuální síti Ethernet:</p> <p>Port:</p> <p>Adaptér NWSH:</p>
Port TCP pro ukončení činnosti systému (SHUTDPORT)	<p>Uvádí port TCP, který se používá pro ukončení činnosti systému.</p> <p><b>Poznámka:</b> Jedná se o rozšířený parametr, který může být vhodný v případě, že síť iSCSI používá firewall.</p> <p><b>8700</b> Jako číslo portu TCP použijte 8700.</p> <p><b>integer</b> Číslo označuje port, který se bude používat pro ukončení činnosti systému. Platné hodnoty jsou v rozsahu 1024 až 65 535.</p>	
Řídicí port virtuální sítě Ethernet (VRTETHCTLP)	<p>Uvádí port TCP, který slouží k řízení virtuální sítě Ethernet.</p> <p><b>Poznámka:</b> Jedná se o rozšířený parametr, který může být vhodný v případě, že v síti typu iSCSI je ochranná bariéra (firewall).</p> <p><b>8800</b> Jako číslo portu TCP použijte 8800.</p> <p><b>integer</b> Číslo označuje port, který se bude používat k řízení virtuální sítě Ethernet. Platné hodnoty jsou v rozsahu 1024 až 65 535.</p>	
NWSCFG ve vzdáleném systému (RMTNWSCFG)	<p>Uvádí konfiguraci síťového serveru ve vzdáleném systému, která se má používat s tímto serverem.</p> <p><b>Poznámka:</b> Je vhodné, někdy dokonce nezbytné, vytvořit konfiguraci vzdáleného systému dříve, než spustíte příkaz INSWNTSVR. Další informace najdete v tématu “Vytvoření konfigurace servisního procesoru a konfigurace vzdáleného systému” na stránce 63.</p> <p><b>*DFT</b> Použijte systémem generované předvolené jméno konfigurace síťového serveru ve vzdáleném systému 'nwsdnameRM', kde nwsdname je jméno popisu síťového serveru.</p> <p><b>jméno</b> Zadejte jméno existující konfigurace síťového serveru ve vzdáleném systému.</p>	

Pole	Popis a instrukce	Hodnota
NWSCFG se servisním procesorem (SPNWSCFG)	<p>Uvádí konfiguraci síťového serveru se servisním procesorem, která se má používat s tímto serverem.</p> <p><b>Poznámka:</b> Je vhodné, někdy dokonce nezbytné, vytvořit konfiguraci servisního procesoru dříve, než spustíte příkaz INSWNTSVR. Další informace najdete v tématu “Vytvoření konfigurace servisního procesoru a konfigurace vzdáleného systému” na stránce 63.</p> <p><b>*DFT</b> Použijte systémem generované předvolené jméno konfigurace síťového serveru se servisním procesorem 'nwsdnameSP', kde nwsdname je jméno popisu síťového serveru.</p> <p><b>jméno</b> Zadejte jméno existující konfigurace síťového serveru se servisním procesorem.</p>	
NWSCFG se zabezpečeným připojením (CNNNWSCFG)	<p>Uvádí konfiguraci síťového serveru se zabezpečeným připojením, která se má používat s tímto serverem.</p> <p><b>*DFT</b> Použijte systémem generované předvolené jméno konfigurace síťového serveru se zabezpečeným připojením 'nwsdnameCN', kde nwsdname je jméno popisu síťového serveru.</p> <p><b>jméno</b> Zadejte jméno existující konfigurace síťového serveru se zabezpečeným připojením.</p>	
Předvolené pravidlo zabezpečení IP (DFTSECRULE)	<p>Uvádí předvolené pravidlo zabezpečení IP (IPSec) používané mezi hostitelským a vzdáleným systémem.</p> <p><b>Poznámka:</b> Pro tento parametr nemůžete zadat žádnou hodnotu, pokud jste do parametru CNNNWSCFG zadali existující konfiguraci zabezpečeného připojení.</p> <p><b>*NONE</b> Pravidla zabezpečení IP nejsou konfigurována.</p> <p><b>*GEN</b> Systém bude automaticky generovat náhodný předem sdílený klíč.</p> <p><b>předem-nasdílený-klíč</b> Zadejte předem nasdílený klíč. Předem nasdílený klíč je netriviální řetězec o délce až 32 znaků.</p>	
Pravidlo zabezpečení IP (IPSECRULE)	<p>Zadejte relativní hodnotu parametru IPSECRULE (Pravidla zabezpečení IP), definovanou ve stávající konfiguraci síťového serveru se zabezpečeným připojením, která se použije jako výchozí nastavení zabezpečení IP mezi hostitelským a vzdáleným systémem.</p> <p><b>*DFTSECRULE</b> Použije se hodnota uvedená v parametru DFTSECRULE (Předvolené pravidlo zabezpečení IP).</p> <p><b>*NONE</b> Vzdálené rozhraní nebude používat žádné pravidlo zabezpečení.</p> <p><b>1-16</b> Vzdálené rozhraní bude používat zde uvedené pravidlo zabezpečení.</p>	



Pole	Popis a instrukce	Hodnota
Inicializace servisního procesoru (INZSP)	<p>Uvádí, jakým způsobem je zabezpečen servisní procesor ve vzdáleném systému.</p> <p><b>Poznámka:</b> Nelze zadat *SYNC, pokud již existuje konfigurace servisního procesoru. V případě, že konfigurace servisního procesoru existuje, používají se pouze hodnoty *MANUAL, *AUTO a *NONE.</p> <p><b>*MANUAL</b> Jedná se o nejbezpečnější metodu. Musíte manuálně konfigurovat jméno uživatele, heslo a certifikát pro servisní procesor. Je požadována správa certifikátů. Tato metoda je vhodná, pokud chcete ochránit heslo svého servisního procesoru, když se k němu připojíte přes veřejné síť.</p> <p><b>*AUTO</b> Nemusíte manuálně konfigurovat parametry u servisního procesoru vzdáleného systému. Servisní procesor vzdáleného systému certifikát vygeneruje automaticky. Připojení je zabezpečeno, jakmile je inicializováno. Tato volba je vhodná, pokud se připojíte k servisnímu procesoru přes síť, která je fyzicky zabezpečená nebo je chráněná firewallem.</p> <p><b>*SYNC</b> Tato konfigurace síťového serveru synchronizuje uživatele, heslo a automaticky podepsaný certifikát se servisním procesorem.</p> <p><b>*NONE</b> Heslo servisního procesoru není chráněno. Tuto možnost nepoužívejte, pokud se nepřipojíte k servisnímu procesoru prostřednictvím fyzicky zabezpečené sítě.</p>	
Umožnit unicast (ENBUNICAST)	<p>Unicast je metoda přenosu, kdy jsou pakety odesílány přímo do parametru SPNAME (Specifikované jméno servisního procesoru) nebo SPINTNETA (Adresa servisního procesoru). Identifikace systému pro parametr EID (Identifikátor krytu) se bude automaticky načítat, pokud je zadáno *AUTO a hardware systému tuto možnost podporuje.</p> <p><b>Poznámka:</b> Pro tento parametr nemůžete zadat žádnou hodnotu, pokud jste do parametru SPNWSCFG zadali existující konfiguraci servisního procesoru.</p> <p><b>*NO</b> Zakázat unicast.</p> <p><b>*YES</b> Povolit unicast.</p>	

Pole	Popis a instrukce	Hodnota
Identifikátor krytu (EID)	<p>Uvádí identifikační sériové číslo, typ a model krytu obsahujícího servisní procesor. Tyto informace jsou požadovány pro vyhledání vzdáleného systému v síti, je-li uvedeno ENBUNICAST(*NO). Uvedené hodnoty vyhledejte na štítku systému.</p> <p><b>Poznámka:</b> Pro tento parametr nemůžete zadat žádnou hodnotu, pokud jste do parametru SPNWSCFG zadali existující konfiguraci servisního procesoru.</p> <p><b>*AUTO</b> Automaticky načítá identifikátor, pokud je uvedeno ENBUNICAST(*YES).</p> <p><b>Prvek 1: Sériové číslo</b> Uveďte sériové číslo počítače vzdáleného systému s použitím alfanumerických znaků bez lomítek.</p> <p><b>Prvek 2: Výrobní typ a model</b> Zadejte typ a model počítače vzdáleného systému ve tvaru tttmmm, kde tttt je typ počítače a mmm je číslo modelu počítače.</p>	
Jméno servisního procesoru (SPNAME)	<p>Uvádí jméno hostitele servisního procesoru ve vzdáleném systému.</p> <p><b>Poznámka:</b> Pro tento parametr nemůžete zadat žádnou hodnotu, pokud jste do parametru SPNWSCFG zadali existující konfiguraci servisního procesoru.</p> <p><b>*SPINTNETA</b> Vzdálený systém je identifikován pomocí hodnoty specifikované v parametru SPINTNETA (Adresa servisního procesoru).</p> <p><b>jméno-hostitele:</b> Zadejte jméno hostitele servisního procesoru ve vzdáleném systému.</p>	
Adresa servisního procesoru (SPINTNETA)	<p>Uvádí internetovou adresu servisního procesoru ve vzdáleném systému. Internetové adresy se vyjadřují v desítkovém tvaru nnn.nnn.nnn.nnn, kde nnn je desítkové číslo v rozsahu od 0 do 255.</p> <p><b>Poznámka:</b> Pro tento parametr nemůžete zadat žádnou hodnotu, pokud jste do parametru SPNWSCFG zadali existující konfiguraci servisního procesoru.</p> <p><b>internetová-adresa:</b> Uveďte internetovou adresu servisního procesoru.</p>	
Autentizace SP (SPAUT)	<p>Uvádí jméno uživatele a heslo servisního procesoru.</p> <p><b>Poznámka:</b> Pro tento parametr nemůžete zadat žádnou hodnotu, pokud jste do parametru SPNWSCFG zadali existující konfiguraci servisního procesoru.</p> <p><b>*DFT</b> Použijí se předvolené hodnoty ID a hesla uživatele.</p> <p><b>Prvek 1: Jméno uživatele</b> Uveďte jméno uživatele servisního procesoru vzdáleného systému.</p> <p><b>Prvek 2: Heslo uživatele</b> Uveďte heslo servisního procesoru vzdáleného systému. Heslo musí mít minimálně 5 znaků a obsahovat alespoň jeden abecední znak a jeden numerický znak nebo znak symbolu.</p>	<p>Jméno:</p> <p>Heslo:</p>

Pole	Popis a instrukce	Hodnota
Identifikátor certifikátu SP (SPCERTID)	<p>Identifikátor certifikátu SP uvádí jedno ze tří možných polí, které identifikují certifikát servisního procesoru. Účelem tohoto parametru je poskytnout další ověření, že certifikát pochází ze servisního procesoru. Obsah vybraných polí musí přesně odpovídat poli, které bylo zadáno při generování certifikátu nebo bylo požadováno od vydavatele certifikátů.</p> <p><b>Poznámka:</b> Pro tento parametr nemůžete zadat žádnou hodnotu, pokud do parametru SPNWSCFG zadáte stávající konfiguraci servisního procesoru.</p> <p><b>Jednotlivé hodnoty:</b></p> <p><b>*NONE</b> Certifikát servisního procesoru není nakonfigurován.</p> <p><b>Prvek 1: Komponenta</b></p> <p><b>*COMMONNAME</b>            Vybírá obecné jméno certifikátu zadané při generování certifikátu nebo požadované vydavatelem certifikátů. Na vzdáleném dohlížecím adaptéru II tato hodnota odpovídá poli "Jméno domény ASM", které se používá při generování certifikátu s automatickým podpisem nebo při požadavku na podpis certifikátu.</p> <p><b>*EMAIL</b>            Vybírá emailovou adresu certifikátu zadanou při generování certifikátu nebo požadovanou vydavatelem certifikátů. Na vzdáleném dohlížecím adaptéru II tato hodnota odpovídá poli <b>Emailová adresa</b>, které se používá při generování certifikátu s automatickým podpisem nebo při požadavku na podpis certifikátu.</p> <p><b>*ORGUNIT</b>            Vybírá organizační jednotku certifikátu zadanou při generování certifikátu nebo požadovanou vydavatelem certifikátů. Na vzdáleném dohlížecím adaptéru II tato hodnota odpovídá poli <b>Organizační jednotka</b>, které se používá při generování certifikátu s automatickým podpisem nebo při požadavku na podpis certifikátu.</p> <p><b>Prvek 2: Porovnávací hodnota</b></p> <p><b>porovnávací-hodnota</b>            Zadejte porovnávací hodnotu komponenty certifikátu. Uveďte maximálně 255 znaků a ohraničte je apostrofy.</p>	<p>Komponenta:</p> <p>Hodnota komponenty:</p>

Pole	Popis a instrukce	Hodnota
Identifikátor vzdáleného systému (RMTSYSID)	<p>Uvádí identifikační sériové číslo, typ a model vzdáleného systému. Je-li tato hodnota zadána, používá se k vyhledání vzdáleného systému v síti. Tyto hodnoty vyhledejte na štítku vzdáleného systému.</p> <p><b>Poznámka:</b> Pro tento parametr nemůžete zadat žádnou hodnotu, pokud do parametru RMTNWSCFG zadáte stávající konfiguraci vzdáleného systému.</p> <p><b>Jednotlivé hodnoty:</b></p> <p><b>*EID</b> Použije se identifikátor krytu servisního procesoru.</p> <p><b>Prvek 1: Sériové číslo</b></p> <p><b>sériové-číslo</b> Zadejte sériové číslo počítače vzdáleného systému.</p> <p><b>Prvek 2: Výrobní typ a model</b></p> <p><b>typ-model</b></p> <p>Zadejte typ a model počítače vzdáleného systému ve tvaru tttmmm, kde tttt je typ počítače a mmm je číslo modelu počítače.</p>	<p>Sériové číslo:</p> <p>Výrobní typ a model:</p>
Metoda dodání (DELIVERY)	<p>Uvádí, jakým způsobem budou dodány parametry nezbytné pro konfiguraci vzdáleného systému.</p> <p><b>Poznámka:</b> Pro tento parametr nemůžete zadat žádnou hodnotu, pokud do parametru RMTNWSCFG zadáte stávající konfiguraci vzdáleného systému.</p> <p><b>*DYNAMIC</b></p> <p>Parametry jsou dodávány vzdálenému systému dynamicky pomocí DHCP.</p> <p><b>*MANUAL</b></p> <p>Parametry jsou ve vzdáleném systému konfigurovány manuálně pomocí obslužných programů BIOS (System BIOS nebo Adapter BIOS - CTRL-Q).</p>	
Autentizace CHAP (CHAPAUT)	<p>Uvádí protokol CHAP (Challenge Handshake Authentication Protocol) pro cíl iSCSI hostitelského systému za účelem autentizace vzdáleného uzlu iniciátoru.</p> <p><b>Poznámka:</b> Pro tento parametr nemůžete zadat žádnou hodnotu, pokud do parametru RMTNWSCFG zadáte stávající konfiguraci vzdáleného systému.</p> <p><b>Jednotlivé hodnoty:</b></p> <p><b>*NONE</b> Autentizace CHAP není povolena.</p> <p><b>Prvek 1: Jméno CHAP</b></p> <p>Zadejte jméno CHAP.</p> <p><b>Prvek 2: Šifrovací klíč CHAP</b></p> <p>Uveďte šifrovací klíč, který chcete použít pro protokol CHAP (Challenge Handshake Authentication Protocol), jako hodnotu o délce až 24 znaků.</p>	<p>Jméno CHAP:</p> <p>Šifrovací klíč CHAP:</p>

Pole	Popis a instrukce	Hodnota
ID zaváděcího zařízení (BOOTDEVID)	<p>Uvádí adresu prvku PCI (sběrnice/zařízení/funkce) adaptéru iSCSI ve vzdáleném systému, který bude sloužit k zavedení operačního systému. Tato informace je přístupná pomocí obslužných programů BIOS (System BIOS nebo Adapter BIOS - CTRL-Q).</p> <p><b>Poznámka:</b> Pro tento parametr nemůžete zadat žádnou hodnotu, pokud do parametru RMTNWSCFG zadáte stávající konfiguraci vzdáleného systému.</p> <p><b>Jednotlivé hodnoty:</b></p> <p><b>*SINGLE</b> Ve vzdáleném systému se používá jediný adaptér typu iSCSI. Poznámka: Pokud má vzdálený systém na serveru více než jeden adaptér iSCSI, musí být specifikováno, ze kterého adaptéru se bude systém zavádět.</p> <p><b>Prvek 1: Číslo sběrnice</b> Zadejte číslo adaptéru typu iSCSI ve vzdáleném systému, který bude sloužit k zavedení systému.</p> <p><b>Prvek 2: Číslo zařízení</b> Zadejte číslo zařízení adaptéru typu iSCSI ve vzdáleném systému, které bude sloužit k zavedení systému.</p> <p><b>Prvek 3: Funkce</b> <b>číslo-funkce</b> Zadejte číslo funkce adaptéru typu iSCSI ve vzdáleném systému, která bude sloužit k zavedení systému.</p>	<p>Číslo sběrnice:</p> <p>Zařízení:</p> <p>Funkce:</p>

Pole	Popis a instrukce	Hodnota
Volby dynamického zavádění systému (DYNBOOTOPT)	<p>Jedná se o rozšířenou funkci.</p> <p>Tento parametr se používá při konfiguraci interního DHCP serveru, který je součástí firmwaru adaptéru iSCSI Target Host Bus Adapter a je požadován vzdáleným iniciátorem typu iSCSI pro poskytování adresy a parametrů pro zavádění systému bez použití disků.</p> <p><b>Poznámka:</b> Pro tento parametr nemůžete zadat žádnou hodnotu, pokud do parametru RMTNWSCFG zadáte stávající konfiguraci vzdáleného systému.</p> <p><b>Prvek 1:</b></p> <p><b>ID prodejce</b> Klient a server jsou předem nakonfigurovány na pevný ID prodejce. Správci sítě mohou konfigurovat klienty tak, aby si mohli sami nadefinovat vlastní identifikační hodnoty, které budou předávat hardwaru a operačnímu systému, případně další identifikační informace. Pro tuto funkci se používá DHCP, volba 60 popsaná v dokumentu IETF RFC 2132.</p> <p><b>*DFT</b> Použijí se předvolené hodnoty ID prodejce.</p> <p><b>id-prodejce</b> ID prodejce adaptéru typu iSCSI ve vzdáleném systému, který se použije.</p> <p><b>Prvek 2:</b></p> <p><b>ID alternativního klienta</b> Tuto hodnotu používají klienti, aby uvedli jejich jedinečný identifikátor serveru. Každý identifikátor klienta musí být jedinečný mezi ostatními identifikátory klientů používanými v aktivní síti typu DHCP, k níž je klient připojen (to znamená ve všech vzdálených podsítích dosažitelných prostřednictvím relé DHCP). Prodejci a systémoví administrátoři jsou odpovědní za výběr identifikátorů klienta, které vyhovují těmto požadavkům na jedinečnost. Pro tuto funkci se používá DHCP, volba 61 popsaná v dokumentu IETF RFC 2132.</p> <p><b>*ADPT</b> Předvolený ID klienta je tvořen adresou adaptéru pro adaptér typu iSCSI ve vzdáleném systému. Tato hodnota se použije při identifikaci vzdáleného systému.</p> <p><b>id-klienta</b> Zadejte ID klienta adaptéru typu iSCSI ve vzdáleném systému, který bude sloužit k zavedení systému.</p>	ID prodejce:  Alternativní ID klienta:

Pole	Popis a instrukce	Hodnota
Vzdálená rozhraní (RMTIFC)	<p>Uvádí rozhraní vzdáleného systému. Tato informace se používá k identifikaci a konfiguraci rozhraní vzdáleného systému. Každý port adaptéru má dvě funkce pro podporu rozhraní SCSI a LAN.</p> <p><b>Poznámka:</b> Pro tento parametr nemůžete zadat žádnou hodnotu, pokud do parametru RMTNWSCFG zadáte stávající konfiguraci vzdáleného systému.</p> <p><b>Prvek 1: Rozhraní SCSI</b></p> <p><b>Prvek 1: Adresa adaptéru</b> Zadejte 12znakovou hexadecimální adresu adaptéru pro rozhraní SCSI vzdáleného systému.</p> <p><b>Prvek 2: Internetová adresa</b> <b>internetová-adresa</b> pro rozhraní SCSI vzdáleného systému.</p> <p><b>Prvek 3: Maska podsítě</b> <b>maska-podsítě</b> pro rozhraní SCSI vzdáleného systému.</p> <p><b>Prvek 4: Adresa brány</b> <b>adresa-brány</b> pro rozhraní SCSI vzdáleného systému.</p> <p><b>Prvek 5: Kvalifikované jméno iSCSI</b></p> <p><b>*GEN</b></p> <p>System bude automaticky generovat kvalifikované jméno iSCSI.</p> <p><b>iqn-jméno</b></p> <p>kvalifikované jméno iSCSI pro rozhraní SCSI vzdáleného systému.</p>	<p>Rozhraní SCSI</p> <ul style="list-style-type: none"> <li>• Adresa adaptéru:</li> <li>• Internetová adresa:</li> <li>• Maska podsítě:</li> <li>• Adresa brány (volitelné):</li> <li>• Kvalifikované jméno iSCSI:</li> </ul>
Vzdálená rozhraní (RMTIFC) - pokračování	<p><b>Prvek 2: Rozhraní LAN</b></p> <p><b>Prvek 1: Adresa-adapteru</b></p> <p>12znaková hexadecimální adresa adaptéru pro rozhraní LAN nebo TOE (TCP Offload Engine) vzdáleného systému.</p> <p><b>Prvek 2: Internetová adresa</b></p> <p>pro rozhraní LAN vzdáleného systému.</p> <p><b>Prvek 3: Maska podsítě</b></p> <p>pro rozhraní LAN vzdáleného systému.</p> <p><b>Prvek 4: Adresa brány</b></p> <p>pro rozhraní LAN vzdáleného systému.</p>	<p>Rozhraní LAN</p> <ul style="list-style-type: none"> <li>• Adresa-adapteru:</li> <li>• Internetová adresa:</li> <li>• Maska podsítě:</li> <li>• Adresa brány (volitelné):</li> </ul>

## Informace týkající se klastrové služby Windows

### Poznámky:

1. Tento pracovní formulář vyplňte pouze v případě, že instalujete klastrovaný integrovaný server a váš hardwarový model podporuje klastrovou službu Windows Cluster Service. (Servery Integrated Netfinity Server nepodporují klastrovou službu Windows.)
2. V operačním systému i5/OS se síťové adaptéry nazývají porty.



Položka	Popis a instrukce	Hodnota
Jméno klastru	<p>Uvádí jméno klastru. Administrátor bude toto jméno používat pro připojení ke klastru. Jméno klastru musí být odlišné od jména domény, od jmen všech počítačů v doméně a od jmen dalších klastrů v doméně.</p> <p>Jméno klastru se také použije při vytváření paměťového prostoru síťového serveru, který bude sloužit jako prostředek kvora klastru Windows.</p> <p><b>*NONE:</b> Klastr Windows se nevytvoří ani nepřipojí.</p> <p><b>jméno-klastru:</b> Zadejte jméno klastru.</p>	

Položka	Popis a instrukce	Hodnota
Konfigurace klastru (prvky 1 až 4)	<p>Uvádí parametry požadované při konfiguraci nového klastru Windows.</p> <p><b>Poznámky:</b></p> <p>Tento parametr se používá k ověření konfigurace klastrů i5/OS. K instalaci klastrové služby se používají průvodci konfigurací Microsoft.</p> <p>Tento parametr je vyžadován pouze při tvorbě nového klastru Windows pomocí parametru CLU (Jméno klastru).</p> <p><b>Prvek 1: Jméno domény klastru</b> Uvádí doménu, do které klastr patří. Pokud klastr již existuje, bude připojen, jinak bude vytvořen. Při vytváření klastru je nutné uvést parametr CLUCFG (Konfigurace klastru).</p> <p><b>jméno-domény-klastru:</b> Zadejte jméno domény, do které klastr patří, vytváříte-li nový klastr.</p> <p><b>Prvek 2: Velikost prostředku kvora</b> Uvádí v megabajtech velikost paměťového prostoru, který se použije jako prostředek kvora Windows.</p> <p><b>*CALC</b> Uvádí, že velikost by se měla vypočítat a měla by to být předvolená hodnota vycházející z parametru WNTVER (Verze Windows serveru).</p> <p><b>velikost-kvora</b> Uvádí velikost prostředku kvora Windows v megabajtech. Velikost musí být v rozsahu 550 megabajtů až 1024000 megabajtů.</p> <p><b>Prvek 3: ASP prostředku kvora</b> Uvádí společnou oblast pro paměťový prostor sloužící jako prostředek kvora Windows. Zadejte jednu z níže uvedených hodnot:</p> <p><b>1:</b> Paměťový prostor se vytvoří ve společné oblasti paměti 1 v systémovém ASP.</p> <p><b>ASP-kvora:</b> Zadejte hodnotu identifikátoru ASP od 2 do 255. Platné hodnoty závisí na tom, kolik ASP je v systému definováno.</p> <p><b>Prvek 4: Zařízení ASP kvora</b> Uvádí jméno zařízení nezávislého ASP používané pro společnou oblast paměti, která se použije jako prostředek kvora Windows. <b>Poznámka:</b> Není možné zadat zároveň hodnotu "ASP prostředku kvora" i hodnotu "Zařízení ASP kvora".</p>	<p>Jméno domény klastru:</p> <p>Velikost prostředku kvora:</p> <p>ASP prostředku kvora:</p> <p>Zařízení ASP kvora:</p>

Položka	Popis a instrukce	Hodnota
Konfigurace klastru (prvky 5 až 7)	<p><b>Prvek 5: Port pro připojení klastru</b> Uvádí port použitý pro komunikace klastrové služby.</p> <p><b>*VRTETHx:</b> Je konfigurován port <i>x</i> virtuální sítě Ethernet, kde <i>x</i> nabývá hodnoty 0 až 9.</p> <p><b>Poznámka:</b> Port virtuální sítě Ethernet musí být konfigurován tak, aby odpovídal této hodnotě.<b>Prvek 6: Internetová adresa klastru</b> Uvádí internetovou adresu klastru.</p> <p><b>IP adresa:</b> Zadejte internetovou adresu klastru ve tvaru xxx.yyy.zzz.nnn, kde xxx, yyy, zzz a nnn jsou desítková čísla v rozsahu od 0 do 255.</p> <p><b>Poznámka:</b> Zvolená internetová adresa musí být jedinečná ve všech objektech NWSD a v konfiguraci i5/OS TCP/IP.</p> <p><b>Prvek 7: Masky podsítě klastru</b></p> <p><b>maska-podsítě:</b> Uvádí masku podsítě klastru ve tvaru nnn.nnn.nnn.nnn, kde nnn je desítkové číslo v rozsahu od 0 do 255.</p>	<p>Port připojení:</p> <p>Internetová adresa klastru:</p> <p>Maska podsítě klastru:</p>

## Porovnání systémů souborů FAT, FAT32 a NTFS

- | Windows 2000 Server nebo Windows Server 2003 vám umožňují volit mezi systémy souborů typu NTFS a FAT32.
- | Produkt IBM i5/OS Integrated Server Support použijte při instalaci vašich systémových jednotek odpovídající systém souborů, který závisí na hardwarových prostředcích, verzi Windows a zamýšleném použití. Instalační příkaz převede jednotky ve formátu FAT32 na formát NTFS, pokud nezadáte parametr CVTNTFS(\*NO).

### Poznámka:

**Nekonvertujte** jednotku **D** na formát NTFS. Musí zůstat ve formátu FAT.

Možnost konvertovat jednotku C však máte. Zde je několik srovnání, která vám mohou pomoci v rozhodování:

FAT	FAT32	NTFS
Nosič od velikosti diskety až do 4 GB.	Nosiče od 512 MB do 2 TB.	Nosič 10 MB až 2 TB.
Maximální velikost souboru 2 GB.	Maximální velikost souboru 4 GB.	Velikost souboru omezena velikostí nosiče.
Nepodporuje produkt Windows 2000 ani Windows Server 2003 Active Directory.	Nepodporuje produkt Windows 2000 ani Windows Server 2003 Active Directory.	Požadováno při použití produktu Windows 2000 nebo Windows Server 2003 Active Directory nebo sdílených klastrovaných jednotek.
Umožňuje přístup k souborům na pevném disku v PC-DOS.	Umožňuje přístup k souborům na pevném disku v PC-DOS.	Neumožňuje přístup k souborům na pevném disku v PC-DOS.
Umožňuje uživatelské přizpůsobení vašeho serveru prostřednictvím konfiguračních souborů NWSD.	Umožňuje uživatelské přizpůsobení vašeho serveru prostřednictvím konfiguračních souborů NWSD.	Nemůže používat konfigurační soubory NWSD.
Umožňuje použít nástroj pro výpis paměti NWSD (QFPDMPLS) k načtení souborů z disku kvůli servisu.	Umožňuje použít nástroj pro výpis paměti NWSD k načtení souborů z disku kvůli servisu.	Nelze použít nástroj pro výpis paměti k načtení souborů z disku.

## Rada: Vyhledejte jména prostředků, máte-li více integrovaných serverů

Na serveru iSeries můžete mít nainstalováno několik integrovaných serverů stejného typu. V takovém případě je nebudete schopni na obrazovce Zobrazení komunikačních prostředků od sebe rozeznat.

Chcete-li zjistit, kterého integrovaného Windows serveru se jméno prostředku týká, postupujte takto:

1. Pokud již nejste na obrazovce Zobrazení komunikačních prostředků, napište DSPHDWRSC \*CMN; pak stiskněte klávesu Enter.
2. Do pole Volba vedle jména prostředku pro IOA souborového serveru napište hodnotu 7. Objeví se obrazovka Zobrazení podrobností o prostředku. U serverů připojených pomocí iSCSI vyhledejte Adaptér NWSH. To je prostředek, který se musí použít při vytváření objektu NWSH. Jméno objektu NWSH se používá při instalaci NWSH.
3. Podívejte se na pole Pozice karty pod záhlavím Fyzické umístění.
4. Podívejte se na popis slotů vašeho serveru iSeries. Jeden slot by měl být označen stejným číslem nebo kombinací písmen a číslic, jaké jsou v poli Pozice karty. Tento slot obsahuje hardware serveru Integrated xSeries Server, na který se odkazuje jméno prostředku.

Vraťte se zpět k části “Pracovní formulář pro parametry instalace i5/OS” na stránce 65.

## Podporované jazykové verze

Tyto jazyky jsou podporovány v parametru LNGVER (Verze jazyka) příkazu INSWNTSVR (Instalace Windows serveru):

LNGVER	Národní jazyk
*PRIMARY	Používá jazykovou verzi primárního jazyka, který je instalovaný na serveru iSeries
2911	Slovinština
2922	Portugalština
2923	Holandština
2924	Angličtina velká/malá písmena
2925	Finština
2926	Dánština
2928	Francouzština
2929	Němčina
2931	Španělština
2932	Italština
2933	Norština
2937	Švédština
2938	Angličtina velká písmena DBCS
2939	Němčina MNCS
2940	Francouzština MNCS
2942	Italština MNCS
2950	Angličtina velká písmena
2962	Japonština DBCS
2963	Holandština MNCS
2966	Belgická francouzština
2975	Čeština
2976	Maďarština

LNGVER	Národní jazyk
2978	Polština
2979	Ruština
2980	Brazilská portugálština
2981	Kanadská francouzština MNCS
2984	Angličtina velká/malá písmena DBCS
2986	Korejština DBCS
2987	Čínština tradiční
2989	Čínština zjednodušená
2994	Slovenština
2996	Portugalština MNCS


Produkt IBM i5/OS Integrated Server Support podporuje rozhraní Windows Multi-Language User Interface.

## Instalace serverů Windows 2000 Server nebo Windows Server 2003




Co budete potřebovat:

- Disk CD, který obsahuje software Windows 2000 Server nebo Windows Server 2003 (nebo obraz tohoto CD).
- Váš licenční klíč Windows (vytištěný na zadní straně obalu instalačního CD nebo na certifikátu).
- Vyplněný a vytištěný “Pracovní formulář pro parametry instalace i5/OS” na stránce 65 nebo příkazový řetězec vygenerovaný pomocným programem pro instalaci.

**Poznámka:** Dokumentace Microsoft uvádí, že máte před instalací Windows serveru nebo před jeho převedením na vyšší verzi zablokovat zrcadlení disků a odpojit UPS. Pamatujte si, že se to netýká zrcadlení disků ani UPS na serveru iSeries.

**Poznámka:** Pokud máte server IXS (Integrated xSeries Server) nebo adaptér IXA (Integrated xSeries Adapter) nebo iSCSI HBA, které nejsou uvedeny v tématu “Hardwarové požadavky” na stránce 55, podívejte se na webovou stránku IBM Integrated xSeries solutions , kde jsou uvedeny pokyny pro instalaci.

Proveďte tyto kroky:

1. Připravte hardware integrovaného serveru xSeries. Další informace najdete pod těmito odkazy:
  - IXA install read me first   
([www.ibm.com/servers/eserver/series/integratedxseries/ixareadme](http://www.ibm.com/servers/eserver/series/integratedxseries/ixareadme))
  - iSCSI install read me first   
([www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme](http://www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme))
  - IXS install read me first   
([www.ibm.com/servers/eserver/series/integratedxseries/ixsreadme](http://www.ibm.com/servers/eserver/series/integratedxseries/ixsreadme))
2. Pokud instalujete server připojený pomocí iSCSI, podívejte se na téma “Příprava hardwaru iSCSI na instalaci Windows” na stránce 87.
3. “Spuštění instalace z konzole i5/OS” na stránce 87.
4. “Pokračování instalace z konzole integrovaného Windows serveru” na stránce 91.
5. “Dokončení instalace serveru” na stránce 91.

Narazíte-li v průběhu instalace na nějaké chybové zprávy, podívejte se do části “Odpovědi na chybové zprávy během instalace” na stránce 102.

## Příprava hardwaru iSCSI na instalaci Windows

U serverů připojených pomocí iSCSI je třeba provést ještě další činnosti týkající se konfigurace poté, co připravíte hardware.

- “Inicializace zabezpečení servisního procesoru”
- “Vytvoření a spuštění adaptéru NWSH”

## Inicializace zabezpečení servisního procesoru

Pokud pro nový servisní procesor vytvoříte novou konfiguraci servisního procesoru, měli byste změnit nastavení zabezpečení z předvoleného jména uživatele a hesla servisního procesoru na nové jméno uživatele a heslo, které vyberete.

Z níže uvedeného seznamu vyberte proceduru odpovídající metodě zabezpečení, kterou jste se rozhodli použít.

- U hesla servisního procesoru bez SSL použijte metodu popsanou v tématu “Heslo servisního procesoru” na stránce 126.
- U hesla servisního procesoru se SSL použijte metodu popsanou v tématu “Konfigurace zabezpečení SSL servisního procesoru” na stránce 125.

## Vytvoření a spuštění adaptéru NWSH

Před instalací Windows na server připojený pomocí iSCSI musíte na serveru iSeries nakonfigurovat cílový adaptér iSCSI HBA. Tato konfigurace se nazývá zařízení NWSH (Network Server Host Adapter).

Zařízení NWSH může používat více aktivních serverů, ne pouze jeden. Pokud váš nový server bude používat stávající zařízení NWSH, ověřte, že toto zařízení je spuštěno.

Chcete-li vytvořit a spustit (logicky zapnout) nové zařízení NWSH, postupujte takto:

1. Pomocí produktu iSeries Navigator identifikujte hardwarové prostředky NWSH:
  - a. Rozbalte **Konfigurace a služba** → **Hardware** → **Komunikace**.
  - b. Poznamenejte si jméno pro každý prostředek s popisem adaptéru NWSH (Network Server Host Adapter).
  - c. Jestliže chcete použít CL příkaz, napište WRKHDWRSC TYPE(\*CMN).
2. Vytvořte zařízení NWSH. Další informace najdete v tématu “Vytvoření objektu NWSH” na stránce 113.
3. Spusíte zařízení NWSH. Další informace najdete v tématu “Spuštění objektu NWSH” na stránce 115.

## Spuštění instalace z konzole i5/OS

Chcete-li na server iSeries instalovat Windows 2000 Server nebo Windows Server 2003, potřebujete zvláštní oprávnění \*IOSYSCFG, \*ALLOBJ a \*JOBCTL. Dále je nutno mít licenční klíč k vašemu Windows serveru. Ve většině případů je vytištěn na zadní straně obalu instalačního CD.

1. Když provádíte instalaci typu \*FULL (úplnou), vložte instalační CD do optické jednotky serveru iSeries (pokud nemáte v plánu použít obraz instalačního CD).

Při provádění instalace typu \*BASIC, vložte CD ServerGuide do jednotky CD-ROM připojeného serveru xSeries.
2. Ke spuštění instalace použijte jednu u následujících metod:
  - Je-li k dispozici příkaz INSWNTSVR (Instalace Windows serveru), který je generován pomocným programem pro instalaci Windows serveru, postupujte takto:
    - a. Z příkazového řádku i5/OS zavolejte náznak pro zadávání příkazů (QCMD) a stiskněte F11=Zobrazit vše.
    - b. Na příkazový řádek i5/OS vložte příkaz INSWNTSVR vygenerovaný pomocným programem pro instalaci Windows serveru a stisknutím klávesy Enter příkaz spusíte.
    - c. Instalace se spustí a může trvat až jednu hodinu. Může po vás požadovat, abyste zadali další informace. Potom přejděte k části “Pokračování instalace z konzole integrovaného Windows serveru” na stránce 91.
  - Jinak začněte instalaci na příkazovém řádku i5/OS napsáním příkazu INSWNTSVR a stiskem klávesy F4, kterou zobrazíte parametry příkazu. Do každého z níže uvedených polí zadejte hodnoty z tématu “Pracovní formulář pro parametry instalace i5/OS” na stránce 65:

3. Do pole Popis síťového serveru (viz “Popisy síťového serveru” na stránce 65) zadejte jméno serveru, které obsahuje “Pracovní formulář pro parametry instalace i5/OS” na stránce 65 a stiskněte klávesu Enter.
4. Do pole Typ instalace zadejte hodnotu (\*FULL nebo \*BASIC), kterou jste vyplnili v tématu “Pracovní formulář pro parametry instalace i5/OS” na stránce 65.
5. Do pole Jméno prostředku zadejte informace, které jste vyplnili v tématu “Pracovní formulář pro parametry instalace i5/OS” na stránce 65.
6. Vyberte si Verzi Windows serveru, kterou chcete instalovat, a stiskněte klávesu Enter.

**Poznámka:** U serverů připojených pomocí iSCSI je požadován Windows Server 2003.

7. Chcete-li instalovat server z uloženého obrazu místo z fyzického disku CD, zadejte cestu k tomuto obrazu do pole Zdrojový adresář Windows.
8. V poli Volba instalace použijte předvolbu \*INSTALL.
9. Požadujete-li, aby instalace konfigurovala vlastnosti TCP/IP síťových adaptérů instalovaných na serveru iSeries, které budou řízeny novým integrovaným serverem, zadejte konfigurační hodnoty TCP/IP ve Windows, které uvádí “Pracovní formulář pro parametry instalace i5/OS” na stránce 65. Jinak tento krok přeskočte a použijte předvolenou hodnotu \*NONE.
10. Chcete-li instalovat a konfigurovat volitelný port virtuální sítě Ethernet, zadejte do pole Port Virtual Ethernet konfigurační hodnoty TCP/IP ve Windows, které uvádí “Pracovní formulář pro parametry instalace i5/OS” na stránce 65.
11. Napište hodnoty, které obsahuje “Pracovní formulář pro parametry instalace i5/OS” na stránce 65, do těchto polí:
  - Jméno lokální domény TCP/IP
  - Systém serveru jmen TCP/IP
  - Fronta zpráv serveru
  - Knihovna
12. Do pole Protokol událostí zadejte, které zprávy protokolu událostí má operační systém i5/OS získávat od serveru.
13. Do polí Paměťové prostory serveru zadejte hodnoty, které uvádí “Pracovní formulář pro parametry instalace i5/OS” na stránce 65:
  - Uveďte hodnoty do polí Velikost instalačního zdroje a Velikost systému nebo vyberte předvolbu \*CALC, která umožní systému vypočítat minimální velikost.
  - Chcete-li pro instalační zdrojovou a systémovou jednotku zvolit jiné ASP, zadejte je v odpovídajícím prvku buď do pole ASP paměťového prostoru, nebo do pole Zařízení ASP prostoru serveru.
  - U systémových jednotek až do 32 GB můžete v poli Konverze na NTFS zadat \*NO a nechat systémovou jednotku integrovaného serveru naformátovanou na FAT32. Jinak je předvolbou hodnota \*YES pro konverzi systémové jednotky na NTFS (New Technology File System) během instalace. Při rozhodování vám mohou pomoci informace v tématu “Porovnání systémů souborů FAT, FAT32 a NTFS” na stránce 84. Příkaz INSWNTSVR v případě nutnosti automaticky konvertuje systémové jednotky větší než 32 GB na NTFS.
14. **Volitelné:** Do odpovídajících parametrů V pracovní skupině nebo V doméně zadejte buď pracovní skupinu Windows, nebo doménu.
15. **Volitelné:** Do pole Úplné jméno zadejte jméno uživatele, který je vlastníkem licence pro instalovaný Windows server.
16. **Volitelné:** Do pole Organizace Zadejte jméno organizace, která je vlastníkem licence pro instalovaný Windows server.
17. Do pole Jazyková verze zadejte \*PRIMARY, chcete-li, aby licencovaný program IBM i5/OS Integrated Server Support používal váš primární jazyk. Chcete-li předejít problémům s předdefinovanými jmény, která není možné zapsat, zajistěte, aby licencovaný program pro integraci a Windows server používaly stejný jazyk. Chcete-li vědět, které jazyky příkaz podporuje, přečtěte si téma “Podporované jazykové verze” na stránce 85.
18. Do pole Synchronizace data a času zadejte \*YES, aby se datum a čas v operačním systému i5/OS synchronizoval s integrovaným serverem každých 30 minut. Jestliže chcete, aby operační systém i5/OS prováděl synchronizaci data a času s integrovaným serverem pouze při jeho logickém zapnutí, napište \*NO.



19. Do pole Přenesení uživatele domény zadejte, zda se má server použít k synchronizaci a přenesení uživatelů do domény Windows nebo aktivního adresáře.
20. Do pole Licenční klíč Windows zadejte klíč z disku CD (včetně pomlčky) od firmy Microsoft. Ve většině případů naleznete klíč vytištěný na zadní straně obalu instalačního disku CD s operačním systémem Windows.
21. Do pole Typ licence zadejte licenci na Windows server, kterou jste zakoupili.
22. Pokud jste do pole Typ licence zadali \*PERSERVER, pak do pole Klientské licence zadejte počet klientských licencí, které jste zakoupili.
23. Do pole Terminálové služby zadejte, které volby Terminálových služeb se mají instalovat.
24. Do pole Vyhrazené prostředky zařízení napište hodnotu uvedenou v tématu “Pracovní formulář pro parametry instalace i5/OS” na stránce 65.
25. Do pole Doba do ukončení práce systému zadejte hodnotu v minutách pro časový limit ukončení činnosti integrovaného Windows serveru. Používá se k omezení času, který poskytnete operačnímu systému integrovaného Windows serveru předtím, než bude server logicky vypnut.
26. Pokud instalujete server připojený pomocí IXA nebo IXS, pokračujte krokem 34 na stránce 90 a vyplňte dodatečné parametry. Jestliže instalujete server připojený pomocí iSCSI, napište do následujících polí hodnoty pro parametry iSCSI, které uvádí “Pracovní formulář pro parametry instalace i5/OS” na stránce 65:
  - Časovač aktivace
  - Fronta zpráv komunikací
27. Do pole Cesta k paměťovým prostorům zadejte jméno adaptéru NWSH, který se bude používat pro komunikaci s diskovou pamětí typu iSCSI. Další informace najdete v tématu “Adaptéry hostitele síťového serveru” na stránce 41.
28. Do pole Cesta k virtuální síti Ethernet zadejte jméno jednoho nebo více adaptérů NWSH, které se budou používat pro komunikaci typu iSCSI LAN.
  - Do pole Port Virtual Ethernet zadejte alespoň jednu hodnotu pro port \*VRTETHPTP a všechny další výše uvedené porty.
29. **Volitelné:** Specifikujte Port TCP pro ukončení práce systému a Řídicí port Virtual Ethernet.
30. Do níže uvedených polí zadejte jméno existující konfigurace síťového serveru nebo vyberte předvolené hodnoty.
  - NWSCFG ve vzdáleném systému.
  - NWSCFG se servisním procesorem.
  - NWSCFG se zabezpečeným připojením.

Stiskněte klávesu Enter.
31. Zadejte pravidlo zabezpečení IP (IPSec), které se bude používat:
  - U všech stávajících NWSCFG se zabezpečeným připojením:
    - a. Do pole Pravidlo zabezpečení IP zadejte konfigurované pravidlo zabezpečení, které se bude používat.
    - b. Stiskněte klávesu Enter.
  - U předvolené NWSCFG se zabezpečeným připojením:
    - a. Do pole Předvolené pravidlo zabezpečení IP zadejte předvolené pravidlo zabezpečení IP (IPSec), které se bude používat.
    - b. Stiskněte klávesu Enter.
32. Pokud k tomu budete vyzváni, zadejte v případě, že používáte předvolené Jméno NWSCFG se servisním procesorem do následujících polí informace o konfiguraci servisního procesoru, které uvádí “Pracovní formulář pro parametry instalace i5/OS” na stránce 65:
  - Do pole Inicializace servisního procesoru zadejte tyto hodnoty:
    - a. Pokud má inicializace servisního procesoru jakoukoli jinou hodnotu než \*NONE, zadejte do pole Identifikátor certifikátoru SP hodnotu Komponenta a Porovnávací hodnota.
  - V poli Povolit unicast vyberte volbu pro použití unicast:
    - a. Jestliže nepoužíváte unicast zadejte do pole Identifikátor krytu hodnoty pro Sériové číslo a Výrobní typ a model.

- l b. Pokud používáte unicast, zadejte hodnotu do pole Jméno servisního procesoru, nebo do pole Internetová
  - l adresa SP zadejte IP adresu.
  - l • V případě, že používáte předvolené Jméno NWSCFG ve vzdáleném systému a pro inicializaci servisního
  - l procesoru se používá jiná hodnota než \*NONE, zadejte do polí Jméno uživatele a Heslo uživatele hodnoty
  - l Autentizace SP.
  - l 33. Pokud k tomu budete vyzváni, zadejte v případě, že používáte předvolené Jméno NWSCFG ve vzdáleném
  - l systému, do následujících polí informace o konfiguraci vzdáleného systému, které uvádí “Pracovní formulář pro
  - l parametry instalace i5/OS” na stránce 65:
  - l • Do pole Identifikátor vzdáleného systému zadejte jednu z níže uvedených hodnot:
  - l a. Použijte sériové číslo uvedené v poli Identifikátor krytu nebo NWSCFG se servisním procesorem.
  - l b. Zadejte hodnotu pro Sériové číslo a volitelně pro Výrobní typ a model do pole Identifikátor vzdáleného
  - l systému.
  - l • Do pole Metoda dodání zadejte hodnotu, která se použila pro konfiguraci vzdáleného systému.
  - l • Do pole Autentizace CHAP zadejte hodnoty protokolu CHAP (Challenge Handshake Authentication
  - l Protocol) používané k ověřování identity vzdáleného systému.
  - l • Do pole ID zařízení pro zavádění systému uveďte adaptér typu iSCSI, který se používá k zavádění
  - l vzdáleného systému. Pokud ve vzdáleném systému existuje pouze jedno zařízení pro zavádění systému typu
  - l iSCSI, použijte předvolenou hodnotu \*SINGLE.
  - l • Jestliže používáte Metodu dodání \*DYNAMIC, zadejte volitelně všechny další volby v poli Volby
  - l dynamického zavádění systému.
  - l • Do pole Vzdálená rozhraní zadejte hodnoty pro rozhraní používané ve vzdáleném systému.
  - l a. Do pole Rozhraní iSCSI zadejte hodnoty pro funkci SCSI, mezi které patří:
  - l 1) Adresa adaptéru typu SCSI.
  - l 2) Internetová adresa typu SCSI.
  - l 3) Maska podsítě typu SCSI.
  - l 4) **Volitelně:** Zadejte adresu brány SCSI,
  - l 5) Kvalifikované jméno iSCSI nebo zadejte \*GEN, čímž povolíte systému, aby automaticky
  - l generoval adresu.
  - l b. Do pole Rozhraní LAN zadejte hodnoty pro funkci LAN, mezi které patří:
  - l 1) Adresa adaptéru typu LAN (TOE).
  - l 2) Internetová adresa typu LAN.
  - l 3) Maska podsítě typu LAN.
  - l 4) **Volitelně:** Zadejte adresu brány LAN.
  - l 34. Vyplnění dodatečných parametrů vám umožňuje provádět tyto činnosti:
  - l • Instalovat jiný než předvolený typ klávesnice na integrovaný server. (Platné identifikátory stylu klávesnice jsou
  - l uvedeny v souboru TXTSETUP.SIF v adresáři I386 instalačního zdroje Windows serveru.)
  - l • Použít pro dvoubodovou virtuální síť Ethernet vlastní IP adresy.
  - l • Použít konfigurační soubor NWSD. Další informace najdete v tématu Kapitola 15, “Konfigurační soubory
  - l popisu síťového serveru”, na stránce 235.
  - l • Konfigurovat novou nebo stávající konfiguraci Windows klastru.
- Doplňte případné další informace, které mohou být pro vaše potřeby důležité, a stiskněte klávesu Enter.

Integrovaný Windows server se začne instalovat. Druhá etapa procesu instalace je v tématu “Pokračování instalace z konzole integrovaného Windows serveru” na stránce 91. Proces potrvá přibližně 1 hodinu v závislosti na konfiguraci hardwaru.

## Pokračování instalace z konzole integrovaného Windows serveru

Po dokončení fáze instalace na straně i5/OS se spustí integrovaný server. Začíná fáze instalace na straně Windows serveru. Tato fáze instalace je snadná, pokud jste dokončili kroky uvedené v tématu “Příprava na instalaci integrovaných Windows serverů” na stránce 58 a zadali instalační atributy u příkazu INSWNTSVR (Instalace Windows serveru).

Chcete-li dokončit instalaci Windows serveru bez použití produktu ServerGuide, proveďte tyto úlohy:

1. V kroku **License Agreement** (v okně Windows Server Setup) klepněte na rádiové tlačítko **I accept this agreement**. Potom klepněte na **Next**.
2. Dostanete-li chybové zprávy, klepněte na **OK** a instalační program vám umožní situaci napravit nebo dodat nezbytné informace. Příklady těchto chybových zpráv a informace o tom, jak na ně odpovídat, najdete v tématu “Odpovědi na chybové zprávy během instalace” na stránce 102.
3. Zadejte a potvrďte heslo v okně **Computer Name and Administrator Password**.
4. V dialogovém okně **Date/Time Settings**:
  - a. Potvrďte, že časové pásmo i5/OS je správné a odpovídá systémové hodnotě časového pásma uvedené v pomocném programu pro instalaci Windows serveru. Další informace najdete v tématu “Synchronizace času” na stránce 60.
  - b. Jste-li v oblasti, která dodržuje letní čas, zaškrtněte políčko **Automatically adjust clock**.  
Víte-li jistě, že se u vás letní čas nedodržuje, nechte políčko “Automatically adjust clock for daylight savings changes” nezaškrtnuté.
5. Na panelu Completing the Windows Setup Wizard klepněte na **Finish**.
6. V okně **Windows Setup** klepněte na tlačítko **Restart Now** nebo počkejte 15 sekund a server se automaticky restartuje.

### Poznámka:

Při instalaci Windows serveru jako řadiče domény by měl být zadáním příkazu DCPRMO současně nainstalován produkt Active Directory. Další informace o instalaci Active Directory najdete v dokumentaci Microsoft.


Chcete-li dokončit instalaci Windows serveru, když nepoužíváte produkt ServerGuide, proveďte tyto kroky:

- Vložte CD s programem ServerGuide do lokální optické jednotky serveru připojeného pomocí HSL. (Server xSeries připojený adaptérem IXA.)
- Odpovězte **G** na zprávu NTA100C “Insert ServerGuide CD-ROM into &2 optical device”. (C G)”
- Postupujte podle pokynů průvodce instalací ServerGuide.

Další informace najdete v tématu “Dokončení instalace serveru”.

## Dokončení instalace serveru

Po instalaci severu Windows 2000 Server nebo Windows Server 2003 do operačního systému i5/OS proveďte několik závěrečných kroků k ověření, že je server správně nainstalován a připraven.

1. Doporučuje se nainstalovat nejnovější podporovaný servisní balík Microsoft. Informace týkající se servisních balíků a seznam nejnovějších podporovaných servisních balíků najdete pod heslem Microsoft Service packs v tématu Service Information na webových stránkách IBM Integrated xSeries Solutions . Zde rovněž najdete informace pro spuštění aktualizace Windows.
2. Požadujete-li, aby se integrovaný Windows server automaticky logicky zapnul, když spustíte TCP/IP, prostudujte si téma “Nastavení integrovaného Windows serveru na automatické logické zapnutí s TCP/IP” na stránce 102.
3. Jestliže pro instalaci serveru připojeného pomocí iSCSI nebyla dosud aktivována systémová hodnota QRETSVRSEC, změňte systémovou hodnotu QRETSVRSEC v operačním systému i5/OS tak, abyste zajistili, že bude operační systém i5/OS uchovávat hesla (předejete tak prodlevám při přihlašování uživatelů).
  - Na příkazový řádek operačního systému i5/OS zadejte příkaz:  
WRKSYSVAL SYSVAL(QRETSVRSEC)

- Chcete-li hodnotu změnit, zadejte 2 do pole Volba a stiskněte klávesu Enter.
  - Změňte hodnotu Retain server security data na 1.
4. Pokud chcete, aby server měl jméno, které se liší od jména NWSA (například jméno, které má více než 8 znaků), můžete změnit jméno počítače z konzole Windows. Více informací najdete v dokumentaci Windows.
  5. Můžete vytvořit další diskové jednotky pro aplikace a data místo toho, abyste ukládali tyto položky na systémovou jednotku. Další informace najdete v tématu “Přidání diskových jednotek na integrované Windows servery” na stránce 156.
  6. Pro váš server můžete definovat další virtuální lokální síť Ethernet, takže se bude moci připojit k ostatním serverům ve stejné logické části nebo částech. Další informace najdete v tématu Kapitola 6, “Správa virtuálních sítí Ethernet a externích sítí”, na stránce 107.
  7. Můžete zapsat některé z vašich uživatelů v operačním systému i5/OS na server nebo do domény Windows. Další informace najdete v tématu Kapitola 11, “Administrace uživatelů integrovaných Windows serverů v operačním systému i5/OS”, na stránce 169.
  8. Můžete zabránit tomu, aby se změnilo písmeno optické jednotky, kdykoliv připojíte k serveru uživatelský paměťový prostor. Použijte **Disk Management** a přiřaďte optické jednotce integrovaného serveru písmeno. (Například byste z ní mohli udělat jednotku X.)
  9. Servery můžete uživatelsky přizpůsobit vytvořením vlastního konfiguračního souboru NWSA. Další informace najdete v tématu Kapitola 15, “Konfigurační soubory popisu síťového serveru”, na stránce 235.
  10. Požadujete-li klastrování Windows, přečtěte si téma “Klastrová služba Windows” na stránce 95.
  11. Je-li váš server nainstalovaný se serverem Windows Server 2003 a má instalovaný Active Directory (například jde o řadič domény), prostudujte si téma “Použití služby Kerberos se serverem Windows Server 2003 Active Directory Server” na stránce 100.
  12. Pokud používáte server IXS typu 2892-002 nebo 4812-001 se serverem Microsoft Windows 2000 Server, měli byste instalovat zvláštní ovladače videozařízení, abyste využili videočip ATI Radeon, který se nachází na serveru IXS typu 2892-002 nebo 4812-001. Další informace najdete v tématu “Instalace ovladačů videozařízení ATI Radeon 7000M pro Windows 2000 na serveru IXS 2892-002 nebo 4812-001” na stránce 101.
  13. Jestliže používáte server IXS typu 2892-002 nebo 4812-001 se serverem Microsoft Windows Server 2003, měli byste přizpůsobit nastavení akcelerace hardwaru, abyste dosáhli optimálního výkonu. Další informace najdete v tématu “Přizpůsobení akcelerace hardwaru u serveru Windows Server 2003 na serveru IXS 2892-002 nebo 4812-001” na stránce 102.

**Upozornění:** Pokud plánujete, že budete u integrovaného serveru používat firewall, zajistěte, abyste nesměrovali internetové adresy dvoubodové virtuální sítě Ethernet do serveru SOCKS (software common knowledge IR system), který funguje jako firewall. Vyvolávalo by to poruchy spojení. Informace o nastavení firewallu najdete v tématu Firewall: Getting started.

V případě serverů připojených pomocí iSCSI můžete provést tyto kroky:

1. Můžete nakonfigurovat server, aby používal další adaptéry iSCSI HBA, a tím zlepšit výkon nebo dostupnost. Další informace najdete v tématu “Správa využití adaptéru iSCSI HBA” na stránce 128.
2. Pokud vaše síť typu iSCSI podporuje velké velikosti rámců, máte možnost zlepšit výkon vaší virtuální sítě Ethernet. Další informace najdete v tématu “Posouzení velikosti maximální přenosové jednotky (MTU)” na stránce 131.

## Přechod na vyšší verzi licencovaného programu IBM iSeries Integration for Windows Server

Když přecházíte na verzi V5R3 operačního systému i5/OS a produktu IBM iSeries Integration for Windows Server, potřebujete disk CD, který obsahuje produkt 5722-WSV. Máte-li zároveň v plánu instalovat hardware nového serveru IXS (Integrated xSeries Server), určitě nejprve dokončete instalaci tohoto softwaru. V průběhu provádění procedury

přechodu na vyšší verzi popsané v publikaci iSeries Software Installation  proveďte navíc tyto kroky:

### Příprava na přechod na vyšší verzi:

1. Zajistěte, abyste na všech stávajících integrovaných Windows serverech i v operačním systému i5/OS měli instalovány nejnovější opravy kódu. Další informace najdete v tématu “Opravy kódu” na stránce 103.
2. Zajistěte, abyste měli k dispozici zálohování systému, které zahrnuje paměť alokovanou vašim integrovaným serverům.
3. Jako předběžné opatření si poznamenejte prostředky vztahující se k vašemu hardwaru:
  - a. Na příkazový řádek operačního systému i5/OS napište `WRKCFGSTS *NWS` a stiskněte klávesu Enter.
  - b. Do sloupce pro volbu vedle popisu síťového serveru napište 8. Objeví se obrazovka *Práce s popisy síťového serveru*.
  - c. Do sloupce pro volbu vedle popisu síťového serveru napište 5.
  - d. Odstráňte pomocí klávesy Page down dolů, dokud nevidíte pole *Jméno prostředku* a poznamenejte si hodnotu platnou pro tento síťový server (například LIN05).
  - e. Stiskněte dvakrát klávesu F12 a vraťte se z tohoto příkazu.
  - f. Na příkazový řádek operačního systému i5/OS napište příkaz `WRKHDWRSC TYPE(*CMN)` a stiskněte klávesu Enter.
  - g. Do sloupce pro volbu vedle jména prostředku, které jste určili v kroku 3d, napište 7 (*Zobrazit podrobnosti o prostředku*). Ve sloupci *typ* je číslo CCIN hardwaru serveru IXS (*Integrated xSeries Server*) a textový popis by měl být *IOP souborového serveru* nebo *IOA souborového serveru*.
  - h. Máte-li na serveru iSeries nainstalováno několik serverů IXS stejného typu, můžete správný server určit podle umístění karty:
    - 1) Podívejte se na pole *Pozice karty* pod záhlavím *Fyzické umístění*.
    - 2) Podívejte se na popis slotů vašeho serveru iSeries. Jeden slot by měl být označen stejným číslem nebo kombinací písmen a číslic, jaké jsou v poli *Pozice karty*. Tento slot obsahuje server IXS, na který se odkazuje jméno prostředku.
  - i. Informace, které se objeví, zaznamenejte do polí *Typ-model* a *Sériové číslo*.
  - j. Stiskněte dvakrát klávesu F12 a opusťte tento příkaz.
4. Logicky vypněte všechny integrované servery. Další informace najdete v tématu “Spuštění a zastavení integrovaného serveru” na stránce 141.

Chcete-li nainstalovat novou verzi operačního systému i5/OS na server iSeries, vraťte se k proceduře popsané

v publikaci *iSeries Software Installation* .

#### **Po přechodu na vyšší verzi operačního systému i5/OS proveďte ještě tyto kroky:**

1. Spusťte integrovaný server (viz “Spuštění a zastavení integrovaného serveru” na stránce 141) a ověřte, zda má stejné jméno prostředku:
  - a. Na příkazový řádek operačního systému i5/OS napište příkaz `WRKHDWRSC TYPE(*CMN)` a stiskněte klávesu Enter.
  - b. Do sloupce pro volbu vedle jména prostředku, které jste určili v kroku 3d, napište 7 (*Zobrazit podrobnosti o prostředku*). Ověřte, zda informace, které se objeví v poli *Typ-model* a *Sériové číslo* odpovídají tomu, co jste si u tohoto prostředku zaznamenali.
  - c. Jestliže pole neodpovídají tomu, co jste zaznamenali, postupujte takto:
    - 1) Stiskněte klávesu F12 a vraťte se na předchozí obrazovku.
    - 2) Pomocí volby 7 zobrazte podrobnosti pro další jména prostředků na seznamu a vyhledejte prostředek, jehož informace v polích *Typ-model* a *Sériové číslo* odpovídají hodnotám, které jste si zaznamenali. Poznamenejte si jméno prostředku, které operační systém i5/OS nyní asociuje s tímto hardwarem integrovaného serveru IXS. Stiskněte klávesu F12 a opusťte tento příkaz.
    - 3) Na příkazový řádek operačního systému i5/OS napište příkaz `WRKNWSD` a stiskněte klávesu Enter. Objeví se obrazovka *Práce s popisy síťových serverů*.
    - 4) Do sloupce pro volbu vedle popisu síťového serveru napište 2 (*Změna*) a stiskněte klávesu Enter. Objeví se obrazovka *Změna popisu síťového serveru*.



- 5) Změňte jméno prostředku tohoto serveru na nové, správné jméno prostředku.
2. Na svoje stávající integrované servery nainstalujte produkt IBM i5/OS Integrated Server Support. Další informace najdete v tématu “Instalace licencovaného programu IBM i5/OS Integrated Server Support” na stránce 62.

## Přechod na vyšší verzi licencovaného produktu IBM i5/OS Integrated Server Support na straně integrovaného serveru

Licencovaný program IBM i5/OS Integrated Server Support je software, který propojuje server iSeries a jeho integrované Windows servery. Dívejte se na něj jako na překladový program. Polovina programu běží na serveru iSeries a překládá z jazyka Windows do jazyka i5/OS a druhá polovina běží na integrovaných serverech a překládá z jazyka i5/OS do jazyka Windows.

Nové verze licencovaného programu IBM i5/OS Integrated Server Support jsou instalovány do operačního systému i5/OS. Pak je nutné zkopírovat a nainstalovat na integrovaný server tu část licencovaného programu, která se týká integrovaného serveru.

Je nutné, abyste přešli na vyšší verzi licencovaného programu vašeho stávajícího integrovaného Windows serveru, pokud instalujete tyto produkty:

- Novou verzi licencovaného programu IBM i5/OS Integrated Server Support.
- Novou verzi Windows serveru od firmy Microsoft.

### Nová verze licencovaného programu IBM i5/OS Integrated Server Support.

Když instalujete novou verzi licencovaného programu IBM i5/OS Integrated Server Support, musíte provést přechod všech stávajících integrovaných serverů na tuto úroveň. Pokud máte několik integrovaných serverů, můžete přejít na jejich vyšší verzi vzdáleně z operačního systému i5/OS.

Tato procedura vyžaduje, abyste měli stejné ID a heslo uživatele na integrovaných Windows serverech a v operačním systému i5/OS.

Chcete-li přejít na vyšší verzi integrovaného serveru, postupujte takto:

1. Ukončete všechny prováděné aplikace.
2. Zajistěte, aby na integrovaném serveru nebyli přihlášení žádní uživatelé.  
**Upozornění:** Integrovaný server se po dokončení instalace automaticky restartuje, takže přeskočíte-li krok 1 a 2, riskujete ztrátu dat.
3. Z nabídky **Start** vyberte **Programs**, potom **IBM iSeries**, dále **Integration for Windows Server** a nakonec **Software Level**.

#### Poznámka:

Když je nová úroveň licencovaného programu dostupná pro instalaci, pak (přihlásíte-li se na integrovaný server jako administrátor) se automaticky spustí Software Level.

4. Pokud provádíte přechod z verze V5R3 nebo vyšší, vyberte volbu **Synchronize**. V ostatních případech vyberte volbu **Install Release from iSeries**.
5. Řiďte se pokyny uživatelského rozhraní a dokončete instalaci.
6. **Rada:** Potom zálohujte předdefinované instalační a systémové jednotky na tomto serveru. Informace o zálohování jednotek najdete v tématu “Zálohování předdefinovaných diskových jednotek pro integrované Windows servery” na stránce 181. Poněvadž je bezpečnější zálohovat všechny paměťové prostory současně, měli byste zálohovat také asociovaný uživatelsky vytvořený paměťový prostor (viz “Zálohování uživatelem definovaných diskových jednotek u integrovaného Windows serveru” na stránce 181).

### Nová verze Windows serveru

Chcete-li provést přechod serverů z Windows NT 4.0 na Windows 2000, přečtěte si téma Přechod serveru z Windows NT 4.0 na Windows 2000 Server uváděné v rámci aplikace iSeries Information Center verze V5R3.

## Migrace z hardwaru 285x nebo 661x na hardware integrovaného serveru IXS 2890

U serverů IPCS nebo INS (typ 2850 a 6617) musí být před instalací verze V5R4 připojen nového hardware nebo musí být tyto servery migrovány na hardware 2890 IXS. Informace k této problematice uvádí téma Migrace hardwaru serveru Integrated xSeries Server z 285x nebo 661x na 2890 v rámci aplikace iSeries Information center verze V5R3.

### Migrace na servery připojené pomocí iSCSI

Migrace na server připojený pomocí iSCSI není podporována. Všechny servery připojené pomocí iSCSI vyžadují novou instalaci.

## Klastrová služba Windows

Klastrová služba Windows spojuje jednotlivé servery tak, aby mohly provádět společné úlohy. Kdyby některý server přestal fungovat, přesune proces zvaný přepnutí při selhání automaticky jeho pracovní zátěž na jiný a zajistí tak průběžnou službu. Kromě přepnutí při selhání využívají některé formy klastrování také vyvážení zatížení, které umožňuje, aby se zátěž rozložila v síti propojených počítačů.

Windows 2000 Advanced Server podporuje dvouuzlový klastr, zatímco Windows Server 2003 Enterprise Edition podporuje osmiuzlové klustry. Verze Windows Datacenter nejsou podporovány.

Klastrová služba Windows je podporována pouze u integrovaných Windows serverů, které provozují buď Windows 2000 Advanced Server, nebo Windows Server 2003 Enterprise Edition.

### Poznámky:

1. Aby mohly být klastrované uzly síťových Windows serverů spojeny do klastru, musí být tyto uzly umístěny v jediné logické části systému iSeries.
2. Systém xSeries připojený pomocí iSCSI nemůže být spojen do klastru se servery připojenými pomocí IXS/IXA.

Ačkoliv tradiční řešení klastrovaného Windows serveru vyžaduje sdílené fyzické rozhraní SCSI nebo zařízení Fibre Channel, používá řešení integrovaného Windows serveru ke sdílení virtuálních diskových jednotek mezi uzly klastru virtuální sběrnici Fibre Channel.

Kromě toho umožňuje nová podpora virtuální sítě Ethernet vysoce výkonnou a zabezpečenou komunikaci mezi jednotlivými klastrovanými uzly.

Podrobné kontrolní seznamy pro plánování a vytvoření klastru serverů jsou k dispozici v online nápovědě Microsoft ke klastrům serverů a měli byste si ji před instalací a konfigurováním klastru Windows serverů projít. Doplnující informace, včetně podrobných průvodců k instalaci klastrové služby, jsou k dispozici na webových stránkách firmy

Microsoft .

Další informace týkající se podpory klastrové služby Windows najdete v těchto tématech:

#### “Instalace klastrové služby Windows” na stránce 96


Zde zjistíte, jak instalovat a konfigurovat klastrovou službu Windows na integrovaném Windows serveru.

#### “Instalace klastrové služby Windows na stávající server” na stránce 96

Zde se dozvíte, jak vytvořit klustry na stávajícím integrovaném Windows serveru.

### Podpora klastrů na serveru připojeném pomocí iSCSI

Informace o podpoře poskytované serverem iSeries pro produkt MSCS (Microsoft Cluster Service) na serveru

připojeném pomocí iSCSI najdete v tématu MSCS on an iSCSI attached server  na webových stránkách Integrated xSeries Solutions ([www.ibm.com/servers/eserver/series/integratedxseries/windows/iscsiclusters.html](http://www.ibm.com/servers/eserver/series/integratedxseries/windows/iscsiclusters.html)).



## Instalace klastrové služby Windows

Dříve než klastrovou službu nainstalujete, přečtete si všechny kontrolní seznamy Microsoft pro instalaci klastrů serverů, abyste se v budoucnu vyvarovali problémů při plánování a instalaci.

**Poznámka:** Během instalace klastrové služby na první uzel logicky vypněte všechny ostatní uzly účastníci se klastrem, a to dříve, než spustíte Windows.

V informacích o klastrech serverů se všechny odkazy na sdílené rozhraní SCSI nebo zařízení Fibre Channel týkají implementace virtuálního Fibre Channel používaného pro přístup ke sdílenému paměťovému prostoru síťového serveru.

Chcete-li instalovat a spustit klastrovou službu Windows, proveďte tyto úkoly:

1. Instalace klastrové služby Windows na server IXS (Integrated xSeries Server).
  - “Instalace klastrové služby Windows na nový integrovaný Windows server”
  - “Instalace klastrové služby Windows na stávající server”
2. “Instalace klastrové služby Windows do operačního systému Windows” na stránce 98

## Instalace klastrové služby Windows na nový integrovaný Windows server

Nejnashší způsob, jak instalovat a konfigurovat klastrovaný Windows server je, když to uděláte při prvním konfigurování integrovaného serveru. Použijte příkaz INSWNTSVR (Instalace Windows serveru) s následujícími parametry, které uvádějí informace o konfiguraci:

- Parametr CLU (Jméno klastru).
- Parametr CLUCFG (Konfigurace klastru).

Další informace o instalaci integrovaného serveru najdete v tématu “Instalace serverů Windows 2000 Server nebo Windows Server 2003” na stránce 86.

Po provedení příkazu INSWNTSVR (a po dokončení instalace Windows serveru) a předtím, než budete instalovat klastrovou službu Windows na stranu Windows, musíte provést další konfigurační kroky z konzole integrovaného serveru. Další informace najdete v tématu “Příprava Windows před instalací klastrové služby Windows” na stránce 97.

### Jméno klastru:

Parametr CLU (jméno klastru) dodává jméno, pod kterým bude klastr znám. Používají jej administrátoři k připojení ke klastru a představuje skupinu uzlů nezávislých síťových serverů, které budou spolupracovat jako jediný systém. Jméno uvedené jako jméno klastru se také používá jako jméno paměťového prostoru síťového serveru, který je vytvořen a bude sloužit jako prostředek kvora pro tento klastr.

### Konfigurace klastru:

Parametr CLUCFG pro konfiguraci klastru se používá k definování klastru a konfigurování paměťového prostoru síťového serveru prostředku kvora. Tyto informace se používají také k ověření, zda libovolný sekundární uzel má správnou konfiguraci i5/OS nezbytnou k vytvoření virtuálního propojení klastru pro sdílená paměťová zařízení a port virtuální sítě Ethernet, který se bude používat pro vzájemná propojení u soukromého klastrování. Konfigurační hodnota klastru \*CLU načte konfiguraci klastru ze stávající hodnoty paměťového prostoru síťového serveru prostředku kvora, která je uvedena v parametru CLU.

### Poznámka:

Port klastrového propojení vyžaduje konfiguraci odpovídajícího portu virtuální sítě Ethernet. Další informace o konfigurování portu virtuální sítě Ethernet najdete v tématu “Konfigurace virtuálních sítí Ethernet” na stránce 107.

## Instalace klastrové služby Windows na stávající server

Klastrovou službu Windows můžete nainstalovat na stávající server Windows 2000 Advanced Server nebo server Windows Server 2003 Enterprise Edition.

Ujistěte se, že je úroveň produktu Integrated Server Support na serveru synchronizována s operačním systémem i5/OS. Další informace najdete v tématu “Přechod na vyšší verzi licencovaného produktu IBM i5/OS Integrated Server Support na straně integrovaného serveru” na stránce 94. Tím se zajistí dostupnost všech funkcí serveru požadovaných při instalaci klastrové služby Windows.

Chcete-li instalovat klastrovou službu Windows na stávající server, proveďte následující úkoly:

- Vytvořte paměťový prostor (prostředek kvora).
- Konfigurujte port pro připojení k virtuální síti Ethernet.
- Připojte jednotku prostředku kvora k popisu síťového serveru.

Po dokončení uvedených kroků a předtím, než budete instalovat klastrovou službu Windows na straně integrovaného serveru Windows, musíte na konzoli integrovaného Windows serveru provést některé dodatečné konfigurační kroky. Další informace najdete v tématu “Příprava Windows před instalací klastrové služby Windows”.

### **Vytvoření paměťového prostoru (prostředku kvora):**

Prvním krokem je vytvoření paměťového prostoru, který bude sloužit jako prostředek kvora. K vytvoření paměťového prostoru použijte CL příkaz CRTNWSSTG (Vytvoření paměťového prostoru síťového serveru) a zadejte speciální formát \*NTFSQR.

Jméno paměťového prostoru síťového serveru by mělo odpovídat jménu klastru, který vytváříte. Doporučená velikost je 550 MB nebo více. Příkaz požádá o následující informace o klastru, které musíte dodat:

- Jméno klastrové domény.
- Port Virtual Ethernet.
- IP adresa klastru Windows.
- Masku podsítě klastru Windows.

### **Konfigurace portu pro připojení k virtuální síti Ethernet:**

Dalším krokem je konfigurovat port pro připojení k virtuální síti Ethernet, který budete chtít používat pro komunikaci soukromých klastrů. Další informace najdete v tématu “Konfigurace virtuálních sítí Ethernet” na stránce 107. Port virtuální sítě Ethernet, který používáte, musí odpovídat portu pro připojení, který uvádíte u paměťového prostoru síťového serveru prostředku kvora.

### **Připojení jednotky prostředku kvora k popisu síťového serveru:**

Připojte paměťový prostor prostředku kvora k síťovému serveru příkazem ADDNWSSTGL (Připojení paměťového prostoru síťového serveru) a zadejte ACCESS(\*SHRUPD), DYNAMIC(\*YES) a DRVSEQNBR(\*QR).

#### **Poznámka:**

Během instalace klastrové služby na první uzel musí být všechny uzly před spuštěním integrovaného serveru logicky vypnuty. V tuto dobu je možné vytvořit a připojit další sdílená paměťová zařízení. Všechny sdílené paměťové prostory musí být \*NTFS a musí být připojeny pomocí ACCESS(\*SHRUPD).

### **Příprava Windows před instalací klastrové služby Windows**

Po instalaci integrovaného serveru potřebujete připravit server k instalaci klastrové služby Windows.

Chcete-li připravit Windows před instalací klastrové služby Windows, proveďte následující úkoly:

1. Naformátujte prostředek kvora.
2. Konfigurujte soukromý síťový adaptér.

Po dokončení těchto kroků je operační systém Windows připraven na instalaci klastrové služby Windows. Další informace najdete v tématu “Instalace klastrové služby Windows do operačního systému Windows” na stránce 98.

## Formátování prostředku kvora:

Prvním krokem k přípravě Windows na instalaci klastru Windows je naformátování prostředku kvora jako NTFS. Formátování prostředku kvora je nutné nejen k instalaci klastrové služby Windows, je to zároveň první krok při instalaci prvního uzlu klastru. Další informace najdete v tématu “Formátování diskových jednotek integrovaného Windows serveru” na stránce 158.

- | V případě serverů připojených pomocí IXS nebo IXA se prostředek kvora jeví jako neformátovaná disková jednotka,
- | která je obvykle označená jako zařízení E. Umístění prostředku kvora je sběrnice číslo 1, cílový identifikátor 0 a číslo
- | logické jednotky (LUN) 0.

Měli byste naformátovat diskový svazek a označit jej pomocí stejného jména, které má klastr a které je zároveň jménem pro paměťový prostor prostředku kvora síťového serveru. Současně naformátujte případné další sdílené paměťové prostory. Rovněž se doporučuje, abyste jednotce prostředku kvora přiřadili pevné písmeno označující jednotku, které je odlišné od ostatních paměťových jednotek.

### Poznámka:

Písmeno označující jednotku, přidělené všem paměťovým prostorům na sběrnici sdílené paměti, musí být stejné ve všech uzlech klastru.

## Konfigurace soukromého síťového adaptéru:

Jako další konfigurujete adaptér soukromé sítě pro používání klastrové služby Windows tak, že u prvního uzlu klastru provedete následující kroky:

1. Na konzoli integrovaného Windows serveru klepněte pravým tlačítkem myši na **My Network Places** a vyberte **Properties**.
2. Klepněte pravým tlačítkem myši na ikonu **Local Area Connection 2**.

### Poznámka:

To, který síťový adaptér je soukromý a který je veřejný, závisí na tom, jak je konfigurován server. Informace v tomto dokumentu předpokládají následující skutečnosti:

- První síťový adaptér (Local Area Connection) je připojen k veřejné síti prostřednictvím fyzického adaptéru LAN pod integrovaným Windows serverem.
- Druhý síťový adaptér (Local Area Connection 2) je virtuální adaptér Ethernet, konfigurovaný jako port pro připojení konfigurace klastru, kterou chcete používat jako soukromou síť klastru.
- Třetí síťový adaptér (Local Area Connection 3) je virtuální dvoubodové připojení typu Ethernet k operačnímu systému i5/OS a nemělo by být povoleno pro žádné účely klastrování.

Počet a pořadí síťových adaptérů nemusí být stejné, závisí na fyzické a virtuální konfiguraci serveru a sítě.

3. Klepněte na **Status** a zobrazte okno **Local Area Connection 2 Status**, které ukazuje stav připojení a také jeho rychlost.
4. V okně **Local Area Connection 2 Status** klepněte na **Properties**.
5. V dialogovém okně **Properties** se ujistěte, že pole **Connect using** obsahuje IBM iSeries Virtual Ethernet x, kde x odpovídá hodnotě \*VRTETHx, kterou jste zadali v portu pro připojení u konfigurace klastru.
6. Klepněte na **Close** pak ještě jednou na **Close**.

Kvůli srozumitelnosti byste měli přejmenovat ikony sítě LAN. Například byste mohli změnit jméno Local Area Connection 2 třeba na Soukromé klastrové připojení.

## Instalace klastrové služby Windows do operačního systému Windows

Vlastní instalace klastrové služby Windows závisí na verzi Windows nainstalované během instalace prostředí Windows pro server iSeries. Během větší části instalace budete postupovat v souladu pokyny pro instalaci klastrové služby Windows, které jsou uvedeny v dokumentaci od firmy Microsoft. Tyto informace zdůrazňují specifické kroky požadované pro instalaci klastrové služby Windows na integrovaný Windows server. Pak si prostudujte části:

- “Instalace klastrové služby Windows na Windows 2000 Server”
- “Instalace klastrové služby Windows na Windows Server 2003”

**Poznámka:** Ujistěte se, že je klastrová služba Windows nainstalovaná a spuštěná na jednom serveru ještě předtím, než na jiném serveru klastru spustíte Windows. Spuštění operačního systému na více serverech předtím, než je klastrová služba Windows spuštěná na jednom serveru, může poškodit paměť klastru. Až nakonfigurujete první server, můžete souběžně instalovat zbývající servery.

**Instalace klastrové služby Windows na Windows 2000 Server:** K instalaci klastrové služby Windows použijte průvodce konfigurací klastrové služby. Průvodci dodejte všechny výchozí informace o konfiguraci klastru.

Chcete-li instalovat klastrovou službu Windows proveďte následující úkoly:

1. Spusťte průvodce konfigurací klastrové služby.
2. Pomocí průvodce konfigurujte klastrovou službu.

#### **Spuštění průvodce konfigurací klastrové služby:**

Průvodce konfigurací klastrové služby spustíte tímto postupem:

1. V nabídce Windows **Start** klepněte na **Settings**, pak klepněte na **Control Panel**.
2. V okně **Control Panel** klepněte dvakrát na **Add/Remove Programs**.
3. V okně **Add/Remove Programs** klepněte na **Add/Remove Windows Components**.
4. V dialogovém okně **Windows Components Wizard** vyberte **Cluster Service**, pak klepněte na **Next**.

#### **Konfigurace klastrové služby Windows:**

Po spuštění vám průvodce konfigurací klastrové služby nabídne náznaky, které vás provedou instalací klastrové služby Windows. Dodejte průvodci všechny výchozí informace o konfiguraci klastru, které potřebuje k jeho vytvoření.

Až budete vyzváni, abyste zadali prostředek kvora, vyberte jednotku, kterou jste naformátovali a označili písmenem. Ačkoliv je to u nové instalace obvykle jednotka E:, může správce disků pro jednotku stanovit jiné písmeno.

Síťová spojení vyžadují zvláštní pozornost:

#### **Poznámka:**

Pořadí, ve kterém průvodce konfigurací klastrové služby předkládá informace o konfiguraci sítě, se může měnit.

- Zrušte zaškrtnutí políčka **Enable this network for cluster use** u IBM iSeries virtual Ethernet Point to point (obvykle Local Area Connection 3).
- Vyberte volbu **Internal cluster communications only** pro IBM iSeries virtual Ethernet x, kde x odpovídá hodnotě \*VRTETHx uvedené u portu pro připojení v konfiguraci klastru (obvykle Local Area Connection 2).
- Konfigurujte zbývající síťová spojení podle toho, co potřebují.

Označte adaptér IBM iSeries virtual Ethernet xAdapter (obvykle Local Area Connection 2) jako primární síť pro interní komunikaci klastru.

**Instalace klastrové služby Windows na Windows Server 2003:** K instalaci klastrové služby Windows na serveru Windows Server 2003 a připojení stávajícího klastru použijte produkt Cluster Administrator. Jak instalace klastrové služby, tak připojení stávajícího klastru vyžaduje, abyste otevřeli produkt Cluster Administrator. Otevřete **Cluster Administrator** z nabídky Windows **Start** a postupně vyberte volby **All Programs**, **Administrative Tools** a **Cluster Administrator**.

Nainstalujte a nakonfigurujte klastrovou službu Windows provedením následujících kroků.

1. Otevřete **Cluster Administrator**.

2. V dialogovém okně **Open Connection to Cluster**, které se objeví, vyberte v poli **Action** volbu **Create new cluster**.
3. Klepněte na **OK**. Zobrazí se průvodce New Server Cluster Wizard, který vás provede instalací klastrové služby u prvního uzlu.
4. Klepněte na **Next**.
5. Zadejte předvolené jméno domény do pole **Domain** a jméno klastru do pole **Cluster name**.
6. Zadejte předvolené jméno počítače do pole **Computer name**.
7. Zadejte IP adresu pro správu klastru do pole **IP Address**.
8. Zadejte jméno uživatelského účtu klastrové služby do pole **Cluster Service Account User name**, pak zadejte heslo do pole **Password** a nakonec doménu do pole **Domain**.
9. Ověřte si **Proposed Cluster Configuration**.


### Připojení stávajícího klastru:

Připojení stávajícího klastru provedete následujícími kroky:

1. Otevřete **Cluster Administrator**.
2. V dialogovém okně **Open Connection to Cluster**, které se objeví, vyberte v poli **Action** volbu **Add nodes to cluster**.
3. Pak do pole **Cluster or server name** buď napište jméno stávajícího klastru, vyberte jméno ze seznamu, nebo klepněte na **Browse** a vyhledejte dostupný klastr.
4. Klepnutím na **OK** zobrazíte průvodce přidáním klastru serverů.
5. Vyberte jedno nebo více jmen, která chcete do klastru přidat, a klepněte na **Add**.
6. Zadejte heslo účtu domény (domain account password) pro klastrovou službu.
7. Až klastrová služba instalaci dokončí, použijte produkt Cluster Administrator k vyhledání a výběru klastru, který jste právě vytvořili.
8. Rozbalte **Cluster Configuration, Network Interfaces**. Vpravo se otevře dialogové okno se seznamem všech **Local Area Connections**.
9. Napište jméno sítě (Local Area Connection x) pro virtuální síť IBM iSeries virtual Ethernet x, kde x odpovídá hodnotě \*VRTETHx uvedené u portu pro připojení v konfiguraci klastru. Tuto síť budete muset později identifikovat, takže si jméno zapamatujte.
10. Určete jméno sítě (Local Area Connection x) pro virtuální síť IBM iSeries virtual Ethernet point to point. Tuto síť budete muset později identifikovat, takže si jméno zapamatujte.
11. V okně **Cluster Administrator** rozbalte **Cluster Configuration, Networks**.
12. Klepněte pravým tlačítkem myši na jméno sítě (Local Area Connection x) pro síť virtuální IBM iSeries virtual Ethernet x a vyberte **Properties**.
13. Vyberte pro tuto síť volbu **Internal cluster communications only**.
14. Klepněte pravým tlačítkem myši na jméno sítě (Local Area Connection x) pro virtuální síť IBM iSeries virtual Ethernet point to point a vyberte **Properties**.
15. U této sítě zrušte zaškrtnutí políčka **Enable this network for cluster use**.

Konfigurujte zbývající síťová spojení podle toho, co potřebují.

## Použití služby Kerberos se serverem Windows Server 2003 Active Directory Server

QNTC, SBMNWSCMD a File Level Backup mohou používat službu Kerberos k ověřování identity členských serverů domény Windows Active Domain. Chcete-li používat službu Kerberos, bude možná nutné, abyste na servery Microsoft Active Directory Controller Server nainstalovali aktualizovaný Windows Server 2003. Tato aktualizace je dostupná v servisním balíku 1 nebo jako oprava typu hotfix KB833708 firmy Microsoft. Další informace týkající se instalace servisního balíku nebo opravy typu hotfix, najdete na webových stránkách firmy Microsoft .

- | Po nainstalování opravy typu hotfix nebo servisního balíku 1 musíte také aktualizovat registr systému Windows Server 2003. Proveďte tyto kroky:
- | 1. Klepněte na **Start>Run**.
- | 2. Do pole **Open** napište regedit.
- | 3. Klepněte na **OK**.
- | 4. Vyberte podklíč registru **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc**.
- | 5. Klepněte pravým tlačítkem myši na **Kdc**.
- | 6. Vyberte **New**.
- | 7. Klepněte na **DWORD Value**.
- | 8. Do pole New Value zadejte KdcUseRequestedEtypesForTickets.
- | 9. Klepněte pravým tlačítkem myši na **KdcUseRequestedEtypesForTickets**.
- | 10. Vyberte **Modify**.
- | 11. Nastavte hodnotu registru **KdcUseRequestedEtypesForTickets** na 1.
- | 12. Klepněte na **OK**.
- | 13. Opusťte program Registry Editor.
- | 14. Chcete-li, aby se změny aktivovaly, restartujte službu Centrum distribuce klíčů nebo na serveru znovu zaveďte operační systém.

## Instalace ovladačů videozařízení ATI Radeon 7000M pro Windows 2000 na serveru IXS 2892-002 nebo 4812-001

Integrovaný server IXS (Integrated xSeries Server) 2892-002 a 4812-001 zahrnuje videočip ATI Radeon 7000M. Požadované ovladače nejsou obsaženy na distribučním CD pro Microsoft Windows 2000 Server. Na integrovaný Windows server bude zapotřebí instalovat video ovladač obrazovky ATI, aby se plně využily možnosti videočipu ATI.

Předtím, než budete instalovat video ovladače, musí mít systém nainstalovaný DirectX verze 8.1 nebo vyšší.

Při instalaci video ovladače pro Windows 2000 postupujte takto:

1. Nainstalujte DirectX verze 8.1 nebo vyšší. Windows 2000 se dodává s DirectX 7.0, ale pro video ovladače ATI je zapotřebí DirectX verze 8.1 nebo vyšší a musí být nainstalovaná před instalací video ovladačů ATI. Microsoft udržuje webovou stránku pro informace o DirectX a stahování. Viz <http://www.microsoft.com/directx>.
2. Nainstalujte video ovladač ATI:
  - a. Zavřete všechny programy.
  - b. Klepněte na tlačítko **Start** a vyberte položku nabídky **Run**.
  - c. Klepněte na tlačítko **Browse**.
  - d. Přejděte do adresáře %SystemDrive%\WSV, kde je uložen program atidrvr.exe.
  - e. Vyberte atidrvr.exe a klepněte na OK, čímž program spustíte.
  - f. Postupujte podle pokynů pro instalaci na obrazovce.
3. Volitelně je možné instalovat karty ovládacího panelu Advanced ATI.
  - a. Zavřete všechny programy.
  - b. Klepněte na tlačítko **Start** a vyberte položku nabídky **Run**.
  - c. Klepněte na tlačítko **Browse**.
  - d. Přejděte do adresáře %SystemDrive%\WSV, kde se nachází aticp.exe.
  - e. Vyberte aticp.exe a klepněte na OK, čímž program spustíte.
  - f. Postupujte podle pokynů pro instalaci na obrazovce.



## Přizpůsobení akcelerace hardwaru u serveru Windows Server 2003 na serveru IXS 2892-002 nebo 4812-001

Pokud instalujete Windows Server 2003 na server IXS 2892-002 nebo 4812-001, je k zajištění optimálního výkonu nutné dodatečné nastavení. Při přizpůsobení výkonu postupujte takto:

1. V nabídce systému Windows **Start** klepněte na **Settings -> Control Panel -> Display**.
2. Na panelu **Display Properties** vyberte kartu **Settings**.
3. Klepněte na **Advanced**.
4. Klepněte na kartu **Troubleshoot**.
5. Přizpůsobte posuvný ovladač **Hardware Acceleration**, jak je požadováno.
6. Klepněte na **Apply**.
7. Klepněte na **OK**.
8. Klepnutím na **OK** bude změna přijata.

## Odpovědi na chybové zprávy během instalace

Ve fázi instalace integrovaného Windows serveru se označí chybějící informace, které jste nedodali během fáze instalace v operačním systému i5/OS. Tyto informace budete mít možnost doplnit. Toto téma obsahuje několik příkladů takových chybových zpráv a návod, jak na ně odpovídat.

### **Error (Installing Server)** (chyba při instalaci serveru)

Možná, že jste nezadali hodnotu do pole **V pracovní skupině** nebo **V doméně** na obrazovce Instalace Windows serveru v operačním systému i5/OS. Pokud jste tak neučinili, uvidíte následující chybovou zprávu:

Error (Installing Server) (chyba při instalaci serveru)

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

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

You may wish to inform your system administrator or computer manufacturer that the "JoinWorkgroup" value is missing or invalid. (Parametr nastavení, který zadal administrátor systému nebo výrobce počítače chybí nebo je neplatný. Během instalace budete vyzváni k doplnění těchto informací.

Jakmile požadované informace dodáte, bude operace plně automatizované instalace pokračovat.

Měli byste informovat správce vašeho systému nebo výrobce počítače, že hodnota "JoinWorkgroup" chybí nebo je neplatná.)

Klepněte na **OK**.

Instalační program vás pak vyzve, abyste počítač začlenili do pracovní skupiny nebo domény.

---

## Nastavení integrovaného Windows serveru na automatické logické zapnutí s TCP/IP

Integrovaný server můžete nastavit tak, aby se automaticky logicky zapnul, když spustíte TCP/IP. Jestliže však několik integrovaných serverů používá jeden prostředek souborového serveru, konfiguruje pro automatické spuštění pouze jeden z nich. Prostředek souborového serveru může používat vždy jen jeden síťový server. Konfigurování několika rozhraní TCP/IP pro automatické spuštění síťových serverů, které sdílejí tentýž prostředek, může způsobit nepředvídatelné následky.

Chcete-li, aby se integrovaný server automaticky logicky zapnul, když spustíte TCP/IP, postupujte takto:



1. Na příkazový řádek operačního systému i5/OS zadejte příkaz CFGTCP (Konfigurace TCP/IP).
2. Vyberte volbu 1 **Práce s rozhraním TCP/IP** a stiskněte klávesu Enter.
3. Zadejte 2 (Změna) do pole Volba vedle rozhraní pro popis linky dvoubodové virtuální sítě Ethernet pro server a stiskněte klávesu Enter.

**Poznámka:**

Popis linky dvoubodové virtuální sítě Ethernet má jméno, které se skládá ze jména NWSD (popisu síťového serveru), za nímž následuje 'PP' pro virtuální dvoubodovou lokální síť Ethernet. Jestliže je jméno NWSD například MYSVR, pak popis linky dvoubodové virtuální lokální sítě Ethernet LAN je MYSVRPP.

4. Změňte hodnotu parametru **Autostart** na \*YES a stiskněte klávesu Enter. Integrovaný server se automaticky logicky zapne, když spustíte TCP/IP.

**Poznámka:**

Od verze V5R1 může být TCP/IP automaticky spuštěn systémem při IPL změnou atributů IPL systému. Spouštěcí procedura již není potřebná. Všechna rozhraní TCP, která mají parametr Autostart nastavený na \*YES, budou při IPL spuštěna zároveň s TCP/IP.

**Poznámka:**

Pamatujte si, že IP adresa zadaná u dvoubodové virtuální sítě Ethernet z integrované konzole přepíše hodnotu nastavenou v NWSD pro parametr TCPPRTCFG portu \*VRTETHPTP. Avšak operace, jako je SBMNWSCMD, používají k vyhledání serveru hodnotu nastavenou v NWSD. Obě hodnoty musí být konzistentní.

---

## Opravy kódu

Opravy kódu produktu IBM iSeries Integrated Server Support zajišťují pokud možno aktuální a bezchybný kód, aniž byste museli čekat na další vydání softwaru. Aktualizují kód produktu iSeries Integrated Server Support, který umožňuje použití Microsoft Windows serveru na integrovaném serveru, a jsou oddělené od servisních balíčků, které si musíte obstarat u firmy Microsoft.

Dočtete se o nich v tématu "Typy oprav kódu" na stránce 104.

Proces instalace oprav kódu na integrované servery se nazývá synchronizace. Když synchronizujete integrovaný server, software pro integraci zajistí, aby byl software pro integraci na integrovaném serveru na stejné úrovni servisních balíčků a vydání, jako je software pro integraci v operačním systému i5/OS. Úroveň kódu na straně Windows závisí na úrovni kódu na straně operačního systému i5/OS.

Když použijete integrační software k synchronizaci integrovaného serveru, existují potenciálně čtyři akce, které můžete vyvolat.

1. Při převodu systému i5/OS na nové vydání (například z V5R3 na V5R4) je software starého vydání nahrazen softwarem nového vydání.
2. Pokud byl v operačním systému i5/OS instalován nový servisní balík produktu IBM iSeries Integrated Server Support, pak bude tento servisní balík zkopírován na integrovaný server.
3. Pokud byl servisní balík produktu IBM iSeries Integrated Server Support odstraněn z operačního systému i5/OS, bude odstraněn rovněž z integrovaného serveru a bude nahrazen kódem, který je aktuálně v operačním systému i5/OS.
4. Je-li kód pro integraci v systému i5/OS a kód pro integraci na integrovaném serveru na stejné úrovni, operace synchronizace se přesto provede. To umožňuje obnovení odstraněného nebo poškozeného souboru na integrovaném serveru.

Ve všech případech bude integrovaný server převeden na stejnou úroveň softwaru, jaká je v operačním systému i5/OS.

Synchronizaci je možné provést trojím způsobem. Další informace najdete v částech:



- "Synchronizace úrovně softwaru pro integraci z konzole integrovaného Windows serveru" na stránce 104.

- “Synchronizace úrovně softwaru pro integraci prostřednictvím produktu iSeries Navigator” na stránce 105.
- “Synchronizace úrovně softwaru pro integraci prostřednictvím vzdáleného příkazu” na stránce 105.

Nastanou-li při provádění synchronizace problémy, přečtěte si téma “Program typu snap-in IBM iSeries Integrated Server Support” na stránce 211.

## Typy oprav kódu

Existují čtyři typy oprav kódu:

1. Opravy kódu aplikované na integrační kód i5/OS. Tyto opravy jsou nazývány jako běžná **PTF** (program temporary fix).
  - Chcete-li je aplikovat, stačí je do operačního systému i5/OS nainstalovat.
  - Tyto opravy kódů jsou k dispozici ve středisku podpory IBM nebo na internetové adrese <http://www.ibm.com/servers/eserver/series/integratedxseries> (viz odkaz Service & support na levé navigační liště) .
2. Opravy kódu, které jsou zkopírovány na jednotky integrovaného serveru a kterým se říká **servisní balík PTF**.
  - Licencovaný program IBM iSeries Integrated Server Support má část pro integrovaný server, který se zkopíruje ze strany operačního systému i5/OS. Když aplikujete kumulativní balík PTF pro systém i5/OS, může obsahovat i servisní balík pro produkt Integrated Server Support, který je pak možné aplikovat na integrovaný server. Provedete to synchronizací integrovaného serveru.
  - Tyto opravy kódu jsou také k dispozici ve středisku podpory IBM nebo online na internetové adrese <http://www.ibm.com/servers/eserver/series/integratedxseries/> (viz odkaz Service & support na levé navigační liště) .
3. Opravy kódu aplikované na samotný Microsoft Windows serverů. Těmto opravám říká **servisní balíky**.
  - Tyto opravy pocházejí od firmy Microsoft. Můžete si je stáhnout z webové stránky Windows Update.
  - Neaplikujte žádné opravy kódu od firmy Microsoft, které by mohly změnit části Windows serveru používané produktem IBM iSeries Integrated Server Support. Například nestahujte ze stránky Windows Update žádné ovladače paměťových zařízení SCSI, ani ovladače zařízení LAN.
  - Jiné oblasti jsou zpravidla bezpečné, například ovladače zařízení USB je možné ze stránky Windows Update stáhnout na vlastní riziko.
4. Opravy typu hotfix aplikované na samotný Microsoft Windows server a aplikované pomocí produktu Windows Update.

## Synchronizace úrovně softwaru pro integraci z konzole integrovaného Windows serveru

Chcete-li k synchronizaci úrovně softwaru použít program typu snap-in iSeries Integrated Server Support, musíte mít oprávnění administrátora systému Windows. Před započítím instalace ukončete všechny prováděné aplikace a zajistěte, aby k integrovanému serveru nebyli přihlášení žádní uživatelé. Pokud to neuděláte, riskujete ztrátu dat, protože integrovaný server může po dokončení instalace vyžadovat restartování.

1. Klepněte na **Start -> Programs -> IBM iSeries -> IBM iSeries Integrated Server Support**.
2. Klepněte na jméno integrovaného serveru, pak na **Software Level**.
3. Zobrazí se úroveň softwaru pro integraci i5/OS a softwaru pro integraci Windows. Klepněte na **Synchronize**, chcete-li převést software pro integraci Windows na stejnou úroveň jakou má software pro integraci i5/OS.
4. Je-li instalace provedena úspěšně, objeví se potvrzující zpráva.

**Poznámka:** Když se na konzoli integrovaného Windows serveru přihlásíte jako administrátor a dojde k nesrovnalosti v úrovni softwaru, budete automaticky vyzváni, abyste software synchronizovali.

## Synchronizace úrovně softwaru pro integraci prostřednictvím produktu iSeries Navigator

1. V prostředí produktu iSeries Navigator klepněte na **Administrace integrovaného serveru -> Servery**.
2. Klepněte pravým tlačítkem myši na integrovaný server, který chcete synchronizovat, a vyberte volbu **Synchronizovat iSeries Integration Software**. (Jestliže server i5/OS, k němuž přistupujete, není verze V5R3 nebo vyšší, bude vám předložen seznam dřívějších voleb umožňující nainstalovat či odinstalovat servisní balíky jednotlivě nebo provést pouze aktualizaci vydání.)
3. Klepněte na **Synchronizovat** a potvrďte akci.
4. Obdržíte zprávu sdělující, že synchronizace probíhá a dále zprávu o dokončení s upozorněním, že bude následovat znovuzavedení operačního systému. Nebudete dotázáni, zda je chcete provést nyní nebo později.

Úroveň softwaru nainstalovaného v operačním systému i5/OS a na integrovaném serveru zjistíte následujícím postupem:

1. V prostředí produktu iSeries Navigator klepněte na **Administrace integrovaného serveru -> Servery**.
2. Klepněte pravým tlačítkem myši na integrovaný server, který chcete synchronizovat a vyberte volbu **Synchronizovat iSeries Integration Software**.
3. Klepněte na kartu **Software**. Zobrazí se úrovně softwaru.

## Synchronizace úrovně softwaru pro integraci prostřednictvím vzdáleného příkazu

Zadání příkazu `lvlsync` na příkazovém řádku konzole Windows serveru způsobí, že se integrovaný server bude synchronizovat. Hlavní výhodou tohoto programu z příkazové řádky je, že umožňuje synchronizovat integrovaný server zadáním vzdáleného příkazu. Takové funkční vybavení by bylo užitečné, kdybyste například chtěli napsat program CL, který by pravidelně synchronizoval vaše integrované servery. Další informace o zadávání vzdálených příkazů najdete v tématu “Vzdálené spuštění příkazů integrovaného Windows serveru” na stránce 145.

Níže je uvedena jednoduchá procedura pro vzdálenou synchronizaci integrovaného serveru prostřednictvím vzdáleného příkazu `lvlsync` z konzole i5/OS.

1. Ve znakově orientovaném rozhraní i5/OS napište příkaz `SBMNWSCMD` a stiskněte klávesu **F4**.
2. Do pole **Příkaz** zadejte `lvlsync` a stiskněte klávesu **Tab**.
3. Do pole **Server** zadejte jméno NWSD vašeho integrovaného serveru a stiskněte klávesu **Enter**.

V minulosti povoloval program `lvlsync` volitelné parametry. Tyto parametry již nejsou funkční, i když jejich přítomnost funkčnost příkazu neovlivní.

`lvlsync` vrací následující chybové kódy:

### Chybové kódy programu `lvlsync`

Chybový kód	Chyba
0	Žádné chyby.
01	Program <code>lvlsync</code> smí spustit pouze administrátor.
02	Úroveň vydání na integrovaném Windows serveru je vyšší než v systému i5/OS.
03	Úroveň servisního balíku na integrovaném serveru je vyšší než v i5/OS.
04	Nelze instalovat vydání z operačního systému i5/OS - v i5/OS nejsou soubory jazyků.
05	Neplatná syntaxe.
06	V operačním systému i5/OS nelze získat přístup k informacím o servisních balících..
07	Nelze mapovat síťovou jednotku.
08	Nelze získat přístup k informacím o servisním balíku v registru.

Chybový kód	Chyba
09	Nelze otevřít soubor qvnacfg.txt.
10	V operačním systému i5/OS není nainstalován žádný servisní balík.
11	NWSD nenalezen.
13	NWSD není aktivní.
20	V operačním systému i5/OS není k dispozici žádný servisní balík.
21	Nelze spustit aplikaci InstallShield.
31	Neočekávaná chyba při spouštění lvlsync.
44	Neočekávaná chyba při provádění lvlsync.

**Poznámka:**

Chybová zpráva NTA0218 je diagnostická zpráva (\*DIAG) pro chyby syntaxe, oprávnění a nenalezení popisu síťového serveru (NWSD).

---

## Kapitola 6. Správa virtuálních sítí Ethernet a externích sítí

Toto téma obsahuje procedury, které vás naučí pracovat s virtuálními sítěmi Ethernet a externími sítěmi popsanými v tématu “Koncepce v oblasti sítí” na stránce 27.

- “Konfigurace hodnot IP adresa, brána a MTU”
- “Konfigurace virtuálních sítí Ethernet”
- “Konfigurace virtuálních sítí Ethernet mezi logickými částmi” na stránce 108
- “Prozkoumání dvoubodových virtuálních sítí Ethernet” na stránce 109
- “Externí síť” na stránce 110
- “Odstranění síťových adaptérů” na stránce 111

---

### Konfigurace hodnot IP adresa, brána a MTU

Hodnoty IP adresa, brána a MTU (Maximum transmission unit) pro virtuální a fyzické síťové adaptéry v hostovaném systému jsou spravovány z operačního systému Windows, kromě níže uvedených případů.

- IP adresa a maska podsítě pro popis nové virtuální linky typu Ethernet mohou být volitelně přiřazeny pomocí příkazu INSWNTSVR (Instalace Windows serveru) operačního systému i5/OS. Po nainstalování serveru je možné tyto hodnoty měnit pouze v rámci operačního systému Windows.
- IP adresu a masku podsítě je možné přiřadit při přidávání virtuální linky typu Ethernet ke stávajícímu serveru. Poté, co je popis linky přidán, mohou být tyto hodnoty měněny pouze v rámci operačního systému Windows.
- Změny IP adresy dvoubodové virtuální sítě Ethernet mohou být konfigurovány jak v operačním systému Windows, tak v i5/OS. Další informace najdete v tématu “Konflikty IP adres ve dvoubodové virtuální síti Ethernet” na stránce 226.
- Hodnoty IP adresy a brány pro stranu Windows u sítě typu iSCSI se vždy konfiguruje a mění v rámci konfigurace vzdálených systémů i5/OS. Další informace najdete v tématu “Změna vlastností konfigurace vzdáleného systému” na stránce 117.
- Hodnoty IP adresy, masky podsítě, brány a MTU pro externí adaptéry typu IXS LAN je možné volitelně nastavovat pomocí příkazu INSWNTSVR (Instalace Windows serveru) operačního systému i5/OS. Po nainstalování mohou být tyto hodnoty měněny pouze v rámci operačního systému Windows.

---

### Konfigurace virtuálních sítí Ethernet

Toto téma popisuje postup konfigurace virtuální sítě Ethernet mezi integrovanými servery. (Všimněte si, že při instalaci integrovaného serveru z pracovního média může instalační příkaz INSWNTSVR konfigurovat virtuální síť Ethernet za vás.) Informace o tom, jak lze rozšířit virtuální síť Ethernet do ostatních logických částí serveru iSeries, naleznete v tématu “Konfigurace virtuálních sítí Ethernet mezi logickými částmi” na stránce 108. Procedura se skládá z těchto základních kroků:

1. Nakonfigurujte port virtuální sítě Ethernet a popis linky pro integrovaný server. V prostředí produktu iSeries Navigator:
  - a. Rozbalte **Administrace integrovaného serveru** —>**Servery**.
  - b. Klepněte pravým tlačítkem myši na integrovaný server a vyberte **Vlastnosti**.
  - c. Na panelu vlastností serveru klepněte na kartu **Virtuální Ethernet**.
  - d. Klepnutím na tlačítko **Přidat...** přidáte nový port virtuální sítě Ethernet.
  - e. Na panelu vlastností virtuální sítě Ethernet zadejte hodnoty pro nový port.
    - 1) Vyberte číslo portu virtuální sítě Ethernet.
    - 2) Zadejte IP adresu, kterou bude integrovaný server používat.
    - 3) Zadejte masku podsítě, kterou bude integrovaný server používat.

- 4) Můžete ponechat předvolenou hodnotu jména popisu linky, nebo ji změnit na nějakou jinou. Předvolené jméno popisu linky je tvořeno znaky NWS D, za nimiž následuje znak v a dále číslo portu. Pokud například přidáváte port 3 do NWS D nazvaného Mynwsd, potom předvolené jméno popisu linky je Mynwsdv3.
  - 5) Ponechte asociovaný port nastaven na **Žádný**.
  - 6) Ponechte maximální velikost rámce nastavenou na předvolenou hodnotu **8996**.
  - 7) Jestliže se jedná o server připojený pomocí iSCSI, vyberte adaptér NWS H odpovídající adaptéru iSCSI HBA, který by měl operační systém i5/OS používat při této konfiguraci virtuální sítě Ethernet k přístupu k hostovanému systému.
  - 8) Klepnutím na **OK** přidáte na kartu **Virtuální Ethernet** na panelu vlastností serveru nový port.
- f. Na panelu vlastností serveru klepněte na **OK**, aby se změny uložily. Tím se aktualizuje NWS D a vytvoří popis linky pro nový port virtuální sítě Ethernet.
  - g. Pokud chcete, aby byl tento integrovaný server připojen k více než jedné virtuální síti Ethernet, opakujte výše uvedené kroky a vytvořte tak port virtuální sítě Ethernet a popis linky pro každou síť pomocí různých čísel portů virtuální sítě Ethernet.
2. Opakujte proceduru u všech integrovaných serverů, které chcete do sítě připojit, a u každého uveďte stejnou adresu portu virtuální sítě Ethernet.
  3. Znovu spusťte integrované servery. Ovladač zařízení virtuální sítě Ethernet bude automaticky nainstalován a nastaven na Windows TCP/IP adresu, která pro něj byla zadána v popisu síťového serveru. Avšak IP adresa zadaná z konzole integrovaného serveru potlačí hodnoty, které jsou v popisu síťového serveru nastavené.
  4. Vyzkoušejte, zda virtuální síť Ethernet funguje, například testováním spojení z jednoho serveru na IP adresy, které jste zadali u ostatních serverů.

---

## Konfigurace virtuálních sítí Ethernet mezi logickými částmi

### Sítě navzájem propojených logických částí s konzolí HMC

Požadujete-li, aby integrovaný server komunikoval s jinými logickými částmi (LPAR) nebo s integrovanými servery řízenými jinými logickými částmi s operačním systémem i5/OS, musíte konfigurovat jednu nebo více sítí navzájem propojených logických částí. Síť navzájem propojených logických částí se konfiguruje v systémech iSeries s konzolí HMC (Hardware Management Console) jinak než v jiných systémech. V operačním systému iSeries s konzolí HMC existuje vzájemné propojení mezi logickými částmi nebo integrovanými servery používajícími stejný ID sítě VLAN. Zúčastněné integrované servery ID sítě VLAN přímo nepodporují. Místo toho potřebuje každý zúčastněný integrovaný server popis linky Ethernet, který spojuje hodnotu portu virtuální sítě Ethernet s virtuálním adaptérem, který má ID sítě VLAN. Konfigurační procedura se skládá z následujících kroků:

1. Pro každou logickou část integrovaného serveru, která bude v síti navzájem propojených logických částí, vytvořte pomocí konzole HMC virtuální adaptér a adaptér Ethernet. Další informace najdete v tématu eServer i5 a rozdělování na logické části v rámci aplikace Information Center a v tématu Konfigurace virtuálních sítí Ethernet mezi logickými částmi. U každého virtuálního adaptéru, který bude připojovat integrovaný server nebo logickou část s operačním systémem i5/OS k interní síti mezi logickými částmi, zadejte konzistentní ID portu virtuální sítě LAN (Port virtual LAN ID) a zrušte zaškrtnutí u hodnoty **IEEE 802.1Q compatible adapter**.
2. Nakonfigurujte port virtuální sítě Ethernet a popis linky, jak bylo popsáno v kroku 1 na stránce 107 v odstavci “Konfigurace virtuálních sítí Ethernet” na stránce 107, pokud popis linky pro port, který nás zajímá (0 až 9), nebyl dosud vytvořen. Vyberte jméno asociovaného portu (Cmnxx) pro odpovídající prostředek 268C.
3. Pokračujte krokem 2 z odstavce “Konfigurace virtuálních sítí Ethernet” na stránce 107 (ve všech logických částech s operačním systémem i5/OS, které řídí zúčastněný integrovaný server) a krokem 3 z odstavce “Konfigurace virtuálních sítí Ethernet” na stránce 107.
4. Aby se logická část plně účastnila, budete muset odpovídajícím způsobem konfigurovat protokol(y), které uvnitř jsou. V každé logické části s operačním systémem i5/OS vytvořte popis linky typu Ethernet na odpovídajícím vyhrazeném zařízení portu 268C. V každé logické části, která se bude podílet na komunikaci TCP/IP, konfiguruje příslušnou jedinečnou IP adresu.
5. Vyzkoušejte, zda síť mezi logickými částmi systému funguje, například testováním spojení mezi integrovanými servery a logickými částmi.



## Sítě navzájem propojených logických částí bez konzole HMC

- V jiném systému, než je systém iSeries s konzolí HMC, existuje propojení mezi logickými částmi používajícími stejné číslo sítě; integrované servery jsou propojeny pouze tehdy, jsou-li propojeny jejich řídicí logické části s operačním systémem i5/OS. Síťová čísla 0-9 se vztahují k integrovaným serverům. Je-li například logická část s operačním systémem i5/OS konfigurována pro spojení mezi logickými částmi v sítích 1 a 5, pak se integrované servery řízené touto částí mohou účastnit komunikace na portech 1 a 5 virtuální sítě Ethernet. Konfigurační procedura je tvořena těmito kroky:
1. Konfigurujte číslo sítě, ke které chcete jednotlivé logické části připojit. Řiďte se pokyny, které uvádí téma Koncepce logických částí systému a informace online nápovědy produktu iSeries Navigator. Pamatujte si, že integrované servery jsou propojeny jenom tehdy, jsou-li propojeny jejich řídicí logické části s operačním systémem i5/OS.
  2. Nakonfigurujte port virtuální sítě Ethernet a popis linky, jak bylo popsáno, pokud popis linky pro port, který chcete používat (0 až 9), nebyl dosud vytvořen. Viz krok 1 v odstavci “Konfigurace virtuálních sítí Ethernet” na stránce 107. Ponechte jméno asociovaného portu nastaveno na **Žádný**.
  3. Pokračujte krokem 2 z odstavce “Konfigurace virtuálních sítí Ethernet” na stránce 107 (ve všech logických částech s operačním systémem i5/OS, které řídí zúčastněný integrovaný server) a krokem 3 z odstavce “Konfigurace virtuálních sítí Ethernet” na stránce 107.
  4. Pokud chcete, aby se logická část plně účastnila, budete muset odpovídajícím způsobem konfigurovat protokol(y), které jsou v rámci dané logické části. V každé logické části s operačním systémem i5/OS, která se má účastnit, použijte příkaz WRKHDWRSC \*CMN a zjistěte jméno odpovídajícího portu hardwarového typu 268C, který byl automaticky vytvořen. Viz krok 1 v odstavci “Konfigurace virtuálních sítí Ethernet” na stránce 107. Potom vytvořte popis linky typu Ethernet na prostředku portu 268C. V každé logické části, která se bude podílet na komunikaci TCP/IP, konfigurujte příslušnou jedinečnou IP adresu.
  5. Vyzkoušejte, zda síť mezi logickými částmi systému funguje, například testováním spojení mezi integrovanými servery a logickými částmi.

---

## Prozkoumání dvoubodových virtuálních sítí Ethernet

Každý integrovaný server je spojen se serverem iSeries dvoubodovou virtuální sítí Ethernet, díky které může server iSeries řídit integrovaný server. Zde se dozvíte, jak prohlížet nebo měnit tato připojení, ačkoliv jsou automaticky konfigurována během instalace.

### Zobrazení dvoubodových připojení typu Ethernet z operačního systému i5/OS

Dvoubodová připojení typu Ethernet se v operačním systému i5/OS skládají z popisu linky a z položky v NWSD integrovaného serveru.

1. Chcete-li si prohlédnout popis linky, vydejte příkaz WRKCFGSTS \*NWS ze znakově orientovaného rozhraní i5/OS.
2. Vyhledejte seřazené položky, odpovídající vašemu integrovanému serveru. Jedna z položek ve sloupci Popis linky bude mít stejné jméno jako váš NWSD a bude končit znaky PP. Nalevo od ní zadejte 8 a stiskněte klávesu Enter.
3. Nyní jste v menu Práce s popisem linky. Vlevo od popisu linky napište 5 a stiskněte klávesu Enter, čímž zobrazíte jeho informace.
4. Stiskněte klávesu **F3**, dokud se nevrátíte do základní nabídky.
5. Nyní vydejte příkaz CFGTCP a vyberte volbu 1 - **Práce s rozhraním TCP/IP**.
6. Jedna z položek ve sloupci Popis linky by měla mít stejné jméno jako váš NWSD a končit znaky PP.
7. Volba 5 zobrazí informace o rozhraní TCP/IP, kdežto volba 9 a 10 vám umožní je povolit a zablokovat. Poznamenejte si internetovou adresu. Budete ji potřebovat později.
8. Nyní se rychle podíváme na záznam v NWSD integrovaného serveru. Zadejte příkaz WRKNWSD. Vyhledejte NWSD integrovaného serveru a zadejte volbu 5, aby se NWSD zobrazil. Stiskněte klávesu Enter a projděte atributy NWSD.



9. Jedna z obrazovek se bude jmenovat **Připojené linky** a zobrazí číslo portu \*VRTETHPTP a jméno popisu linky, kterou síť používá.
10. Když se vrátíte zpět do nabídky **Práce s popisy síťových serverů**, můžete pomocí volby 2 tuto informaci změnit.

### Prohlížení dvoubodových připojení typu Ethernet z konzole integrovaného Windows serveru

1. Na konzoli vašeho integrovaného serveru klepněte na **Start** → **Settings** → **Control Panel**. Pak vyberte **Network and Dial-up Connections**.
2. Jedna z ikon se bude jmenovat **Virtual Ethernet point to point**. Dvakrát na ni klepněte.
3. Klepněte na **Properties** v dialogovém okně, které se objeví.
4. Klepněte dvakrát na **Internet Protocol (TCP/IP)** v dalším dialogovém okně.
5. V tomto konečném dialogovém okně byste měli vidět IP adresu asociovanou se stranou integrovaného serveru dvoubodového virtuálního spojení typu Ethernet. Měla by to být hodnota IP adresy v operačním systému i5/OS zvýšená o jednu, aby byla sudá namísto liché.
6. Zavřete všechna okna, která jste otevřeli, klepněte na **Start** → **Run** a zadejte příkaz cmd. Stiskněte klávesu Enter. Tím se spustí příkazová řádka Windows.
7. Na náznak příkazu C:\>, který se objeví, zadejte příkaz ping následovaný IP adresou operačního systému i5/OS, kterou jste si poznamenali v posledním kroku. Například ping 192.168.3.1. Příkaz by měl vrátit Reply from ..... To je v pořádku. Příkaz ping odešle paket dat na určitou internetovou adresu a změří, jak dlouho to potrvá.
8. (volitelné) Vraťte se do znakově orientovaného rozhraní i5/OS a zadejte příkaz call qcnd. (Tím se zvětší prostor pro zobrazení tak, že uvidíte výsledky svých příkazů.) Příkazem i5/OS otestujte spojení integrovaného serveru. Například ping '192.168.3.2'. Gratulujeme! Pokud všechno proběhlo správně, dokázali jste, že máte řádně fungující dvoubodovou virtuální síť Ethernet.

---

## Externí síť

Do otevřeného slotu PCI můžete instalovat novou síťovou kartu. Přitom musíte konfigurovat nový adaptér na integrovaný Windows server.

Informace o instalaci nové síťové karty adaptéru uvádí téma **Instalace komponent systému iSeries**. Vyberte svůj model serveru iSeries a vyhledejte instrukce označené **Instalace karty PCI a karty IXA**.

Chcete-li instalovat nový síťový adaptér, naleznete příslušné informace v tématu "Instalace ovladačů zařízení síťových adaptérů a přidání informací o adrese adaptéru do integrovaného Windows serveru".

Popis vytvoření virtuálního spojení typu Ethernet najdete v tématu "Konfigurace virtuálních sítí Ethernet" na stránce 107.

Popis odstranění síťového adaptéru najdete v tématu "Odstranění síťových adaptérů" na stránce 111.

## Instalace ovladačů zařízení síťových adaptérů a přidání informací o adrese adaptéru do integrovaného Windows serveru

Zde se dozvíte, jak nainstalovat ovladače zařízení adaptéru a přidat informace o adresách nových adaptérů do integrovaného Windows serveru.


Adaptéry a ovladače zařízení pod servery Windows 2000 Server a Windows Server 2003 podporují Plug-n-Play. Až bude adaptér fyzicky nainstalovaný, spusíte integrovaný server znovu tak, že jej logicky zapnete, aby byly adaptéry dostupné. Nezapomeňte u každého adaptéru (spojení) konfigurovat IP adresu.

Jestliže u serveru IXS provádíte přechod z Windows NT 4.0 na Windows 2000 Server, odstraňte starý adaptér dříve, než přidáte nový. Další informace najdete v tématu "Odstranění síťových adaptérů" na stránce 111.

Windows 2000 Server nebo Windows Server 2003 nový adaptér rozpozná. IP adresy u daného adaptéru nakonfigurujete takto:

1. Klepněte pravým tlačítkem myši na **My Network Places**; potom v rozbalovací nabídce klepněte na **Properties**.
2. Klepněte dvakrát na správný adaptér (Local Area Connection), abyste mohli nakonfigurovat IP adresu.
3. Klepněte na tlačítko **Properties**.
4. Vyberte **Internet Protocol (TCP/IP)**, pak klepněte na tlačítko **Properties**.
5. Pokud ještě není vybrán, klepněte na přepínač **Use the following IP address**.
6. Do pole **IP address** uveďte IP adresu.
7. Do pole **Subnet Mask** zadejte masku podsítě.
8. Do pole **Default Gateway** zadejte adresu předvolené brány.
9. Klepněte na **OK**, **OK a Close** a dokončete nastavení IP adresy.

**Poznámka:**

Jestliže Windows sdělí, že IP adresa je již konfigurována pro jiný adaptér, ale vy nemůžete najít adaptér, který adresu již používá, jde o to, že operační systém Windows si pravděpodobně pamatuje předešlé hardwarové prostředí, které adresu používalo. Způsob, jak zobrazit adaptér LAN z předchozího hardwarového prostředí, abyste mohli IP adresu uvolnit, najdete v článku Q241257 na webových stránkách Microsoft Knowledge Base: Device Manager Does Not Display Devices Not Currently Present in Windows 2000 .

---

## Odstranění síťových adaptérů

- | Než odstraníte síťovou kartu z integrovaného Windows serveru, musíte ji z něho odinstalovat.
- | Chcete-li odinstalovat síťové adaptéry z integrovaného serveru, postupujte takto:
  1. Klepněte na **Start**, pak na **Settings** a nakonec na **Control Panel**.
  2. Spusíte průvodce **Add/Remove Hardware** a v úvodním dialogovém okně klepněte na **Next**.
  3. Klepněte na **Uninstall/unplug a device**.
  4. V dialogovém okně **Choose a remove task** klepněte na **Next** a přijměte předvolbu (Uninstall a device).
  5. Vyberte ze seznamu zařízení, které chcete odinstalovat (například IBM PCI Token-ring adapter).
  6. Klepněte na **Yes** a potvrďte, že chcete adaptér odstranit.
  7. Protože Windows 2000 Server a Windows Server 2003 jsou operační systémy typu Plug and Play, musíte adaptér z operačního systému i5/OS buď fyzicky odebrat, nebo jej před restartováním serveru zakázat. Jestliže integrovaný server restartujete se stále ještě zapojeným adaptérem, bude jej operační systém detekovat jako nový hardware a ovladač zařízení znovu nainstaluje. Chcete-li adaptér pouze zakázat, nikoli odebrat, postupujte takto:
    - a. Z menu **Ovládací panel** vyberte **Síťová a vytáčená připojení**.
    - b. Vyberte adaptér LAN.
    - c. Klepněte pravým tlačítkem myši a vyberte **Zablokovat**.
  8. Po dokončení procedury server restartujte.



---

## Kapitola 7. Administrace připojení k serverům připojeným pomocí iSCSI

Následující sekce vás provedou některými postupy prováděnými na integrovaných serverech s adaptéry iSCSI HBA.

- “Práce s objekty konfigurace iSCSI”
- “Konfigurace zabezpečení mezi operačním systémem i5/OS a hostovanými systémy” na stránce 123
- “Správa adaptérů iSCSI HBA” na stránce 127
- “Zjišťování vzdálených serverů a jejich správa” na stránce 134

---

### Práce s objekty konfigurace iSCSI

Objekty i5/OS jsou určeny ke konfiguraci a správě adaptérů iSCSI HBA pro systém iSeries, vzdálený systém xSeries a systém IBM BladeCenter, servisní procesor vzdáleného systému a atributy zabezpečení sítě iSCSI. Podrobnější informace najdete v následujících tématech.

- “Správa objektů NWSH”
- “Správa konfigurací síťových serverů ve vzdáleném systému” na stránce 116
- “Správa konfigurací síťových serverů se servisními procesory” na stránce 118
- “Správa konfigurací síťových serverů se zabezpečeným připojením” na stránce 121

### Správa objektů NWSH

Objekty NWSH, tj. adaptéry hostitele síťového serveru, jsou používány při konfiguraci cílového adaptéru iSCSI HBA na serveru iSeries. Objekt NWSH musí být spuštěn (logicky zapnut), aby mohl integrovaný server používat příslušný adaptér iSCSI HBA pro tok dat v rámci paměťových prostorů a virtuální sítě Ethernet. Zastavení (logické vypnutí) objektu NWSH způsobí, že příslušný adaptér iSCSI HBA se stane nedostupným pro všechny integrované servery, jejichž cesty k paměťovým prostorům nebo k virtuální síti Ethernet jsou definovány tak, aby jej používaly. Další informace najdete v tématu “Adaptéry hostitele síťového serveru” na stránce 41.

S objekty NWSH lze provádět následující úlohy:

- “Vytvoření objektu NWSH”
- “Vytvoření objektu NWSH na základě jiného objektu” na stránce 114
- “Zobrazení vlastností objektu NWSH” na stránce 114
- “Změna vlastností objektu NWSH” na stránce 115
- “Spuštění objektu NWSH” na stránce 115
- “Zastavení objektu NWSH” na stránce 115
- “Výmaz objektu NWSH” na stránce 116

### Vytvoření objektu NWSH

Pro každý cílový adaptér iSCSI HBA na serveru iSeries musí být vytvořen objekt NWSH (adaptér hostitele síťového serveru).

Chcete-li vytvořit objekt NWSH pomocí produktu iSeries Navigator, postupujte takto:

1. Rozbalte **Administrace integrovaných serverů**.
2. Rozbalte **Připojení iSCSI**.
3. Klepněte pravým tlačítkem myši na **Adaptéry lokálního hostitele**.
4. Vyberte **Nový NWSH**.
5. Na kartě **Obecné**:
  - Zadejte **Jméno** a **Popis** zařízení NWSH.

- | • Vyberte **Hardwarový prostředek**.
  - | • Vyberte **Oprávnění k objektu**.
- | 6. Na kartě **Lokální rozhraní** zadejte údaje, které definují atributy rozhraní sítě SCSI a LAN pro adaptér iSCSI HBA.
  - | 7. Klepněte na **OK**.

- | **Poznámka:** Adaptér hostitele síťového serveru (NWSH) a konfigurace vzdáleného systému definují IP adresy pro opačné strany sítě iSCSI. Jsou-li propojeny jednoduchou komutovanou sítí, platí následující pravidla:
- | • Internetové adresy SCSI v těchto dvou objektech, které jsou propojeny přepínačem, musejí být ve stejné podsíti. Například u IP adres ve tvaru a.b.x.y a masek podsítě 255.255.255.0 musí být hodnota a.b.x stejná pro oba objekty.
  - | • Internetové adresy sítě LAN v těchto dvou objektech, které jsou propojeny přepínačem, musejí být ve stejné podsíti.
  - | • V objektu NWSH mohou být prvky brány libovolné nepřifažené IP adresy v kterékoli podsíti, pokud v síti není brána.
  - | • V konfiguraci vzdáleného systému by prvky brány měly být prázdné, pokud v síti není brána.

| Chcete-li použít CL příkazy, podívejte se na příkazy CRTDEVNWSH a WRKDEVD.

### | **Vytvoření objektu NWSH na základě jiného objektu**

| Při vytváření nového objektu NWSH (adaptér hostitele síťového serveru) můžete zkopírovat existující objekt.  
| V případě, že některé atributy nového objektu NWSH jsou stejné jako atributy existujícího objektu NWSH nebo podobné, ušetříte tím čas.

| Chcete-li objekt NWSH vytvořit na základě existujícího objektu pomocí produktu iSeries Navigator, postupujte takto:

- | 1. Rozbalte **Administrace integrovaných serverů**.
- | 2. Rozbalte **Připojení iSCSI**.
- | 3. Vyberte **Adaptéry lokálního hostitele**.
- | 4. Klepněte pravým tlačítkem myši na adaptér lokálního hostitele a v zobrazeném seznamu jej zkopírujte.
- | 5. Vyberte **Nová podle**.
- | 6. Zadejte jméno nového zařízení NWSH do pole **Jméno**.
- | 7. Uveďte libovolné další atributy, které by měly být odlišné od atributů kopírovaného objektu NWSH.
- | 8. Klepněte na **OK**.

| Chcete-li použít CL příkaz, podívejte se na příkaz WRKDEVD.

### | **Zobrazení vlastností objektu NWSH**

| Objekt NWSH obsahuje informace o konfiguraci cílového adaptéru iSCSI HBA serveru iSeries.

| Chcete-li zobrazit atributy objektu NWSH pomocí produktu iSeries Navigator, postupujte takto:

- | 1. Rozbalte **Administrace integrovaných serverů**.
- | 2. Rozbalte **Připojení iSCSI**.
- | 3. Vyberte **Adaptéry lokálního hostitele**.
- | 4. Klepněte pravým tlačítkem myši na adaptér lokálního hostitele v zobrazeném seznamu.
- | 5. Vyberte **Vlastnosti**.
- | 6. Klepněte na příslušné karty a vyberte vlastnosti, které chcete zobrazit.
- | 7. Klepnutím na **Zrušit** zavřete panel.

| Chcete-li použít CL příkazy, podívejte se na příkazy DSPDEVD a WRKDEVD.

## | **Změna vlastností objektu NWSH**

| Objekt NWSH obsahuje informace o konfiguraci cílového adaptéru iSCSI HBA serveru iSeries.

| Chcete-li změnit atributy objektu NWSH pomocí produktu iSeries Navigator, postupujte takto:

- | 1. Rozbalte **Administrace integrovaných serverů**.
- | 2. Rozbalte **Připojení iSCSI**.
- | 3. Vyberte **Adaptéry lokálního hostitele**.
- | 4. Klepněte pravým tlačítkem myši na adaptér lokálního hostitele v zobrazeném seznamu.
- | 5. Vyberte **Vlastnosti**.
- | 6. Klepněte na příslušné karty a vyberte vlastnosti, které chcete změnit.
- | 7. Klepnutím na **OK** uložte změny.

| Chcete-li použít CL příkazy, podívejte se na příkazy CHGDEVNWSH a WRKDEVD.

## | **Spuštění objektu NWSH**

| Integrovaný server může pro toky dat v rámci paměťových prostorů a virtuální síti Ethernet používat cílový adaptér iSCSI HBA na serveru iSeries pouze tehdy, je-li spuštěn (logicky zapnut) příslušný objekt NWSH.

| Chcete-li spustit objekt NWSH pomocí produktu iSeries Navigator, postupujte takto:

- | 1. Rozbalte **Administrace integrovaných serverů**.
- | 2. Rozbalte **Připojení iSCSI**.
- | 3. Vyberte **Adaptéry lokálního hostitele**.
- | 4. Klepněte pravým tlačítkem myši na adaptér lokálního hostitele v zobrazeném seznamu.
- | 5. Vyberte **Spustit**.

| Chcete-li použít CL příkazy, podívejte se na příkazy VRYCFG a WRKCFGSTS.

## | **Zastavení objektu NWSH**

| Zastavení (logické vypnutí) objektu NWSH způsobí, že se příslušný cílový adaptér iSCSI HBA na serveru iSeries stane nedostupným pro všechny integrované servery, jejichž cesty k paměťovým prostorům nebo k virtuální síti Ethernet jsou definovány tak, aby jej používaly.

| Zastavení objektu NWSH, který aktivní servery právě používají, může způsobit selhání serverů, pokud bez použití adaptéru iSCSI HBA, který tomuto NWSH odpovídá, nelze získat přístup k důležitým paměťovým prostředkům. Obvykle by zastavení objektu NWSH mělo předcházet ukončení práce všech integrovaných serverů, které tento objekt NWSH používají. Další informace najdete v tématu “Spuštění a zastavení integrovaného Windows serveru pomocí produktu iSeries Navigator” na stránce 141.

| Chcete-li zastavit objekt NWSH pomocí produktu iSeries Navigator, postupujte takto:

- | 1. Rozbalte **Administrace integrovaných serverů**.
- | 2. Rozbalte **Připojení iSCSI**.
- | 3. Vyberte **Adaptéry lokálního hostitele**.
- | 4. Klepněte pravým tlačítkem myši na adaptér lokálního hostitele v zobrazeném seznamu.
- | 5. Vyberte **Zastavit**.
- | 6. Klepněte na **Zastavit** na potvrzovacím panelu.
- | 7. Pokud aktivní servery objekt NWSH právě používají, zobrazí se varovná zpráva. Klepněte na **Pokračovat**.

| Chcete-li použít CL příkazy, podívejte se na příkazy VRYCFG a WRKCFGSTS.

## | **Výmaz objektu NWSH**

| Chcete-li vymazat objekt NWSH pomocí produktu iSeries Navigator, postupujte takto:

- | 1. Rozbalte **Administrace integrovaných serverů**.
- | 2. Rozbalte **Připojení iSCSI**.
- | 3. Vyberte **Adaptéry lokálního hostitele**.
- | 4. Klepněte pravým tlačítkem myši na adaptér lokálního hostitele v zobrazeném seznamu.
- | 5. Vyberte **Vymazat**.
- | 6. Klepněte na volbu **Vymazat** na potvrzovacím panelu.

| Chcete-li použít CL příkazy, podívejte se na příkazy DLTDEVD a WRKDEVD.

## | **Správa konfigurací síťových serverů ve vzdáleném systému**

| Objekty konfigurace síťových serverů ve vzdáleném systému (objekty NWSCFG s podtypem RMTSYS) jsou určeny ke konfiguraci atributů vzdáleného serveru xSeries nebo blade serveru IBM BladeCenter, které jsou připojeny pomocí iSCSI. Konfigurace vzdáleného systému slouží k identifikaci konkrétního hardwaru serveru xSeries nebo IBM BladeCenter, na kterém bude spuštěn integrovaný server. Určuje také, jak se bude vzdálený systém zavádět a jak bude komunikovat se systémem iSeries. Další informace najdete v tématu “Konfigurace vzdáleného systému” na stránce 41.

| S objekty konfigurace vzdáleného systému lze provádět následující úlohy:

- | • “Vytvoření objektu konfigurace vzdáleného systému”
- | • “Vytvoření objektu NWSH na základě jiného objektu” na stránce 117
- | • “Zobrazení vlastností konfigurace vzdáleného systému” na stránce 117
- | • “Změna vlastností konfigurace vzdáleného systému” na stránce 117
- | • “Zobrazení stavu vzdáleného systému” na stránce 118
- | • “Výmaz objektu konfigurace vzdáleného systému” na stránce 118

## | **Vytvoření objektu konfigurace vzdáleného systému**

| Pro každý server xSeries nebo IBM BladeCenter, na kterém bude spuštěn integrovaný server připojený pomocí iSCSI, musí být vytvořen objekt konfigurace síťového serveru ve vzdáleném systému (objekt NWSCFG s podtypem RMTSYS).

| Chcete-li vytvořit konfiguraci vzdáleného systému pomocí produktu iSeries Navigator, postupujte takto:

- | 1. Rozbalte **Administrace integrovaných serverů**.
- | 2. Rozbalte **Připojení iSCSI**.
- | 3. Klepněte pravým tlačítkem myši na **Vzdálené systémy**.
- | 4. Vyberte **Nová konfigurace vzdáleného systému**.
- | 5. Na kartě **Obecné**:
  - | • Do polí **Jméno** a **Popis** zadejte jméno a popis nové konfigurace.
  - | • Vyberte **Konfigurace servisního procesoru**.
  - | • Zadejte odpovídající hodnotu do pole **Identita vzdáleného systému**.
  - | • Vyberte **Oprávnění k objektu**.
- | 6. Na kartě **Síťová rozhraní** zadejte informace, které definují atributy rozhraní sítí SCSI a LAN pro vzdálený systém.
- | 7. V případě potřeby uveďte hodnoty na kartách **Parametry zavádění** a **Autentizace protokolem CHAP**.
- | 8. Klepněte na **OK**.

| **Poznámka:** Adaptér hostitele síťového serveru (NWSH) a konfigurace vzdáleného systému definují IP adresy pro opačné strany sítě iSCSI. Jsou-li propojeny jednoduchou komutovanou sítí, platí následující pravidla:



- | • Internetové adresy SCSI v těchto dvou objektech, které jsou propojeny přepínačem, musejí být ve stejné podsíti. Například u IP adres ve tvaru a.b.x.y a masek podsítě 255.255.255.0 musí být hodnota a.b.x stejná pro oba objekty.
- | • Internetové adresy sítě LAN v těchto dvou objektech, které jsou propojeny přepínačem, musejí být ve stejné podsíti.
- | • V objektu NWSH mohou být prvky brány libovolné nepřijížené IP adresy v kterékoli podsíti, pokud v síti není brána.
- | • V konfiguraci vzdáleného systému by prvky brány měly být prázdné, pokud v síti není brána.

| Chcete-li použít CL příkazy, podívejte se na příkazy CRTNWSCFG a WRKNWSCFG.

## | Vytvoření objektu NWSH na základě jiného objektu

| Při vytváření nového objektu konfigurace síťového serveru ve vzdáleném systému (objekt NWSCFG s podtypem RMTSYS) můžete zkopírovat existující objekt. V případě, že některé atributy nové konfigurace ve vzdáleném systému jsou stejné jako atributy existující konfigurace ve vzdáleném systému nebo podobné, ušetříte tím čas.

| Chcete-li vytvořit konfiguraci vzdáleného systému na základě existující konfigurace pomocí produktu iSeries Navigator, postupujte takto:

- | 1. Rozbalte **Administrace integrovaných serverů**.
- | 2. Rozbalte **Připojení iSCSI**.
- | 3. Vyberte **Vzdálené systémy**.
- | 4. Klepněte pravým tlačítkem myši na konfiguraci vzdáleného systému a v zobrazeném seznamu ji zkopírujte.
- | 5. Vyberte **Nová podle**.
- | 6. Do pole **Jméno** zadejte jméno nové konfigurace vzdáleného systému.
- | 7. Uveďte libovolné další atributy, které by měly být odlišné od atributů kopírované konfigurace vzdáleného systému.
- | 8. Klepněte na **OK**.

| **Poznámka:** Pro tuto úlohu neexistuje ekvivalentní CL příkaz.

## | Zobrazení vlastností konfigurace vzdáleného systému

| Objekt konfigurace síťového serveru ve vzdáleném systému (objekt NWSCFG s podtypem RMTSYS) obsahuje informace o konfiguraci pro server IBM xSeries nebo BladeCenter, na kterém bude spuštěn integrovaný server připojený pomocí iSCSI.

| Chcete-li zobrazit atributy konfigurace vzdáleného systému pomocí produktu iSeries Navigator, postupujte takto:

- | 1. Rozbalte **Administrace integrovaných serverů**.
- | 2. Rozbalte **Připojení iSCSI**.
- | 3. Vyberte **Vzdálené systémy**.
- | 4. Klepněte pravým tlačítkem myši na konfiguraci vzdáleného systému v zobrazeném seznamu.
- | 5. Vyberte **Vlastnosti**.
- | 6. Klepněte na příslušné karty a vyberte vlastnosti, které chcete zobrazit.
- | 7. Klepnutím na **OK** zavřete panel.

| Chcete-li použít CL příkazy, podívejte se na příkazy DSPNWSCFG a WRKNWSCFG.

## | Změna vlastností konfigurace vzdáleného systému

| Objekt konfigurace síťového serveru ve vzdáleném systému (objekt NWSCFG s podtypem RMTSYS) obsahuje informace o konfiguraci pro server xSeries nebo IBM BladeCenter, na kterém bude spuštěn integrovaný server připojený pomocí iSCSI.

| Chcete-li změnit atributy konfigurace vzdáleného systému pomocí produktu iSeries Navigator, postupujte takto:

- | 1. Rozbalte **Administrace integrovaných serverů**.
- | 2. Rozbalte **Připojení iSCSI**.
- | 3. Vyberte **Vzdálené systémy**.
- | 4. Klepněte pravým tlačítkem myši na konfiguraci vzdáleného systému v zobrazeném seznamu.
- | 5. Vyberte **Vlastnosti**.
- | 6. Klepněte na příslušné karty a vyberte vlastnosti, které chcete změnit.
- | 7. Klepnutím na **OK** uložte změny.

| Chcete-li použít CL příkazy, podívejte se na příkazy CHGNWSCFG a WRKNWSCFG.

### | **Zobrazení stavu vzdáleného systému**

| Můžete zobrazit stav hardwaru serveru xSeries nebo IBM BladeCenter. Můžete jej například potřebovat, až budete chtít zjistit, zda je k dispozici a zda jej může libovolný z integrovaných serverů připojených pomocí iSCSI použít.

| Chcete-li zobrazit stav vzdáleného systému pomocí produktu iSeries Navigator, postupujte takto:

- | 1. Rozbalte **Administrace integrovaných serverů**.
- | 2. Rozbalte **Připojení iSCSI**.
- | 3. Vyberte **Vzdálené systémy**.
- | 4. Klepněte pravým tlačítkem myši na konfiguraci vzdáleného systému v zobrazeném seznamu.
- | 5. Vyberte **Stav**.
- | 6. Zobrazí se stav vzdáleného systému.
- | 7. Klepnutím na **Zrušit** zavřete panel.

| Chcete-li použít CL příkaz, podívejte se na příkaz WRKNWSCFG.

### | **Výmaz objektu konfigurace vzdáleného systému**

| Chcete-li vymazat konfiguraci vzdáleného systému pomocí produktu iSeries Navigator, postupujte takto:

- | 1. Rozbalte **Administrace integrovaných serverů**.
- | 2. Rozbalte **Připojení iSCSI**.
- | 3. Vyberte **Vzdálené systémy**.
- | 4. Klepněte pravým tlačítkem myši na konfiguraci vzdáleného systému v zobrazeném seznamu.
- | 5. Vyberte **Vymazat**.
- | 6. Klepněte na volbu **Vymazat** na potvrzovacím panelu.

| Chcete-li použít CL příkazy, podívejte se na příkazy DLTNWSCFG a WRKNWSCFG.

## | **Správa konfigurací síťových serverů se servisními procesory**

| Objekty konfigurace síťových serverů se servisními procesory (objekty NWSCFG s podtypem SRVPRC) jsou určeny ke konfiguraci atributů servisního procesoru nebo modulu Management Module jednotlivých vzdálených serverů xSeries nebo serverů IBM BladeCenter, které jsou připojeny pomocí iSCSI. Konfigurace servisního procesoru definuje atributy, které slouží ke zjišťování a bezpečnému připojení k servisnímu procesoru nebo k modulu Management Module v síti. Objekty konfigurace síťových serverů ve vzdáleném systému obsahují odkaz na příslušný objekt konfigurace servisního procesoru, který řídí hardware vzdáleného systému. Další informace najdete v tématu “Konfigurace servisního procesoru” na stránce 41.

| **Poznámka:** Konfigurace servisního procesoru není nezbytná pro každý server IBM BladeCenter ve skříni BladeCenter. Pro celou skříň serveru IBM BladeCenter stačí jen jeden servisní procesor.

| S objekty konfigurace servisního procesoru lze provádět následující úlohy:

- | • “Vytvoření objektu konfigurace servisního procesoru” na stránce 119

- | • “Vytvoření objektu konfigurace servisního procesoru na základě jiného objektu”
- | • “Zobrazení vlastností konfigurace servisního procesoru”
- | • “Změna vlastností konfigurace servisního procesoru” na stránce 120
- | • “Inicializace servisního procesoru” na stránce 120
- | • “Výmaz objektu konfigurace servisního procesoru” na stránce 121

## Vytvoření objektu konfigurace servisního procesoru

| Pro servisní procesor nebo Management Module každého serveru xSeries nebo IBM BladeCenter, na kterém bude spuštěn integrovaný server připojený pomocí iSCSI, musí být vytvořen objekt konfigurace síťového serveru se servisním procesorem (objekt NWSCFG s podtypem SRVPRC).

| **Poznámka:** Konfigurace servisního procesoru není nezbytná pro každý blade server ve skříni IBM BladeCenter. Pro celou skříň serveru BladeCenter stačí jen jeden servisní procesor.

| Chcete-li vytvořit konfiguraci servisního procesoru pomocí produktu iSeries Navigator, postupujte takto:

- | 1. Rozbalte **Administrace integrovaných serverů**.
- | 2. Rozbalte **Připojení iSCSI**.
- | 3. Klepněte pravým tlačítkem myši na **Servisní procesory**.
- | 4. Vyberte **Nová konfigurace servisního procesoru**.
- | 5. Na kartě **Obecné**:
  - | • Do polí **Jméno** a **Popis** zadejte jméno a popis nové konfigurace.
  - | • Zadejte identifikaci servisního procesoru v síti vyplněním jednoho z polí **Jméno hostitele**, **Internetová adresa** a **Sériové číslo**.
  - | • Vyberte **Oprávnění k objektu**
- | 6. Na kartě **Zabezpečení** určete typ zabezpečení, který má být při připojení k servisnímu procesoru použit.
- | 7. Klepněte na **OK**.

| Chcete-li použít CL příkazy, podívejte se na příkazy CRTNWSCFG a WRKNWSCFG.

## Vytvoření objektu konfigurace servisního procesoru na základě jiného objektu

| Při vytváření nového objektu konfigurace síťového serveru se servisním procesorem (objekt NWSCFG s podtypem SRVPRC) můžete zkopírovat existující objekt. V případě, že některé atributy nové konfigurace servisního procesoru jsou stejné jako atributy existující konfigurace servisního procesoru nebo podobné, ušetříte tím čas.

| Chcete-li vytvořit konfiguraci servisního procesoru na základě existující konfigurace pomocí produktu iSeries Navigator, postupujte takto:

- | 1. Rozbalte **Administrace integrovaných serverů**.
- | 2. Rozbalte **Připojení iSCSI**.
- | 3. Vyberte **Servisní procesory**.
- | 4. Klepněte pravým tlačítkem myši na konfiguraci servisního procesoru a v zobrazeném seznamu jej zkopírujte.
- | 5. Vyberte **Nová podle**.
- | 6. Zadejte jméno nové konfigurace do pole **Jméno**.
- | 7. Uveďte libovolné další atributy, které by měly být odlišné od atributů kopírované konfigurace servisního procesoru.
- | 8. Klepněte na **OK**.

| **Poznámka:** Pro tuto úlohu neexistuje ekvivalentní CL příkaz.

## Zobrazení vlastností konfigurace servisního procesoru

| Objekt konfigurace síťového serveru se servisním procesorem (objekt NWSCFG s podtypem SRVPRC) obsahuje informace o konfiguraci servisního procesoru nebo modulu Management Module serveru xSeries nebo IBM BladeCenter, na kterém bude spuštěn integrovaný server připojený pomocí iSCSI.

Chcete-li změnit atributy konfigurace servisního procesoru pomocí produktu iSeries Navigator, postupujte takto:

1. Rozbalte **Administrace integrovaných serverů**.
2. Rozbalte **Připojení iSCSI**.
3. Vyberte **Servisní procesory**.
4. Klepněte pravým tlačítkem myši na konfiguraci servisního procesoru v zobrazeném seznamu.
5. Vyberte **Vlastnosti**.
6. Klepněte na příslušné karty a vyberte vlastnosti, které chcete zobrazit.
7. Klepnutím na **OK** zavřete panel.

Chcete-li použít CL příkazy, podívejte se na příkazy DSPNWSCFG a WRKNWSCFG.

### Změna vlastností konfigurace servisního procesoru

Objekt konfigurace síťového serveru se servisním procesorem (objekt NWSCFG s podtypem SRVPRC) obsahuje informace o konfiguraci servisního procesoru nebo modulu Management Module serveru IBM xSeries nebo BladeCenter, na kterém bude spouštěn integrovaný server připojený pomocí iSCSI.

Chcete-li změnit atributy konfigurace servisního procesoru pomocí produktu iSeries Navigator, postupujte takto:

1. Rozbalte **Administrace integrovaných serverů**.
2. Rozbalte **Připojení iSCSI**.
3. Vyberte **Servisní procesory**.
4. Klepněte pravým tlačítkem myši na servisní procesor v zobrazeném seznamu.
5. Vyberte **Vlastnosti**.
6. Klepněte na příslušné karty a vyberte vlastnosti, které chcete změnit.
7. Klepnutím na **OK** uložte změny.

Chcete-li použít CL příkazy, podívejte se na příkazy CHGNWSCFG a WRKNWSCFG.

### Inicializace servisního procesoru

Objekt konfigurace síťového serveru se servisním procesorem (objekt NWSCFG s podtypem SRVPRC) obsahuje informace o konfiguraci servisního procesoru nebo modulu Management Module serveru xSeries nebo IBM BladeCenter, na kterém bude spouštěn integrovaný server připojený pomocí iSCSI. Než může být servisní procesor používán s integrovaným serverem, musí být nejprve inicializován. Můžete také znovu vygenerovat nebo synchronizovat uživatele, heslo a certifikát, které zabezpečují připojení servisního procesoru, nebo změnit uživatele či heslo pro připojení k servisnímu procesoru.

Chcete-li inicializovat servisní procesor pomocí produktu iSeries Navigator, postupujte takto:

1. Rozbalte **Administrace integrovaných serverů**.
2. Rozbalte **Připojení iSCSI**.
3. Vyberte **Servisní procesory**.
4. Klepněte pravým tlačítkem myši na konfiguraci servisního procesoru v zobrazeném seznamu.
5. Vyberte **Inicializovat**.
6. Vyberte jednu z následujících možností:
  - **Inicializace nového servisního procesoru**
  - **Nové generování certifikátu servisního procesoru**
  - **Synchronizace certifikátu servisního procesoru**
  - **Změna ID a hesla uživatele servisního procesoru**
7. V případě potřeby vyplňte pole **Uživatel** a **Heslo**.
8. Klepnutím na **Inicializovat** proveďte vybranou akci.

Chcete-li použít CL příkazy, podívejte se na příkazy INZNWSCFG a WRKNWSCFG.

## Výmaz objektu konfigurace servisního procesoru

Chcete-li vymazat konfiguraci servisního procesoru pomocí produktu iSeries Navigator, postupujte takto:

1. Rozbalte **Administrace integrovaných serverů**.
2. Rozbalte **Připojení iSCSI**.
3. Vyberte **Servisní procesory**.
4. Klepněte pravým tlačítkem myši na konfiguraci servisního procesoru v zobrazeném seznamu.
5. Vyberte **Vymazat**.
6. Klepněte na volbu **Vymazat** na potvrzovacím panelu.

Chcete-li použít CL příkazy, podívejte se na příkazy DLTNWSCFG a WRKNWSCFG.

## Správa konfigurací síťových serverů se zabezpečeným připojením

Objekty konfigurace síťového serveru se zabezpečeným připojením (objekty NWSCFG s podtypem CNNSEC) slouží k definování pravidel zabezpečení IPsec, která zabezpečují toky dat v rámci paměťových prostorů a virtuální sítě Ethernet přes síť iSCSI mezi blade servery iSeries a xSeries nebo IBM BladeCenter. Další informace najdete v tématu “Konfigurace zabezpečeného připojení” na stránce 45.

**Poznámka:** Nepodporuje-li hardware adaptéru iSCSI HBA zabezpečení IPsec ani na straně serveru iSeries, ani na straně připojení sítě iSCSI k serveru xSeries/Center, pak toky dat přes síť iSCSI nelze pomocí IPsec zabezpečit. Nepodporuje-li hardware adaptéru iSCSI HBA zabezpečení IPsec, pak je nutné objekt zabezpečeného připojení vytvořit, ale neměla by být definována žádná pravidla IPsec.

S objekty konfigurace zabezpečeného připojení lze provádět následující úlohy:

- “Vytvoření objektu konfigurace zabezpečeného připojení”
- “Vytvoření objektu konfigurace zabezpečeného připojení na základě jiného objektu” na stránce 122
- “Zobrazení vlastností konfigurace zabezpečeného připojení” na stránce 122
- “Změna vlastností konfigurace zabezpečeného připojení” na stránce 122
- “Výmaz objektu konfigurace zabezpečeného připojení” na stránce 123

## Vytvoření objektu konfigurace zabezpečeného připojení

Je třeba vytvořit objekty konfigurací síťových serverů se zabezpečeným připojením (objekty NWSCFG s podtypem CNNSEC), které definují pravidla zabezpečení IPsec. Tato pravidla zabezpečují toky dat v rámci paměťových prostorů a virtuální sítě Ethernet přes síť iSCSI mezi blade servery iSeries a xSeries nebo IBM BladeCenter.

**Poznámka:** Není-li zabezpečení IPsec podporováno hardwarem adaptéru iSCSI HBA ani na straně serveru iSeries, ani na straně serveru xSeries, ani na straně serveru IBM BladeCenter v rámci spojení iSCSI, pak nelze IPsec použít k zabezpečení toků dat přes síť iSCSI. Nepodporuje-li hardware adaptéru iSCSI HBA zabezpečení IPsec, pak je sice nutné objekt zabezpečeného připojení vytvořit, ale nedefinuje žádná pravidla IPsec.

Chcete-li vytvořit konfiguraci zabezpečeného připojení pomocí produktu iSeries Navigator, postupujte takto:

1. Rozbalte **Administrace integrovaných serverů**.
2. Rozbalte **Připojení iSCSI**.
3. Klepněte pravým tlačítkem myši na **Zabezpečit připojení**.
4. Vyberte **Nová konfigurace zabezpečeného připojení**.
5. Na kartě **Obecné**:
  - Do polí **Jméno** a **Popis** zadejte jméno a popis nové konfigurace.
  - Vyberte **Oprávnění k objektu**
6. Na kartě **Pravidla zabezpečení IP**:

- | • Podporuje-li hardware vašeho iSCSI HBA zabezpečení IPsec, definujte pravidla zabezpečení IPsec, která zabezpečí toky dat v rámci paměťových prostorů a virtuální sítě Ethernet přes síť iSCSI.
  - | • V opačném případě nemusíte žádná pravidla zabezpečení IPsec definovat.
- | 7. Klepněte na **OK**.

| Chcete-li použít CL příkazy, podívejte se na příkazy CRTNWSCFG a WRKNWSCFG.

### | **Vytvoření objektu konfigurace zabezpečeného připojení na základě jiného objektu**

| Při vytváření nového objektu konfigurace síťového serveru se zabezpečeným připojením (objekt NWSCFG s podtypem CNNSEC) můžete zkopírovat existující objekt. V případě, že některé atributy nové konfigurace zabezpečeného připojení jsou stejné jako atributy existující konfigurace zabezpečeného připojení nebo podobné, ušetříte tím čas.

| Chcete-li vytvořit konfiguraci zabezpečeného připojení na základě existující konfigurace pomocí produktu iSeries Navigator, postupujte takto:

- | 1. Rozbalte **Administrace integrovaných serverů**.
- | 2. Rozbalte **Připojení iSCSI**.
- | 3. Vyberte **Zabezpečit připojení**.
- | 4. Klepněte pravým tlačítkem myši na konfiguraci zabezpečeného připojení a v zobrazeném seznamu ji zkopírujte.
- | 5. Vyberte **Nová podle**.
- | 6. Do pole **Jméno** zadejte jméno nové konfigurace zabezpečeného připojení.
- | 7. Uveďte libovolné další atributy, které by měly být odlišné od atributů kopírované konfigurace zabezpečeného připojení.
- | 8. Klepněte na **OK**.

| **Poznámka:** Pro tuto úlohu neexistuje ekvivalentní CL příkaz.

### | **Zobrazení vlastností konfigurace zabezpečeného připojení**

| Objekt konfigurace síťového serveru se zabezpečeným připojením (objekt NWSCFG s podtypem CNNSEC) obsahuje pravidla zabezpečení IPsec, která zabezpečují toky dat v rámci paměťových prostorů a virtuální sítě Ethernet přes síť iSCSI mezi blade servery iSeries a xSeries nebo IBM BladeCenter.

| Chcete-li zobrazit atributy konfigurace zabezpečeného připojení pomocí produktu iSeries Navigator, postupujte takto:

- | 1. Rozbalte **Administrace integrovaných serverů**.
- | 2. Rozbalte **Připojení iSCSI**.
- | 3. Vyberte **Zabezpečit připojení**.
- | 4. V zobrazeném seznamu klepněte pravým tlačítkem myši na objekt zabezpečeného připojení.
- | 5. Vyberte **Vlastnosti**.
- | 6. Klepněte na příslušné karty a vyberte vlastnosti, které chcete zobrazit.
- | 7. Klepnutím na **OK** zavřete panel.

| Chcete-li použít CL příkazy, podívejte se na příkazy DSPNWSCFG a WRKNWSCFG.

### | **Změna vlastností konfigurace zabezpečeného připojení**

| Objekt konfigurace síťového serveru se zabezpečeným připojením (objekt NWSCFG s podtypem CNNSEC) obsahuje pravidla zabezpečení IPsec, která zabezpečují toky dat v rámci paměťových prostorů a virtuální sítě Ethernet přes síť iSCSI mezi blade servery iSeries a xSeries nebo IBM BladeCenter.

| **Poznámka:** Nepodporuje-li hardware adaptéru iSCSI HBA zabezpečení IPsec ani na straně serveru iSeries ani na straně připojení sítě iSCSI k serveru xSeries/IBM BladeCenter, pak toky dat přes síť iSCSI nelze pomocí IPsec zabezpečit. Nepodporuje-li hardware adaptéru iSCSI HBA zabezpečení IPsec, nedefinujte žádná pravidla IPsec.



- | Chcete-li změnit atributy konfigurace zabezpečeného připojení pomocí produktu iSeries Navigator, postupujte takto:
- | 1. Rozbalte **Administrace integrovaných serverů**.
  - | 2. Rozbalte **Připojení iSCSI**.
  - | 3. Vyberte **Zabezpečit připojení**.
  - | 4. V zobrazeném seznamu **klepněte pravým tlačítkem myši** na konfiguraci zabezpečeného připojení.
  - | 5. Vyberte **Vlastnosti**.
  - | 6. Klepněte na příslušné karty a vyberte vlastnosti, které chcete změnit.
  - | 7. Klepnutím na **OK** uložte změny.

| Chcete-li použít CL příkazy, podívejte se na příkazy CHGNWSCFG a WRKNWSCFG.

### | **Výmaz objektu konfigurace zabezpečeného připojení**

- | Chcete-li vymazat konfiguraci zabezpečeného připojení pomocí produktu iSeries Navigator, postupujte takto:
- | 1. Rozbalte **Administrace integrovaných serverů**.
  - | 2. Rozbalte **Připojení iSCSI**.
  - | 3. Vyberte **Zabezpečit připojení**.
  - | 4. V zobrazeném seznamu klepněte pravým tlačítkem myši na objekt zabezpečeného připojení.
  - | 5. Vyberte **Vymazat**.
  - | 6. Klepněte na volbu **Vymazat** na potvrzovacím panelu.

| Chcete-li použít CL příkazy, podívejte se na příkazy DLTNWSCFG a WRKNWSCFG.

---

## | **Konfigurace zabezpečení mezi operačním systémem i5/OS a hostovanými systémy**

| Prostudujte téma “Zabezpečení u systémů připojených pomocí iSCSI” na stránce 47, pomůže vám určit, které z následujících akcí zabezpečení jsou vhodné pro vaše prostředí:

- | • “Konfigurace protokolu CHAP”
- | • “Konfigurace IPSec” na stránce 124
- | • “Konfigurace zabezpečení SSL servisního procesoru” na stránce 125
- | • “Heslo servisního procesoru” na stránce 126
- | • “Konfigurace firewallu” na stránce 126

### | **Konfigurace protokolu CHAP**

| **Poznámka:** Chcete-li vytvořit, změnit nebo zobrazit informace protokolu CHAP, musíte mít speciální oprávnění administrátora zabezpečení (\*SECADM).

| Chcete-li konfigurovat protokol CHAP nebo změnit pověření protokolu CHAP, postupujte takto:

- | 1. Chcete-li pro server změnit vlastnosti konfigurace vzdáleného systému, ukončete práci serveru (logicky vypněte objekt NWSD) a postupujte podle pokynů uvedených v tématu “Změna vlastností konfigurace vzdáleného systému” na stránce 117. Přejděte na kartu **Autentizace protokolem CHAP**.
  - | • Chcete-li protokol CHAP povolit, vyberte možnost **Použít následující hodnoty pro autentizaci CHAP** a zadejte **Jméno CHAP** a vyberte možnost **Generovat klíč CHAP jednou**.
  - | • Chcete-li protokol CHAP zakázat, vyberte možnost **Nepoužívat CHAP**.
- | 2. Chcete-li pro server zobrazit vlastnosti konfigurace vzdáleného systému, postupujte podle pokynů uvedených v tématu “Zobrazení vlastností konfigurace vzdáleného systému” na stránce 117.
  - | • Poznamenejte si hodnoty v polích **Jméno CHAP** a **Klíč CHAP** na kartě **Autentizace protokolem CHAP**.
  - | • Poznamenejte si metodu dodání parametrů pro zavádění na kartě **Parametry zavádění**.



3. Tento krok je požadovaný, je-li jako metoda dodání parametrů pro zavádění vybrána jedna z možností **Manuálně konfigurované ve vzdáleném systému** a **Dynamicky doručené do vzdáleného systému pomocí CHAP**. Při příštím spuštění serveru (logickém zapnutí objektu NWS) sledujte konzoli hostovaného systému a čekejte, až vás vyzve ke stisknutí kombinace kláves CTRL-Q. Jakmile se náznak zobrazí, stiskněte kombinaci kláves CTRL-Q. V obslužném programu CTRL-Q vyberte adaptér, který je konfigurován tak, že zavádí operační systém hostitele. Zadejte jméno a šifrovací klíč CHAP z vlastností konfigurace vzdáleného systému do polí Jméno CHAP a Klíč CHAP na cílovém panelu konfigurace zabezpečení obslužného programu CTRL-Q. Nezasílejte tyto informace na panelu konfigurace iniciátoru CTRL-Q.

**Poznámka:** Všechny adaptéry iSCSI HBA v hostovaném systému, které nejsou určeny pro zavádění systému, jsou automaticky konfigurovány v rámci konfigurace i5/OS.

## Konfigurace IPSec

**Poznámka:** Použití zabezpečení IPSec, které chrání toky dat přes síť iSCSI, vyžaduje adaptér iSCSI HBA pro server iSeries s podporou zabezpečení IPSec. Nepodporuje-li hardware adaptéru iSCSI HBA zabezpečení IPSec, pak je nutné objekt zabezpečeného připojení vytvořit, ale neměli byste definovat žádná pravidla zabezpečení IPSec.

Chcete-li konfigurovat IPSec nebo změnit pověření IPSec, postupujte takto:

1. Tento krok je vyžadován, pokud jste ještě nevygenerovali první předem nasdílený klíč. Můžete jej také provést kdykoli, až budete chtít předem nasdílený klíč změnit: Ukončete práci serveru (logicky vypněte objekt NWS) a změňte vlastnosti konfigurace zabezpečeného připojení podle procedury popsané v tématu “Změna vlastností konfigurace zabezpečeného připojení” na stránce 122.

- Přejděte na kartu **Pravidla zabezpečení IP**.
- Klepněte na tlačítko **Přidat** a vyberte volbu **Generovat předem nasdílený klíč jednou**.
- Klepnutím na **OK** přidejte do tabulky nové pravidlo IPSec. Dalším klepnutím na **OK** uložte konfiguraci zabezpečeného připojení. Potom bude předem nasdílený klíč vygenerován.

**Poznámka:** Musíte mít speciální oprávnění administrátora zabezpečení (\*SECADM), chcete-li předem nasdílený klíč vytvořit, změnit nebo zobrazit.

2. Vlastnosti konfigurace zabezpečeného připojení pro server můžete zobrazit, použijte-li proceduru popsanou v tématu “Zobrazení vlastností konfigurace zabezpečeného připojení” na stránce 122.

- Přejděte na kartu **Pravidla zabezpečení IP**.
- Poznamenejte si první řádek hodnot v tabulce. Obsahuje náhodný předem nasdílený klíč vygenerovaný operačním systémem i5/OS. Tyto informace budou použity v kroku 5 na stránce 125.

3. V prostředí produktu iSeries Navigator:

- Vyberte **Administrace integrovaných serverů -> Servery**.
- Klepněte pravým tlačítkem myši na integrovaný server a vyberte **Vlastnosti**.
- Přejděte na kartu **Zabezpečení iSCSI**.
- V poli **Předvolené pravidlo zabezpečení IP** vyberte hodnotu **1**, potom klepnutím na **OK** uložte změnu. Oznamujete tím operačnímu systému i5/OS, že má postupovat takto: Jakmile se v nastavení pravidla zabezpečení IP ve vlastnostech serveru objeví hodnota **Předvolené**, bude použita první hodnota v konfiguraci zabezpečeného připojení (určená hodnotou **Konfigurace zabezpečeného připojení** na kartě **Zabezpečení iSCSI** ve vlastnostech serveru).

4. Tento krok je požadován pouze tehdy, jestliže nechcete povolit zabezpečení IPSec na všech připojeních objektu NWS na serveru nebo jestliže se změnila předvolená hodnota pro pravidla vzdálených rozhraní ve vlastnostech serveru.

V prostředí produktu iSeries Navigator:

- Vyberte **Administrace integrovaných serverů -> Servery**.
- Klepněte pravým tlačítkem myši na integrovaný server a vyberte **Vlastnosti**.

- Přejděte na kartu **Cesty k paměťovým prostorům**.
  - Každý sloupec **Pravidlo zabezpečení IP vzdáleného rozhraní** odpovídá dvojici adaptérů iSCSI HBA, která sestává z adaptéru iSCSI HBA pro port serveru iSeries a portu iSCSI HBA hostovaného systému.
- Opakujte následující postup pro všechny sloupce **Pravidlo zabezpečení IP vzdáleného rozhraní** na kartách **Cesty k paměťovým prostorům** a **Cesty k virtuální síti Ethernet**.

**Poznámka:** Každý objekt NWSH použitý v objektu NWSO více než jednou musí mít ve sloupci Pravidlo zabezpečení IP vzdáleného rozhraní identické množiny hodnot v každé z cest k paměťovým prostorům nebo cest k virtuální síti Ethernet, které na něj odkazují.

Nastavte každé pravidlo zabezpečení IP vzdáleného rozhraní buď na hodnotu **Žádné**, nebo na hodnotu **Předvolené** podle způsobu, jakým používáte konkrétní dvojici portů iSCSI HBA:

- Hodnotu **Žádné** použijte, chcete-li, aby síťový provoz mezi porty iSCSI HBA probíhal hladce bez ohledu na schopnost obou adaptérů iSCSI HBA podporovat IPsec.
- Hodnotu **Předvolené** použijte, jestliže příslušný adaptér iSCSI HBA pro server iSeries podporuje zabezpečení IPsec a chcete-li povolit pouze šifrovaný provoz (nebo žádný provoz, pokud port iSCSI HBA hostovaného systému nepodporuje IPsec).

5. Tento krok je požadován pouze tehdy, je-li pro metodu dodání v konfiguraci vzdáleného systému nastavena volba **Manuálně konfigurované ve vzdáleném systému** nebo **Dynamicky doručené do vzdáleného systému pomocí CHAP**: Při příštím spuštění serveru (logickém zapnutí objektu NWSO) sledujte konzoli hostovaného systému a čekejte, až vás vyzve ke stisknutí kombinace kláves CTRL-Q. Jakmile se náznak zobrazí, stiskněte kombinaci kláves CTRL-Q. V obslužném programu CTRL-Q vyberte adaptér, který je konfigurován tak, že zavádí hostovaný systém. Zadejte předem nasdílený klíč z vlastností konfigurace zabezpečeného připojení do odpovídajícího pole na panelu cílové konfigurace zabezpečení. Další informace o obslužném programu CTRL-Q najdete v tématu “Zavádění systému bez disku přes iSCSI” na stránce 22.

**Poznámka:** Všechny adaptéry iSCSI HBA v hostovaném systému, které nejsou určeny pro zavádění systému, jsou automaticky konfigurovány v rámci konfigurace i5/OS.

## Konfigurace zabezpečení SSL servisního procesoru

Připojení SSL a heslo servisního procesoru spolupracují při zabezpečování provozu správy systému mezi adaptérem sítě LAN systému iSeries a servisními procesory hostovaného systému.

Při inicializaci zabezpečení SSL servisního procesoru můžete použít libovolnou z následujících metod.

- “Automatická inicializace zabezpečení SSL”
- “Manuální inicializace zabezpečení SSL” na stránce 126

Informace o hesle servisního procesoru najdete v tématu “Heslo servisního procesoru” na stránce 126.

### Automatická inicializace zabezpečení SSL

Při automatické inicializaci zabezpečení SSL postupujte takto:

1. Používá-li připojení mezi servisním procesorem a serverem iSeries sdílenou síť, zvažte dočasné propojení servisního procesoru a serveru iSeries samostatnou sítí. V opačném případě bude během krátké doby, po kterou je spuštěna úloha inicializace v kroku 3, automatická metoda o něco méně bezpečná než manuální metody.
2. Chcete-li pro server změnit vlastnosti konfigurace servisního procesoru, postupujte podle pokynů uvedených v tématu “Změna vlastností konfigurace servisního procesoru” na stránce 120. Přejděte na kartu **Zabezpečení** a vyberte volbu **Automaticky nastavit uživatele a certifikát**. Stisknutím OK uložte změny.
3. Chcete-li inicializovat servisní procesor, použijte proceduru v tématu “Inicializace servisního procesoru” na stránce 120:
  - a. Vyberte volbu **Inicializovat nový servisní procesor**.


**Poznámka:** Jedná-li se o další konfiguraci téhož servisního procesoru, který již byl dříve inicializován pro použití s jiným integrovaným serverem, použijte volbu **Synchronizovat certifikát ze servisního procesoru**.

- b. Zadejte hodnoty do polí **Uživatel** a **Heslo**.
- c. Stisknutím **Inicializovat** proveďte operaci.

**Poznámka:** Servisní procesor automaticky vygeneruje certifikát s automatickým podpisem, který bude operačním systémem i5/OS uložen. Certifikát je uložen do adresáře /QIBM/UserData/Director/classes/com/ibm/sysmgmt/app/iide/ integrovaného systému souborů pod jménem souboru, které odpovídá jménu konfigurace servisního procesoru. Tento soubor bude mít příponu 'kdb'.

## Manuální inicializace zabezpečení SSL

Při manuální inicializaci zabezpečení SSL s použitím certifikátu podepsaného důvěryhodným vydavatelem certifikátů postupujte takto:

1. Pomocí webového rozhraní servisního procesoru a požádejte důvěryhodného vydavatele certifikátů o certifikát SSL. Podrobný postup najdete v publikaci IBM Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide  (www.ibm.com/pc/support/site.wss/). Pod nadpisem **Procházet** vyberte **Servery**, Skupina: **xSeries 236**, **publikace**.

**Poznámka:** Certifikát pro vydavatele certifikátů musí být v paměti certifikátů \*SYSTEM operačního systému i5/OS.

2. Přijímáte-li od vydavatele certifikátů nový certifikát, importujte jej do servisního procesoru přes webové rozhraní servisního procesoru.
3. Chcete-li pro server změnit vlastnosti konfigurace servisního procesoru, postupujte podle pokynů uvedených v tématu "Změna vlastností konfigurace servisního procesoru" na stránce 120. Přejděte na kartu Zabezpečení a proveďte následující kroky:
  - a. Vyberte volbu **Nastavit uživatele a certifikát manuálně**.
  - b. Pro volbu **Komponenta** vyberte jednu z následujících možností: **Společné jméno**, **E-mailová adresa** a **Organizační jednotka**.
  - c. V poli **Porovnávací hodnota** uveďte příslušné informace z nového certifikátu. Umožníte tak, aby zabezpečení SSL odlišilo vaše certifikáty v paměti certifikátů \*SYSTEM operačního systému i5/OS od ostatních certifikátů podepsaných důvěryhodným vydavatelem certifikátů. Můžete například zadat e-mailovou adresu, kterou jste použili při přijetí certifikátu od dobře známého vydavatele certifikátů.
  - d. Stisknutím **OK** uložte změny.
4. Změňte heslo a dokončete inicializaci. Další informace najdete v tématu "Heslo servisního procesoru".

Chcete-li zabezpečení SSL zakázat, použijte výše uvedenou proceduru, ale vyberte volbu **Nepoužívat certifikát (vyžaduje fyzické zabezpečení)**.

## Heslo servisního procesoru

Chcete-li změnit heslo servisního procesoru, postupujte podle pokynů uvedených v tématu "Inicializace servisního procesoru" na stránce 120.

1. Vyberte volbu **Změnit ID a heslo uživatele servisního procesoru**.
2. Zadejte nové hodnoty do polí **Uživatel**, **Heslo** a **Potvrdit nové heslo**.
3. Stisknutím **Inicializovat** proveďte operaci.

## Konfigurace firewallu

Pokud je mezi serverem iSeries a sítí iSCSI firewall, musí být tento firewall konfigurován tak, aby dovolil průchod příchozího provozu virtuální sítě Ethernet. Hodnoty, které mají vliv na konfiguraci firewallu, jsou uvedeny níže:

**Pro cesty k paměťovým prostorům a připojení k virtuální síti Ethernet chráněné firewallem:**

l • **IP adresa vzdáleného systému:** Vlastnosti konfigurace vzdáleného systému pro server můžete zobrazit, použijte-li proceduru popsanou v tématu “Zobrazení vlastností konfigurace vzdáleného systému” na stránce 117. Přejděte na kartu **Síťová rozhraní** a poznamenejte si hodnoty v polích **Internetová adresa SCSI** a **Internetová adresa LAN**.

l • **IP adresa lokálního systému a port TCP:** Vlastnosti objektu NWSH můžete zobrazit, použijte-li proceduru popsanou v tématu “Zobrazení vlastností objektu NWSH” na stránce 114. Přejděte na kartu **Lokální rozhraní**. Zobrazí se informace, které objekt NWSH používá. Poznamenejte si následující hodnoty:

- l – Rozhraní lokální sítě SCSI: Internetová adresa.
- l – Rozhraní lokální sítě SCSI: Port TCP.
- l – Rozhraní lokální sítě LAN: Internetová adresa.
- l – Rozhraní lokální sítě LAN: Základní port virtuální sítě Ethernet.
- l – Rozhraní lokální sítě LAN: Horní port virtuální sítě Ethernet.

l **Poznámka:** Provoz virtuální sítě Ethernet je zapouzdřený v paketech UDP. Každému adaptéru virtuální sítě Ethernet je automaticky přiřazen port UDP z rozsahu, který začíná číslem zadaného základního portu virtuální sítě Ethernet a končí číslem základního portu virtuální sítě Ethernet zvýšeným o počet konfigurovaných adaptéru virtuální sítě Ethernet. Každému adaptéru virtuální sítě Ethernet je také přiřazen port UDP na Windows serveru. Porty UDP pro virtuální síť Ethernet jsou obvykle automaticky přidělovány systémem Windows. Chcete-li automatické přidělení potlačit, můžete port UDP přidělit manuálně provedením následujících kroků pomocí konzole Windows.

- l 1. Přejděte do okna **Síťová připojení**.
- l 2. Dvakrát klepněte na adaptér **IBM iSeries Virtual Ethernet x**, který chcete konfigurovat.
- l 3. Klepněte na **Vlastnosti**.
- l 4. Klepněte na **Konfigurace**.
- l 5. Klepněte na **Upřesnit**.
- l 6. Klepněte na **Port iniciátoru LAN UDP**.
- l 7. Zadejte port UDP, který má adaptér virtuální sítě Ethernet používat.

l • **Porty TCP přiřazené ke všem IP adresám lokálního systému:**

l V prostředí produktu iSeries Navigator:

- l 1. Rozbalte **Administrace integrovaných serverů**.
- l 2. Vyberte **Servery**.
- l 3. Klepněte pravým tlačítkem myši na server v zobrazeném seznamu a vyberte **Vlastnosti**.
- l 4. Přejděte na kartu **Systém** a klepněte na tlačítko **Rozšířené**.
- l 5. Poznamenejte si následující hodnoty:
  - l – **Port TCP pro ukončení práce systémem**.
  - l – **Řídicí port sítě Ethernet**.

l Je-li použito zabezpečení IPSec, existují další důvody pro použití firewallů mezi adaptérem iSCSI HBA a sítí iSCSI:

- l • **Povolit IPSec:** Tato volba není u všech firewallů k dispozici.
- l • Při konfiguraci firewallů by měly být brány v úvahu pouze IP adresy. Porty TCP a UDP jsou zašifrovány zabezpečením IPSec, a firewall tedy nemůže na tyto informace působit.

---

## Správa adaptérů iSCSI HBA

l Při správě adaptérů hostitele iSCSI (objektů NWSH) použijte následující postupy.

- l • “Výměna adaptérů v lokálním hostitelském systému iSCSI za chodu” na stránce 128
- l • “Správa využití adaptérů iSCSI HBA” na stránce 128
- l • “Posouzení velikosti maximální přenosové jednotky (MTU)” na stránce 131
- l • “Integrovaný server DHC” na stránce 133

## Výměna adaptérů v lokálním hostitelském systému iSCSI za chodu

Hardware adaptérů lokálního hostitelského systému iSCSI na serveru iSeries umožňuje výměnu za chodu. Zvyšuje tak spolehlivost a obnovitelnost prostředí Windows serveru. Selže-li adaptér lokálního hostitele, který je právě používán Windows serverem, můžete server snadno a rychle přepnout za chodu tak, aby používal jiný adaptér lokálního hostitele iSCSI. Zvyšuje také flexibilitu tím, že umožňuje použití jednoho "rezervního" adaptéru lokálního hostitele iSCSI jako ochrany adaptérů lokálního hostitele iSCSI s vícenásobným využitím.

**Poznámka:** Tato schopnost výměny adaptérů lokálního hostitele iSCSI za chodu doplňuje možnost výměny za chodu, která je poskytována pro hardware integrovaného serveru. Další informace najdete v tématu "Výměna hardwaru serveru za chodu" na stránce 148.

Chcete-li adaptéry lokálního hostitele iSCSI vyměnit za chodu pomocí produktu iSeries Navigator, postupujte takto:

1. Rozbalte **Administrace integrovaných serverů**.
2. Rozbalte **Připojení iSCSI**.
3. Vyberte **Adaptéry lokálního hostitele**.
4. V případě, že objekt NWSH, pro který chcete vyměnit hardware, ještě není zastaven:
  - Klepněte pravým tlačítkem myši na objekt NWSH a vyberte **Zastavit**.
  - Klepněte na **Zastavit** na potvrzovacím panelu.
  - Pokud aktivní servery objekt NWSH právě používají, zobrazí se varovná zpráva. Klepněte na **Pokračovat**.
5. Chcete-li změnit objekt NWSH tak, aby ukazoval na připravený volný adaptér lokálního hostitele, postupujte takto:
  - Klepněte pravým tlačítkem myši na objekt NWSH a vyberte **Vlastnosti**.
  - Vyberte kartu **Obecné** a vyberte novou hodnotu pro náznak **Hardwarový prostředek**.
  - Klepněte na **OK**.
6. Chcete-li objekt NWSH spustit, klepněte na něj pravým tlačítkem myši a vyberte **Spustit**.

Můžete také použít příkaz VRYCFG (Logické zapnutí/vypnutí konfigurace) a objekt NWSH logicky vypnout. Potom použijte CL příkaz CHGDEVNWSH (Změna popisu zařízení (NWSH)) a změňte hodnotu parametru RSRCNAME (Jméno prostředku). Uvedete tím jméno nového hardwarového prostředku.

## Správa využití adaptérů iSCSI HBA

K serveru iSeries můžete připojit několik hostovaných systémů (serverů xSeries nebo blade serverů IBM BladeCenter) pomocí jediného adaptéru iSCSI HBA na serveru iSeries. Můžete také k serveru iSeries připojit jeden hostovaný systém pomocí několika adaptérů iSCSI HBA pro server iSeries. Existuje několik způsobů konfigurace hostovaného systému, ve kterých je pro server iSeries použito několik adaptérů iSCSI HBA. Lze také použít kombinace těchto technik.

Informace o několika běžných konfiguracích najdete v následujících tématech:

- "Sdílení adaptéru iSCSI HBA několika hostovanými servery"
- "Rozložení zatížení na několik adaptérů iSCSI HBA" na stránce 129
- "Použití několika adaptérů iSCSI HBA za účelem redundance" na stránce 130
- "Správa alokací iSCSI HBA na straně Windows sítě iSCSI" na stránce 131

## Sdílení adaptéru iSCSI HBA několika hostovanými servery

Jeden adaptér iSCSI HBA pro server iSeries může obsluhovat zatížení několika serverů, které pro provoz sítě SCSI a virtuální sítě Ethernet LAN nevyžadují větší šířku pásma. Adaptér iSCSI HBA pro server iSeries může například sdílet několik vývojových a testovacích serverů, není-li jejich zatížení příliš velké.

Počet cest k paměťovým prostorům a cest k virtuální síti Ethernet, které iSCSI HBA může podporovat, je omezený. Každá cesta k paměťovým prostorům aktivního serveru bude používat prostředek souborového serveru v objektu NWSH, který odpovídá tomuto adaptéru iSCSI HBA. Podobně každá cesta k virtuální síti Ethernet na aktivním



l serveru bude používat prostředek virtuální sítě Ethernet v objektu NWSH. Počet prostředků souborového serveru a virtuální sítě Ethernet, které určitý objekt NWSH podporuje, je omezen. Je tedy omezen i počet aktivních serverů, které mohou tento objekt NWSH používat.

l Chcete-li zobrazit limity prostředků souborového serveru objektu NWSH a virtuální sítě Ethernet pomocí produktu iSeries Navigator, postupujte takto:

1. Rozbalte **Administrace integrovaných serverů**.
2. Rozbalte **Připojení iSCSI**.
3. Vyberte **Adaptéry lokálního hostitele**.
4. Klepněte pravým tlačítkem myši na objekt NWSH v zobrazeném seznamu.
5. Vyberte **Vlastnosti**.
6. Klepněte na kartu **Využití prostředků**.
7. Zobrazená tabulka ukazuje aktivní servery, které právě používají objekt NWSH a prostředky souborového serveru a virtuální sítě Ethernet, které aktivní servery právě používají. Pod tabulkou je uveden počet prostředků souborového serveru a virtuální sítě Ethernet, které jsou ještě k dispozici pro použití aktivními servery, a celkový počet prostředků souborového serveru a virtuální sítě Ethernet, které objekt NWSH podporuje.
8. Klepnutím na **Zrušit** na panelu vlastností objektu NWSH tento panel zavřete.

l Chcete-li použít CL příkaz, podívejte se na příkazy WRKDEVD a DSPDEVD.

l Existuje také praktické omezení počtu serverů, které může iSCSI HBA podporovat. Není však přesně definováno. Toto praktické omezení je určeno dostupnou šířkou pásma adaptéru iSCSI HBA a zatížením, které adaptér iSCSI HBA právě zpracovává. Toto praktické omezení bude mít pravděpodobně vliv na počet hostovaných systémů, které může adaptér iSCSI HBA podporovat, než bude dosaženo limitu prostředků souborových serverů a virtuální sítě Ethernet. Praktické omezení závisí na konfiguraci a zatížení konkrétního serveru.

## l **Rozložení zatížení na několik adaptérů iSCSI HBA**

l Servery, které požadují větší šířku pásma, mohou vyžadovat více než jeden adaptér iSCSI HBA, aby mohl server iSeries zpracovávat zatížení. Můžete provést další segmentaci, označíte-li, které virtuální disky a virtuální sítě Ethernet LAN vyžadují větší šířku pásma a které ne. Můžete například adaptéru iSCSI HBA vyhradit disk, který potřebuje větší šířku pásma a sdílet jiný adaptér iSCSI HBA s disky nebo jinými servery, které větší šířku pásma nevyžadují.

l Způsob, jakým je zatížení sítě SCSI a virtuální sítě Ethernet serveru rozloženo na několika adaptérech iSCSI HBA, znamená definovat vícenásobné cesty k paměťovým prostorům nebo k virtuální síti Ethernet v popisu síťového serveru (NWS) a určit, které virtuální disky a virtuální sítě Ethernet budou jednotlivé cesty používat.

l Chcete-li definovat další cesty k paměťovým prostorům pomocí produktu iSeries Navigator, ukončete nejprve práci serveru (viz “Spuštění a zastavení integrovaného serveru” na stránce 141), potom postupujte takto:

1. Rozbalte **Administrace integrovaných serverů**.
2. Rozbalte **Servery**.
3. Klepněte pravým tlačítkem myši na server v zobrazeném seznamu.
4. Vyberte **Vlastnosti**.
5. Klepněte na kartu **Cesty k paměťovým prostorům**.
6. Klepnutím na tlačítko **Přidat** definujte novou cestu k paměťovým prostorům.
7. Vyberte objekt NWSH (adaptér hostitele síťového serveru), který odpovídá adaptéru iSCSI HBA, který chcete používat pro cestu k paměťovým prostorům.
8. Klepnutím na **OK** přidejte cestu k paměťovým prostorům do panelu vlastností serveru.
9. Poznamenejte si číslo cesty, které je přiřazeno nové cestě. Číslo cesty umožňuje tuto cestu rozpoznat, až budete později propojovat disky.
10. Klepnutím na **OK** na panelu vlastností serveru uložte novou cestu k paměťovým prostorům do objektu NWS.

l Chcete-li použít CL příkaz, prostudujte klíčové slovo STGPTH v příkazu CHGNWS.

l Je-li již nová cesta k paměťovým prostorům definovaná, potřebujete znovu připojit jeden nebo více virtuálních disků serveru tak, aby tuto novou cestu k paměťovým prostorům používaly. Nejprve disk odpojte (viz “Odpojení diskových jednotek integrovaného Windows serveru” na stránce 160). Potom disk znovu propojte se serverem (viz “Propojení diskové jednotky s integrovaným serverem” na stránce 157) pomocí čísla nové cesty k paměťovým prostorům, která již byla přidána.

l Chcete-li definovat další cesty k virtuální síti Ethernet pomocí produktu iSeries Navigator, ukončete nejprve práci serveru (viz “Spuštění a zastavení integrovaného serveru” na stránce 141), potom postupujte takto:

1. Rozbalte **Administrace integrovaných serverů**.
2. Rozbalte **Servery**.
3. Klepněte pravým tlačítkem myši na server v zobrazeném seznamu.
4. Vyberte **Vlastnosti**.
5. Klepněte na kartu **Virtuální síť Ethernet**.
6. Vyberte port virtuální síť Ethernet, pro který chcete novou cestu použít, a klepněte na tlačítko **Vlastnosti**.
7. Vyberte objekt NWSH, který chcete použít pro port virtuální síť Ethernet.
8. Klepnutím na **OK** aktualizujte informace o portu virtuální síť Ethernet na panelu vlastností serveru. Cesta k virtuální síti Ethernet pro tento port bude také implicitně aktualizována.
9. Klepnutím na **OK** na panelu vlastností serveru uložte změny objektu NWSD.

l Chcete-li použít CL příkaz, prostudujte klíčové slovo VRTETHPTH v příkazu CHGNWSD.

### **Použití několika adaptérů iSCSI HBA za účelem redundance**

l I když požadavky serveru na šířku pásma nenaznačují, že by byl potřebný více než jeden adaptér iSCSI HBA pro server iSeries, můžete použít několik adaptérů iSCSI HBA, abyste zajistili odolnost proti chybám a redundanci. Sníží se tak pravděpodobnost selhání serveru, která jsou způsobena selháním adaptéru iSCSI HBA nebo jedné ze síťových komponent (přepínače, kabely apod.), které připojují server iSeries k hostovanému systému. Redundance je zajištěna schopností sítě iSCSI provádět I/O operace přes více cest (viz “Rozšířená podpora sítě iSCSI” na stránce 20). Výhody I/O operací přes více cest můžete využít, vytvoříte-li skupinu několika cest, která rozpozná dva nebo více adaptérů iSCSI HBA. Potom určete, které virtuální disky budou tuto skupinu cest používat. Skupinu několika cest můžete volitelně použít jako předvolenou cestu při připojování diskových jednotek.

l Chcete-li definovat skupinu cest pomocí produktu iSeries Navigator, ukončete nejprve práci serveru (viz “Spuštění a zastavení integrovaného serveru” na stránce 141), potom postupujte takto:

1. Rozbalte **Administrace integrovaných serverů**.
2. Rozbalte **Servery**.
3. Klepněte pravým tlačítkem myši na server v zobrazeném seznamu.
4. Vyberte **Vlastnosti**.
5. Klepněte na kartu **Cesty k paměťovým prostorům**.
6. Definujte alespoň dvě cesty k paměťovým prostorům (v případě potřeby použijte tlačítko **Přidat**).
7. Pod tabulkou cest k paměťovým prostorům klepněte na tlačítko **Vlastnosti** pro skupinu několika cest.
8. Zaškrtnutím příslušných okének označte dvě nebo více definovaných cest k paměťovým prostorům, které budou členy skupiny cest.
9. Klepnutím na **OK** aktualizujte informace o skupině cest na panelu vlastností serveru.
10. **Volitelné:** Vyberte skupinu cest jako předvolenou cestu pro diskové jednotky.
11. Klepnutím na **OK** na panelu vlastností serveru uložte změny objektu NWSD.

l Chcete-li použít CL příkaz, prostudujte klíčová slova MLTPHGRP a DFTSTGPTH v příkazu CHGNWSD.

l Je-li již nová skupina cest definovaná, potřebujete znovu připojit jeden nebo více virtuálních disků serveru tak, aby tuto novou skupinu cest používaly. Nejprve disk odpojte (viz “Odpojení diskových jednotek integrovaného Windows serveru” na stránce 160). Potom disk znovu propojte se serverem (viz “Propojení diskové jednotky s integrovaným



serverem” na stránce 157), zadejte přitom buď explicitně skupinu cest, nebo předvolenou cestu (pokud předvolená cesta pro diskové jednotky byla definována tak, aby používala skupinu cest).

## **Správa alokací iSCSI HBA na straně Windows sítě iSCSI**

Windows server může mít několik fyzických portů iSCSI HBA. Portem iSCSI HBA mohou procházet přenosy pro cesty k paměťovým prostorům a k virtuální síti Ethernet na serveru iSeries. Povahu přenosů, které procházejí jednotlivými porty iSCSI HBA na Windows serveru ovlivňuje mnoho faktorů.

### **IP adresy**

Porty iSCSI HBA mohou mít IP adresy v síti SCSI, v síti LAN nebo obojí. Port s IP adresou v síti SCSI je kandidátem pro průchod paměťových přenosů. Port s IP adresou v síti LAN je kandidátem pro průchod přenosů virtuální sítě Ethernet.

### **Konfigurace zaváděcí paměti**

Vyberete port iSCSI HBA, který bude obsluhán programem CTRL-Q používán při zavádění Windows. Až bude systém Windows zaveden, vybraný port iSCSI HBA bude nadále zajišťovat připojení k cestám k paměťovým prostorům serveru iSeries, které odpovídají systémové jednotce.

### **Automatické přidělení portů iSCSI HBA k virtuální síti Ethernet a cestám k paměťovým prostorům, které nejsou určeny pro zavádění systému**

Prostředí Windows na serveru iSeries zahrnuje programy, které se spouštějí ve Windows a které automaticky načtou objekty operačního systému i5/OS s informacemi o konfiguraci serveru. Adaptéry iSCSI HBA pro server iSeries jsou konfigurovány v objektech operačního systému i5/OS na rozdíl od portů iSCSI HBA pro hostovaný systém. Místo toho programy automaticky přidělují porty iSCSI HBA virtuální síti Ethernet a cestám k paměťovým prostorům, které nejsou určeny pro zavádění systému.

### **Manuální přidělení adaptéru virtuální sítě Ethernet k fyzickému portu iSCSI HBA**

Chcete-li automatické přidělení potlačit, můžete port iSCSI HBA přidělit manuálně provedením následujících kroků na konzoli Windows.

1. Přejděte do okna **Síťová připojení**.
2. Dvakrát klepněte na adaptér **IBM iSeries Virtual Ethernet x**, který chcete konfigurovat.
3. Klepněte na **Vlastnosti**.
4. Klepněte na **Konfigurace**.
5. Klepněte na **Upřesnit**.
6. Klepněte na **Initiator LAN IP Address**.
7. Zadejte IP adresu portu iSCSI HBA ve Windows, kterým se má adaptér virtuální sítě Ethernet fyzicky připojit.

## **Posouzení velikosti maximální přenosové jednotky (MTU)**

**Poznámka:** Velikosti rámců, o kterých zde diskutujeme, nezahrnují 14bajtové záhlaví MAC Ethernet.

Na rozdíl od 9000bajtových rámců typu jumbo, které jsou poskytovány na serverech IXS a serverech připojených pomocí IXA, je předvolená velikost rámce virtuální sítě Ethernet v systémech připojených pomocí sítě iSCSI menší a lze tedy tyto rámce přenášet ve standardním 1500bajtovém rámci Ethernet.

Povoluje-li síť iSCSI větší velikost rámců, můžete konfigurovat virtuální síť Ethernet tak, aby používala větší velikost rámců až do 9000 bajtů, což zvyšuje výkon. Ve složité síti iSCSI může být několik různých maximálních velikostí rámců v závislosti na topologii sítě a složitosti vybavení.

| **Poznámka:** Náznaky MTU v příkazu INSWNTSVR (Instalace Windows serveru) nemají žádný dopad s výjimkou  
| externích adaptérů LAN používaných u IXS.

| Informace o konfiguraci MTU najdete v následujících tématech:

- | • “Konfigurace virtuální sítě Ethernet na maximální výkon v sítích iSCSI, které podporují rámce větší než 1500 bajtů”
- | • “Konfigurace virtuální sítě Ethernet pro sítě iSCSI, které mají maximální velikost rámce menší než 1500 bajtů”
- | • “Konfigurace virtuální sítě Ethernet, která podporuje neobvyklé aplikace nevyužívající TCP a nevyjednávající MTU”

## | **Konfigurace virtuální sítě Ethernet na maximální výkon v sítích iSCSI, které podporují rámce větší než 1500 bajtů**

| Na konzoli Windows proveďte následující kroky:

- | 1. Přejděte do okna **Síťová připojení**.
- | 2. Dvakrát klepněte na adaptér iSCSI, který je připojen k síti iSCSI podporující rámce větší než 1500 bajtů.
- | 3. Klepněte na **Vlastnosti**.
- | 4. Klepněte na **Konfigurace**.
- | 5. Klepněte na **Upřesnit**.
- | 6. Klepněte na **Ethernet Frame Size**.
- | 7. Vyberte co možná největší hodnotu, která nepřekračuje maximální velikost rámce sítě iSCSI.

| **Poznámka:** Níže uvedené související položky konfigurace by měly mít předvolené hodnoty:

- | • Pro adaptéry virtuální sítě Ethernet ve Windows je předvolbou položky Maximum Frame Size hodnota Auto. Hodnota Auto způsobí, že virtuální síť Ethernet vypočítá maximální velikost rámce na základě položky Ethernet Frame Size použitého portu iSCSI HBA. Vysvětlení použití portu iSCSI HBA najdete v tématu “Správa alokací iSCSI HBA na straně Windows sítě iSCSI” na stránce 131.
- | • V popisech linky virtuální sítě Ethernet v operačním systému i5/OS je předvolbou položky **MAXFRAME (Maximální velikost rámce)** hodnota **8996**.
- | • V rozhraních TCP/IP pro virtuální síť Ethernet v operačním systému i5/OS je předvolbou položky **MTU (Maximální přenosová jednotka)** hodnota **\*LIND**.

## | **Konfigurace virtuální sítě Ethernet pro sítě iSCSI, které mají maximální velikost rámce menší než 1500 bajtů**

| Na konzoli Windows proveďte následující kroky:

- | 1. Přejděte do okna **Síťová připojení**.
- | 2. Dvakrát klepněte na adaptér **IBM iSeries Virtual Ethernet x**, který bude používat iSCSI HBA připojený k síti iSCSI s maximální velikostí rámce menší než 1500 bajtů.
- | 3. Klepněte na **Vlastnosti**.
- | 4. Klepněte na **Konfigurace**.
- | 5. Klepněte na **Upřesnit**.
- | 6. Klepněte na **Maximální velikost rámce**.
- | 7. Vyberte co možná největší hodnotu, která nepřekračuje maximální velikost rámce sítě iSCSI.

## | **Konfigurace virtuální sítě Ethernet, která podporuje neobvyklé aplikace nevyužívající TCP a nevyjednávající MTU**

| **Poznámka:** Chcete-li zabránit ovlivnění obvyklých aplikací, které vyjednávají MTU, můžete pro aplikaci, která  
| nevyjednává MTU, definovat před provedením této procedury samostatné IP adresy virtuální sítě Ethernet  
| nebo samostatné IP adresy .

- | 1. Proveďte jednu z následujících akcí.

- a. Budou-li všechny koncové body systému Windows používat síť iSCSI s maximální velikostí rámce 1500 bajtů nebo větší, nakonfigurujte položku Ethernet frame size pro adaptér iSCSI HBA ve všech koncových bodech systému Windows na co největší hodnotu, která nepřekročí vynucenou maximální velikost rámce sítě iSCSI.
  - b. Bude-li libovolný koncový bod systému Windows používat síť iSCSI s maximální velikostí rámce 1500 bajtů, nakonfigurujte položku Maximum frame size pro virtuální síť Ethernet ve všech koncových bodech systému Windows na co největší hodnotu, která nepřekročí vynucenou maximální velikost rámce sítě iSCSI.
2. V ostatních koncových bodech nastavte MTU na hodnotu, kterou dostanete odečtením hodnoty 116 od menší z hodnot Ethernet frame size pro adaptér iSCSI HBA ve Windows a Maximum frame size pro virtuální síť Ethernet. Pro koncové body operačního systému i5/OS toho můžete dosáhnout následujícím postupem.
- a. V prostředí produktu iSeries Navigator rozbalte **Síť** → **Konfigurace TCP/IP** → **IPv4** → **Rozhraní**.
  - b. Klepněte pravým tlačítkem myši na požadované rozhraní s IP adresou a jménem popisu linky a vyberte **Vlastnosti**.
  - c. Na kartě **Rozšířené** zadejte vypočítanou hodnotu do pole Maximální přenosová jednotka a klepnutím na **OK** uložte změnu.

**Poznámka:** Chcete-li použít rozhraní příkazového řádku, použijte příkaz CFGTCP a vyberte volbu 1, Práce s rozhraními TCP/IP.

## Integrovaný server DHC

Řešení se serverem iSeries připojeným pomocí iSCSI poskytuje integrovaný server DHCP. Tento server je určen k instalaci zaváděcích parametrů do adaptéru iSCSI HBA hostovaného systému v případě, že je ve vzdáleném objektu konfigurace vzdáleného systému v i5/OS vybrána volba Dynamicky doručené do vzdáleného systému pomocí DHCP a na serveru hostitele adaptéru iSCSI HBA je zadán režim AUTO nebo DHCP.

Integrovaný server DHCP není server pro obecné účely. Je určen výhradně pro instalaci zaváděcích parametrů do adaptéru iSCSI HBA hostovaného serveru. Tento server je automaticky konfigurován při logickém zapnutí objektu NWS D s parametry, které poskytuje konfigurace vzdáleného systému.

Server DHCP odpovídá pouze hostovanému klientovi DHCP adaptéru iSCSI HBA serveru. Všechny požadavky klienta DHCP adaptéru iSCSI HBA používají ID prodejce definované IBM. Server je naprogramován tak, aby odpovídal na požadavky, které používají předvolený ID prodejce. Všechny ostatní požadavky jiných zařízení v síti budou serverem DHCP ignorovány.

Poskytování adres MAC hostovaných adaptéru iSCSI HBA serveru v objektu konfigurace vzdáleného systému je velice důležité. Aby mohl integrovaný server DHCP řádně instalovat zaváděcí parametry, používá kromě výše popsaného ID prodejce také adresu MAC. Adresa MAC je částí specifického rozsahu, který zajišťuje řádnou instalaci parametrů.

Tento rozsah určený pomocí ID prodejce a adresy MAC můžete změnit. I když je tato změna považována za rozšířenou funkci, byla učiněna opatření, která zkušeným uživatelům umožní provést v případě potřeby vlastní konfiguraci tohoto nastavení. Předvolenou hodnotu ID prodejce lze konfigurovat na jinou hodnotu. Obrazovky konfigurace jsou k dispozici v obslužném programu CTRL-Q na serveru hostitele adaptéru iSCSI HBA a v příslušném objektu konfigurace vzdáleného systému. Tato rozšířená funkce vyhovuje specifikaci RFC 2132.

Podrobnější informace o rozšířených konfiguracích najdete v publikaci iSCSI install read me first 

Přijme-li integrovaný server příchozí požadavek DHCP a odpovídají-li všechny požadované rozsahy, integrovaný server DHCP dodá klientovi DHCP IP adresu cílového zaváděcího zařízení. Cílovým zaváděcím zařízením je objekt NWSH (adaptér hostitele síťového serveru) s nakonfigurovaným virtuálním zaváděcím diskem. Tento server také dodává IP adresu pro iniciátor nebo klienta DHCP. Iniciátor je adaptér iSCSI HBA na serveru hostitele, který bude použit při zavádění systému přes síť iSCSI.

Integrovaný server DHCP navíc zajišťuje jedinečná jména IQN (kvalifikovaná jména sítě iSCSI), která představují cílové zařízení a zařízení adaptéru iniciátoru iSCSI HBA v systému hostitele.

Obě tyto množiny IP adres a jmen IQN jsou v objektech konfigurace serveru iSeries, které definují server hostitele. IP adresa cíle je definována v objektu NWSH. IP adresa a jméno IQN iniciátoru jsou definovány v objektu konfigurace vzdáleného systému. Jméno IQN cíle je automaticky konfigurováno a definováno v objektu NWSD. Další informace o těchto objektech najdete v tématu “Popis síťového serveru” na stránce 42.

Integrovaný server DHCP je klíčovou a integrální komponentou při implementaci výměny serverů za chodu. Režim zavádění systému na serveru DHCP umožňuje instalovat požadované parametry definované v softwarových objektech serveru iSeries, aniž by bylo nutné server manuálně konfigurovat při změně zaváděcích parametrů (IP adres a jmen).

---

## Zjišťování vzdálených serverů a jejich správa

Při vyhledávání a správě připojených serverů se používá produkt IBM Director a informace z objektů konfigurací vzdálených systémů a servisních procesorů operačního systému i5/OS. Prostudujte následující informace.

- “Instalace a konfigurace produktu IBM Director”
- “Zjišťování vzdálených serverů a servisních procesorů” na stránce 135
  - “Konfigurace zjišťování servisních procesorů” na stránce 135
  - “Dynamické IP adresování (DHCP)” na stránce 137
  - “Metody zjišťování servisních procesorů” na stránce 137
- “Použití webového rozhraní modulu Management Module a adaptéru RSA II” na stránce 139

## Instalace a konfigurace produktu IBM Director

Produkt IBM Director je používán při zjišťování vzdálených serverů a správě serverů připojených pomocí iSCSI. Není nutno použít žádné rozhraní produktu IBM Director, produkt IBM Director stačí jen nainstalovat a spustit. Informace o instalaci produktu IBM Director najdete v tématu “Softwarové požadavky” na stránce 57.

Prostředí Windows na serveru iSeries používá produkt IBM Director pro tyto účely:

- **Zjišťování vzdálených serverů a servisních procesorů**  
Vyhledání serveru v síti
- **Řízení napájení**  
Zapnutí serveru nebo ukončení práce odpovídajícího operačního systému i5/OS pomocí příkazů Logické zapnutí/vypnutí konfigurace.
- **Vyvolání stavu napájení**
- **Konfigurace vzdáleného serveru**  
Některé funkce vzdáleného serveru lze konfigurovat na serveru iSeries vzdáleně prostřednictvím servisního procesoru serveru.

Produkt IBM Director závisí na TCP/IP. Produkt IBM Director nemůže pracovat správně, není-li spuštěno rozhraní TCP/IP. Protože produkt IBM Director je server TCP v systému i5/OS, lze jej konfigurovat tak, aby se automaticky spustil při spuštění TCP. Doporučuje se, aby byl server TCP produktu IBM Director konfigurován tak, aby se spouštěl automaticky. Bude tak zajištěno, že bude produkt IBM Director k dispozici, až jej bude adaptér iSCSI HBA pro server iSeries potřebovat.

Chcete-li konfigurovat server TCP produktu IBM Director tak, aby se automaticky spouštěl při spuštění TCP/IP, proveďte v prostředí produktu iSeries Navigator následující kroky:

1. Vyberte **Síť -> Servery -> Uživatelsky definované**.
2. Klepněte pravým tlačítkem myši na **IBM DIRECTOR** a vyberte **Vlastnosti**.
3. Vyberte volbu **Spustit při spuštění TCP/IP**.
4. Klepněte na **OK**.

Můžete také použít příkaz CHGTCPSPVR (Změna serveru TCP/IP).

l Nespouští-li se IBM Director automaticky, spusťte server TCP produktu IBM Director v prostředí produktu iSeries Navigator:

- l 1. Vyberte **Síť -> Servery -> Uživatelsky definované**.
- l 2. Klepněte pravým tlačítkem myši na **IBM DIRECTOR** a vyberte **Spustit**.

l **Poznámka:** Serveru IBM Director bude trvat několik minut nebo i déle, než se spustí. Stav procesu spouštění můžete zobrazit, obnovíte-li seznam produktu iSeries Navigator. Opakujte tuto akci, dokud server IBM DIRECTOR nezobrazí stav Spuštěn.

## l **Zjišťování vzdálených serverů a servisních procesorů**

l Operační systém i5/OS používá produkt IBM Director při vyhledávání a rozpoznávání vzdálených serverů v síti LAN pomocí komunikace se servisním procesorem vzdáleného serveru. Vzdálené systémy jsou rozpoznávány podle informací uložených v objektech konfigurace vzdáleného systému a konfigurace servisního procesoru serveru iSeries.

l Jedná se o odlišné spojení, než je spojení mezi cílovým adaptérem sítě iSCSI na serveru iSeries a adaptérem iniciátoru sítě iSCSI na vzdáleném serveru. Adaptér sítě LAN pro servisní procesor vzdáleného serveru musí být připojen k síti, která je přístupná adaptéru sítě LAN na serveru iSeries.


l Jak objekty operačního systému i5/OS, tak objekty servisního procesoru musejí být konfigurovány. Můžete konfigurovat metodu zjišťování použitou v objektech konfigurace síťových serverů operačního systému i5/OS.

l Prostudujte následující informace:

- l • “Konfigurace zjišťování servisních procesorů”
- l • “Dynamické IP adresování (DHCP)” na stránce 137
- l • “Metody zjišťování servisních procesorů” na stránce 137
- l • “Použití webového rozhraní modulu Management Module a adaptéru RSA II” na stránce 139

## l **Konfigurace zjišťování servisních procesorů**

l Informace o servisním procesoru v protokolu IP musejí být konfigurovány tak, aby odpovídaly konfiguraci operačního systému i5/OS. Volby konfigurace závisejí na typu servisního procesoru. Informace o rozpoznání typu servisního

l procesoru na serveru xSeries najdete v dokumentu [xSeries and BladeCenter models supported with iSCSI](http://www.ibm.com/servers/eserver/series/integratedxseries/iscsiservermodels/)  (www.ibm.com/servers/eserver/series/integratedxseries/iscsiservermodels/)

## l **Řadič BMC (Baseboard Management Controller)**



l U některých modelů serveru xSeries je k dispozici servisní procesor s řadičem BMC.

- l • Při konfiguraci BMC použijte menu nastavení systému BIOS.
- l • BMC podporuje statické IP adresování.
- l • BMC podporuje zjišťování podle IP adres. Další informace najdete v tématu “Zjišťování podle IP adresy” na stránce 138.
- l • BMC podporuje zabezpečení heslem. Další informace najdete v tématu “Heslo servisního procesoru” na stránce 126.

## l **Adaptér RSA II (Remote Supervisor Adapter II)**

l U některých modelů serveru xSeries je k dispozici servisní procesor s adaptérem RSA II.

- l • Při konfiguraci RSA II proveďte jednu z následujících akcí.
  - l – Použijte menu nastavení systému BIOS. Tuto metodu nelze použít při konfiguraci jména hostitele.
  - l – Další informace najdete v tématu “Použití webového rozhraní modulu Management Module a adaptéru RSA II” na stránce 139.


- | • Adaptér RSA II může získat informace o IP adrese pomocí jedné z následujících metod. Použijte tu, která nejlépe odpovídá vaší síti.
  - | – “Dynamické IP adresování (DHCP)” na stránce 137. Tato metoda je předvolena výrobcem.
  - | – Statické IP adresování.
- | • RSA II podporuje následující metody zjišťování. Použijte tu, která nejlépe odpovídá vaší síti.
  - | – “Protokol SLP (Service Location Protocol) s využitím výběrového adresování” na stránce 137.
  - | – “Zjišťování podle IP adresy” na stránce 138.
  - | – “Zjišťování podle jména” na stránce 138.
- | • RSA II podporuje následující metody zabezpečení:
  - | – Heslo. Postup konfigurace najdete v tématu “Heslo servisního procesoru” na stránce 126.
  - | – Zabezpečení SSL a heslo. Další informace najdete v tématu “Konfigurace zabezpečení SSL servisního procesoru” na stránce 125.
- | • Další informace o adaptéru RSA II najdete v následujících publikacích.
  - | – IBM Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II Installation Guide - Servers  (www.ibm.com/pc/support/site.wss/). Pod nadpisem **Procházet** vyberte **Servery**, Skupina: **xSeries 236**, Typ: **Všechny typy, Pokračovat**. Vyberte **Publikace**.
  - | – IBM Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User’s Guide - Servers  (www.ibm.com/pc/support/site.wss/). Pod nadpisem **Procházet** vyberte **Servery**, Skupina: **xSeries 236**, Typ: **Všechny typy, Pokračovat**. Vyberte **Publikace**.

## | Management Module

| Management Module je k dispozici na serverech IBM BladeCenter.

- | • Chcete-li Management Module konfigurovat, prostudujte část “Použití webového rozhraní modulu Management Module a adaptéru RSA II” na stránce 139.
- | • Management Module může získat informace o IP adrese pomocí jedné z následujících metod. Použijte tu, která nejlépe odpovídá vaší síti.
  - | – “Dynamické IP adresování (DHCP)” na stránce 137. Tato metoda je předvolena výrobcem.
  - | – Statické IP adresování.
- | • Management Module podporuje následující metody zjišťování. Použijte tu, která nejlépe odpovídá vaší síti.
  - | – “Protokol SLP (Service Location Protocol) s využitím výběrového adresování” na stránce 137
  - | – “Zjišťování podle IP adresy” na stránce 138.
  - | – “Zjišťování podle jména” na stránce 138
- | • Servery IBM BladeCenter mají další pravidla pro zjišťování. Identita vzdáleného systému v konfiguraci vzdáleného systému musí být vždy nastavena na sériové číslo serveru IBM BladeCenter, které je uvedeno na štítku na serveru. Informace o změně konfigurace vzdáleného systému najdete v tématu “Změna vlastností konfigurace vzdáleného systému” na stránce 117. Identita krytu v konfiguraci servisního procesoru může být pro každý blade server nastavena na sériové číslo krytu (skříně) IBM BladeCenter. Servisní procesor modulu Management Module v systému IBM BladeCenter musí být zjištěn dříve, než mohou být zjišťovány libovolné blade servery. Parametry v konfiguraci servisního procesoru určuje metodu zjišťování u modulu Management Module. Informace o změně těchto vlastností najdete v tématu “Změna vlastností konfigurace servisního procesoru” na stránce 120. Až bude Management Module zjištěn, shromáždí IBM Director informace o blade serverech obsažených v krytu. Při provádění druhé fáze zjišťování bude použita identita vzdáleného systému, aby mohl být zjištěn konkrétní blade server.
- | • Management Module II podporuje následující metody zabezpečení:
  - | – Heslo. Další informace najdete v tématu “Heslo servisního procesoru” na stránce 126.
  - | – Zabezpečení SSL a heslo. Další informace najdete v tématu “Konfigurace zabezpečení SSL servisního procesoru” na stránce 125.



- V Červené knize IBM BladeCenter Systems Management  (www.redbooks.ibm.com/abstracts/redp3582.html) najdete další informace o produktu IBM eServer BladeCenter Systems Management.

## Dynamické IP adresování (DHCP)

Servisní procesor, který používá DHCP, se okamžitě inicializuje, až bude server napájen a spustí proces DHCP. Nelze-li získat adresu pomocí DHCP, použije servisní procesor předvolenou statickou IP adresu 192.168.70.125.

**Poznámka:** Nepodaří-li se servisnímu procesoru získat IP adresu pomocí DHCP, může být tento proces restartován pouze vypnutím napájení a opětným zapnutím.

## Metody zjišťování servisních procesorů

Zjišťování servisních procesorů lze provádět několika způsoby.

- “Protokol SLP (Service Location Protocol) s využitím výběrového adresování”
- “Zjišťování podle IP adresy” na stránce 138
- “Zjišťování podle jména” na stránce 138

**Protokol SLP (Service Location Protocol) s využitím výběrového adresování:** Pokud při zjišťování serveru v síti nepoužíváte jméno hostitele servisního procesoru ani internetovou adresu, použije se výběrového adresování s protokolem SLP (Service Location Protocol). Chcete-li konfigurovat zjišťování pomocí protokolu SLP, musíte konfigurovat svůj server iSeries. Postupujte takto:

1. Postupujte podle pokynů uvedených v tématu “Změna vlastností konfigurace servisního procesoru” na stránce 120:
  - a. Zajistěte, aby nebyla vybrána volba **Použití připojení servisního procesoru při určení identity krytu vzdáleného systému**.
  - b. Do pole **Sériové číslo** zadejte sériové číslo krytu samostatného serveru nebo skříně serveru IBM BladeCenter.
2. Pomocí procedury popsané v tématu “Změna vlastností konfigurace vzdáleného systému” na stránce 117 zajistěte, aby identita vzdáleného systému byla nastavena správně:
  - a. Pro samostatný server vyberte volbu **Použití identity krytu z konfigurace servisního procesoru**.
  - b. Pro blade server IBM BladeCenter vyberte volbu **Použití následující hodnoty** a zadejte sériové číslo blade serveru.

Servisní procesor o sobě dává vědět pomocí paketu SLP odeslaného do sítě pomocí výběrového adresování. Tento paket zahrnuje atributy, jako jsou například sériové číslo, typ a model vzdáleného serveru. IBM Director tento paket přijme a uloží informace o serveru. Sériová čísla z identifikátoru přílohy konfigurace servisního procesoru a z identifikátoru vzdáleného systému v konfiguraci vzdáleného systému jsou namapována na atributy získané v procesu zjišťování pomocí protokolu SLP při identifikaci určitého vzdáleného serveru.

Výhody:

- Při zjišťování vzdáleného serveru potřebujete pouze sériové číslo, které lze získat ze štítku na serveru.
- Získá-li servisní procesor IP adresu ze serveru DHCP a podporuje-li síť výběrové vysílání, pak lze použít předvolené nastavení servisního procesoru od výrobce.

Nevýhody:

- Protokol SLP je podporován pouze servisními procesory s adaptérem RSA II a servisními procesory modulu Management Module serveru IBM BladeCenter. Není podporován servisními procesory s řadiči BMC.
- Směrovače a prepínače mezi servisními procesory a adaptérem sítě LAN na serveru iSeries musejí být konfigurovány tak, aby podporovaly výběrové adresování. Pokud nebudou řádně konfigurovány, nebudou směrovače přenášet pakety výběrového vysílání. Chcete-li zjistit, jak provést konfiguraci, která by umožňovala výběrové adresování, prostudujte dokumentaci svého směrovače. Protokol SLP (Service Location Protocol) používá IP adresu 239.255.255.253 a číslo portu 427. Při konfiguraci směrovačů, která podporuje pakety SLP výběrového vysílání, mohou být tyto informace vyžadovány.



| **Zjišťování podle IP adresy:** Tato metoda zjišťování používá adresování unicast. Při konfiguraci zjišťování podle IP adresy postupujte takto.

- | 1. V hostovaném systému proveďte konfiguraci statické IP adresy, která je vhodná pro síť v servisním procesoru. Pokud je to možné, proveďte tento krok před připojením servisního procesoru k síti LAN. Použijte buď menu nastavení systému BIOS, nebo webové rozhraní podle toho, kterou z těchto možností váš servisní procesor podporuje. Podrobnosti o připojení a použití webového prohlížeče najdete v tématu “Použití webového rozhraní modulu Management Module a adaptéru RSA II” na stránce 139.
- | 2. Na serveru iSeries proveďte konfiguraci servisního procesoru:
  - | a. Zajistěte, aby byla zaškrtnuta volba **Použit připojení servisního procesoru při určování identity krytu vzdáleného systému**.
  - | b. Vyberte volbu **Internetová adresa** a zadejte IP adresu servisního procesoru.
  - | c. (Volitelné) Zadejte sériové číslo samostatného serveru nebo sériové číslo skříně serveru IBM BladeCenter. Bude-li sériové číslo servisního procesoru zjištěného podle IP adresy odlišné od konfigurovaného sériového čísla, dojde k chybě.

| Další informace najdete v tématu “Změna vlastností konfigurace servisního procesoru” na stránce 120.

- | 3. Pomocí procedury popsané v tématu “Změna vlastností konfigurace vzdáleného systému” na stránce 117 zajistěte, aby identita vzdáleného systému byla nastavena správně:
  - | • Pro samostatný server vyberte volbu **Použit identitu krytu z konfigurace servisního procesoru**.
  - | • Pro blade server IBM BladeCenter vyberte volbu **Použit následující hodnoty** a zadejte sériové číslo blade serveru.

| Výhody:

- | • Tato metoda zjišťování je velice jednoduchá, je-li IP adresa servisního procesoru známa a konfigurována v servisním procesoru.

| Nevýhody:

- | • IP adresa musí být konfigurována v servisním procesoru.

| **Zjišťování podle jména:** Tato metoda zjišťování používá adresování unicast. Při konfiguraci zjišťování podle jména hostitele postupujte takto.

- | 1. V hostovaném systému proveďte konfiguraci jména hostitele statické IP adresy v servisním procesoru. Pokud je to možné, proveďte tento krok před připojením servisního procesoru k síti LAN.
  - | a. V tomto kroku musíte použít webové rozhraní. Při připojování k webovému rozhraní RSA II použijte aktuální IP adresu. Podrobnosti o připojení a použití webového prohlížeče najdete v tématu “Použití webového rozhraní modulu Management Module a adaptéru RSA II” na stránce 139.
  - | b. V prohlížeči změňte jméno hostitele tak, aby vyhovovalo vaší síti.
  - | c. **Volitelné:** Můžete také konfigurovat statickou IP adresu, která je vhodná pro vaši síť.
- | 2. Na serveru iSeries proveďte konfiguraci servisního procesoru:
  - | a. Zajistěte, aby byla zaškrtnuta volba **Použit připojení servisního procesoru při určování identity krytu vzdáleného systému**.
  - | b. Vyberte volbu **Jméno hostitele** a zadejte jméno hostitele servisního procesoru.
  - | c. **Volitelné:** Zadejte sériové číslo samostatného serveru nebo sériové číslo skříně serveru IBM BladeCenter. Bude-li sériové číslo servisního procesoru zjištěného podle jména hostitele odlišné od konfigurovaného sériového čísla, dojde k chybě.

| Další informace najdete v tématu “Změna vlastností konfigurace servisního procesoru” na stránce 120.

- | 3. Pomocí procedury popsané v tématu “Změna vlastností konfigurace vzdáleného systému” na stránce 117 zajistěte, aby identita vzdáleného systému byla nastavena správně:
  - | • Pro samostatný server vyberte volbu **Použit identitu krytu z konfigurace servisního procesoru**.
  - | • Pro blade server IBM BladeCenter vyberte volbu **Použit následující hodnoty** a zadejte sériové číslo blade serveru.

| Výhody:

- | • Je-li k dispozici server DNS, není nutné udržovat specifickou IP adresu v konfiguraci vzdáleného systému i5/OS.

| Nevýhody:

- | • Jméno hostitele musí být konfigurováno v servisním procesoru přes webové rozhraní servisního procesoru.
- | • Je požadován server DNS (Domain Name System).

## | **Použití webového rozhraní modulu Management Module a adaptéru RSA II**



| Webové rozhraní adaptéru RSA II (Remote Supervisor Adaptor II) nebo modulu Management Module můžete použít při provádění následujících úloh:

- | • Změna jména hostitele servisního procesoru v protokolu IP.
- | • Správa certifikátů pro manuální nastavení zabezpečení v konfiguraci servisního procesoru.
  - | – Požadavek na podepsání certifikátu za účelem získání certifikátu od vydavatele certifikátů, jako je například Verisign.
  - | – Import certifikátu do servisního procesoru.
- | • Konfigurace statických IP adres.
- | • Aktualizace firmwaru RSA II.

| **Upozornění:** Nepoužívejte webové rozhraní, chcete-li změnit jméno uživatele nebo heslo servisního procesoru. Použití webového rozhraní při změně jména uživatele nebo hesla způsobí, že objekty operačního systému i5/OS budou mít starší jména uživatele a hesla a operační systém i5/OS se pak nebude moci připojit k servisnímu procesoru.

| Chcete-li změnit jméno uživatele a heslo, použijte metodu popsanou v tématu “Inicializace servisního procesoru” na stránce 120 nebo příkaz INZNWSCFG (Inicializace konfigurace NWS) s volbou \*CHGSPAUT. Objekty operačního systému i5/OS tak zůstanou synchronizovány se jménem uživatele a heslem servisního procesoru.

| Pomocí níže uvedených odkazů můžete získat informace o použití webového rozhraní k servisnímu procesoru:

- | • Kapitola 2 publikace IBM Remote Supervisor Adapter II SlimLine and Remote Supervisor Adapter II User's Guide - Servers  ([www.ibm.com/pc/support/site.wss/](http://www.ibm.com/pc/support/site.wss/)). Pod nadpisem **Procházet** vyberte **Servery**, Skupina: **xSeries 236**, Typ: **Všechny typy, Pokračovat**. Vyberte **Publikace**.
- | • IBM xSeries and BladeCenter Server Management, SG24-6495 

## | **Připojení k adaptéru RSA II nebo k modulu IBM BladeCenter Management Module pomocí webového prohlížeče**

- | 1. **Volitelné:** Potřebujete-li adaptér RSA II připojit přes směrovač, konfigurujte nejprve IP adresu adaptéru RSA II pomocí rozhraní BIOS.
- | 2. Nejprve zadejte IP adresu adaptéru nebo jméno hostitele RSA II nebo modulu Management Module do pole adresy (URL) webového prohlížeče.
- | 3. Měla by se zobrazit výzva k zadání jména uživatele a hesla pro RSA II či Management Module. Zadejte jméno uživatele a heslo pro RSA II či Management Module. Adaptér RSA II a Management Module jsou dodávány s předvoleným jménem uživatele "USERID" a s předvoleným heslem "PASSWORD" (0 = nula). Předvolby RSA II a Management Module od výrobce jsou nastaveny takto:
  - | DHCP "Zkuste DHCP. V případě neúspěchu použijte statickou IP adresu v konfiguraci." Statická IP adresa je 192.168.70.125. Povšimněte si, že se jedná o adresu, kterou nelze směřovat. To znamená, že pomocí této adresy nebudete moci prohlížeč připojit k adaptéru RSA II ani k modulu Management Module přes směrovač. Prohlížeč byste mohli k adaptéru RSA II či k modulu Management Module připojit pomocí předvolené IP adresy přes většinu (ale ne všechny) značkových přepínačů a většinu rozbočovačů Ethernet.

| **Po připojení k webovému rozhraní RSA II/Management Module můžete provádět následující úlohy:**

- | • Vyberte “Síťová rozhraní” pod ovládacím prvkem ASM. Zadejte jméno hostitele. Doporučuje se nastavit jméno hostitele na nekvalifikovanou část jména IP hostitele. Nekvalifikované jméno IP hostitele se skládá z části plně kvalifikovaného jména IP hostitele do první tečky. Například pro plně kvalifikované jméno IP hostitele asmcards1.us.company.com je nekvalifikovaným jménem IP hostitele asmcards1.
- | • Chcete-li změnit jméno uživatele a hesla, vyberte “Profily přihlášení” pod ovládacím prvkem ASM. Tato volba je požadována v režimu manuálního zabezpečení.
- | • Vyberte “Aktualizace firmwaru” pod možností Úlohy, chcete-li firmware RSA II nebo Management Module aktualizovat na nejnovější úroveň.

---

## Kapitola 8. Administrace integrovaných Windows serverů

Níže uvedené postupy vás provedou některými běžnými každodenními úkoly práce s integrovanými servery.

- “Spuštění a zastavení integrovaného serveru”
  - “Spuštění a zastavení integrovaného Windows serveru pomocí produktu iSeries Navigator”
  - “Spuštění a zastavení integrovaného Windows serveru v prostředí znakově orientovaného rozhraní” na stránce 142
  - “Ukončení práce integrovaného Windows serveru z konzole Windows serveru” na stránce 142
  - “Bezpečné ukončení práce systému iSeries, když jsou přítomny integrované Windows servery” na stránce 142
- “Připojení k virtuální sériové konzoli serveru IXS 4812” na stránce 143
- “Prohlížení a změna informací o konfiguraci integrovaného Windows serveru” na stránce 144
- “Protokolování zpráv” na stránce 144
- “Vzdálené spouštění příkazů integrovaného Windows serveru” na stránce 145
  - “Pokyny pro spouštění vzdálených příkazů” na stránce 146
  - “Příkaz SBMNWSCMD a podpora zálohování na úrovni souborů pro protokol Kerberos v5 a mapování EIM” na stránce 147
- “Výměna hardwaru serveru za chodu” na stránce 148

---

### Spuštění a zastavení integrovaného serveru

Integrovaný Windows server nemá síťový vypínač (tlačítko Power). Jeho stav je řízen serverem iSeries. Integrované servery se obvykle spouštějí a ukončují práci v prostředí produktu iSeries Navigator nebo v prostředí znakově orientovaného rozhraní. Práci integrovaného serveru můžete částečně ukončit z jeho vlastní nabídky **Start** → **Shut Down**, ale bez prostředí produktu iSeries Navigator nebo znakově orientovaného rozhraní jej nelze opět spustit.

Zajistěte, aby integrované servery byly logicky vypnuty předtím, než ukončíte práci serveru iSeries, jinak může dojít k poškození dat. Některé příkazy použité k ukončení práce serveru iSeries způsobí ukončení práce systému na připojených integrovaných serverech a budou po určitou dobu čekat, než se tyto integrované servery vypnou. Teprve pak ukončí práci serveru iSeries. Jiné příkazy ukončí práci systému iSeries okamžitě.

Jestliže používáte program QEZPWROFFP pro plánování zapínání a vypínání, budete jej muset konfigurovat tak, aby pracoval s integrovaným serverem.

Metody spuštění a ukončení práce systému popisují následující témata:

- “Spuštění a zastavení integrovaného Windows serveru pomocí produktu iSeries Navigator”
- “Spuštění a zastavení integrovaného Windows serveru v prostředí znakově orientovaného rozhraní” na stránce 142
- “Ukončení práce integrovaného Windows serveru z konzole Windows serveru” na stránce 142
- “Bezpečné ukončení práce systému iSeries, když jsou přítomny integrované Windows servery” na stránce 142

### Spuštění a zastavení integrovaného Windows serveru pomocí produktu iSeries Navigator

1. Chcete-li zastavit integrovaný server pomocí produktu iSeries Navigator, vyberte **Administrace integrovaných serverů** -> **Servery**.
2. Klepněte pravým tlačítkem myši na server, který chcete zastavit, a vyberte **Ukončit**. Jestliže chcete ukončit práci všech integrovaných serverů, klepněte pravým tlačítkem myši na ikonu **Integrované servery xSeries** v levé navigační liště a vyberte volbu **Ukončit všechny**. Stav se změní na **Probíhá ukončování...**, **Částečně ukončeno** a nakonec na **Ukončeno**.

3. Chcete-li integrovaný server spustit, klepněte na něj pravým tlačítkem myši a vyberte volbu **Spustit**. Stav se změní na **Spouštění** a nakonec na **Spuštěno**.

## Spuštění a zastavení integrovaného Windows serveru v prostředí znakově orientovaného rozhraní

1. Chcete-li zastavit integrovaný server v prostředí znakově orientovaného rozhraní, napište příkaz `WRKCFGSTS *NWS`.
2. Vyhledejte integrovaný server, který chcete zastavit, a napište `2`. Integrovaný server se *logicky vypne*.
3. Stav se změní z hodnoty **AKTIVNÍ** na **UKONČOVÁNÍ** a potom na **LOGICKY VYPNUTO**. Stiskem klávesy **F5** můžete aktualizovat obrazovku.

**Poznámka:** U serverů připojených pomocí iSCSI se stav změní z hodnoty **AKTIVNÍ** na hodnotu **LOGICKY VYPNUTO**.

4. Ke spuštění integrovaného serveru použijte stejný příkaz `WRKCFGSTS *NWS` s hodnotou `1`. Integrovaný server tak *logicky zapnete* nebo spustíte.
5. Chcete-li integrovaný server restartovat, musíte jej manuálně logicky vypnout a pak opět zapnout. Neexistuje žádný příkaz, který by integrovaný server automaticky restartoval v prostředí znakově orientovaného rozhraní.

## Ukončení práce integrovaného Windows serveru z konzole Windows serveru

Chcete-li ukončit integrovaný Windows server z jeho vlastní konzole, vyberte v nabídce **Start** → **Shut Down**. Tato metoda se však nedoporučuje, protože způsobí jen částečné ukončení práce systému integrovaného serveru. Operační systém Windows ukončí práci a ponechá na obrazovce zprávu *It is now safe to turn off your computer*. Chcete-li ale server úplně vypnout a restartovat, musíte jej *logicky vypnout* pomocí produktu iSeries Navigator nebo znakově orientovaného rozhraní.

Na rozdíl od ukončení práce je **restart** integrovaného serveru neefektivnější, je-li proveden z jeho vlastní konzole.

Proveďte následující kroky:

1. V nabídce **Start** vyberte **Shut down**.
2. V rozevíracím menu vyberte **Restart** a klepněte na **Ok**.

**Poznámka:** U serverů připojených pomocí iSCSI nebude objekt `NWSD` po ukončení práce z konzole Windows serveru logicky vypnut. Objekt `NWSD` přejde ze stavu **AKTIVNÍ** do stavu **LOGICKY ZAPNUTO**. Na stav serveru se lze dotazovat pomocí produktu iSeries Navigator nebo pomocí příkazu `WRKNWSSTS` (Práce se stavem síťových serverů). Stav se načítá při každém vydání příkazu. Windows server neohlašuje svůj stav automaticky.

## Bezpečné ukončení práce systému iSeries, když jsou přítomny integrované Windows servery

Bezpečné ukončení práce integrovaných serverů nejnáze zajistíte tak, že vždy manuálně ukončíte práci jejich systémů předtím, než ukončíte práci serveru iSeries. Časem vás to ale může unavit. CL příkaz `PWRDWNSYS *CNTRLD` se pokusí vypnout jednotlivé integrované servery a poskytnout jim čas (atribut `SHUTDTIMO` v `NWSD`, předvolba je 15 minut), během něhož mají ukončit svou práci. Pověšimněte si, že neexistuje žádná záruka, že servery za tuto dobu svou práci skutečně ukončí.

**Poznámka:** Použití CL příkazu `PWRDWNSYS *IMMED` se nedoporučuje. Tento příkaz okamžitě vypne server iSeries, aniž by se pokusil ukončit práci integrovaných serverů.

Tabulka 2.

Akce	Výsledek
------	----------

Tabulka 2. (pokračování)

Manuální ukončení práce integrovaného serveru.	Integrovaný server je řádně logicky vypnut bez rizika ztráty dat.
Je vydán CL příkaz <code>pwrdownsys *cntrld</code> .	Integrovanému serveru je poskytnut určitý časový limit, který je uveden v atributu Shutdown Timeout v objektu NWS D, do kterého má ukončit práci. Po uplynutí této doby bude server iSeries pokračovat v ukončování práce systému a vypnutí serveru.
Je vydán CL příkaz <code>pwrdownsys *immed</code> .	Server iSeries ukončí práci systému okamžitě a neukončí práci žádného z integrovaných serverů. Může dojít k poškození dat.

Používá-li operační systém i5/OS plán zapínání a vypínání, měl by být ukončovací program (QEZPWROFFP) změněn tak, aby logicky vypnul všechny objekty NWS D před vyvoláním příkazu PWRDWN SYS. Plánování je třeba pečlivě uvážit, protože počet a aktivita jednotlivých serverů budou určovat dobu nezbytnou na úplné logické vypnutí každého serveru. Chcete-li logicky zapnout a vypnout několik serverů současně v dávkovém zpracování, použijte příkaz VRYCFG (Logické zapnutí/vypnutí konfigurace) s parametry SBMMLTJOB (Zadání více úloh) a JOB D (Popis úlohy). K plánovanému zapnutí nesmí dojít dříve, než bude mít systém možnost logicky vypnout všechny servery a vydat příkaz PWRDWN SYS. Další informace najdete v tématu Plánování ukončení práce systému a jeho restartování.

## Připojení k virtuální sériové konzoli serveru IXS 4812

Virtuální sériová konzole poskytuje funkce konzole Windows pro server Windows Server 2003, který pracuje na serveru IXS 4812. Další informace o konzolích Windows naleznete v tématu “Konzole Windows” na stránce 23. Toto připojení konzole lze použít před konfigurací TCP/IP na serveru.

Jako virtuální sériovou konzoli je možné použít libovolného klienta Telnet. Několik klientů Telnet může sdílet přístup k téže virtuální sériové konzoli. Chcete-li se připojit ke konzoli, použijte Telnet a připojte se k portu 2301 té logické části operačního systému i5/OS, která sdílí své prostředky. TCP/IP musí být konfigurován a spuštěn v logické části s operačním systémem i5/OS.

Chcete-li se připojit k virtuální sériové konzoli pomocí klienta IBM Personal Communications, postupujte takto:

1. Klepněte na **Start -> Programs -> IBM Personal Communications -> Start or Configure Session**.
2. V dialogovém okně Customize Communication vyberte v poli **Type of Host** hodnotu **ASCII**.
3. Klepněte na **Link Parameters**.
4. V dialogovém okně TelnetASCII zadejte jméno hostitele nebo IP adresu logické části s operačním systémem i5/OS, ke které se chcete připojit, do pole **Primary Host Name or IP Address**.
5. Napište **2301** do pole **Primary Port Number**.
6. Klepněte na **OK**.
7. Klepněte na **OK**. Otevře se dialogové okno relace.
8. V menu Virtual Consoles operačního systému i5/OS vyberte **Integrated xSeries Server Consoles**.
9. V dialogovém okně Integrated xSeries Server Consoles vyberte jméno hardwarového prostředku pro adaptér IOA 4812, který chcete připojit jako konzoli. Při určování jména hardwarového prostředku adaptéru IOA 4812 zobrazte popis síťového serveru (objekt NWS D) a použijte hodnotu parametru Jméno prostředku.
10. Zadáním ID a hesla servisních nástrojů operačního systému i5/OS se připojte k virtuální konzoli integrovaného serveru xSeries.

Chcete-li se připojit k virtuální sériové konzoli pomocí Telnet z příkazového řádku operačního systému DOS, postupujte takto:

1. Na příkazový řádek napište `telnet partitionname 2301`, kde *partitionname* je jméno logické části s operačním systémem i5/OS, ke které se chcete připojit.
2. Stiskněte klávesu Enter.



3. V menu Virtual Consoles operačního systému i5/OS vyberte **Integrated xSeries Server Consoles**.
4. V dialogovém okně Integrated xSeries Server Consoles vyberte jméno hardwarového prostředku pro adaptér IOA 4812, který chcete připojit jako konzoli. Při určování jména hardwarového prostředku adaptéru IOA 4812 zobrazte popis síťového serveru (objekt NWS) a použijte hodnotu parametru Jméno prostředku.
5. Zadáním ID a hesla servisních nástrojů operačního systému i5/OS se připojte k virtuální konzoli integrovaného serveru xSeries.

---

## Prohlížení a změna informací o konfiguraci integrovaného Windows serveru

Produkt iSeries Navigator umožňuje prohlížet a měnit většinu informací o konfiguraci integrovaného serveru.

1. V prostředí produktu iSeries Navigator vyberte **Administrace integrovaných serverů** -> **Servery**.
2. Klepněte pravým tlačítkem na integrovaný server a vyberte **Vlastnosti**.

Pro servery připojené pomocí iSCSI můžete zobrazit a měnit další informace o konfiguraci pomocí produktu iSeries Navigator. Postupujte takto:

1. V prostředí produktu iSeries Navigator vyberte **Administrace integrovaných serverů** -> **Připojení iSCSI**.
2. Vyberte jednu z následujících složek, zobrazí se příslušný seznam objektů. Klepněte pravým tlačítkem myši na objekt v tomto seznamu a vyberte **Vlastnosti**.
  - **Adaptéry lokálního hostitele**
  - **Vzdálené systémy**
  - **Servisní procesory**
  - **Zabezpečené připojení**

Pomocí znakově orientovaného rozhraní můžete prohlížet a měnit všechny informace o konfiguraci integrovaného serveru. Následující tabulka shrnuje důležité CL příkazy.

Tabulka 3.

Úkoly	CL příkaz
Logické zapnutí a vypnutí integrovaných serverů, kontrola stavu integrovaných serverů a objektů přiřazených k popisu síťového serveru (NWS).	WRKCFGSTS CFGTYPE(*NWS)
Správa integrovaných serverů.	WRKNWSD
Správa popisů linek, které jste vytvořili při instalaci integrovaného serveru.	WRKLIND
Správa rozhraní TCP/IP vytvořených během instalace serveru.	Práce se stavem sítě TCP/IP, volba 1: NETSTAT Konfigurace TCP/IP, volba 1: CFGTCP
Monitorování paměťových prostorů síťového serveru.	WRKNWSSTG
Správa konfigurací síťových serverů	WRKNWSCFG
Správa adaptérů hostitele síťového serveru	WRKDEVD DEVD(*NWSH)

---

## Protokolování zpráv

Integrované Windows servery zapisují informace do protokolů na různá místa. Dojde-li k problémům, mohou tyto informace pomoci určit příčinu. Následující sekce popisují protokoly zpráv.

**Protokol monitorovací úlohy** je klíčovým zdrojem informací při odstraňování problémů integrovaných serverů. Obsahuje zprávy od události běžného zpracování až po podrobné chybové zprávy. Monitorovací úloha běží vždy v podsystému QSYSWRK se stejným jménem jako integrovaný server.




Jak vyhledat protokol úlohy pomocí produktu iSeries Navigator:

1. Klepněte na **Work Management** —> **Aktivní úlohy**.
2. Jedna z úloh uvedená v sekci QSYSWRK bude mít stejné jméno jako váš integrovaný server. Klepněte na ni pravým tlačítkem myši a vyberte **Protokol úlohy**.
3. Otevře se okno úlohy integrovaného serveru. Dvakrát klepněte na ID zprávy, zobrazí se podrobnosti.

Jak vyhledat protokol úlohy ze znakově orientovaného rozhraní:

1. Na příkazový řádek operačního systému i5/OS napište WRKACTJOB SBS(QSYSWRK).
2. Jedna z uvedených úloh bude mít stejné jméno jako váš integrovaný server. Vyberte volbu 5 (Práce s úlohou).
3. Napište 10 a stiskněte klávesu Enter, čímž protokol úloh zobrazíte.
4. Stiskněte klávesu F10 a uvidíte podrobné zprávy.

Existují ještě další důležité protokoly úloh, které byste měli také zkontrolovat. Červená kniha Microsoft Windows

Server 2003 Integration with iSeries, SG24-6959  obsahuje vynikající sekci týkající se protokolů události integrovaných serverů i5/OS a na konzoli Windows.

---

## Vzdálené spuštění příkazů integrovaného Windows serveru

Při vzdáleném zadávání dávkových příkazů na integrovaném serveru můžete použít operační systém i5/OS. Fungovat budou ty příkazy Windows serveru, které se mohou provést v dávkovém režimu bez zásahu uživatele. Před spuštěním vzdáleného příkazu si ověřte, že jsou splněny následující podmínky:

- Server je integrovaným Windows serverem v tomto operačním systému i5/OS a je aktivní.
- Váš uživatelský profil je zapsán na integrovaném Windows serveru nebo v doméně, nebo se přihlašujete s profilem QSECOFR.
- Máte oprávnění spustit SBMNWSCMD, což vyžaduje zvláštní oprávnění \*JOBCTL. Také musíte mít alespoň oprávnění \*USE k objektu QSYS/SBMNWSCMD \*CMD.
- Je-li hodnota uživatelského profilu \*LCLPMDMGT nastavena na \*YES, potom systémová hodnota QRETSVRSEC musí být nastavena na 1 a je třeba změnit uživatelské heslo, nebo uživatel musí být přihlášený až po změně hodnoty QRETSVRSEC.
- Jestliže je hodnota uživatelského profilu \*LCLPMDMGT \*NO, pak se používá autentizace sítě (Kerberos). Uživatel musí mít přístup k operacím iSeries prostřednictvím aplikací podporujících protokol Kerberos (jako je jediné přihlášení produktu iSeries Navigator). Další informace najdete v tématu “Příkaz SBMNWSCMD a podpora zálohování na úrovni souborů pro protokol Kerberos v5 a mapování EIM” na stránce 147.
- Heslo v uživatelském profilu operačního systému i5/OS musí být stejné jako heslo ve Windows. Jejich konzistence nejspíše docílíte tehdy, když budete používat funkci pro zápis uživatelů a skupin.

Mohli byste si také přečíst téma “Pokyny pro spuštění vzdálených příkazů” na stránce 146.

### Spuštění příkazů integrovaného serveru pomocí produktu iSeries Navigator

1. V prostředí produktu iSeries Navigator vyberte **Administrace integrovaných serverů** —> **Servery**.
2. Klepněte pravým tlačítkem myši na server, na kterém je spuštěn dávkový příkaz, a vyberte **Spustit příkaz**.
3. Na panelu **Spuštění příkazu** zadejte příkaz Windows, který chcete spustit (například dir \).  
**Rada:** Příkaz si můžete vybrat ze seznamu 10 příkazů, které jste předtím ze serveru spustili.
4. Klepnutím na **Spustit příkaz** spustíte.

#### Poznámka:

Příkaz, který používá panel Spuštění příkazu, používá doménu \*PRIMARY jako doménu autentizace. Pro jiné domény použijte příkaz SBMNWSCMD.

### Spuštění příkazů integrovaného Windows serveru ze znakově orientovaného rozhraní

1. Napište CALL QCMD a stiskněte klávesu Enter.

2. Napište SBMNWSCMD a stiskněte klávesu F4.
3. Napište příkaz, který chcete spustit na vzdáleném serveru. Použijte klávesu Page down.
4. Zadejte objekt NWSD serveru, na kterém chcete příkaz spustit, a stiskněte klávesu Enter.
5. Účet operačního systému i5/OS, který používáte, by měl být zapsán na integrovaném serveru, aby mu byla udělena autentizace ke spuštění vzdáleného příkazu. Pole Doména autentizace umožňuje zadat, kde má být provedena autentizace ID uživatele.
6. Výstup vrácený příkazem bude zobrazen na konzoli. Stiskněte klávesu F10 a uvidíte všechny zprávy.

## Pokyny pro spuštění vzdálených příkazů

Chcete-li spouštět vzdálené příkazy integrovaného Windows serveru, mějte na paměti následující informace:

**Poznámka:** Mnohé z parametrů příkazu SBMNWSCMD popisovaných v této části nejsou k dispozici, jestliže spouštíte příkazy Windows v prostředí produktu iSeries Navigator. Potřebujete-li použít parametr, který produkt iSeries Navigator nepodporuje, musíte použít přímo příkaz SBMNWSCMD.

- Požadovaný příkaz se spouští pod příkazem konzole Windows "cmd.exe." Příkaz SBMNWSCMD nevrátí řízení tomu, kdo jej vyvolal, dokud nebude příkaz ve Windows dokončen a dokud nebude ukončen program cmd.exe.
- Pole domény autentizace příkazu SBMNWSCMD ukazuje doménu Windows, kde se autentizuje ID uživatele. Předvolba \*PRIMARY se přihlásí k primární doméně serveru, pokud je server členem domény. \*LOCAL se přihlásí k samotnému serveru. Je možné také uvést jméno důvěryhodné domény.
- S uživatelským profilem QSECOFR se zachází jinak, než se všemi ostatními uživatelskými profily. Autentizace uživatele se ve Windows neprovádí, když profil QSECOFR spouští příkaz SBMNWSCMD. Požadovaný příkaz Windows se spouští pod účtem lokálního systému Windows. Účet lokálního systému se použije i v případě, že profil QSECOFR je zapsán. Účet lokálního systému nemá heslo a postrádá přístupová práva k síti.
- U příkazu Windows "cmd" nepoužívejte parametr "/u".
- Příkaz SBMNWSCMD má omezenou podporu autentizace protokolem Kerberos v5. Protokol Kerberos bude použit pouze tehdy, má-li atribut uživatelského profilu LCLPDMGT hodnotu \*NO. Další informace najdete v tématu "Příkaz SBMNWSCMD a podpora zálohování na úrovni souborů pro protokol Kerberos v5 a mapování EIM" na stránce 147.
- Služba pro vzdálené příkazy (Remote Command) a příkaz SBMNWSCMD mohou rozeznávat výstupní data ve vícebajtovém formátu ASCII a ve formátu Unicode a patřičným způsobem je konvertovat.
- Příkazy integrovaného Windows serveru můžete kombinovat do jediného příkazového řetězce pomocí funkcí interpretu příkazů Windows "cmd.exe". Například na příkazový řádek příkazu SBMNWSCMD můžete zadat `net statistics workstation && net statistics server` a shromažďovat statistiku. Avšak příkazy, které kombinujete do jediného požadavku příkazu SBMNWSCMD, by neměly vracet smíšená data (například kombinaci dat ASCII a Unicode), ani data ve smíšených kódovaných souborech. Pokud příkazy vracejí různé typy dat, může příkaz SBMNWSCMD skončit abnormálně zprávou, která indikuje, že "došlo k problému v konverzi výstupních dat". V takovém případě spusťte příkazy samostatně.
- Nepoužívejte znaky, které na klávesnici integrovaného serveru nejsou běžně k dispozici. Ve vzácných případech nemusí mít znaky EBCDIC v kódových znakových sadách aktivních úloh ekvivalent v aktivní kódové stránce ve Windows. Každá odlišná aplikace Windows bude mít odlišný výsledek konverze.
- Příkaz SBMNWSCMD (Zadání příkazu síťového serveru) neiniculuje úplně prostředí vašeho přihlášení. Proměnné uživatelského prostředí jsou nastaveny, ale nemusejí být úplně stejné jako proměnné poskytnuté při interaktivním přihlášení. Proměnné prostředí, které interaktivní přihlášení normálně nastaví na hodnoty specifické pro uživatele, nemusí existovat nebo mohou být nastaveny na předvolené systémové hodnoty. Skripty nebo aplikace, které se spoléhají na proměnné prostředí specifické pro uživatele, nemusí fungovat správně.
- Je-li domovský adresář pro ID uživatele na integrovaném serveru zaveden na lokální server, nastaví příkaz SBMNWSCMD (Zadání příkazu síťového serveru) aktuální adresář na tento domovský adresář. Jinak se pokusí použít adresář /home/default nebo lokální systémovou jednotku.
- Je-li \*YES klíčovým slovem příkazu LODUSRPRF (Zavedení uživatelského profilu) a existuje-li uživatelský profil, pokusí se příkaz SBMNWSCMD zavést profil Windows. Pak můžete použít příkazy, které používají nebo pozměňují

závislosti profilu. Selhání při zavádění profilu se však neoznamuje, s výjimkou zpráv v protokolu událostí, které by systém Windows mohl vytvořit. Profil systému Windows může být aktivní pouze v jedné relaci přihlášení k systému Windows.

- Příkazem SBMNWSCMD můžete také spustit aplikace integrovaného serveru, pokud nevyžadují zásah uživatele. Příkazy se provádějí v okně na pozadí, ne na konzoli integrovaného serveru. Jestliže aplikace vyžaduje zásah uživatele, jako je rozevření okna zprávy, příkaz SBMNWSCMD se zastaví a bude čekat na doplnění - ale žádný zásah není možný. Ukončíte-li příkaz SBMNWSCMD i5/OS, pokusí se ukončit zastavený příkaz Windows. Příkaz na pozadí se ukončí, ať už z grafického uživatelského rozhraní, nebo z konzole.
- Spouštěč můžete také příkazy, které požadují odpověď **yes** nebo **no**, aby mohly pokračovat. Odpověď můžete dodat pomocí propojení procesů syntaxe vstupu. Například `echo y | format f: /fs:ntfs` umožní, aby formátování pokračovalo poté, co příkaz pro formátování vydá otázku **Pokračovat ve formátování**. Všimněte si, že mezi znakem "y" a symbolem propojení procesů "|" není mezer. Některé dávkové příkazy Windows však propojování procesů vstupu nepodporují (například příkaz "net"). Pokusy o předání předvolené odpovědi nemusí být možné.
- Můžete zabránit tomu, aby SBMNWSCMD zapisoval příkaz do protokolu. Jestliže příkazový řetězec obsahuje citlivá data, například hesla, která nechcete mít v protokolu chybových zpráv, postupujte takto:
  1. Jako příkazový řetězec zadejte \*NOLOGCMD.
  2. Až se zobrazí pole Příkaz (neprotokolovaný), zadejte příkaz, který má být spuštěn.

Všimněte si však, že volba \*NOLOGCMD neovlivní data, která příkaz vrací. Jestliže příkaz vrací citlivá data, můžete použít parametr CMDSTDOUT (Standardní výstup příkazu) a uložit výstup na zabezpečené místo, například do souboru integrovaného systému souborů.

- Standardní výstup z příkazu můžete nasměrovat do protokolu úlohy (\*JOBLOG), do souboru pro souběžný tisk (\*PRINT) nebo do objektu integrovaného systému souborů (IFS). Standardní chybová data jdou vždycky do protokolu úlohy.

Když zadáte \*PRINT, pak se na obrazovce WRKSPLF (Work with Spool File) zobrazí v poli User Data u souboru pro souběžný tisk hodnota SBMNWSCMD. Když vyberete volbu 8 pro zobrazení atributů, objeví se v poli pro uživatelem definovaná data jméno specifikovaného integrovaného serveru a příkaz Windows.

Když zadáte objekt integrovaného systému souborů, musí jméno cesty již existovat. Pokud jméno objektu integrovaného systému souborů neexistuje, SBMNWSCMD je vytvoří.

- Do pole Konvertovat standardní výstup můžete zadat hodnotu \*YES, chcete-li konvertovat výstup ze znakové sady systému Windows do znakové sady s identifikátorem CCSID úlohy systému i5/OS.

Vytvoří se nové soubory IFS s CCSID úlohy. Výstup směřovaný do existujícího objektu IFS je konvertován do CCSID objektu IFS. Výstup směřovaný do nového členu existujícího souboru v systému souborů /QSYS.LIB je konvertován na CCSID existujícího souboru.

- Je-li v poli Konvertovat standardní výstup hodnota (\*NO), bude standardní výstup Windows zapsán do objektu IFS nebo do souboru pro souběžný tisk s konverzí CCSID.

## Příkaz SBMNWSCMD a podpora zálohování na úrovni souborů pro protokol Kerberos v5 a mapování EIM

Operace zálohování na úrovni souborů na integrovaný Windows server využívají funkce iSeries NetClient a příkazu SBMNWSCMD (Zadání příkazu síťového serveru). V operačním systému i5/OS verze V5R3 a novější poskytují tyto funkce omezenou podporu protokolu Kerberos v5, která je také známa jako autentizace sítě iSeries. Proto je nutné uvědomit si některé skutečnosti, pokud chcete autentizaci sítě s těmito funkcemi používat.

1. Chcete-li, aby iSeries používal autentizaci Kerberos, musíte na serveru iSeries nakonfigurovat:
  - Volbu zabezpečení iSeries Navigator.
  - Službu autentizace sítě.
  - Mapování EIM (Enterprise Identity Mapping).
  - Produkt Cryptographic Access Provider (5722-AC2 nebo AC3).
2. iSeries NetServer by měl být konfigurován tak, aby používal autentizaci pomocí hesla nebo protokolu Kerberos v5, a NetServer musí být aktivní.

3. Distribuční centrum klíčů (KDC) pro protokol Kerberos musí být řadičem domény služby Active Directory ve Windows (Windows 2000 Server nebo Windows Server 2003). Další informace najdete v tématu "Použití služby Kerberos se serverem Windows Server 2003 Active Directory Server" na stránce 100.
4. Autentizace protokolem Kerberos bude použita jen tehdy, má-li uživatelský profil úlohy i5/OS atribut LCLPMDMGT nastavený na hodnotu \*NO. Je-li LCLPMDMGT nastaven na \*YES, bude vždy použita autentizace hesla.
5. Zápis uživatelů podporuje použití EIM při mapování jména uživatele Windows na jméno odlišného profilu i5/OS. Tak může zápis uživatelů hledat v registru EIM, který je určen pro jméno domény Windows Active Directory nebo případně v registru EIM, který je určen pro jméno integrovaného serveru. Zápis uživatelů bude používat mapování EIM bez ohledu na to, zda je možné použít autentizaci protokolem Kerberos. Příkaz SBMNWSCMD a NetClient však použijí jméno mapované pomocí EIM **pouze** v případě, že je použita autentizace protokolem Kerberos. Zápis uživatele tak může vytvořit lokálního uživatele Windows s jiným jménem, než je profil i5/OS, podle hodnot uvedených v mapování EIM. Ale příkaz SBMNWSCMD a NetClient použijí odlišné jméno Windows pouze tehdy, když se provádí autentizace protokolem Kerberos (když LCLPMDMGT = \*NO). Jinak se pokusí o autentizaci se jménem Windows, které je rovno jménu v profilu i5/OS.
6. Aby se mohly příkazy Windows spuštěné pomocí příkazu SBMNWSCMD připojit k jiným síťovým serverům, když je použita autentizace protokolem Kerberos, musí být cílový Windows server *ověřen jako důvěryhodný pro účely delegování*. Ve Windows 2000 je tato vlastnost v předvoleném nastavení řadičů domény povolena. U členských serverů domény je v předvoleném nastavení zakázána. Povolení lze provést pomocí administračního nástroje: **Active Directory User and Computers** v řadiči domény. V prostředí tohoto nástroje klepněte na **Computers** a vyberte správný počítač. Pak klepněte na **Computer properties** → **General**. Dále zkontrolujte **Trust computer for delegation**.

## Výměna hardwaru serveru za chodu

Integrace a virtualizace paměti serverů iSeries a xSeries poskytuje možnosti, které mohou zvýšit spolehlivost a obnovitelnost prostředí Windows serveru. Selže-li Windows server, můžete snadno a rychle přepnout paměťové prostory serveru na připravený volný server xSeries, aniž byste museli server iSeries restartovat. Tím lze snížit celkový počet serverů s procesory Intel, který je nutný pro zajišťování zvýšené dostupnosti. Tím, že umožňuje chránit několik provozních serverů použitím jednoho "rezervního" serveru, dodává také flexibilitu.

**Poznámka:** U serverů připojených pomocí iSCSI mohou adaptéry lokálního hostitele iSCSI také využívat výhod podpory výměny za chodu. Další informace najdete v tématu "Výměna adaptérů v lokálním hostitelském systému iSCSI za chodu" na stránce 128.

Procedury pro výměnu hardwaru integrovaných serverů za chodu jsou uvedeny níže.

### V prostředí produktu iSeries Navigator:

1. Rozbalte **Administrace integrovaných serverů**.
2. Vyberte **Servery**.
3. V případě, že server, pro který vyměnit hardware, ještě neukončil práci:
  - Klepněte pravým tlačítkem myši na server a vyberte **Ukončit práci**.
  - Klepněte na **Ukončit práci** na potvrzovacím panelu.
4. Změňte konfiguraci serveru tak, aby odkazovala na hardware serveru, který lze použít při výměně za chodu.
  - a. Klepněte pravým tlačítkem myši na server a vyberte **Vlastnosti**.
  - b. Vyberte kartu **Systém** a změňte jednu z následujících hodnot:
    - U serverů, které nejsou v síti iSCSI, vyberte nové **Jméno a typ prostředku**.
    - U serverů iSCSI vyberte nové **Jméno konfigurace vzdáleného systému**.
- Klepněte na **OK**.
5. Chcete-li spustit integrovaný server, klepněte pravým tlačítkem myši na server a vyberte **Spustit**.

### Použití znakově orientovaného rozhraní:

- | 1. V případě, že server, pro který chcete vyměnit hardware, ještě není logicky vypnut, vypněte jej pomocí příkazu **VRYCFG (Logické zapnutí/vypnutí konfigurace)**.
- | 2. Chcete-li změnit konfiguraci serveru tak, aby odkazovala na hardware serveru, který lze použít při výměně za chodu, použijte příkaz **CHGNWSD (Změna popisu síťového serveru)** a změňte jednu z následujících hodnot:
  - | • U serverů, které nejsou v síti iSCSI, změňte hodnotu parametru **RSRCNAME (Jméno prostředku)** tak, aby udával nové jméno hardwarového prostředku IXS nebo IXA.
  - | • U serverů iSCSI změňte hodnotu prvku **Jméno vzdáleného systému** parametru **NWSCFG (Konfigurace síťového serveru)** tak, aby udávala nové jméno objektu konfigurace síťového serveru ve vzdáleném systému.
- | 3. Spusťte integrovaný server příkazem **VRYCFG (Logické zapnutí/vypnutí konfigurace)**.





---

## Kapitola 9. Správa systému pro ukládání dat

Integrované Windows servery nemají vlastní diskové jednotky a používají místo nich při ukládání dat klientů a sdílení síťových souborů diskovou paměť i5/OS. Disková paměť i5/OS alokovaná integrovanému serveru se nazývá *paměťový prostor síťového serveru*. Instalace nové pevné jednotky na PC serveru je na integrovaném serveru ekvivalentní vytvoření paměťového prostoru síťového serveru v systému i5/OS a propojení tohoto prostoru s integrovaným serverem. Představa, že paměťový prostor síťového serveru je spravován prostřednictvím operačního systému i5/OS, ovlivní vaše rozhodování o velikostech jednotek, členění na diskové oblasti a diskových svazcích. Další informace najdete v tématu “Správa systému pro ukládání dat operačního systému i5/OS”. Můžete si přečíst také témata “Předdefinované diskové jednotky pro integrované Windows servery” na stránce 154 a “Diskové jednotky pro integrované Windows servery” na stránce 152.

Prostředí Windows na serveru iSeries vám pomáhá pracovat s datovou pamětí následujícím způsobem:

- Umožňuje vám používat operační systém i5/OS při administraci diskových jednotek integrovaného serveru podle popisu uvedeného v tématu “Administrace diskových jednotek integrovaného Windows serveru v systému i5/OS” na stránce 155.
- Poskytuje vám možnost používat program Windows Disk Management s integrovanými servery podle popisu uvedeného v tématu “Použití programu Windows Disk Management s integrovanými Windows servery” na stránce 161.

---

### Správa systému pro ukládání dat operačního systému i5/OS

Tento stručný přehled koncepcí správy paměťových prostorů operačního systému i5/OS je určen pro administrátory, kteří jsou lépe obeznámeni se způsobem, jakým Windows servery spravují diskovou paměť. Protože operační systém i5/OS spravuje paměť jinak než PC server, nejsou některé techniky, které potřebujete v prostředí PC serverů, v prostředí Windows na serveru iSeries nezbytné.

#### Operační systém i5/OS a diskové jednotky

Operační systém i5/OS provozovaný na serverech iSeries nemusí pracovat přímo s diskovými jednotkami. Pod operačním systémem je úroveň softwaru nazývaná SLIC (System Licensed Internal Code), která “skrývá” diskové jednotky a spravuje paměť objektů na těchto jednotkách. Virtuální adresový prostor je mapován přes existující místo na disku a je využíván spíše k adresování objektů než ID diskových jednotek, cylindrů a sektorů. Potřebné objekty se kopírují (“stránkují”) z tohoto adresového prostoru na disku do adresového prostoru hlavní paměti.

Vzhledem k tomu, jak operační systém i5/OS spravuje data na discích, se obvykle nemusíte starat o rozčlenění rychle rostoucích databází, defragmentaci disků nebo o data rozptýlená na několika discích (tzv. “disk striping”) na integrovaném serveru. Při sdílení diskových jednotek i5/OS používá integrovaný server ovladače zařízení. Tyto ovladače zařízení odesílají a přijímají údaje o discích do podsystému pro správu systému ukládání dat operačního systému i5/OS. Správa systému pro ukládání dat operačního systému i5/OS pracuje s pevnými disky včetně šíření obrazů diskových jednotek systému Windows na několik pevných disků, použití RAID a zrcadlení souborů (pokud bylo konfigurováno). Software pro defragmentaci disků spravuje fragmentaci logických souborů obrazů pevných disků. Protože správa systému pro ukládání dat operačního systému i5/OS tyto úlohy zpracovává, pomáhá spuštění defragmentačního programu na integrovaném serveru především v případech, kdy mohou být defragmentovány “kritické struktury systému souborů”.

#### Společné diskové oblasti (ASP)

V operačním systému i5/OS jsou fyzické jednotky pevných disků seskupeny do jednoho paměťového prostoru nazývaného společná disková oblast, nebo také společná oblast pomocné paměti (ASP). Pokud je v systému souborů nedostatek prostoru, můžete do společné diskové oblasti přidat novou diskovou jednotku a nový paměťový prostor bude okamžitě k dispozici. Každý systém má alespoň jedno ASP, a to systémové ASP. Systémovým ASP je vždy ASP



1. Máte možnost nakonfigurovat i další *uživatelská* ASP s číslem 2 - 255. Společné diskové oblasti můžete také používat při distribuci dat operačního systému i5/OS přes různé skupiny disků. Tuto koncepci můžete také použít k přesunu méně důležitých aplikací nebo dat na starší, pomalejší diskové jednotky. Podporu nezávislých ASP (33-255) zajišťuje produkt iSeries Navigator. V aplikaci Information Center a v produktu iSeries Navigator jsou ASP označovány také jako společné diskové oblasti.

### Ochrana disků:

Disky operačního systému i5/OS mohou být chráněny dvěma způsoby:

- **Zrcadlení pro více počítačů**

Zrcadlení mezi servery zrcadlí data na discích serverů, které mohou být od sebe značně vzdáleny, pomocí funkce geografického zrcadlení operačního systému v nezávislých ASP.

- **RAID-5**

Technika RAID-5 sdružuje několik disků dohromady do jednoho pole. Každý disk obsahuje informace o kontrolních součtech ostatních disků ve stejném poli. Pokud dojde k poruše disku, může řadič disků RAID-5 znovu vytvořit data vadného disku pomocí informací o kontrolních součtech na ostatních discích. Vyměníte-li vadný disk za nový, může operační systém i5/OS informace z vadného disku znovu vytvořit na novém (a tedy prázdném) disku.

- **Zrcadlení**

Zrcadlení udržuje dvě kopie dat na dvou různých discích. Operační systém i5/OS provádí operace zápisu na obou discích zároveň a může souběžně provádět dvě různé operace čtení na obou discích zrcadleného páru. Pokud jeden disk selže, použije operační systém i5/OS informace z druhého disku. Až vadný disk vyměníte za nový, zkopíruje operační systém i5/OS data z neporušeného disku na nový disk.

Chcete-li dále zvýšit úroveň ochrany, můžete zrcadlené disky připojit ke dvěma různým řadičům disků. I když jeden řadič selže a s ním i jedna sada disků, může pak druhý řadič udržet systém v chodu. U větších modelů serveru iSeries můžete připojit řadiče na více než jednu sběrnici. Připojením obou řadičů disků, které tvoří zrcadlený pár, na dvě odlišné sběrnice se dostupnost ještě zvýší.

Pro společné diskové oblasti systému i5/OS můžete definovat různé úrovně ochrany, mohou být také definovány úplně bez ochrany. Pak můžete uložit aplikace a data do společné diskové oblasti se správnou úrovní ochrany podle toho, jak je jejich dostupnost důležitá. Další informace o ochraně a možnostech dostupnosti disků v operačním systému i5/OS najdete v tématu Zálohování a obnova.

## Diskové jednotky pro integrované Windows servery

Integrované servery nemají vlastní diskové jednotky. Operační systém i5/OS vytváří paměťové prostory na síťovém serveru v rámci vlastního systému souborů a integrované servery je používají, jako by to byly normální jednotky pevných disků.

Integrovaný Windows server rozpozná diskovou jednotku integrovaného serveru (paměťový prostor síťového serveru) jako jednotku pevného disku pouze tehdy, pokud je navzájem propojíte. Diskovou jednotku musíte před propojením vytvořit. Další informace najdete v tématech “Vytvoření diskové jednotky integrovaného serveru” na stránce 156 a “Propojení diskové jednotky s integrovaným serverem” na stránce 157. Po vytvoření a propojení nové diskové jednotky integrovaného serveru se tato jednotka bude integrovanému serveru jevit jako jednotka pevného disku. Před použitím ji musíte naformátovat. Další informace najdete v tématu “Formátování diskových jednotek integrovaného Windows serveru” na stránce 158.

Diskové jednotky mohou být se servery propojeny jedním z následujících způsobů:

1. Pevná (statická) propojení diskových jednotek umožňují propojovat diskové jednotky se serverem podle uživatelsky definované pozice v posloupnosti propojení. Pořadí, v jakém server vidí jednotky, je určeno jejich relativní pozicí v posloupnosti propojení. Při přidávání pevného (statického) propojení diskové jednotky musí být server logicky vypnut.

**Poznámka:** Statická propojení jednotek se u serverů xSeries připojených pomocí iSCSI nepoužívají.

2. Připojení diskové jednotky prostředku kvora klastru se používá k propojení diskové jednotky prostředku kvora se servery v klastru.
3. Propojení sdílených diskových jednotek v klastru umožňuje, aby disková jednotka byla sdílena mezi klastrovanými integrovanými servery. Sdílenou jednotku je možné propojit pouze s uzly, které sdílejí společný prostředek kvora. Jednotky tohoto typu jsou k dispozici všem uzlům, které jsou vzájemně spojeny propojením prostředku kvora klastru. Každý uzel má přístup ke sdíleným jednotkám pod kontrolou klastrových služeb Windows, které jsou spuštěny na každém uzlu.

**Poznámka:** Jednotky, které jsou propojeny jako sdílené, by měly být propojeny se VŠEMI uzly ve společném klastru.

4. Dynamické propojení diskové jednotky umožňuje, aby se s integrovaným serverem propojily další diskové jednotky pomocí dynamicky přidělených pozic pořadí propojení. Pozice v pořadí propojení disku se přiděluje dynamicky v době, kdy je disková jednotka propojena s aktivním serverem. Pozice v pořadí propojení disku může být zadána, ale použije se teprve při restartování serveru. Když přidáváte dynamické propojení diskové jednotky, může být integrovaný server být buď ukončený, nebo aktivní.

l Když se integrovaný server, který není v síti iSCSI, spustí, vidí diskové jednotky v následujícím pořadí:

1. Staticky propojené diskové jednotky.
2. Diskovou jednotku prostředku kvora klastru.
3. Diskové jednotky sdílené v klastru.
4. Dynamicky propojené diskové jednotky.

l U severů připojených pomocí iSCSI se disk kvora klastru zobrazí na konci seznamu diskových jednotek. Dynamicky propojené disky a disky, které sdílejí klastry, mohou být použity společně.

V každé z těchto kategorií typu propojení se disky jeví v pořadí pozice uživatelsky specifikovaného pořadí propojení. Při dynamickém propojování diskové jednotky s aktivním serverem se nový disk objeví až za všemi ostatními propojenými diskovými jednotkami.

l Následující tabulka ukazuje funkce virtuálních diskových jednotek serveru iSeries podporované pro různé typy popisů síťových serverů (objektů NWSO) s operačním systémem i5/OS verze V5R4 nebo vyšší.

#### Podporované funkce disků

Funkce	Typ NWSO <sup>5</sup> *WINDOWSNT nebo *IXSVR s OS typu *WIN32	Typ NWSO <sup>5</sup> *ISCSI s OS typu *WIN32
Počet pevných (statických) propojení	16	0
Počet dynamických propojení	16	63 <sup>1</sup>
Počet propojení kvora klastru	1	1
Počet propojení sdílených v klastru	15	61 <sup>1</sup>
Maximální počet virtuálních disků, které lze se serverem propojit	48 s klastrováním <sup>2</sup> ; 32 jinak	64 s klastrováním <sup>2</sup> ; 63 jinak
Maximální kapacita na virtuální disk	1000 GB	1000 GB
Maximální celková kapacita virtuálních disků, za předpokladu 1000 GB na disk	46,9 TB s klastrováním <sup>2</sup> ; 31,3 TB jinak	62,5 TB s klastrováním <sup>2</sup> ; 61,5 TB jinak
Je možné virtuální disky propojit, je-li server aktivní?	Ano Výjimky: pevné linky	Ano Výjimky: dynamické linky 1-2
Je možné virtuální disky odpojit, je-li server aktivní?	Ano Výjimky: pevné linky, disk nemůže být částí sady svazků, disk nemůže být svazek nasazený v adresáři	Ano Výjimky: dynamické linky 1-2, disk nemůže být částí sady svazků, disk nemůže být svazek nasazený v adresáři

Funkce	Typ NWS <sup>5</sup> *WINDOWSNT nebo *IXSVR s OS typu *WIN32	Typ NWS <sup>5</sup> *ISCSI s OS typu *WIN32
Typy formátů virtuálních disků povolené při propojování <sup>3</sup>	*NTFS, *NTFSQR, *FAT, *FAT32, *OPEN	*NTFS, *NTFSQR, *FAT, *FAT32, *OPEN
Typy přístupů virtuálních disků povolené při propojování	Výhradní aktualizace, sdílená aktualizace <sup>4</sup>	Výhradní aktualizace, sdílená aktualizace <sup>4</sup>
Propojení disků, která vyžadují typ adresy výhradní aktualizace	Všechna propojení pevných disků a všechna dynamická propojení	Všechna dynamická propojení
Propojení disků, která vyžadují typ adresy sdílené aktualizace	Propojení kvora klastru a všechna propojení disků sdílených v klastru	Propojení kvora klastru a všechna propojení disků sdílených v klastru

### Poznámky:

- U Windows serverů v síti iSCSI používají dynamické disky a disky sdílené v klastru stejnou řadu pozic v posloupnosti a mohou být použity společně. Celkový počet dynamických a v klastru sdílených diskových propojení je při tomto společném použití 63.
- Použití klastrů u Windows serverů vyžaduje službu MSCS (Microsoft Cluster Service), která řídí přístup ke sdíleným diskům v klastru.
- Popis těchto typů formátu najdete v textu nápovědy k příkazu CRTNWSSTG (Vytvoření paměťového prostoru NWS).
- Propojuje-li se několik serverů s diskem pomocí sdílené aktualizace, pak ve skutečnosti může mít v libovolném časovém okamžiku přístup umožňující zápis na disk pouze jeden server. Například u Windows serverů určuje služba MSCS (Microsoft Cluster Service), který server v klastru má přístup umožňující zápis na disk.
- Popis typů NWS a typů souvisejících operačních systémů (OS) najdete v textu nápovědy příkazu CRTNWS (Vytvoření popisu síťového serveru).

Paměťové prostory síťového serveru mohou být umístěny buď ve společné systémové diskové oblasti operačního systému i5/OS (ASP 1) nebo ve společné uživatelské diskové oblasti. Můžete zkopírovat jednu diskovou jednotku na druhou nebo ji přesunout do jiné společné diskové oblasti.

Poté, co byl vytvořen paměťový prostor síťového serveru a propojen s integrovaným serverem, musíte jej z konzole Windows naformátovat. Můžete si vybrat ze tří typů diskového formátu. Pravděpodobně vyberete NTFS, protože je nejúčinnější a nejbezpečnější. Diskové oblasti formátované pomocí NTFS mohou mít velikost až 1024000 MB. Jiný typ formátu je FAT-32. Jednotky formátované pomocí FAT-32 mohou mít velikost v rozmezí 512 – 32000 MB. Nejstarší typ formátu je FAT. Maximální možná velikost diskové oblasti FAT je 2047 MB. Předdefinovaná disková oblast instalační zdrojové jednotky (D), která musí být ve formátu FAT, je proto omezena na velikost 2047 MB.

Paměťové prostory síťového serveru jsou jedním ze dvou typů síťového systému pro ukládání dat, které integrované servery používají. Integrované servery mohou mít také přístup k prostředkům v operačním systému i5/OS, které administrátor sdílí přes iSeries NetServer.

Proces instalace produktu Integrated Server Support na serveru IBM iSeries vytvoří několik diskových jednotek, které slouží k instalaci a spouštění integrovaných Windows serverů. Další informace najdete v tématu “Předdefinované diskové jednotky pro integrované Windows servery”.

Informace o vytváření jednotek najdete v tématu “Vytvoření diskové jednotky integrovaného serveru” na stránce 156

## Předdefinované diskové jednotky pro integrované Windows servery

Proces instalace produktu Integrated Server Support na serveru IBM iSeries vytvoří dvě diskové jednotky (paměťové prostory síťového serveru) pro instalaci a spouštění integrovaných serverů. Další informace najdete v tématu “Diskové jednotky pro integrované Windows servery” na stránce 152. Operační systém i5/OS vytvoří tyto diskové jednotky podle předvoleného nastavení v systémové společné diskové oblasti (ASP), ale během instalace můžete zvolit jiné umístění. Operační systém i5/OS používá tyto diskové jednotky také při zavádění a spouštění integrovaného serveru.

Servery mají tyto předdefinované diskové jednotky:

### Zaváděcí a systémová jednotka (C)

Tato jednotka slouží jako systémová jednotka. Operační systém i5/OS tuto jednotku nazývá *server1*, kde *server* je jméno objektu NWSD. Tato disková jednotka je umístěna v integrovaném systému souborů a je automaticky propojována jako první jednotka.

Velikost jednotky C má rozmezí 1024 až 1024000 MB. Můžete zvolit, že chcete jednotku ponechat ve formátu FAT. Jednotka C je automaticky konvertována do formátu NTFS, pokud to vyžaduje velikost paměťového prostoru.

**Poznámka:** Plánujete-li vytvoření konfiguračních souborů NWSD, pamatujte si, že podpora těchto souborů existuje pouze pro diskové jednotky, které jsou formátovány jako FAT nebo FAT32. Další informace uvádí Kapitola 15, “Konfigurační soubory popisu síťového serveru”, na stránce 235. Systémová jednotka, která byla konvertována do formátu NTFS, není přístupná pro konfigurační soubory NWSD. Další informace o různých systémech souborů najdete v tématu “Porovnání systémů souborů FAT, FAT32 a NTFS” na stránce 84.

### Instalační zdrojová jednotka (D)

Jednotka D může mít velikost 200 - 2047 MB a je na ní uložena kopie instalačního kódu Windows serveru a kódu produktu IBM iSeries Integrated Server Support. Operační systém i5/OS nazývá tuto jednotku *server2*, kde *server* je jméno objektu NWSD. Tato disková jednotka je umístěna v integrovaném systému souborů a je automaticky propojena jako druhá jednotka. Operační systém i5/OS formátuje jednotku D jako FAT (file allocation table).

**Upozornění:** Tato jednotka musí zůstat jako jednotka FAT. Neprovádějte na ní žádné změny. Operační systém i5/OS tuto jednotku používá při provádění aktualizací kódu. Změníte-li tuto jednotku, můžete provádění aktualizací znemožnit.

**Poznámka:** Další informace o přechodu serverů z nižších verzí systému i5/OS než V4R5 na vyšší verzi najdete v tématu Předdefinované diskové jednotky pro integrované Windows servery v aplikaci Information Center pro verzi V5R3 serveru iSeries.

---

## Administrace diskových jednotek integrovaného Windows serveru v systému i5/OS

Administrace diskových jednotek integrovaného Windows serveru (paměťových prostorů síťového serveru) v systému i5/OS zahrnuje tyto úlohy:

- “Přístup k integrovanému systému souborů operačního systému i5/OS z integrovaného serveru”
- “Získání informací o diskových jednotkách integrovaného serveru” na stránce 156
- “Přidání diskových jednotek na integrované Windows servery” na stránce 156
- “Kopírování diskové jednotky” na stránce 158
- “Rozbalení diskové jednotky” na stránce 159
- “Rozbalení systémové jednotky” na stránce 160
- “Odpojení diskových jednotek integrovaného Windows serveru” na stránce 160
- “Výmaz diskových jednotek integrovaného Windows serveru” na stránce 160

## Přístup k integrovanému systému souborů operačního systému i5/OS z integrovaného serveru

K integrovanému systému souborů operačního systému i5/OS můžete z integrovaného serveru přistupovat prostřednictvím produktu IBM iSeries Support for Windows Network Neighborhood (iSeries NetServer). Usnadní vám to práci s prostředky systému souborů v systému i5/OS. Informace o použití serveru iSeries NetServer najdete v tématech:

- Vytvoření sdílení souborů na serveru iSeries NetServer.

- Nastavení PC klienta, aby používal iSeries NetServer.
- Přístup ke sdílení souborů serveru iSeries NetServer s klientem Windows.

Další informace najdete v tématu “Povolení serveru iSeries NetServer” na stránce 61.

## Získání informací o diskových jednotkách integrovaného serveru

Chcete-li zjistit, jaké procento z diskové jednotky integrovaného serveru (paměťového prostoru síťového serveru) je právě používáno nebo jaký je její formát, můžete tyto informace získat z operačního systému i5/OS.

Informace o diskové jednotce získáte takto:

1. V prostředí produktu iSeries Navigator vyberte **Administrace integrovaných serverů** —> **Všechny virtuální disky**.
2. Ze seznamu vyberte diskovou jednotku.
3. Klepněte pravým tlačítkem myši na diskovou jednotku a vyberte **Vlastnosti** nebo klepněte na odpovídající ikonu panelu nástrojů produktu iSeries Navigator.

Chcete-li použít CL příkaz, podívejte se na příkaz WRKNWSSTG (Práce s paměťovými prostory síťového serveru).

## Přidání diskových jednotek na integrované Windows servery

Vytvoření a formátování diskových jednotek pro aplikace a data tak, jak je chápe integrovaný server, zahrnuje vytvoření paměťových prostorů v systému i5/OS. Informace o koncepci paměťových prostorů síťového serveru najdete v tématu “Diskové jednotky pro integrované Windows servery” na stránce 152. Chcete-li přidat diskovou jednotku integrovaného serveru (paměťový prostor síťového serveru) proveďte tyto úkoly:

1. “Vytvoření diskové jednotky integrovaného serveru”.
2. “Propojení diskové jednotky s integrovaným serverem” na stránce 157.
3. “Formátování diskových jednotek integrovaného Windows serveru” na stránce 158.

## Vytvoření diskové jednotky integrovaného serveru

Vytvoření diskové jednotky integrovaného serveru (paměťového prostoru síťového serveru) je prvním krokem k přidání diskového prostoru na integrovaný Windows server. Doba, kterou potřebujete k vytvoření diskové jednotky, je úměrná její velikosti. Diskovou jednotku musíte po vytvoření propojit s popisem síťového serveru svého integrovaného serveru a naformátovat ji. (Viz “Propojení diskové jednotky s integrovaným serverem” na stránce 157). Další informace najdete v tématu “Formátování diskových jednotek integrovaného Windows serveru” na stránce 158.

Chcete-li vytvořit diskovou jednotku integrovaného serveru, postupujte takto:

1. V prostředí produktu iSeries Navigator vyberte **Administrace integrovaných serverů**.
2. Klepněte pravým tlačítkem myši na složku **Všechny virtuální disky** a vyberte **Nový disk** nebo klepněte na odpovídající ikonu na panelu nástrojů produktu iSeries Navigator.
3. Zadejte jméno a popis diskové jednotky.
4. Chcete-li zkopírovat data z jiného disku, vyberte volbu **Inicializovat disk daty z jiného disku**. Pak vyberte zdrojový disk, ze kterého se mají data zkopírovat.
5. Zadejte kapacitu disku.
6. Vyberte společnou diskovou oblast, která bude disk obsahovat.
7. Vyberte systém souborů plánovaný pro disk.

**Poznámka:** Formátujete-li disk ve Windows, můžete v případě potřeby zvolit jiný systém souborů.

8. Vytváříte-li disk prostředku kvora klastru ve Windows, uveďte atributy klastru.
9. Pokud chcete disk okamžitě po vytvoření propojit se serverem, zaškrtněte volbu **Propojit disk se serverem** a zadejte atributy propojení.
10. Klepněte na **OK**.



| Chcete-li použít CL příkaz, podívejte se na příkaz CRTNWSSTG.

#### | **Poznámky:**

- | 1. Chcete-li propojení nového disku provést jako samostatnou operaci, prostudujte část “Propojení diskové jednotky s integrovaným serverem”.
- | 2. Vytvořené disky musejí být rozděleny na oddíly a naformátovány pomocí nástroje Správa disků ve Windows nebo pomocí obslužného programu příkazového řádku DISKPART.
- | 3. Vytvoření nebo spuštění serveru z diskové jednotky v nezávislé společné diskové oblasti vyžaduje, aby bylo zařízení se společnou diskovou oblastí dostupné.

### **Propojení diskové jednotky s integrovaným serverem**

Aby byl integrovaný Windows server schopen rozpoznat diskovou jednotku integrovaného serveru (síťový paměťový prostor) jako jednotku pevného disku, musíte oba propojit. Předtím, než diskovou jednotku propojíte, ji musíte vytvořit. Další informace najdete v tématu “Vytvoření diskové jednotky integrovaného serveru” na stránce 156. Poté, co vytvoříte a propojíte novou diskovou jednotku integrovaného serveru, tato jednotka se bude integrovanému serveru jevit jako jednotka pevného disku. Pak ji musíte naformátovat, abyste ji mohli použít. Další informace najdete v tématu “Formátování diskových jednotek integrovaného Windows serveru” na stránce 158.

Chcete-li propojit diskovou jednotku s integrovaným serverem, postupujte takto:

1. Jestliže nepropojujete diskovou jednotku dynamicky, ukončete práci integrovaného serveru. Další informace najdete v tématu “Spuštění a zastavení integrovaného serveru” na stránce 141.
- | 2. V prostředí produktu iSeries Navigator vyberte **Administrace integrovaných serverů** —> **Všechny virtuální disky**.
- | 3. Klepněte pravým tlačítkem myši na diskovou jednotku a vyberte volbu **Přidat propojení** nebo vyberte jednotku a klepněte na odpovídající ikonu panelu nástrojů produktu iSeries Navigator.
4. Vyberte server, se kterým chcete disk propojit.
5. Vyberte jeden z dostupných typů propojení a umístění v pořadí propojení.
- | 6. Propojujete-li disk se serverem připojeným pomocí iSCSI, vyberte jednu z dostupných cest k paměťovým prostorům.
- | 7. Vyberte jeden z dostupných typů přístupu k datům.
8. Klepněte na **OK**.
9. Jestliže nepropojujete diskovou jednotku dynamicky, spusťte integrovaný server. Další informace najdete v tématu “Spuštění a zastavení integrovaného serveru” na stránce 141.

Chcete-li použít CL příkaz, podívejte se na příkaz ADDNWSSTGL.

Jestliže je disková jednotka nová a nebyla ještě naformátována, postupujte podle informací v tématu “Formátování diskových jednotek integrovaného Windows serveru” na stránce 158.

### **Správa diskových jednotek, když dojdou písmena pro jejich označení:**

Maximální počet diskových jednotek, které lze propojit s integrovaným serverem, je větší než počet diskových jednotek, které jsou dostupné ve Windows. Vzhledem k tomu, že ne všechny jednotky budou označeny písmenem, je nutné využít jiné volby, aby byly využity veškeré paměťové prostory propojené se serverem. Zde jsou dvě volby pro využití všech diskových jednotek propojených se serverem.

1. Písmeno diskové jednotky může být vytvořeno z několika diskových jednotek používajících sadu segmentovaných diskových svazků.

| **Poznámka:** Při vytváření sady svazků budou vymazána veškerá existující data v diskových oblastech, které  
| použijete pro novou sadu svazků. Provádíte-li nastavení serveru, neměli byste zapomenout na sady  
| svazků.

- a. V programu **Disk Management** klepněte pravým tlačítkem myši na číslo diskové jednotky a v rozevíracím menu vyberte **Upgrade to Dynamic Disk...**

- b. Klepněte pravým tlačítkem myši na diskovou oblast jednotky a v rozevíracím menu vyberte **Create Volume...**
  - c. Sledujte průvodce vytvořením segmentovaného svazku a určité přidejte všechny další disky. Poznámka: Tato funkce je příjemná, protože když dojde k naplnění svazku, může se dynamicky přidat disk, který se okamžitě připojí k segmentovanému svazku, aniž by bylo nutné server restartovat.
2. Disková jednotka může být zavedena přes podadresář písmene existující diskové jednotky.
- a. Vytvořte adresář na jednotce označené písmenem, která je naformátována jako NTFS. Například MD C:\MOUNT1.
  - b. V okně **Disk Management** klepněte na diskovou oblast jednotky, kterou chcete formátovat a v rozevíracím menu vyberte **Format**.
  - c. Jakmile bude jednotka naformátována, klepněte znovu na diskovou oblast a v rozevíracím menu vyberte **Change Drive Letter and Path...**
  - d. Vyberte **Add**.
  - e. Vyberte přepínač **Mount in this NTFS folder:**
  - f. Tlačítkem **Browse** vyhledejte adresář C:\MOUNT1, který byl vytvořen v kroku 1.
  - g. Klepněte na **OK** a udělejte z tohoto adresáře místo zavedení pro tuto diskovou jednotku.

## Formátování diskových jednotek integrovaného Windows serveru

Chcete-li diskové jednotky integrovaného Windows serveru (paměťové prostory síťového serveru) používat, musíte je nejprve naformátovat. Před formátováním musejí být diskové jednotky nejprve vytvořeny (viz “Vytvoření diskové jednotky integrovaného serveru” na stránce 156) a propojeny (viz “Propojení diskové jednotky s integrovaným serverem” na stránce 157). Potom musíte spustit Windows server v operačním systému i5/OS (viz “Spuštění a zastavení integrovaného serveru” na stránce 141).

- Poznámka:** Servery mohou dynamicky propojovat diskové jednotky, zatímco je server logicky zapnut, pomocí parametru dynamické propojení paměťových prostorů v příkazu ADDNWSSTGL (Přidání propojení s pamětí serveru).

Formátování diskových jednotek proveďte následujícím způsobem:

1. Na konzoli integrovaného Windows serveru otevřete nabídku **Start**, vyberte **Programs**, pak vyberte **Administrative Tools** a nakonec **Computer Management**.
2. Klepněte dvakrát na **Storage**.
3. Klepněte dvakrát na **Disk Management**.
4. Chcete-li vytvořit novou diskovou oblast, klepněte pravým tlačítkem myši na nealokované místo na základním disku, na kterém chcete diskovou oblast vytvořit, a potom klepněte na **Nová disková oblast**.
5. Při formátování nové jednotky postupujte podle pokynů na obrazovce.
  - a. Zadejte jméno paměťového prostoru pro označení svazku.
  - b. Vyberte systém souborů, který jste zadali při vytváření diskové jednotky.
  - c. Vyberte rychlé formátování pro právě vytvořený paměťový prostor. Byl již naformátován na nižší úroveň operačním systémem i5/OS, když byl alokován.

## Kopírování diskové jednotky

Novou diskovou jednotku integrovaného Windows serveru (paměťový prostor síťového serveru) můžete vytvořit zkopírováním dat z existující diskové jednotky.

Při kopírování diskové jednotky postupujte takto:

1. Rozbalte **Administrace integrovaných serverů** —> **Všechny virtuální disky**.
2. Z dostupného seznamu vyberte diskovou jednotku.
3. Klepněte pravým tlačítkem myši na diskovou jednotku a vyberte **Nová podle** nebo klepněte na odpovídající ikonu panelu nástrojů produktu iSeries Navigator.



4. Zadejte jméno a popis diskové jednotky.
5. Zadejte kapacitu disku. Podrobnosti o platných velikostech disků přiřazených k určitému formátu systému souborů najdete v online nápovědě. Chcete-li při kopírování zvětšit velikost disku, můžete zadat větší velikost. Rozšířenou část disku bude tvořit volný prostor nerozdělený na sekce.

**Poznámka:** Chcete-li rozbalit existující diskovou oblast, aby bylo možné využít další volný prostor, můžete použít obslužný program příkazového řádku DISKPART. V člancích znalostní báze Knowledge Base firmy Microsoft najdete podrobnosti a omezení pro obslužný program DISKPART.

6. Vyberte společnou diskovou oblast, která bude disk obsahovat.
7. Klepněte na **OK**.

Chcete-li použít CL příkaz, podívejte se na příkaz CRTNWSSTG (Vytvoření paměťového prostoru síťového serveru).

## Rozbalení diskové jednotky

Virtuální diskovou jednotku (paměťový prostor síťového serveru) můžete rozbalit, aniž byste ji kopírovali. Informace o rozbalení zaváděcího disku najdete v tématu “Rozbalení systémové jednotky” na stránce 160.


Chcete-li rozbalit diskovou jednotku, postupujte takto:

1. Rozbalte **Administrace integrovaných serverů -> Všechny virtuální disky**.
2. Z dostupného seznamu vyberte diskovou jednotku.
3. Klepněte pravým tlačítkem myši na diskovou jednotku a vyberte **Vlastnosti** nebo klepněte na odpovídající ikonu na panelu nástrojů produktu iSeries Navigator.
4. Klepněte na kartu **Kapacita** na listu vlastností diskové jednotky.
5. Zadejte zvýšenou velikost disku v poli **Nová kapacita**. Podrobnosti o platných velikostech disků přiřazených k určitému formátu systému souborů najdete v online nápovědě. Rozšířenou část disku bude tvořit volný prostor nerozdělený na sekce.
6. Klepněte na **OK**.
7. Pokud je disk propojen s aktivním serverem, zobrazí se potvrzovací panel s informací, že disková jednotka bude pro server dočasně nedostupná, dokud se bude disk rozbalovat. Na potvrzovacím panelu potvrďte klepnutím na **Změnit**, že tuto skutečnost uznáváte, nebo klepnutím na **Zrušit** operaci zrušte.

### Poznámky:

1. Disk nelze propojit s aktivním serverem, pokud je právě rozbalován. Podporuje-li server dynamické odpojování diskových jednotek, potom může být výše uvedená procedura provedena i tehdy, je-li server aktivní. V takovém případě bude disk dynamicky odpojen, potom bude rozbalen a znovu dynamicky propojen se serverem. Proto je disk aktivnímu serveru dočasně nedostupný, dokud se rozbaluje.
2. Chcete-li rozbalit existující diskovou oblast, aby bylo možné využít další volný prostor, můžete použít obslužný program příkazového řádku DISKPART.

**Poznámka:** Podle předvoleného nastavení je program DISKPART dostupný na serveru Windows Server 2003.

Můžete jej také stáhnout z webové stránky firmy Microsoft  (www.microsoft.com). V člancích znalostní báze Knowledge Base firmy Microsoft najdete podrobnosti a omezení pro obslužný program DISKPART.

3. Rozbalení existujícího paměťového prostoru síťového serveru má určitá omezení, která závisejí na tom, jak byl paměťový prostor původně alokovan.

Chcete-li použít CL příkaz, podívejte se na příkaz CHGNWSSTG (Změna paměťového prostoru sítě). Pověšměte si, že při rozbalování disku pomocí příkazu CHGNWSSTG nelze disk propojit s aktivním serverem. Příkaz CHGNWSSTG neprovede automatické odpojení a opětné propojení disku, je-li server aktivní.

## Rozbalení systémové jednotky

**Upozornění:** Před rozbalením byste měli systémovou jednotku zálohovat. Informace o použití obslužného programu DISKPART najdete na webové stránce firmy Microsoft  (www.microsoft.com).

Chcete-li rozbalit systémovou jednotku, postupujte takto:

1. Ukončete práci serveru. Další informace najdete v tématu “Spuštění a zastavení integrovaného serveru” na stránce 141.
2. Odpojte systémovou diskovou jednotku od serveru. Další informace najdete v tématu “Odpojení diskových jednotek integrovaného Windows serveru”.
3. Změňte velikost disku. Další informace najdete v tématu “Rozbalení diskové jednotky” na stránce 159.
4. Propojte disk s popisem síťového serveru dočasně jako datový disk. Další informace najdete v tématu “Propojení diskové jednotky s integrovaným serverem” na stránce 157.
5. Spusťte dočasný server. Další informace najdete v tématu “Spuštění a zastavení integrovaného serveru” na stránce 141.
6. Na konzoli Windows dočasně serveru rozbalte diskovou oblast pomocí obslužného programu DISKPART.
7. Ukončete práci dočasně serveru. Další informace najdete v tématu “Spuštění a zastavení integrovaného serveru” na stránce 141.
8. Odpojte disk od dočasně serveru. Další informace najdete v tématu “Odpojení diskových jednotek integrovaného Windows serveru”.
9. Propojte rozbalený disk s původním serverem jako systémový disk. Další informace najdete v tématu “Propojení diskové jednotky s integrovaným serverem” na stránce 157.
10. Spusťte původní server. Další informace najdete v tématu “Spuštění a zastavení integrovaného serveru” na stránce 141.

## Odpojení diskových jednotek integrovaného Windows serveru

Když zrušíte propojení diskových jednotek integrovaného Windows serveru (paměťových prostorů síťového serveru), odpojíte je od integrovaného serveru a pro uživatele budou nedostupné. Informace o podmínkách dynamického odpojení jednotek najdete v tématu “Diskové jednotky pro integrované Windows servery” na stránce 152.

Propojení diskové jednotky zrušíte tímto postupem:

1. Pokud neodpojujete diskovou jednotku dynamicky, ukončete práci integrovaného serveru. Další informace najdete v tématu “Spuštění a zastavení integrovaného serveru” na stránce 141.
2. V prostředí produktu iSeries Navigator vyberte **Administrace integrovaných serverů** —> **Všechny virtuální disky** nebo rozbalte **Administrace integrovaných serverů** —> **Servery** —> *jménoserveru* —> **Propojené virtuální disky**, kde *jménoserveru* je jméno serveru, se kterým je disk propojen.
3. Klepněte pravým tlačítkem myši na diskovou jednotku, která má být odpojena, a vyberte **Odstranit propojení** nebo vyberte jednotku a klepněte na odpovídající ikonu na panelu nástrojů produktu iSeries Navigator.
4. **Volitelné:** Chcete-li změnit pořadí jednotek, klepněte na **Komprimovat posloupnost propojení**.
5. Klepněte na volbu **Odstranit**.

Chcete-li použít CL příkaz, podívejte se na příkaz RMVNWSSTGL.

## Výmaz diskových jednotek integrovaného Windows serveru

Vymazání diskové jednotky (paměťového prostoru síťového serveru) zruší data na diskové jednotce a uvolní diskovou paměť serveru iSeries, takže může být použita pro jiné účely.

Dříve než budete moci vymazat diskovou jednotku, musíte zrušit její propojení s integrovaným serverem. Další informace najdete v tématu “Odpojení diskových jednotek integrovaného Windows serveru”. Jakmile diskovou jednotku odpojíte, můžete ji vymazat.

Při výmazu diskové jednotky postupujte takto:

1. V prostředí produktu iSeries Navigator vyberte **Administrace integrovaných serverů** —> **Všechny virtuální disky**.
2. Z dostupného seznamu vyberte diskovou jednotku.
3. Klepněte pravým tlačítkem myši na diskovou jednotku a vyberte volbu **Vymazat** nebo klepněte na odpovídající ikonu panelu nástrojů produktu iSeries Navigator.
4. Klepněte na volbu **Vymazat** na potvrzovacím panelu.

Chcete-li použít CL příkaz, podívejte se na příkaz DLTNWSSTG.

### Výmaz diskových jednotek při odstranění integrovaného serveru

Když manuálně odstraňujete integrovaný server, musíte vymazat diskové jednotky (paměťové prostory síťového serveru), které jsou přiřazeny k popisu síťového serveru (NWSA) daného serveru. Vymažte také uživatelem vytvořené diskové jednotky, které vlastníte.

Příkaz DLTWNTSVR (Výmaz Windows serveru) je určen k odstraňování objektů vytvořených příkazem INSWNTSVR (Instalace Windows serveru). Odstraní popis síťového serveru (NWSA), popisy linek (LIND), paměťové prostory (NWSSTG), rozhraní TCP, popisy řadičů (CTLD) a popisy zařízení (DEVN). To je doporučený způsob, jak trvale odstranit integrovaný server ze systému.

- l Musíte také vymazat všechny diskové jednotky, které operační systém i5/OS předdefinoval jako systémové jednotky a instalační zařízení pro server.

Chcete-li zjistit, které diskové jednotky jsou přiřazeny k vašemu serveru, prostudujte téma “Získání informací o diskových jednotkách integrovaného serveru” na stránce 156.

---

## Použití programu Windows Disk Management s integrovanými Windows servery

Program Windows Disk Management můžete použít k administraci diskových jednotek (paměťových prostorů síťového serveru), jako kdyby to byly jednotlivé fyzické diskové jednotky. Jeho funkce (jako je přiřazení písmen jednotkám, členění na diskové oblasti a vytvoření sad svazků) jsou plně funkční.

Při použití programu Windows Disk Management musíte vzít v úvahu následující skutečnosti:

- Když propojujete diskové jednotky, můžete jim přiřadit relativní pozice v posloupnosti nebo můžete nechat operační systém i5/OS, aby to provedl automaticky.
- Pokud nechcete, aby program Windows Disk Management přiřadil písmeno optické jednotce, objeví se tato jednotka jako další dostupné písmeno jednotky za všemi diskovými jednotkami na integrovaném serveru. Nejsou-li s popisem síťového serveru propojeny žádné uživatelsky definované diskové jednotky, jeví se optická jednotka obvykle jako jednotka E.



---

## Kapitola 10. Sdílení zařízení

Jednou z výhod integrovaných Windows serverů je jejich schopnost používat zařízení iSeries. Na Windows serveru můžete používat optické jednotky, páskové jednotky a tiskárny serveru iSeries.

Přístup k zařízením serveru iSeries zahrnuje tyto úlohy:

- Operační systém i5/OS a Windows server používají pro odkazy na zařízení odlišná jména, proto se musíte nejprve seznámit se jmény odpovídajících popisů zařízení a hardwarových prostředků, které chcete používat. Další informace najdete v tématu “Určení popisu zařízení a jmen hardwarových prostředků pro zařízení iSeries”.
- Chcete-li použít optickou jednotku na integrovaném serveru, logicky ji zapněte v operačním systému i5/OS. Další informace najdete v tématu “Použití optických jednotek serveru iSeries s integrovanými Windows servery”.
- Informace o alokaci jednotek integrovaným Windows serverům, formátování pásek, přenášení jednotek mezi servery a přenesení jednotek zpět do operačního systému i5/OS najdete v tématu “Použití páskových jednotek serveru iSeries s integrovanými Windows servery” na stránce 164.
- Prostudujte téma “Tisk z integrovaného Windows serveru na tiskárnách serveru iSeries” na stránce 168.

---

### Určení popisu zařízení a jmen hardwarových prostředků pro zařízení iSeries

Odkazujete-li se na zařízení serveru iSeries v operačním systému i5/OS, musíte používat jména popisů těchto zařízení. Když se na tato zařízení odvoláváte z integrovaného Windows serveru, musíte použít jméno hardwarového prostředku. Jsou-li jména odlišná a vy použijete špatné jméno, dostanete nesprávné zařízení.

Chcete-li určit jméno hardwarového prostředku a zjistit, zda je stejné jako jméno popisu zařízení, postupujte takto:

1. Na příkazový řádek operačního systému i5/OS napište `DSPDEVD jméno_popisu_zařízení` a stiskněte klávesu Enter.
2. Pole Jméno prostředku obsahuje jméno hardwarového prostředku tohoto zařízení. Zkontrolujte, zda má stejné jméno jako pole Popis zařízení. Pokud jsou tato jména odlišná, musíte používat odpovídající jméno v závislosti na tom, zda pracujete v prostředí integrovaného Windows serveru nebo v prostředí operačního systému i5/OS.

Některé páskové jednotky se hlásí pod více než jedním popisem zařízení. Páskové knihovny (3590, 3570 atd.) se hlásí jako zařízení (TAPxx), stejně jako páskové knihovny (TAPMLBxx), kde xx je číslo. Produkt IBM Integrated Server Support nepodporuje páskové knihovny. Proto, má-li vaše zařízení popis páskové knihovny, musí být jak pásková jednotka, tak zařízení páskové knihovny ve stavu “logicky vypnuto” dříve, než se toto zařízení na Windows serveru uzamkne.

---

### Použití optických jednotek serveru iSeries s integrovanými Windows servery

Windows server může použít optickou jednotku serveru iSeries stejně jako lokální optickou jednotku. Optická jednotka iSeries se jeví jako běžná optická jednotka ve složce **My Computer** na Windows serveru.

Pokud máte na serveru iSeries logické části, alokuje se optická jednotka jediné logické části. Nemohou ji sdílet integrované servery, které jsou v jiných logických částech a optická jednotka musí být alokována (zamčena) popisu síťového serveru (NWSD), aby mohla být použita.

Optická jednotka musí být logicky zapnuta předtím, než ji můžete alokovat integrovanému Windows serveru. Jestliže optická jednotka není logicky zapnuta, zapněte ji takto:

1. Na příkazový řádek operačního systému i5/OS napište `WRKCFGSTS *DEV *OPT` a stiskněte klávesu Enter.
2. Do pole **Volba** vedle správné optické jednotky, zpravidla OPT01, napište 1 a logicky zapněte optickou jednotku.

3. Stiskněte klávesu Enter. Optická jednotka se logicky zapne.

Chcete-li optickou jednotku uzamknout, postupujte takto:

1. Klepněte na **Start**, potom na **Programs**, na **IBM iSeries** a potom na **IBM iSeries Integrated Server Support**.
2. Rozbalte **IBM iSeries Integrated Server Support**.
3. Rozbalte jméno popisu síťového serveru.
4. Vyberte **iSeries Devices**.
5. Vyberte jméno zařízení.
6. Klepněte pravým tlačítkem myši, vyberte volbu **All Tasks** a pak **Lock Device**.

Budete-li mít problémy s použitím optické jednotky serveru iSeries z integrovaného Windows serveru, přečtěte si téma “Problémy s optickou jednotkou” na stránce 202.

**Poznámka:**

l Selže-li integrovaný server dříve, než uvolní zámek optické jednotky, může být tato jednotka pro operační  
l systém i5/OS nebo pro ostatní integrované servery nedostupná. Zámek můžete uvolnit, jestliže tuto optickou  
l jednotku logicky vypnete pomocí příkazu WRKCFGSTS \*DEV \*OPT a znovu ji zapnete.

### **Navrácení řízení optické jednotky z integrovaného serveru na server iSeries**

Chcete-li tuto optickou jednotku použít v systému i5/OS, musíte ji nejprve odemknout na integrovaném serveru. Chcete-li odemknout optickou jednotku z integrovaného serveru, musíte být buď stejná osoba, která jednotku původně uzamkla, nebo budete potřebovat oprávnění administrátora či operátora zálohování.

Chcete-li převést řízení optické jednotky serveru iSeries z integrovaného serveru na server iSeries, postupujte takto:

1. Klepněte na **Start**, potom na **Programs**, na **IBM iSeries** a potom na **IBM iSeries Integrated Server Support**.
2. Rozbalte **IBM iSeries Integrated Server Support**.
3. Rozbalte jméno popisu síťového serveru.
4. Vyberte **iSeries Devices**.
5. Vyberte zařízení, které chcete odemknout.
6. Klepněte pravým tlačítkem myši a vyberte **All Tasks**, pak **Unlock Device**.

---

## **Použití páskových jednotek serveru iSeries s integrovanými Windows servery**

Páskové jednotky iSeries dokáží pracovat podstatně rychleji, než jednotky, které obvykle připojujete k PC serveru. Tyto páskové jednotky můžete alokovat integrovaným serverům, takže poskytují rychlejší přístupovou metodu pro pásky, než jakou mají k dispozici PC servery. Další informace najdete v tématu “Podporované páskové jednotky iSeries” na stránce 167.

Protože ve stejném systému iSeries může mít k téže páskové jednotce přístup několik integrovaných serverů (i když ne současně), stačí několika integrovaným serverům alokovat jen jednu páskovou jednotku.

**Poznámky:**

1. I když můžete páskové jednotky vyhradit pro integrovaný server i pro operační systém i5/OS, nemohou používat stejnou páskovou jednotku oba systémy současně. Oba operační systémy vyžadují různé páskové formáty. Nemůžete používat stejnou pásku na integrovaném serveru a v systému i5/OS, aniž byste ji přeformátovali.
2. Pokud máte na serveru iSeries logické části, je pásková jednotka alokována do jediné logické části. Nemohou ji sdílet integrované servery, které jsou v jiných logických částech.

Chcete-li použít páskovou jednotku serveru iSeries z integrovaného serveru, musíte provést tyto úlohy:

- “Formátování pásky v i5/OS pro použití s integrovanými Windows servery” na stránce 165.

- Alokovat páskovou jednotku iSeries integrovanému serveru logickým vypnutím této páskové jednotky v systému i5/OS a jejím zamknutím na integrovaném serveru. Další informace najdete v tématu “Alokace páskové jednotky serveru iSeries pro integrovaný Windows server”.
- Přenést řízení páskové jednotky iSeries na jiný integrovaný server. Další informace najdete v tématu “Přenos řízení páskových a optických jednotek iSeries mezi integrovanými Windows servery” na stránce 167.
- Vrátit řízení páskové jednotky z integrovaného serveru tak, aby ji mohl používat operační systém i5/OS. Zajistit, abyste měli správně formátovanou pásku. Další informace najdete v tématu “Předání řízení páskové jednotky z integrovaného Windows serveru zpět na server iSeries” na stránce 166.


Budete-li mít problémy s páskovou jednotkou iSeries, přečtěte si téma “Problémy s páskami” na stránce 202.

## Instalace ovladačů páskových jednotek

Informace o podporovaných ovladačích páskových jednotek najdete v publikaci Supported tape devices for Windows servers.

Při instalaci těchto ovladačů nejsou vyžadovány žádné zvláštní akce. Stačí jen dodržovat pokyny dodavatele ovladače. Nové ovladače páskových jednotek vypadají stejně jako ovladače pro servery xSeries. V obslužném programu pro zamykání a odemykání zařízení jsou zařízení uvedena podle čísla typu a modelu.

Páskové jednotky, které byly uzamčeny, se mohou po restartování serveru zobrazit v produktu Removable Storage Manager a v některých zálohovacích aplikacích jako další instance zařízení. Jedná se o obvyklé chování. Výmaz těchto dalších instancí by měl být bezpečný. Prostudujte příslušnou dokumentaci. Nejnovější informace najdete

v publikaci Tape driver migration  na webové stránce iSeries integrated xSeries ([www.ibm.com/servers/eserver/iseries/integratedxseries/windows/tape\\_driver\\_migration.html](http://www.ibm.com/servers/eserver/iseries/integratedxseries/windows/tape_driver_migration.html)).

## Formátování pásky v i5/OS pro použití s integrovanými Windows servery

Chcete-li použít páskové jednotky serveru iSeries s integrovaným Windows servery, musíte použít formát pásky, který rozpoznají. K vytvoření neoznačené pásky akceptovatelné systémem Windows použijte příkaz INZTAP (Inicializace pásky) operačního systému i5/OS.

Při formátování pásky postupujte takto:

- Nasaďte pásku, kterou chcete použít, do páskové jednotky iSeries.
- Na příkazový řádek operačního systému i5/OS napište:

```
INZTAP DEV(tap01) NEWVOL(*NONE) NEWOWNID(*BLANK) VOL(*MOUNTED)
CHECK(*NO) DENSITY(*CTGTYPE) CODE(*EBCDIC)
```

kde *tap01* je jméno vaší páskové jednotky. Stiskněte klávesu Enter.

## Alokace páskové jednotky serveru iSeries pro integrovaný Windows server

Chcete-li použít páskovou jednotku serveru iSeries z konzole integrovaného Windows serveru, musíte ji v systému i5/OS logicky vypnout a zamknout ji na integrovaném serveru. Zařízení musíte zamknout předtím, než spustíte aplikace nebo jejich služby.

### Poznámka:

Některé páskové jednotky se hlásí pod více než jedním popisem zařízení. Páskové knihovny (3590, 3570 atd.) se hlásí jako zařízení (TAPxx), stejně jako páskové knihovny (TAPMLBxx), kde xx je číslo. Produkt IBM iSeries Integrated Server Support nepodporuje páskové knihovny. Proto, má-li vaše zařízení popis páskové knihovny, musí být jak pásková jednotka, tak zařízení páskové knihovny ve stavu “logicky vypnuto” dříve, než se toto zařízení na integrovaném serveru uzamkne.

Chcete-li převést řízení páskové jednotky iSeries na integrovaný server, postupujte takto:



1. Logicky vypněte páskovou jednotku v systému i5/OS:
  - Chcete-li to provést pomocí produktu iSeries Navigator, postupujte takto:
    - a. Klepněte na **Konfigurace a služba** → **Hardware** → **Páskové jednotky**.
    - b. Klepněte na **Samostatná zařízení** nebo na **Páskové knihovny**.
    - c. Klepněte pravým tlačítkem myši na zařízení nebo knihovnu a vyberte volbu **Zablokovat**.
  - Chcete-li to provést ve znakově orientovaném rozhraní prostředí operačního systému i5/OS, postupujte takto:
    - a. Na příkazový řádek operačního systému i5/OS napište WRKCFGSTS \*DEV \*TAP a stiskněte klávesu Enter. Objeví se obrazovka Práce se stavem konfigurace.

**Poznámka:**

Pomocí příkazu WRKCFGSTS \*DEV \*TAPMLB lze zobrazit seznam zařízení páskové knihovny.

- b. Do pole **Volba** vedle jména zařízení vaší páskové jednotky napište 2 a logicky vypněte páskovou jednotku.
  - c. Stiskněte klávesu Enter. Pásková jednotka se logicky vypne.
2. Uzamknutí páskové jednotky na integrovaném serveru:
    - a. Na konzoli Windows integrovaného serveru klepněte na **Start** → **Programs** → **IBM iSeries** → **IBM iSeries Integrated Server Support**.
    - b. Rozbalte **IBM iSeries Integrated Server Support**.
    - c. Rozbalte jméno popisu síťového serveru.
    - d. Vyberte **iSeries Devices**.
    - e. Vyberte páskový objekt, který chcete uzamknout.
    - f. Klepněte pravým tlačítkem myši a vyberte **All Tasks, Lock Device**.
  3. Jestliže potřebujete další informace o páskové jednotce, aby je aplikace rozpoznala, najdete je v tématu “Identifikace páskových jednotek iSeries pro aplikace” na stránce 167. Nastanou-li problémy, přečtěte si téma “Problémy s páskami” na stránce 202.

## Předání řízení páskové jednotky z integrovaného Windows serveru zpět na server iSeries

Chcete-li v operačním systému i5/OS používat páskovou jednotku, která je na integrovaném serveru momentálně uzamčena, musíte ji nejprve odemknout v prostředí integrovaného serveru a logicky zapnout v systému i5/OS. Chcete-li odemknout páskovou jednotku z Windows serveru, musíte být buď stejná osoba, která jednotku původně uzamkla, nebo potřebujete oprávnění administrátora či operátora zálohování.

Chcete-li převést řízení páskové jednotky serveru iSeries z integrovaného Windows serveru na server iSeries, postupujte takto:

1. Odemkněte páskovou jednotku z konzole integrovaného Windows serveru.
  - a. Klepněte na **Start, Programs, IBM iSeries** a **IBM iSeries Integrated Server Support**.
  - b. Rozbalte **IBM iSeries Integrated Server Support**.
  - c. Rozbalte jméno popisu síťového serveru.
  - d. Vyberte **iSeries Devices**.
  - e. Vyberte páskový objekt, který chcete uzamknout.
  - f. Vyberte **Action, All Tasks** a **Unlock Device**.
2. Zpřístupněte zařízení operačnímu systému i5/OS z konzole i5/OS.
  - V prostředí iSeries Navigator
    - a. Klepněte na **Konfigurace a služba** → **Hardware** → **Páskové jednotky**.
    - b. Klepněte na **Samostatná zařízení** nebo na **Páskové knihovny**.
    - c. Klepněte pravým tlačítkem myši na zařízení nebo knihovnu a vyberte volbu **Zpřístupnit**.
  - V rozhraní příkazového řádku operačního systému i5/OS

- a. Na příkazový řádek operačního systému i5/OS napište `WRKCFGSTS *DEV *TAP` a stiskněte klávesu Enter. Objeví se obrazovka Práce se stavem konfigurace.
- b. Do sloupce pro volbu vedle jména zařízení páskové jednotky (například TAP01) napište hodnotu 1, aby bylo možné páskovou jednotku logicky zapnout.
- c. Stiskněte klávesu Enter. Pásková jednotka se logicky zapne.
- d. Změňte pásku na pásku naformátovanou pro operační systém i5/OS.

## Podporované páskové jednotky iSeries

Schopnost používat páskové jednotky iSeries z integrovaných Windows serverů závisí na modelu páskového zařízení, řadiči pásek a typu médií.

Podporované páskové jednotky jsou uvedeny na webové stránce Integrated xSeries Solutions  .

Páskové knihovny nejsou podporovány jako knihovny, ale mohou být podporovány jako jednotlivá zařízení.

Jak ACF (Auto Cartridge Facilities), tak ACL (Auto Cartridge Loaders) podporují manuální i automatický režim. Jestliže je ACL nebo ACF v automatickém režimu, bude další páska zavedena automaticky, jestliže aplikace zálohování vytočí plnou pásku. Obslužný program Windows pro zálohování to provede automaticky bez zásahu uživatele. Program Veritas Backup Exec zobrazí dialogové okno s následující zprávou: "Please remove the media from the drive, and respond OK". Klepnutí na **Respond OK** v tomto dialogovém okně způsobí, že zálohování bude pokračovat normálně.

## Identifikace páskových jednotek iSeries pro aplikace

Při identifikaci páskových jednotek nepoužívají aplikace popis zařízení ani jméno hardwarového prostředku jako operační systém i5/OS. Místo toho zobrazují páskové jednotky jedním ze tří způsobů:

- Výrobní číslo-komponenta-model.
- Mapa zařízení.
- Port-sběrnice-cíl id-logická jednotka.

Pokud tyto hodnoty potřebujete, postupujte takto:

1. Na konzoli integrovaného Windows serveru klepněte na **Start** → **Programs** → **Administrative Tools** → **Computer Management**.
2. Klepněte na **System Tools**.
3. Klepněte na **Device Manager**.
4. Klepněte dvakrát na **Tape Devices**.
5. Klepněte pravým tlačítkem myši na páskovou jednotku.
6. Vyberte **Vlastnosti**.
7. Okénko Vlastnosti má dvě karty, jednu označenou **General** a jednu označenou **Driver**. Na kartě **Obecné** je zobrazeno jméno zařízení a číslo sběrnice, ID cíle a LUN.

Jestliže jsou všechny páskové jednotky na vašem serveru iSeries odlišného typu, stačí tyto informace k tomu, aby aplikace Windows mezi nimi mohly rozlišovat. Máte-li několik páskových jednotek se stejnými čísly výrobní-komponenta-model, musíte experimentovat, abyste stanovili, která pásková jednotka je která.

## Přenos řízení páskových a optických jednotek iSeries mezi integrovanými Windows servery

Jestliže máte několik integrovaných serverů, může páskovou nebo optickou jednotku iSeries používat vždy jen jeden. Chcete-li přenést ovládání páskových a optických jednotek z jednoho serveru na druhý, musíte je na jednom serveru odemknout a na druhém uzamknout.

**Poznámka:**

Pokud máte na serveru iSeries logické části, alokuje se pásková a optická jednotka do jediné logické části a nemůže být sdílena integrovanými servery, které jsou v jiných logických částech.

Chcete-li převést řízení páskové nebo optické jednotky serveru iSeries z jednoho integrovaného serveru na druhý, postupujte takto:

Na konzoli integrovaného serveru, který má řízení jednotky:

1. Klepněte na **Start, Programs, IBM iSeries** a **IBM iSeries Integrated Server Support**.
2. Rozbalte **IBM iSeries Integrated Server Support**.
3. Rozbalte jméno popisu síťového serveru.
4. Vyberte **iSeries Devices**.
5. Vyberte zařízení, které chcete odemknout.
6. Vyberte **Action**, pak **All Tasks**, pak **Unlock Device**.

Na konzoli integrovaného serveru, kterému chcete řízení předat, uzamkněte páskovou nebo optickou jednotku.


1. Klepněte na **Start, Programs, IBM iSeries** a **IBM iSeries Integrated Server Support**.
2. Rozbalte **IBM iSeries Integrated Server Support**.
3. Rozbalte **Network Server Description name**.
4. Vyberte **iSeries Devices**.
5. Vyberte zařízení, které chcete uzamknout.
6. Vyberte **Action**, pak **All Tasks**, pak **Lock Device**.

---

## Tisk z integrovaného Windows serveru na tiskárnách serveru iSeries

Chcete-li odeslat tiskovou úlohu do operačního systému i5/OS, musíte nastavit tiskárnu v operačním systému i5/OS na tisk pomocí TCP/IP. Také musíte nastavit integrovaný server, aby používal tiskárnu přes protokol LPD/LPR. Integrovaný server musí mít také nainstalovanou síťovou službu **Microsoft TCP/IP Printing**. Další informace o tisku TCP/IP najdete v dokumentaci Windows.

Chcete-li nastavit integrovaný server tak, aby byl tisk prováděn na tiskárnách v operačním systému i5/OS, postupujte takto:

1. Nastavte tiskárnu i5/OS na tisk pomocí TCP/IP. Další informace uvádí publikace Konfigurace TCP/IP a referenční informace  .
2. Nastavte integrovaný server tak, aby byl tisk prováděn na tiskárnách v operačním systému i5/OS:
  - a. V nabídce **Start** na serveru Windows 2000 Server nebo Windows Server 2003 klepněte na **Settings**, pak na **Printers**. Objeví se okno **Printers**.
  - b. Klepněte dvakrát na ikonu **Add Printer**. Spustí se průvodce **Add Printer Wizard**.
  - c. Klepněte na tlačítko **Network Printer**.
  - d. Do dialogového okna **Locate your Printer** napište jméno tiskárny nebo klepněte na **Next** a vyhledejte tiskárnu.

---

## Kapitola 11. Administrace uživatelů integrovaných Windows serverů v operačním systému i5/OS

Jednou z hlavních předností prostředí Windows na serveru iSeries je synchronizovaná a zjednodušená administrace uživatelů. Uživatelské profily a skupiny existující v operačním systému i5/OS lze zapisovat na integrované Windows servery, což znamená, že se tito uživatelé mohou přihlašovat na Windows server pod stejným ID a heslem uživatele jako do operačního systému i5/OS. Změní-li uživatelé svá hesla v systému i5/OS, změní se také jejich hesla ve Windows.

Informace o koncepcích najdete v tématu: “Koncepce týkající se uživatelů a skupin” na stránce 49.

Toto téma popisuje úkoly, které souvisejí s administrací uživatelů:

- “Zápis jednoho uživatele operačního systému i5/OS do prostředí Windows pomocí produktu iSeries Navigator”
- “Zápis skupiny uživatelů operačního systému i5/OS do prostředí Windows pomocí produktu iSeries Navigator” na stránce 170
- “Zápis uživatelů operačního systému i5/OS do prostředí Windows pomocí znakově orientovaného rozhraní” na stránce 170
- “Vytvoření šablony uživatele” na stránce 170
- “Zadání domovského adresáře do šablony” na stránce 171
- “Změna atributu LCLPWDMGT v uživatelském profilu” na stránce 172
- “Mapování EIM” na stránce 172
- “Vyřazení uživatelů zapsaných v prostředí Windows” na stránce 174
- “Vyřazení skupin zapsaných v prostředí Windows” na stránce 174
- “Uživatel QAS400NT” na stránce 175
- “Jak zabránit zápisu a přenesení uživatelského profilu na integrovaný Windows server” na stránce 177

---

### Zápis jednoho uživatele operačního systému i5/OS do prostředí Windows pomocí produktu iSeries Navigator

Pokud pro daného uživatele ještě nebyl vytvořen uživatelský profil v systému i5/OS, vytvořte jej. Informace o vytváření uživatelských profilů v systému i5/OS najdete v publikaci Zabezpečení iSeries - Referenční informace



K zápisu jednoho uživatele do prostředí Windows použijte tento postup:

1. V prostředí produktu iSeries Navigator rozbalte **Administrace integrovaných serverů**—>**Servery** nebo **Domény**.
2. V seznamu klepněte pravým tlačítkem myši na některou doménu nebo na server Windows a vyberte volbu **Zapsat uživatele**.

**Poznámka:** Nevybírejte pracovní skupinu Windows. Zápis do pracovní skupiny není podporován.

3. Zvolte, zda chcete jméno uživatele zadat, nebo vybrat ze seznamu.
4. (Volitelné) Chcete-li při vytváření uživatele použít šablonu, zadejte uživatele Windows, který bude sloužit jako šablona pro vytvoření nového uživatele Windows. Pamatujte si, že jestliže uživatele použitého jako šablonu později změníte, změny se u již vytvořeného uživatele neprojeví.
5. Klepněte na **Zapsat**.

Narazíte-li při zápisu uživatelů na problém, prostudujte téma “Problémy při zápisu uživatelů a skupin” na stránce 208.

---

## Zápis skupiny uživatelů operačního systému i5/OS do prostředí Windows pomocí produktu iSeries Navigator

Tento postup zapíše všechny uživatele ze skupiny operačního systému i5/OS do prostředí Windows. Informace o vytváření uživatelských a skupinových profilů operačního systému i5/OS najdete v publikaci Zabezpečení iSeries -

Referenční informace .

Při zápisu skupiny operačního systému i5/OS a jejích členů do prostředí Windows postupujte takto:

1. Rozbalte **Administrace integrovaných serverů** —> **Servery nebo Domény**.
2. V seznamu klepněte pravým tlačítkem myši na některou Windows doménu nebo server a vyberte **Zapsat skupiny**.  
**Poznámka:** Nevybírejte pracovní skupinu Windows. Zápis do pracovní skupiny není podporován.
3. Zadejte jméno skupiny nebo vyberte dosud nezapsanou skupinu ze seznamu.
4. (Volitelné) Chcete-li při vytváření nových uživatelů použít šablonu, zadejte uživatele Windows, kterého chcete použít jako šablonu pro vytvoření uživatelů této nové skupiny ve Windows. Jestliže použitou šablonu uživatele později změníte, tyto změny se u již vytvořeného uživatele neprojeví.
5. Vyberte **Globální** v případě, že zapisujete skupinu do domény a měla by být pro tuto doménu viditelná. Jinak vyberte **Lokální**. Lokální skupiny Windows serveru mohou obsahovat uživatele i globální skupiny Windows serveru, zatímco globální skupiny Windows serveru mohou obsahovat pouze uživatele. Více informací o typech skupin najdete online nápovědě Windows.
6. Klepněte na **Zapsat**.

Narazíte-li při zápisu skupin na problém, prostudujte téma “Problémy při zápisu uživatelů a skupin” na stránce 208.

---

## Zápis uživatelů operačního systému i5/OS do prostředí Windows pomocí znakově orientovaného rozhraní

### Zápis uživatelů do prostředí Windows

1. Ve znakově orientovaném rozhraní operačního systému i5/OS napište CHGNWSUSRA a stiskněte klávesu **F4**.
2. Do pole **Uživatelský profil** napište jméno uživatelského profilu operačního systému i5/OS, který chcete zapsat do prostředí Windows.
3. Stiskněte dvakrát klávesu **Enter**. Měla by se objevit další pole.
4. Přejděte pomocí klávesy **Page down** dolů a zadejte domény a lokální servery Windows, do kterých chcete uživatele zapsat.
5. Stisknutím klávesy **Enter** změny potvrďte.

### Tabulka používaných CL příkazů

Tabulka 4.

WRKUSRPRF	Práce s uživatelskými profily i5/OS.
WRKNWSEN	Práce s uživatelskými profily i5/OS zapsanými do prostředí Windows.
CHGNSWUSRA	Zápis uživatelů i5/OS do prostředí Windows.

---

## Vytvoření šablony uživatele

Šablona pro zápis uživatelů je nástroj, který usnadňuje zápis uživatelů operačního systému i5/OS do prostředí Windows. Namísto zdoluhavého manuálního konfigurování mnoha nových uživatelů se stejným nastavením můžete s využitím šablony pro zápis uživatelů nakonfigurovat tyto uživatele automaticky. Informace o šablonách pro zápis uživatelů najdete v tématu Šablony pro zápis uživatelů.

Při vytváření šablony pro uživatele Windows postupujte takto:

#### Windows 2000 Server nebo doména Windows Server 2003:

1. Na konzoli integrovaného serveru klepněte na **Start** → **Programs** → **Administrative Tools** → **Active Directory Users and Computers**.
2. Klepněte na jméno domény.
3. Pravým tlačítkem myši klepněte na **Users** a vyberte **New** → **User**.
4. Do polí **Username** a **Logon name** zadejte rozlišovací jméno pro šablonu, například *stduser* nebo *admtemp*. Klepněte na **Next**.
5. Doporučujeme zrušit zaškrtnutí políčka **User must change password at next logon** a zaškrtnout políčka **User cannot change password**, **Password never expires** a **Account is disabled**. Tím vyloučíte možnost, že by se některý uživatel přihlásil k integrovanému serveru pod účtem této šablony.
6. Pro účet šablony nezádávejte žádné heslo.
7. Klepněte na **Finish**.
8. Chcete-li nastavit členství ve skupině, dvakrát klepněte na jméno své šablony v seznamu uživatelů a skupin, který se zobrazí v pravé části okna. Klepněte na kartu **Member of** a potom na **Add**. Tak přidělíte požadované skupiny.

#### Windows 2000 Server nebo Windows Server 2003 server:

1. Z konzole integrovaného serveru
  - Na serveru Windows 2000 Server klepněte na **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **Local Users and Groups**.
  - Na serveru Windows Server 2003 klepněte na **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **System Tools** → **Local Users and Groups**.
2. Vyberte **System Tools** → **Local Users and Groups**.
3. Pravým tlačítkem myši klepněte na **Users** a vyberte **New User**.
4. Do pole **User Name** zadejte rozlišovací jméno pro šablonu, například *stduser* nebo *admtemp*.
5. Doporučujeme zrušit zaškrtnutí políčka **User must change password at next logon** a zaškrtnout políčka **Password never expires**, **User cannot change password** a **Account is disabled**. Tím vyloučíte možnost, že by se některý uživatel přihlásil k Windows serveru pod účtem této šablony.
6. Klepněte na **Create** a potom na **Close**.
7. Klepněte na **Users** nebo aktualizujte okno, aby se nová šablona uživatele zobrazila.
8. Chcete-li nastavit členství ve skupině, dvakrát klepněte na jméno šablony v seznamu uživatelů a skupin, který se zobrazí v pravé části okna. Klepněte na kartu **Member of** a potom na **Add**. Tak přidělíte požadované skupiny.

Uživatelskou šablonu můžete zařadit do libovolné skupiny Windows serveru bez ohledu na to, zda jste tuto skupinu zapsali v systému i5/OS, či nikoli. Uživatele můžete zapsat pomocí šablony, která je členem skupiny, i když nebyla zapsána v systému i5/OS. V takovém případě můžete uživatele ze skupiny odstranit pouze pomocí programu User Manager, který je funkcí Windows serveru.

Vytváříte-li šablonu pro zápis administrátorů, můžete ji začlenit do skupiny *Administrators* na Windows serveru. Podobně, chcete-li zabránit náhodnému výmazu uživatelů Windows z operačního systému i5/OS, zařaďte tuto šablonu do skupiny *AS400\_Permanent\_Users* (nebo *OS400\_Permanent\_Users*).

---

## Zadání domovského adresáře do šablony

Aby řízení uživatelů v prostředí Windows na serveru iSeries probíhalo co nejefektivněji, můžete pro každého uživatele nastavit domovský adresář, do kterého se budou ukládat informace specifické pro uživatele, které jsou generovány aplikacemi. Chcete-li si ušetřit práci, specifikujte domovské adresáře již v účtech šablon. Pro každý nově vytvořený profil se tak při zápisu automaticky vytvoří domovský adresář. Aby byla zajištěna výkonová přizpůsobivost, je důležité nepřirazovat domovské adresáře napevno k určité diskové jednotce. K zajištění přenositelnosti dodržujte univerzální konvence pojmenování (UNC).



K zadání domovského adresáře do profilu šablony použijte na konzoli integrovaného Windows serveru tento postup:

1. Na příslušném serveru vytvořte složku domovského adresáře a nastavte její sdílení.
2. Z konzole Windows serveru klepněte v případě domény na **Start->Programs->Administrative Tools->Active Directory Users and Computers**. V případě lokálního serveru klepněte na **Start->Programs->Administrative Tools-> Computer Management->Local Users and Groups**.
3. Dvojitým klepnutím na šablonu (modelového uživatele) zobrazte její vlastnosti.
4. Klepněte na kartu Profile.
5. V segmentu Home Folder klepněte na **Connect**. Vyberte písmeno jednotky (například Z:). Přejděte na dialog **To:** a zadejte cestu k domovskému adresáři pomocí jména UNC, například: `\\iSeriesWin\homedirs\%username%`. V tomto příkladu je **iSeriesWin** jméno serveru, kde se nachází domovský adresář, a **homedirs** je jméno složky domovského adresáře. Jestliže namísto přihlašovacího nebo uživatelského jména použijete proměnnou `%username%`, Windows server při vytváření účtu vždy automaticky nahradí tuto proměnnou uživatelským jménem. Zároveň pro tohoto uživatele vytvoří domovský adresář.

---

## Změna atributu LCLPWDMGT v uživatelském profilu

Toto téma popisuje, jak změnit v uživatelském profilu atribut LCLPWDMGT (Local Password Management). Atribut LCLPWDMGT je popsán v tématech “Koncepce týkající se uživatelů a skupin” na stránce 49 a “Typy uživatelských konfigurací” na stránce 51.

Chcete-li změnit atribut uživatelského profilu LCLPWDMGT ve *znakově orientovaném rozhraní*, postupujte v operačním systému i5/OS takto:

1. Napište CHGUSRPRF a jméno uživatelského profilu, který chcete změnit.
2. Pokračujte stisknutím klávesy F4.
3. Stisknutím klávesy **F9** zobrazíte všechny atributy a stisknutím klávesy **F11** jejich zkratky.
4. Vyhledejte atribut LCLPWDMGT a nastavte jej na jednu z hodnot \*YES a \*NO.
5. Stiskněte klávesu Enter.

---

## Mapování EIM

### Co je to EIM?

Mapování EIM (Enterprise Identity Mapping) je způsob, jak sjednotit různé ID a hesla jednoho uživatele pod jediným účtem. Při použití této metody se uživatel přihlásí do operačního systému pouze jednou a EIM ve spolupráci s dalšími službami autentizuje tohoto uživatele pod všemi jeho účty.

Toto prostředí se nazývá prostředí s jediným přihlášením (single sign-on). Autentizace sice probíhá při každém pokusu uživatele o přístup k novému systému, není však při ní vyžadováno zadání hesla. Při používání EIM uživatelé nemusí hlídat a spravovat množství uživatelských jmen a hesel pro přístup k dalším systémům v síti. Jakmile je uživatel v síti autentizován, může používat služby a aplikace v rámci celého podniku, aniž by potřeboval další hesla.

V aplikaci Information Center je celé jedno téma věnováno EIM. Další informace najdete v tématu Enterprise Identity Mapping.

Chcete-li se dozvědět více o různých metodách zápisu uživatelů do prostředí Windows, prostudujte téma “Typy uživatelských konfigurací” na stránce 51.

### Atribut uživatelského profilu EIMASSOC

EIMASSOC je atribut uživatelského profilu, který slouží ke konfiguraci prostředí EIM. Na příkazový řádek operačního systému i5/OS napište CHGUSRPRF a jméno uživatelského profilu a potom pokračujte stisknutím klávesy F4. Potom přejděte pomocí klávesy Page Down až na konec do tématu EIM association. Zde je uveden význam jednotlivých polí:



- **Prvek 1: EIM identifier** (identifikátor EIM). Je to ID uživatele, který EIM používá k identifikaci. Můžete jej považovat za váš hlavní ID (Master ID), pod nímž jsou uloženy všechny vaše ostatní ID uživatele. Zadáte-li hodnotu \*USRPRF, použije systém jméno vašeho uživatelského profilu v operačním systému i5/OS jako identifikátor EIM. Jinak můžete zadat libovolný platný znakový řetězec. Jestliže do tohoto pole zadáte hodnotu \*DLT a stisknete klávesu Enter, zobrazí se seznam změněných voleb pro výmaz asociace EIM.
- **Prvek 2: Association type** (typ asociace) Tato hodnota udává, jakým způsobem bude uživatelský profil v operačním systému i5/OS přiřazen k identifikátoru EIM. V prostředí Windows na serveru iSeries umožňují hodnoty \*TARGET, \*TGTSRC a \*ALL automatické vytváření a výmaz cílových asociací operačního systému i5/OS a zdrojových asociací systému Windows.
- **Prvek 3: Association action** (akce asociace). Zvláštní hodnoty jsou:
  - \*REPLACE Ze všech identifikátorů EIM, které jsou svázány s tímto uživatelským profilem, budou odstraněny veškeré zdrojové asociace Windows. Pro zapsaného uživatele bude k danému identifikátoru EIM přidána nová zdrojová asociace Windows.
  - \*ADD Pro zapsaného uživatele bude přidána zdrojová asociace Windows.
  - \*REMOVE Zdrojová asociace Windows bude odstraněna.
- **Prvek 4: Create EIM identifier** (vytvoření identifikátoru EIM). Tato hodnota udává, zda má být vytvořen identifikátor EIM, pokud dosud neexistuje. Povolené zvláštní hodnoty jsou: \*NOCRTEIMID - identifikátor EIM nebude vytvořen, nebo \*CRTEIMID - identifikátor EIM bude vytvořen, pokud neexistuje.

### Automatické a manuální asociace EIM

V typickém prostředí EIM, které používá jediné přihlášení, jsou obvykle definovány cílové asociace operačního systému i5/OS a zdrojové asociace systému Windows. Při administraci uživatelů na integrovaném Windows serveru může administrátor systém nastavit tak, že zapsaní uživatelé Windows budou mít automaticky definovány asociace EIM. Pokud zapsaný uživatel Windows zadal například EIMASSOC(\*USRPRF \*TARGET \*ADD \*CRTEIMID), operační systém i5/OS automaticky vytvoří cílovou asociaci v systému i5/OS a zdrojovou asociaci ve Windows. Hodnota atributu EIMASSOC se v uživatelském profilu neuchovává. Rovněž se neukládá ani neobnovuje s uživatelským profilem. A pokud operační systém i5/OS není konfigurován pro EIM, nebude provedena žádná asociace a informace atributu EIMASSOC budou ignorovány.

Je-li operační systém i5/OS konfigurován pro použití EIM a pro zapsaného uživatele je definováno zpracování atributu EIMASSOC, administrace uživatelů integrovaných Windows serverů automaticky vytvoří nebo vymaže zdrojové asociace Windows pro daného uživatele v registru Windows EIM. Pro uživatele zapsaného do prostředí Windows lokálně je jméno registru Windows EIM plně kvalifikované jméno DNS. Jako typ registru Windows EIM by měl být definován operační systém Windows 2000. Pro uživatele zapsané v doméně Windows je jméno registru Windows plně kvalifikované jméno domény DNS a jako typ registru Windows by měl být definován protokol Kerberos - bez rozlišení velkých a malých písmen. Je-li definován atribut EIMASSOC pro uživatele, operační systém i5/OS je konfigurován pro použití EIM a registr Windows EIM neexistuje, bude registr Windows EIM vytvořen administrací uživatelů integrovaného Windows serveru.

### Používání asociací EIM umožňuje používat různá jména uživatelských profilů Windows

EIM poskytuje mechanismus, jak přiřazovat uživatelské profily v adresářovém systému. EIM umožňuje definovat pro identifikátor EIM cílovou asociaci uživatelského profilu v systému i5/OS a zdrojovou asociaci uživatelského profilu ve Windows. Administrátor uživatelů může definovat zdrojovou asociaci ve Windows pomocí jiného jména uživatelského profilu Windows, než je jméno cílové asociace uživatelského profilu v systému i5/OS. Administrace uživatelů integrovaného Windows serveru bude pro zápis uživatelů používat tento uživatelský profil definovaný ve zdrojové asociaci EIM Windows, pokud existuje. Je nutné definovat cílovou asociaci v systému i5/OS. Při použití identifikátoru EIM musí být zdrojová asociace Windows definována administrátorem. Zdrojová asociace Windows musí být pro tentýž identifikátor EIM nadefinována v registru Windows EIM se správným jménem a typem. Pro uživatele lokálně zapsaného do Windows je jméno registru Windows EIM plně kvalifikované DNS jméno. Jako typ registru Windows EIM by měl být definován EIM\_REGTYPE\_WIN2K. Pro uživatele zapsané v doméně Windows je jméno registru Windows plně kvalifikované DNS jméno domény a jako typ registru Windows by měl být definován EIM\_REGTYPE\_KERBEROS\_IG.

---

## Vyřazení uživatelů zapsaných v prostředí Windows

Ke zrušení zápisu uživatele z domén a serverů Windows použijte tento postup:

1. Rozbalte **Administrace integrovaných serverů** —> **Servery nebo Domény**.
2. Rozbalte doménu nebo server, jenž obsahuje uživatele, kterého chcete vyřadit.
3. Vyberte **Zapsaní uživatelé**.
4. Klepněte pravým tlačítkem myši na uživatele, kterého chcete vyřadit.
5. Vyberte **Vyřadit**.
6. Klepněte na **Vyřadit** v potvrzovacím okně.

### Účinky zrušení zápisu uživatelů v prostředí Windows

Zrušením zápisu uživatele v prostředí Windows odstraníte tohoto uživatele ze seznamu uživatelů zapsaných na Windows serveru i ze skupiny AS400\_Users (nebo OS400\_Users) na Windows serveru. Není-li uživatel členem skupiny AS400\_Permanent\_Users (nebo OS400\_Permanent\_Users) na Windows serveru, je odstraněn i v prostředí Windows.

Uživatele, kteří jsou členy skupiny AS400\_Permanent\_Users (nebo OS400\_Permanent\_Users) na Windows serveru, nemůžete z Windows serveru vymazat ani vyřazením, ani výmazem z operačního systému i5/OS. Vyřazení však odstraní uživatele ze seznamu uživatelů zapsaných na Windows serveru a ze skupiny AS400\_Users (OS400\_Users) na Windows serveru.

- | Uživatele, které jste vyřadili v prostředí Windows, můžete ponechat v operačním systému i5/OS. Tento způsob se ale  
| nedoporučuje, protože umožňuje přidat tyto uživatele do skupin v systému i5/OS a změnit hesla v systému i5/OS,  
| aniž by kdy tyto změny projevil v prostředí Windows. Tyto nesrovnalosti mohou znesnadňovat sledování uživatelů  
| v obou systémech.

Uživatele můžete vyřadit mnoha způsoby. Mezi operace, které uživatele vyřadí, patří:

- Záměrné vyřazení uživatele.
- Výmaz uživatelského profilu i5/OS.
- Vyřazení všech skupin operačního systému i5/OS, do kterých uživatel patří.
- Odstranění uživatele ze zapsané skupiny operačního systému i5/OS v případě, že tento uživatel nepatří do žádné jiné zapsané skupiny.

---

## Vyřazení skupin zapsaných v prostředí Windows

Vyřazením skupiny v prostředí Windows se vyřadí i všichni uživatelé, jejichž zápis je omezen pouze na tuto skupinu. Pokud skupina obsahuje pouze členy zapsané jejím prostřednictvím, tato skupina je v prostředí Windows vymazána.

Obsahuje-li však tato skupina i členy přidané v prostředí Windows a nikoli v prostředí i5/OS, nebude vymazána. Jedinými členy, které tato skupina může ještě obsahovat, jsou nezapsaní uživatelé.

K vyřazení skupiny z domén a serverů Windows použijte v produktu iSeries Navigator tento postup:

- | 1. Rozbalte **Administrace integrovaných serverů** —> **Servery nebo Domény**.
2. Rozbalte doménu nebo server, kde se nachází skupina, jejíž zápis chcete zrušit.
  3. Vyberte **Zapsané skupiny**.
  4. Klepněte pravým tlačítkem myši na skupinu, jejíž zápis chcete zrušit.
  5. Vyberte **Vyřadit**.
  6. Klepněte na **Vyřadit** v potvrzujícím okně.

---

## Uživatel QAS400NT

V níže uvedených případech musíte nastavit uživatele QAS400NT, chcete-li zapsat uživatelský nebo skupinový profil operačního systému i5/OS do domény nebo na lokální server:

- Zapisujete uživatele do domény prostřednictvím členského serveru.
- Zapisujete uživatele na lokální server pomocí šablony, která udává cestu k domovskému adresáři, jak je popsáno v tématu “Zadání domovského adresáře do šablony” na stránce 171).
- Zapisujete uživatele do domény prostřednictvím logické části s operačním systémem i5/OS, která obsahuje v téže doméně jak řadiče domény, tak členské servery.

V níže uvedených případech není nutné nastavit uživatele QAS400NT, chcete-li zapsat uživatelský nebo skupinový profil operačního systému i5/OS do domény nebo na lokální server:

- Zapisujete uživatele do domény prostřednictvím logické části s operačním systémem i5/OS, která má ve stejné doméně řadič domény, ale ne členské servery.
- Zapisujete uživatele na lokální server (nebo lokálně na členský server) pomocí šablony, která neudává cestu k domovskému adresáři.

Je-li třeba nastavit uživatele QAS400NT, použijte tento postup.

1. Vytvořte v systému i5/OS uživatelský profil QAS400NT s třídou uživatele \*USER. Zapamatujte si heslo, neboť je budete potřebovat v dalším kroku. Pokud zapisujete uživatele do domény, zkontrolujte, zda toto heslo vyhovuje pravidlům pro hesla Windows. Další informace najdete v tématu “Posouzení hesla” na stránce 53.
2. Z konzole integrovaného Windows serveru, z níž uživatele zapisujete, vytvořte uživatelský účet QAS400NT. Pamatujte si, že uživatel QAS400NT musí mít stejné heslo pro uživatelský profil v systému i5/OS i pro uživatelský účet ve Windows.

a. Nastavení QAS400NT na řadiči domény

Na řadiči domény, pro něj zápis nastavujete, vytvořte uživatelský účet QAS400NT. Postupujte takto:

1) Z konzole integrovaného serveru

a)

- Na serveru Windows 2000 Server klepněte na **Start → Programs → Administrative Tools → Computer Management → Local Users and Groups**.
- Na serveru Windows Server 2003 klepněte na **Start → Programs → Administrative Tools → Computer Management → System Tools → Local Users and Groups**.

b) Vyberte **System Tools → Local Users and Groups**.

2) Klepněte pravým tlačítkem myši na složku **Users** (nebo na složku, do níž daný uživatel patří) a vyberte **New → User...**

3) Nastavte následující hodnoty:

Full name: qas400nt  
User logon name: qas400nt

4) Klepněte na Next. Nastavte následující hodnoty:

Password: (stejně, jaké jste použili pro QAS400NT v i5/OS)  
Zrušte zaškrtnutí: User must change password at next logon.  
Zaškrtněte:  
User cannot change password.  
Zaškrtněte: Password never expires.

5) Klepněte na Next a potom na Finish.

6) Klepněte pravým tlačítkem myši na ikonu uživatele QAS400NT a vyberte Properties.

7) Klepněte na kartu **Member of** a potom na Add.

8) Do okénka zadejte **Domain Admins**, klepněte na OK a ještě jednou na OK. To dává uživatelskému účtu QAS400NT dostatečné oprávnění k vytváření uživatelů.

b. Nastavení QAS400NT na lokálním serveru

Na lokálním serveru (nebo členském serveru při lokálním zápisu), pro něj zápis nastavujete, vytvořte uživatelský účet QAS400NT. Postupujte takto:

- 1) Z konzole integrovaného serveru
    - Na serveru Windows 2000 Server klepněte na **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **Local Users and Groups**.
    - Na serveru Windows Server 2003 klepněte na **Start** → **Programs** → **Administrative Tools** → **Computer Management** → **System Tools** → **Local Users and Groups**.
  - 2) Klepněte pravým tlačítkem myši na složku **Users** a vyberte **New User...**
  - 3) Nastavte následující hodnoty:
    - User name: qas400nt
    - Full name: qas400nt
    - Password: (stejně, jaké jste použili pro QAS400NT v i5/OS)
    - Zrušte zaškrtnutí: User must change password at next logon.
    - Zaškrtněte:
      - User cannot change password.
      - Zaškrtněte: Password never expires.
  - 4) Klepněte na **Create** a potom na **Close**.
  - 5) Klepněte pravým tlačítkem myši na ikonu uživatele QAS400NT a vyberte **Properties**.
  - 6) Klepněte na kartu **Member of** a potom na **Add**.
  - 7) Do okénka zadejte **Administrators**, klepněte na **OK** a ještě jednou na **OK**. To dává uživatelskému účtu QAS400NT dostatečné oprávnění pro službu **User Administration Service**.
3. Zapište uživatelský profil QAS400NT operačního systému i5/OS do domény nebo na lokální server pomocí produktu **iSeries Navigator** nebo příkazu **CHGNWSUSRA**. Potřebný postup najdete v tématu “Zápis jednoho uživatele operačního systému i5/OS do prostředí Windows pomocí produktu **iSeries Navigator**” na stránce 169. Pro zápis uživatele QAS400NT nepoužívejte šablonu.
  4. V prostředí produktu **iSeries Navigator** nebo příkazu **WRKNWSEN** si ověřte, zda byl uživatel QAS400NT úspěšně zapsán. Nyní můžete zapisovat uživatelské profily do operačního systému i5/OS prostřednictvím řadičů domény nebo členských serverů v doméně.

#### Poznámky:

- Můžete změnit heslo pro profil QAS400NT z operačního systému i5/OS, protože nyní se jedná o zapsaného uživatele.
- Máte-li v jedné logické části s operačním systémem i5/OS více integrovaných serverů, které patří do různých domén, musíte nastavit uživatele QAS400NT pro každou doménu. Všechny uživatelské účty QAS400NT musejí mít stejné heslo, jako má tento uživatelský profil v systému i5/OS. Jinak můžete také použít **Active Directory** nebo spoléhat na vztahy mezi doménami a zapsat uživatele pouze do jedné domény.
- Máte-li více logických částí s operačním systémem i5/OS a více integrovaných serverů, mohou se hesla uživatele QAS400NT pro různé logické části s operačním systémem i5/OS lišit, pokud žádná doména neobsahuje integrované servery ve více než jedné logické části s operačním systémem i5/OS. Pravidlem je, že všechny uživatelské profily QAS400NT v systému i5/OS a odpovídající uživatelské účty ve Windows musí mít pro jednu doménu shodné heslo.
- Dejte pozor, abyste nevymazali uživatelský profil QAS400NT z operačního systému i5/OS a nenechali vypršet platnost jeho hesla. Chcete-li minimalizovat riziko vypršení platnosti hesla QAS400NT v některé z logických částí s operačním systémem i5/OS, které se nacházejí v téže doméně Windows, doporučuje se povolit pouze jedné logické části s operačním systémem i5/OS, aby přenášela změny do uživatelského profilu QAS400NT. Příslušné postupy jsou uvedeny v tématu “Jak zabránit zápisu a přenesení uživatelského profilu na integrovaný Windows server” na stránce 177.
- Máte-li více logických částí s operačním systémem i5/OS, z nichž každá obsahuje integrovaný Windows server ve stejné doméně, může selhání synchronizace hesla QAS400NT ve všech logických částech s operačním systémem i5/OS způsobit problémy se zápisem uživatelů. Chcete-li tento problém minimalizovat, měli byste omezit přenášení změn hesla QAS400NT na jedinou logickou část s operačním systémem i5/OS, ale nadále ponechat ostatním logickým částem dostatečné oprávnění k zápisu uživatelů. Potom selhání při změně hesla v některé z ostatních logických částí zabráni zápisu uživatelů pouze z této logické části. Příslušné postupy jsou uvedeny v tématu “Jak zabránit zápisu a přenesení uživatelského profilu na integrovaný Windows server” na stránce 177.

---

## Jak zabránit zápisu a přenesení uživatelského profilu na integrovaný Windows server

Existuje několik důvodů, proč může být nutné zabránit přenášení uživatelského profilu z operačního systému i5/OS na určitý integrovaný server:

- Patří-li několik integrovaných serverů do téže domény a všechny se nacházejí v jedné logické části s operačním systémem i5/OS, bude v předvoleném nastavení probíhat zápis uživatelského profilu všemi integrovanými servery v této logické části. Abyste snížili provoz na síti, můžete vypnout zápis na všechny integrované servery v doméně kromě jednoho. Tímto jediným integrovaným serverem by měl obvykle být řadič domény, pokud se v dané logické části nachází.
- Patří-li několik integrovaných serverů do téže domény, ale každý z nich se nachází v jiné logické části s operačním systémem i5/OS, existuje riziko, že bude narušena synchronizace hesel QAS400NT a vzniknou problémy se zápisem uživatelského profilu. Riziko problémů se zápisem můžete snížit tím, že zabráníte přenášení uživatelského profilu QAS400NT ze všech logických částí s operačním systémem i5/OS kromě jedné. Ostatním logickým částem s operačním systémem i5/OS zůstane dostatečné oprávnění k zápisu uživatelů. Potom selhání při změně hesla v některé z ostatních logických částí zabráni zápisu uživatelů pouze z této logické části.

Přenesení uživatelského profilu z operačního systému i5/OS na určitý integrovaný server můžete zabránit dvěma způsoby:

- Pomocí parametru PRPDMNUSR (Přenesení uživatele domény). Příslušný postup najdete níže.
- Pomocí příkazu CRTDTAARA vytvořte datové oblasti. Příslušný postup najdete níže.

### Jak pomocí parametru PRPDMNUSR zabránit zápisu do domény přes určitý integrovaný server

Parametr PRPDMNUSR (Přenesení uživatele domény) u příkazu CHGNWSD (Změna popisu síťového serveru) umožňuje zabránit zápisu uživatele do domény prostřednictvím určitého integrovaného serveru. Tento parametr lze rovněž nastavit, instalujete-li integrovaný server pomocí příkazu INSWNTSVR (Instalace Windows serveru). Tato metoda může být užitečná v případě, že jediná logická část s operačním systémem i5/OS řídí několik integrovaných Windows serverů, které náležejí k téže doméně. Může totiž vypnout zápis pro všechny integrované servery s výjimkou jednoho.

Chcete-li zabránit zápisu uživatelů pomocí parametru PRPDMNUSR, postupujte takto:

1. Pomocí příkazu WRKNWSD (Práce s popisy síťového serveru) vyberte integrovaný server, u něhož chcete zakázat zápis. (Logické vypnutí serveru není třeba.)
2. Zadejte příkaz: CHGNWSD NWSD(nwsdname) PRPDMNUSR(\*NO)

### Poznámky:

- Nikdy nezakazujte zápis pro všechny integrované servery v doméně. V takovém případě by všichni uživatelé přešli do stavu \*UPDPND (nevyřízená aktualizace) a nedošlo by k žádnému dalšímu přenesení.
- Můžete také ponechat dva integrované servery s povoleným zápisem uživatelů. Při výpadku jednoho serveru tak budete moci nadále provádět změny.

### Jak pomocí příkazu CRTDTAARA zabránit zápisu přes QAS400NT na určitý integrovaný server

Příkaz CRTDTAARA (Vytvoření datové oblasti) zabráni pouze zápisu uživatelského profilu QAS400NT na určený integrovaný server. Nemá však vliv na přenesení ostatních uživatelských profilů. Tato metoda je vhodná v případě, kdy se jedná o více integrovaných serverů, které náležejí k téže doméně, ale nacházejí se v různých logických částech s operačním systémem i5/OS. Chcete zapsat uživatelské profily z těchto různých logických částí s operačním systémem i5/OS, ale nechcete mít několik uživatelských profilů QAS400NT, které by přenášely hesla do domény. Postupujte takto:

1. Vyberte jednu logickou část s operačním systémem i5/OS, která má sloužit pro zápis QAS400NT v doméně. Zajistěte, aby byl uživatelský profil QAS400NT v této logické části s operačním systémem i5/OS zapsán.
2. Je-li uživatelský profil QAS400NT zapsán v jiných logických částech s operačním systémem i5/OS, postupujte takto:

- a. Na řadiči domény přidejte uživatelský účet QAS400NT do skupiny OS400\_Permanent\_Users. Tím zajistíte, že tento profil nebude vymazán.
  - b. Vymažte uživatelský profil QAS400NT z těch logických částí s operačním systémem i5/OS, ve kterých chcete zápisu QAS400NT zabránit.
3. V logických částech s operačním systémem i5/OS, ve kterých chcete zabránit zápisu QAS400NT, vytvořte datovou oblast pomocí příkazu:

```
CRTDTAARA  
DTAARA(QUSRSYS/nwsdnameAU) TYPE(*CHAR) LEN(10) VALUE( *NOPROP )
```

kde **nwsdname** je jméno popisu síťového serveru pro integrovaný server a **\*NOPROP** je klíčové slovo, které udává, že parametry uživatelského profilu QAS400NT (včetně hesla) nejsou z logické části s operačním systémem i5/OS přenášeny.

4. V každé logické části s operačním systémem i5/OS, ve které jste vytvořili datovou oblast, vytvořte a zapište uživatelský profil QAS400NT. Ve všech logických částech s operačním systémem i5/OS musíte být heslo QAS400NT stále aktuální (platné), aby bylo provádět zápis uživatelských profilů (jiných než QAS400NT). Vzhledem k tomu, že heslo QAS400NT není přenášeno, nezáleží na tom, o jaké heslo se jedná, pokud nevyprší jeho platnost.



---


## Kapitola 12. Zálohování a obnova integrovaných Windows serverů

Při správě zálohování můžete používat obslužné programy buď operačního systému i5/OS, nebo Windows serveru, nebo je můžete kombinovat, protože prostředí Windows na serveru iSeries kombinuje dva operační systémy (Windows 2000 Server nebo Windows Server 2003 a i5/OS). Při plánování strategie zálohování si prostudujte téma Zálohování a obnova a rovněž dokumentaci od firmy Microsoft.

Při zálohování integrovaného serveru v systému iSeries se nabízejí tyto základní možnosti:

- Provést úplné zálohování systému v operačním systému i5/OS. Viz téma Zálohování serveru.
- Zálohovat popis síťového serveru (NWSD) a diskové jednotky, které jsou v systému iSeries přiřazeny k tomuto integrovanému serveru. Další informace najdete v tématu “Zálohování NWSD a dalších objektů přiřazených k integrovanému Windows serveru”.
- Zálohovat jednotlivé soubory integrovaného serveru pomocí příkazů SAV a RST operačního systému i5/OS a serveru i5/OS NetServer nebo obslužného programu pro zálohování. Další informace najdete v tématu “Zálohování jednotlivých souborů a adresářů integrovaného Windows serveru” na stránce 184.

Možnosti obnovy závisí na tom, jakým způsobem byl systém zálohován, a co je třeba obnovit.

- Chcete-li obnovit celý systém, přečtěte si publikaci Zálohování a obnova .
- Chcete-li obnovit popis síťového serveru a k němu přiřazené diskové jednotky v systému i5/OS, prostudujte téma “Obnova NWSD a diskových jednotek integrovaného Windows serveru” na stránce 188.
- Chcete-li obnovit data z integrovaného serveru (soubory, adresáře, sdílení a registr Windows), která jste záložovali příkazem SAV (Uložení), prostudujte téma “Obnova souborů integrovaného Windows serveru” na stránce 192.
- Chcete-li obnovit soubory, které jste záložovali pomocí obslužných programů pro zálohování (například těch, které jsou k dispozici ve Windows), použijte opět tyto programy.

---

### Zálohování NWSD a dalších objektů přiřazených k integrovanému Windows serveru

Při instalaci integrovaného serveru vytvoří operační systém i5/OS pro tento server popis síťového serveru a předdefinované diskové jednotky, které je nutné zálohovat. Další informace najdete v tématu “Předdefinované diskové jednotky pro integrované Windows servery” na stránce 154. Některé z těchto diskových jednotek se vztahují k systému (instalační a systémová jednotka), jiné k uživateli. Vzhledem k tomu, že je Windows server považuje za ucelený systém, je třeba zálohovat všechny tyto diskové jednotky i popis síťového serveru, aby mohla být řádně provedena jejich obnova.

Spuštění integrovaného serveru vyžaduje operační systém Microsoft Windows a soubory, které jsou uloženy na jednotkách C a D tohoto serveru. Prostředí Windows na serveru iSeries umožňuje uložit a obnovit tyto jednotky jako objekty paměťového prostoru síťového serveru i5/OS. Tyto objekty jsou ukládány jako součást operačního systému i5/OS při úplném zálohování operačního systému i5/OS. Můžete také zálohovat výslovně popis síťového serveru a přidružené paměťové prostory. Dobrou praxí je denní zálohování systémové jednotky.

Ukládání paměťových prostorů je nejrychlejší, avšak nejméně flexibilní metodou zálohování integrovaného serveru, protože při ní nelze obnovit jednotlivé soubory. Další možností je zálohovat konkrétní jednotlivé soubory a adresáře a tak vyloučit zálohování BOOT disku, RDISKu a registru, které byste u Windows serveru na bázi PC museli provést. Další informace najdete v tématu “Zálohování jednotlivých souborů a adresářů integrovaného Windows serveru” na stránce 184.



Informace o zálohování popisu síťového serveru a diskových jednotek přiřazených k integrovaným serverům najdete v těchto tématech:

- “Zálohování NWSD integrovaného Windows serveru”.
- “Zálohování objektů iSCSI NWSCFG a ověřovací seznamy”
- “Zálohování předdefinovaných diskových jednotek pro integrované Windows servery” na stránce 181.
- “Zálohování uživatelem definovaných diskových jednotek u integrovaného Windows serveru” na stránce 181.
- “Ukládání a obnova informací o zápisu uživatelů” na stránce 182.
- Tabulku uživatelských a systémových objektů najdete v tématu “Které objekty by se měly ukládat a kde jsou v systému i5/OS umístěny” na stránce 183.

## Zálohování NWSD integrovaného Windows serveru

Když ukládáte objekty paměťových prostorů, které jsou přiřazeny k integrovanému Windows serveru, je třeba uložit také popis síťového serveru (NWSD). Jinak Windows server nebude schopen obnovit některá nastavení, jako například oprávnění k systému souborů Windows serveru. K uložení NWSD použijte příkaz SAVCFG (Uložení konfigurace):

1. Na příkazový řádek operačního systému i5/OS napište SAVCFG.
2. Stiskněte klávesu Enter. Operační systém i5/OS uloží konfiguraci NWSD.

| **Poznámka:** Příkaz SAVCFG (Uložení konfigurace) ukládá objekty přiřazené k NWSD.

## | Zálohování NWSH integrovaného Windows serveru připojeného pomocí iSCSI

| Chcete-li uložit NWSH, použijte příkaz SAVCFG (Uložení konfigurace):

- | 1. Na příkazový řádek operačního systému i5/OS napište SAVCFG.
- | 2. Stiskněte klávesu Enter. Operační systém i5/OS uloží konfiguraci NWSH.

## | Zálohování objektů iSCSI NWSCFG a ověřovací seznamy

Další objekty konfigurace pro servery připojené pomocí adaptérů iSCSI HBA jsou uloženy v knihovně QUSRSYS. Patří mezi ně objekty konfigurace síťových serverů (typu \*NWSCFG) a objekt přiřazeného ověřovacího seznamu (typu \*VLDDL).

**Poznámka:** Objekty \*NWSCFG a \*VLDDL sdílejí stejné jméno.

Chcete-li uložit objekty konfigurace síťového serveru a ověřovacího seznamu, použijte příkaz SAVOBJ (Uložení objektu):

1. Ukládáte-li na pásku, zkontrolujte, zda je nasazená páska naformátována pro operační systém i5/OS.
2. Vypnutím Windows serveru uvolněte případné zámky objektů.
3. Na příkazový řádek operačního systému i5/OS napište příkaz SAVOBJ a stiskněte klávesu F4.
4. Do pole **Objects** zadejte jména NWSCFG. Pokud byla použita předvolená jména, zadejte generické jméno nwsdname\*.
5. Do pole **Library** zadejte QUSRSYS.
6. Ukládáte-li objekty na pásku, zadejte jméno páskové jednotky v poli **Zařízení** (například TAP01). Chcete-li namísto pásky použít soubor typu save, zadejte jako zařízení hodnotu \*SAVF a povolte komprimaci dat.
7. Do pole **Typ objektu** zadejte \*NWSCFG i \*VLDDL.
8. Používáte-li soubor typu save, můžete stisknutím klávesy F10 zobrazit přidavné parametry.
9. Do pole **Soubor typu save** zadejte cestu ke svému souboru typu save (například winbackup/nwscfg).
10. Používáte-li soubor typu save, můžete stisknutím klávesy PageDown změnit hodnotu pro kompresi dat na \*YES.

## Zálohování předdefinovaných diskových jednotek pro integrované Windows servery

Při instalaci integrovaného serveru vytvoří operační systém i5/OS systémovou jednotku a instalační zdrojovou jednotku (C a D) jako předdefinované jednotky, které je nutné zálohovat. Další informace najdete v tématu “Předdefinované diskové jednotky pro integrované Windows servery” na stránce 154.

### Poznámky:

1. S popisem síťového serveru, jeho předdefinovanými diskovými jednotkami a všemi s ním propojenými uživatelsky definovanými diskovými jednotkami zacházejte jako s jedním celkem. Ukládejte a obnovujte je současně. Dohromady tvoří ucelený systém a mělo by s nimi být podle toho nakládáno. Jinak nebude integrovaný server moci obnovit některé položky, například oprávnění k systému souborů na Windows serveru.
2. Pokud byl server vytvořen v nižší verzi operačního systému OS/400, než je verze V4R5, prostudujte téma Back up predefined disk drives for integrated Windows servers created on pre-V4R5 OS/400 systems v aplikaci Information Center pro server iSeries verze V5R3.

Chcete-li uložit diskové jednotky (paměťové prostory síťového serveru), které jsou ve společné systémové diskové oblasti (ASP) systému i5/OS, postupujte takto:

1. Ukládáte-li na pásku, zkontrolujte, zda je nasazená páska naformátována pro operační systém i5/OS.
2. Vypněte integrovaný server, aby uživatelé nemohli během zálohování aktualizovat soubory. Další informace najdete v tématu “Spuštění a zastavení integrovaného serveru” na stránce 141.
3. Na příkazový řádek operačního systému i5/OS napište příkaz SAV a stiskněte klávesu F4.
4. Ukládáte-li paměťový prostor na pásku, zadejte do pole *Device* jméno páskové jednotky (například /QSYS.LIB/TAP01.DEVD).  
Ukládáte-li paměťový prostor do souboru typu save namísto pásky, zadejte do pole *Device* cestu k souboru typu save. Chcete-li například použít soubor se jménem MYSAVF z knihovny WINBACKUP, měli byste jako zařízení zadat cestu '/QSYS.LIB/WINBACKUP.LIB/MYSAVF.FILE'.
5. Do pole *Name* pod *Objects* zadejte '/QFPNWSSTG/stgspc', kde stgspc je jméno paměťového prostoru síťového serveru.
  - Pro systémovou jednotku (C) použijte jméno /QFPNWSSTG/nwsdname1.
  - K uložení jednotky D použijte jméno /QFPNWSSTG/nwsdname2.
  - Pro paměťové prostory vytvořené v uživatelském ASP použijte /QFPNWSSTG/stgspc a také dev/QASPnn/stgspc.UDFS, kde stgspc je jméno paměťového prostoru síťového serveru a nn je číslo uživatelského ASP.
  - Pro nezávislé ASP použijte /QFPNWSSTG/stgspc a také dev/independent ASP name/stgspc.UDFS, kde independent ASP name je jméno nezávislého ASP a stgspc je jméno paměťového prostoru síťového serveru.
6. Dle potřeby zadejte hodnoty *i* pro další parametry a stisknutím klávesy Enter paměťový prostor uložte.
7. Potom spusťte integrovaný server. Další informace najdete v tématu “Spuštění a zastavení integrovaného serveru” na stránce 141.

Další informace najdete v tématu “Které objekty by se měly ukládat a kde jsou v systému i5/OS umístěny” na stránce 183.

## Zálohování uživatelem definovaných diskových jednotek u integrovaného Windows serveru

Diskové jednotky, které vytváříte na integrovaném serveru, se nacházejí v integrovaném systému souborů. Chcete-li uložit tyto paměťové prostory ze společné uživatelské diskové oblasti (ASP) systému i5/OS, použijte příkaz SAV (Uložení).

### Poznámka:

S popisem síťového serveru (NWS), jeho předdefinovanými diskovými jednotkami a všemi s ním propojenými uživatelsky definovanými diskovými jednotkami zacházejte jako s jedním celkem. Ukládejte

a obnovuje je současně. Dohromady tvoří ucelený systém a mělo by s nimi být podle toho nakládáno. Jinak integrovaný server nebude schopen obnovit některá nastavení, jako například oprávnění k systému souborů Windows serveru.

Chcete-li uložit diskové jednotky do společné uživatelské diskové oblasti (ASP) systému i5/OS, postupujte takto:

1. Ukládáte-li na pásku, zkontrolujte, zda je nasazená páska naformátována pro operační systém i5/OS.
2. U paměťových prostorů síťového serveru vytvořených v nezávislé společné diskové oblasti ověřte před uložením objektu 'dev/independent ASP name/stgspc.UDFS', že zařízení společné oblasti pomocné paměti (ASP) je logicky zapnuto.
3. Vypněte integrovaný server logickým vypnutím jeho popisu síťového serveru, aby uživatelé nemohli během zálohování aktualizovat soubory. Další informace najdete v tématu "Spuštění a zastavení integrovaného serveru" na stránce 141.
4. Na příkazový řádek operačního systému i5/OS napište příkaz SAV a stiskněte klávesu F4.
5. Ukládáte-li paměťový prostor na pásku, zadejte do pole *Device* jméno páskové jednotky (například /QSYS.LIB/TAP01.DEVD).  
Ukládáte-li paměťový prostor do souboru typu save namísto pásky, zadejte do pole *Device* cestu k souboru typu save. (Chcete-li například použít soubor se jménem MYSAVF z knihovny WINBACKUP, měli byste jako zařízení zadat cestu '/QSYS.LIB/WINBACKUP.LIB/MYSAVF.FILE'). Jinak zadejte jméno vašeho zařízení (například /QSYS.LIB/TAP01.DEVD).
6. Do pole *Name* pod *Objects* zadejte '/QFPNWSSTG/stgspc' a také 'dev/QASPnn/stgspc.UDFS', kde stgspc je jméno paměťového prostoru síťového serveru a *nn* je číslo ASP.
  - Pro paměťové prostory vytvořené v uživatelském ASP použijte jméno /QFPNWSSTG/stgspc a také dev/QASPnn/stgspc.UDFS, kde stgspc je jméno paměťového prostoru síťového serveru a *nn* je číslo uživatelského ASP.
  - Pro nezávislé ASP použijte /QFPNWSSTG/stgspc a také dev/independent ASP name/stgspc.UDFS, kde independent ASP name je jméno nezávislého ASP a stgspc je jméno paměťového prostoru síťového serveru.
7. Dle potřeby zadejte hodnoty *i* pro další parametry a stisknutím klávesy Enter paměťový prostor uložte.
8. Potom spusťte Windows server. Další informace najdete v tématu "Spuštění a zastavení integrovaného serveru" na stránce 141.

Více informací týkajících se zálohování systémových objektů a příslušných příkazů najdete v tématu Zálohování, obnova a dostupnost.

Výše popsaná metoda umožňuje zálohovat a obnovovat paměťové prostory celého síťového serveru. K zálohování a obnově jednotlivých souborů slouží nová funkce. Další informace najdete v tématu "Zálohování jednotlivých souborů a adresářů integrovaného Windows serveru" na stránce 184.

## Ukládání a obnova informací o zápisu uživatelů

Mohou nastat situace, kdy je třeba obnovit uživatelské profily a informace o jejich zápisu. Níže uvedené informace popisují příkazy a rozhraní API operačního systému i5/OS, které slouží k ukládání a obnově uživatelských profilů používaných pro zápis integrovaných Windows serverů. Další informace o zabezpečení zálohování a obnovy operačního systému i5/OS najdete v tématu Zálohování a obnova informací o zabezpečení v publikaci Zabezpečení

iSeries - Referenční informace  .

Uživatelské profily lze zálohovat prostřednictvím příkazu SAVSECDTA nebo prostřednictvím rozhraní QSRSAVO API. Systémová hodnota QRETSVRSEC operačního systému i5/OS musí být nastavena na hodnotu 1, aby byl podporován zápis na integrovaný Windows server. Uživatelské profily uložené pomocí příkazu SAVSECDTA nebo rozhraní QSRSAVO API lze obnovit příkazem RSTUSRPRF a zadáním parametru USRPRF(\*ALL). Nezádáte-li parametr USRPRF(\*ALL), mohou být uživatelské profily obnoveny tehdy, je-li zadán parametr a hodnota SECDTA(\*PWDGRP).

Jestliže uložíte uživatelské profily pomocí rozhraní QRSOVO API a použijete hodnotu předchozího vydání cílového systému, definice pro zápis uživatelských profilů se neobnoví. Po obnovení uživatelských profilů je třeba definovat jejich zápis. K definici zápisu použijte produkt iSeries Navigator nebo příkaz CHGNWSUSRA (Změna uživatelských atributů síťového serveru).

V případě zápisu na integrovaný Windows server je třeba ukládat a obnovovat uživatelské profily výhradně pomocí výše uvedených metod. Uživatelské profily uložené a obnovené pomocí jiných příkazů nebo jiných rozhraní API nejsou ve Windows podporovány.

## Které objekty by se měly ukládat a kde jsou v systému i5/OS umístěny

V rámci instalace prostředí Windows na serveru iSeries se vytváří mnoho nových objektů. Některé z nich se vztahují k systému, jiné k uživateli. Aby mohla být provedena řádná obnova, je třeba zálohovat všechny tyto objekty. Tyto objekty můžete uložit pomocí voleb příkazu GO SAVE operačního systému i5/OS. Volba 21 ukládá celý systém. Volba 22 ukládá systémová data. Volba 23 ukládá všechna uživatelská data (což zahrnuje objekty v QFPNWSSTG).

Chcete-li určitý objekt uložit, použijte některou z následujících tabulek a vyhledejte v ní umístění objektu v operačním systému i5/OS a příkaz, který máte použít. Další informace o příkazech pro ukládání najdete v tématu "Manuální ukládání částí systému". Kromě ukládání celé jednotky (paměťového prostoru) můžete ukládat a obnovovat i jednotlivé soubory a adresáře. Další informace najdete v tématu "Zálohování jednotlivých souborů a adresářů integrovaného Windows serveru" na stránce 184.

### Objekty, které mají být uloženy

Obsah objektu	Jméno objektu	Umístění objektu	Typ objektu	Příkaz pro ukládání
Zaváděcí a systémová jednotka integrovaného serveru	nwsdname1	/QFPNWSSTG	Předdefinované paměťové prostory síťového serveru v systémovém ASP.	GO SAVE, volba 21 nebo 23 SAV OBJ('/QFPNWSSTG/nwsdname1') DEV('/QSYS.LIB/TAP01.DEVD')
Zaváděcí a systémová jednotka integrovaného serveru	nwsdname1	/QFPNWSSTG	Předdefinované paměťové prostory síťového serveru v uživatelském ASP.	SAV OBJ('/QFPNWSSTG/nwsdname1') (/dev/QASPnn/nwsdname1.UDFS') DEV('/QSYS.LIB/TAP01.DEVD')
Jednotka s instalačním zdrojem integrovaného serveru	nwsdname2	/QFPNWSSTG	Předdefinované paměťové prostory síťového serveru v systémovém ASP.	GO SAVE, volba 21 nebo 23 SAV OBJ('/QFPNWSSTG/nwsdname2') DEV('/QSYS.LIB/TAP01.DEVD')
Jednotka s instalačním zdrojem integrovaného serveru	nwsdname2	/QFPNWSSTG	Předdefinované paměťové prostory síťového serveru v uživatelském ASP.	GO SAVE, volba 21 nebo 23 SAV OBJ('/QFPNWSSTG/nwsdname2') (/dev/QASPnn/nwsdname2.UDFS') DEV('/QSYS.LIB/TAP01.DEVD')
Jednotka s instalačním zdrojem integrovaného serveru	nwsdname2	/QFPNWSSTG	Předdefinované paměťové prostory síťového serveru v nezávislém ASP.	GO SAVE, volba 21 nebo 23 SAV OBJ('/QFPNWSSTG/nwsdname2') (/dev/independent ASP name/nwsdname2.UDFS') DEV('/QSYS.LIB/TAP01.DEVD')
Uživatelská data a aplikace	Různé	/QFPNWSSTG	Uživatelsky definované paměťové prostory síťového serveru v systémovém ASP.	GO SAVE, volba 21 nebo 23 SAV OBJ('/QFPNWSSTG/stgspc') DEV('/QSYS.LIB/TAP01.DEVD')
Uživatelská data a aplikace	Různé	/QFPNWSSTG	Uživatelsky definované paměťové prostory síťového serveru v uživatelském ASP.	GO SAVE, volba 21 nebo 23 SAV OBJ('/QFPNWSSTG/stgspc') (/dev/QASPnn/stgspc.UDFS') DEV('/QSYS.LIB/TAP01.DEVD')
Uživatelská data a aplikace	Různé	/QFPNWSSTG	Uživatelsky definované paměťové prostory síťového serveru v nezávislém ASP.	GO SAVE, volba 21 nebo 23 SAV OBJ('/QFPNWSSTG/stgspc') (/dev/independent ASP name/stgspc.UDFS') DEV('/QSYS.LIB/TAP01.DEVD')
Zprávy z integrovaného serveru	Různé	Různé	Message queue (Fronta zpráv)	GO SAVE, volba 21 nebo 23 SAVOBJ OBJ(msgq) LIB(qlibrary) DEV(TAP01) OBJTYPE(*MSGQ)
Objekty konfigurace i5/OS pro integrované servery	Různé	QSYS	Konfigurační objekty zařízení	GO SAVE, volba 21, 22 nebo 23 SAVCFG DEV(TAP01)

Obsah objektu	Jméno objektu	Umístění objektu	Typ objektu	Příkaz pro ukládání
Kód produktu Integrated Server Support pro server IBM iSeries na bázi operačních systémů i5/OS a Windows	QNTAP, NTAP a podadresáře	QSYS a /QIBM/ProdData/NTAP	Knihovna a adresář	SAVLICPGM LICPGM(5722SS1) OPTION(29)
Sdílení souborů Windows serveru	QNTC a podadresáře	/QNTC/servername /sharename	Adresář	GO SAVE, volba 21 nebo 22 SAV
Rozhraní TCP operačního systému i5/OS	QATOCIFC	QUSRSYS	fyzický soubor	GO SAVE, volba 21 nebo 23 SAVOBJ OBJ(QATOCIFC) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*FILE)
Rozhraní TCP operačního systému i5/OS	QATOCLIFC	QUSRSYS	logický soubor	GO SAVE, volba 21 nebo 23 SAVOBJ OBJ(QATOCLIFC) LIB(QUSRSYS) DEV(TAP01) OBJTYPE(*FILE)
iSCSI NWSFCFG a přiřazený ověřovací seznam	Různé	QUSRSYS	Konfigurace síťového serveru a přiřazené hodnoty	SAVOBJ LIB(QUSRSYS) OBJTYPE(*NWSFCFG *VLDDL)
Paměť certifikátů pro cesty k iSCSI	nwsdname.*	/QIBM/UserData/NWSDCert	Soubor paměti certifikátů	GO SAVE, volba 21 nebo 23 SAV OBJ('/QIBM/UserData/NWSDCert/nwsdname.*')
Paměť certifikátů pro servisní procesory iSCSI	nwsfcfgname.kdb	/QIBM/UserData/Director /classes/com/ibm /sysmgt/app/iide	Soubor paměti certifikátů. Uložit, je-li metodou inicializace zabezpečení 'Automaticky generovat certifikát'.	GO SAVE, volba 21 nebo 23 SAV OBJ('/QIBM/UserData/Director/classes/com/ibm/sysmgt /app/iide/nwsfcfgname.kdb')

**Poznámka:** Pro integrované Windows servery vytvořené v systémech verze nižší než V4R5 prostudujte téma What objects to save and their location on OS/400 v aplikaci iSeries Information Center verze V5R3.

## Zálohování jednotlivých souborů a adresářů integrovaného Windows serveru

Produkt IBM iSeries Integrated Server Support umožňuje ukládat data z integrovaných serverů (soubory, adresáře, sdílené položky a registr Windows) na pásku, optické zařízení nebo disk (\*SAVF) spolu s ostatními daty operačního systému i5/OS a jednotlivě tato data obnovit. Tuto metodu byste však neměli pokládat za svoji primární zálohovací proceduru. Měli byste stále pravidelně zálohovat celý systém a objekt NWSD přiřazený k vašemu Windows serveru pro případ nutnosti obnovy po zhroucení systému. Potom můžete denně zálohovat pouze ty soubory integrovaného serveru, které byly změněny. Další informace najdete v tématu “Zálohování NWSD a dalších objektů přiřazených k integrovanému Windows serveru” na stránce 179.

Informace o funkci zálohování na úrovni souborů najdete v níže uvedených tématech:

- Nejprve si přečtěte téma “Omezení při zálohování na úrovni souborů”.
- Chcete-li svůj integrovaný server zálohovat na úrovni souborů, měli byste si nejprve přečíst téma “Přípravné kroky administrátora” na stránce 185.
- “Ukládání souborů” na stránce 187

Můžete také použít obslužný program, jako je například program Backup, který je dodáván se systémem Windows (viz “Program Windows Backup” na stránce 188). Další informace o možnostech zálohování a obnovy souborů integrovaného Windows serveru najdete v publikaci Backup for Windows servers na webové stránce IBM Integrated xSeries Solutions.

## Omezení při zálohování na úrovni souborů

Používáte-li zálohování na úrovni souborů, měli byste vzít na vědomí následující omezení a požadavky:

### Omezení:

- Tato podpora není pro samostatné Windows servery k dispozici, protože kód je dodáván spolu s produktem IBM i5/OS Integrated Server Support.



- Tato metoda nezalohuje soubory, které jsou částí kódu produktu IBM iSeries Integrated Server Support.
- Nemůžete zabránit uživatelům v přihlášení a v přístupu k datům na server v okamžiku, kdy je spuštěn příkaz SAV (Uložení) nebo RST (Obnova). Produkt IBM iSeries Integrated Server Support umí uložit i soubor, který je právě používán, pokud jej dokáže přečíst. Proto byste měli soubory integrovaného serveru zálohovat v době, kdy do operačního systému přistupuje málo uživatelů. Dobrou praxí je poslat uživatelům zprávu, že nemají na server přistupovat.
- Windows Server 2003 poskytuje funkci se službou VSS (Volume Shadow copy Service). Poskytuje tak aplikacím, které jsou o zálohování informovány, možnost ukládat právě používané soubory, používají-li zálohování na úrovni souborů.
- K zálohování na úrovni souborů se nepoužívá uživatelský profil QSECOFR. I když je na integrovaném serveru zapsán, k zálohování souborů se nepoužije. Namísto něho se použije lokální účet operačního systému Windows. Ten nemusí mít dostatečné oprávnění k zálohování všech požadovaných souborů.
- Je-li hodnota uživatelského profilu \*LCLPWDMGT nastavena na \*YES, potom systémová hodnota QRETSVRSEC musí být nastavena na 1 a je třeba změnit uživatelské heslo, nebo uživatel musí být přihlášený až po změně hodnoty QRETSVRSEC.
- Je-li hodnota uživatelského profilu \*LCLPWDMGT nastavena na \*NO, použije se autentizace sítě (Kerberos). Uživatel musí přistupovat k serveru iSeries prostřednictvím aplikace s podporou EIM (jako je například funkce jediného přihlášení (single-signon) v produktu iSeries Navigator). Další informace najdete v tématu “Příkaz SBMNWSCMD a podpora zálohování na úrovni souborů pro protokol Kerberos v5 a mapování EIM” na stránce 147.

#### Požadavky:

- Integrovaný server musí být aktivní a musí mít funkční připojení TCP/IP dvoubodové virtuální sítě Ethernet k operačnímu systému i5/OS. Soubory integrovaného serveru musíte zálohovat buď před uvedením systému do stavu omezení, při němž se zálohují zbývající soubory operačního systému i5/OS, nebo až po dokončení operací ve stavu omezení.
- Tato procedura vyžaduje, abyste na integrovaném serveru i v operačním systému i5/OS měli stejný ID uživatele a stejné heslo.
- Váš uživatelský účet na integrovaném serveru musí být členem skupiny Administrators.
- Zálohování na úrovni souborů používá při sestavování seznamu souborů pro zálohování systém souborů QNTC (NetClient). Systém QNTC používá při vyhledávání serverů v dané doméně server iSeries NetServer. iSeries NetServer by měl být ve stejné doméně jako integrovaný server, jehož soubory chcete zálohovat (viz “Zajištění stejné domény pro server iSeries NetServer a integrovaný Windows server” na stránce 187).
- Dávejte pozor, chcete-li obnovit všechny soubory na všech jednotkách, které jste uložili prostřednictvím systému souborů QNTC. Určité soubory operačního systému Windows (například soubory umístěné v koši) mohou po obnově vést k nečekaným výsledkům.
- U serveru Windows 2000 Server nebo Windows Server 2003 je třeba při zálohování a obnově souborů operačního systému Windows brát ohled na ochranu systémových souborů (System File Protection). Viz dokumentace od firmy Microsoft.

## Přípravné kroky administrátora

Než přikročíte k zálohování souborů integrovaného Windows serveru, je třeba provést několik přípravných kroků:

1. Zajistěte, aby osoba, která bude zálohování a obnovu provádět, měla stejné heslo v systému i5/OS i na integrovaném serveru. Nejsnadnější způsob je popsán v tématu “Zápis jednoho uživatele operačního systému i5/OS do prostředí Windows pomocí produktu iSeries Navigator” na stránce 169. Dále zkontrolujte, zda je tento uživatel členem skupiny Administrators. Další informace najdete v tématu “Vytvoření šablony uživatele” na stránce 170.
2. Nastavte sdílení pro všechny jednotky nebo diskové svazky, které chcete zálohovat při požadavku na uložení všech souborů na Windows serveru. Produkt IBM iSeries Integrated Server Support přistupuje k systému souborů a převádí tyto sdílené položky na jména cest. Další informace najdete v tématu “Vytvoření sdílených položek na integrovaných Windows serverech” na stránce 186.

3. Přidejte členy do souboru QAZLCSAVL v knihovně QUSRSYS, který obsahuje seznam jmen sdílených položek, které chcete zálohovat. Další informace najdete v tématu “Přidání členů do souboru QAZLCSAVL”.
4. Zajistěte, aby byl iSeries NetServer ve stejné doméně jako integrovaný server, jehož soubory chcete uložit. Další informace najdete v tématu “Zajištění stejné domény pro server iSeries NetServer a integrovaný Windows server” na stránce 187.
5. Zajistěte, aby osoba, která ukládání nebo obnovení provádí, měla oprávnění \*ALLOBJ, které uživateli poskytuje úplný přístup k programům a zařízením požadovaným pro proces ukládání a obnovy. Nelze-li oprávnění \*ALLOBJ udělit, musí mít tento uživatel alespoň oprávnění \*USE pro objekt QNTAP/QVNASBM, aby požadavek na zálohování a obnovu mohl být předán na Windows server.

## Vytvoření sdílených položek na integrovaných Windows serverech

Chcete-li povolit zálohování a obnovu integrovaného serveru na úrovni souborů v systému i5/OS, vytvořte sdílenou položku pro každý adresář, jehož data chcete zálohovat. K vytvoření sdílené položky na integrovaném serveru použijte z konzole integrovaného serveru tento postup:

1. Poklepnáním na ikonu **My Computer** otevřete program **Windows Explorer**.
2. Klepněte pravým tlačítkem myši na požadovanou jednotku nebo svazek.
3. Klepněte na příkaz **Sharing** v místní nabídce.
4. Klepněte na volbu **Share this folder**. Zadejte **Share Name** (znaky ve jménu sdílené položky musí být z omezené sady znaků kódové stránky 500). Předvolené jméno sdílené jednotky je vytvořeno z poslední části jména adresáře. Jména sdílených položek nesmí být delší než 12 znaků a mohou obsahovat vložené mezery.
5. Můžete zvolit neomezený přístup, nebo omezit počet uživatelů, kteří se mohou ke sdílené položce současně připojit. Pomocí tlačítka **Permissions** můžete nastavit úroveň sdílení (No Access, Read, Change nebo Full Control).
6. Klepnutím na **Apply** nastavené sdílení potvrďte.

## Přidání členů do souboru QAZLCSAVL

Chcete-li povolit zálohování a obnovu na úrovni souborů v systému i5/OS, přidejte pro každý integrovaný Windows server člen do souboru QAZLCSAVL v knihovně QUSRSYS. Jako jméno členu vždy použijte NWSD jméno daného serveru (*nwsdname*).

K přidání členu použijte tento postup:

1. Na příkazový řádek operačního systému i5/OS napište:
 

```
ADDPFM FILE(QUSRSYS/QAZLCSAVL)
MBR(nwsdname)
TEXT('popis') EXPDATE(*NONE) SHARE(*NO) SRCTYPE(*NONE)
```
2. Do nově vytvořeného členu souboru zadejte všechny sdílené položky, které chcete mít možnost zálohovat. Jméno každé sdílené položky definované pro server musí být na samostatném řádku. Maximální délka jména sdílené položky Windows je 12 znaků. Jméno může obsahovat vložené mezery. Jestliže jste například na serveru WINSVR1 definovali sdílené položky cshare, dshare, eshare, fshare, gshare a my share, měl by člen WINSVR1 vypadat takto:

```

                                                    QUSRSYS/QAZLCSAVL
                                                    WINSVR1

0001.00  cshare
0002.00  dshare
0003.00  eshare
0004.00  fshare
0005.00  gshare
0006.00  my share
```

### Poznámka:

Zadáte-li několik jmen sdílení, která ukazují na stejný adresář integrovaného serveru, operační systém i5/OS odpoví na požadavek “uložit vše” několikerým uložením dat. Abyste se vyhnuli duplikaci dat při jejich ukládání, nikdy nedefinujte více sdílených jednotek pro jediný adresář nebo skupinu dat.



## Zajištění stejné domény pro server iSeries NetServer a integrovaný Windows server

Při ukládání souborů integrovaného serveru v rámci zálohování na úrovni souborů musíte zajistit, aby server iSeries NetServer a soubory, které chcete uložit, byly ve stejné doméně.

1. Zjistěte doménu pro integrovaný server:
  - a. V prostředí produktu iSeries Navigator vyberte **Administrace integrovaných serverů** → **Servery**.
  - b. V seznamu v pravém podokně vyhledejte svůj integrovaný server, a potom se podívejte do sloupce Doména na doménu pro tento server.
2. Zjistěte doménu pro server iSeries NetServer:
  - a. V prostředí produktu iSeries Navigator vyberte **Síť** → **Servery** → **TCP/IP**.
  - b. V seznamu serverů TCP/IP vyhledejte server iSeries NetServer.
  - c. Klepněte pravým tlačítkem myši na server **iSeries NetServer** a vyberte **Vlastnosti** (nebo dvakrát klepněte na server **iSeries NetServer**, potom vyberte **Soubor** a potom **Vlastnosti**). Jméno domény pro server iSeries NetServer se zobrazí na kartě **Obecné** v informacích o souboru.
3. Není-li server iSeries NetServer ve stejné doméně jako integrovaný server, změňte doménu pro server iSeries NetServer:
  - a. Klepněte na tlačítko **Následující spuštění**.
  - b. Do pole **Jméno domény** napište jméno domény Windows serveru.
  - c. Zastavte server iSeries NetServer a spusťte jej znovu (klepněte pravým tlačítkem myši na server iSeries NetServer a vyberte příkaz **Zastavit** a potom příkaz **Spustit**.)

## Ukládání souborů

Až dokončíte nezbytnou přípravu (viz “Přípravné kroky administrátora” na stránce 185), můžete přikročit k zálohování souborů integrovaného serveru v systému i5/OS. Abyste mohli obnovit adresář nebo soubor podle jména sdílené položky, je třeba zvláště uvést tento soubor nebo jméno sdílené položky v příkazu SAV.

### Poznámka:

Abyste se vyhnuli duplikaci dat, dávejte pozor při zadávání položek, které se mají příkazem SAV zálohovat. Zadáte-li několik jmen sdílení, která ukazují na stejný adresář integrovaného serveru, operační systém i5/OS uloží data několikrát.

Při specifikaci položek, které má operační systém i5/OS uložit, postupujte takto:

1. Postarejte se o to, aby byl integrovaný server aktivní (viz “Spuštění a zastavení integrovaného serveru” na stránce 141). Dále zajistěte, aby byl aktivní i podsystém QSYSWRK, QSERVER a TCP/IP (můžete k tomu použít příkaz WRKACTJOB (Práce s aktivními úlohami)).
2. Na příkazový řádek operačního systému i5/OS napište příkaz **SAV** a stiskněte klávesu F4.
3. Do pole **Zařízení** zadejte zařízení, na které má operační systém i5/OS data uložit. Například příkaz ‘QSYS.LIB/TAP01.DEVD’ uloží data na pásku.
4. Do pole **Object** zadejte objekty, které má operační systém i5/OS uložit. Zadejte je ve tvaru ‘/QNTC/jménoserveru/sharename’.  
Může používat zástupné znaky. V tématu “Příklady: Jak adresovat součásti integrovaného Windows serveru” najdete informace o tom, jak se zadávají konkrétní součásti integrovaného serveru.
5. Do pole **Directory subtree** zadejte, zda chcete uložit i příslušné podadresáře daného adresáře. Předvoleno je uložení všech adresářů.
6. Chcete-li uložit změny od posledního uložení, zadejte do pole **Change period** hodnotu \*LASTSAVE. Můžete také zadat požadované rozmezí pomocí data a času.
7. Stisknutím klávesy Enter se zadané sdílené položky uloží.

## Příklady: Jak adresovat součásti integrovaného Windows serveru

Následující příklady ukazují, jak se v příkazech SAV a RST odkazovat na konkrétní součásti integrovaného serveru *server1*:

<b>K uložení nebo obnově těchto součástí:</b>	<b>Zadejte:</b>
Všechny objekty integrovaného serveru.	OBJ('/QNTC/*') SUBTREE(*ALL)
Všechny objekty pro <i>server1</i> .	OBJ('/QNTC/server1/*') SUBTREE(*ALL)
Všechny objekty pro <i>server1</i> , které se změnilo od posledního uložení souborů.	OBJ('/QNTC/server1/*') SUBTREE(*ALL) CHGPERIOD(*LASTSAVE)
Všechny objekty pro <i>server1</i> , které se změnilo během určeného období (v tomto případě mezi 10/19/99 a 10/25/99).	OBJ('/QNTC/server1/*') SUBTREE(*ALL) CHGPERIOD('10/19/99' '00:00:00' '10/25/99' '23:59:59')
Všechny adresáře, soubory a sdílené položky na něž se odkazuje daná sdílená položka (například 'fshare'). Operační systém i5/OS neuloží ani neobnoví adresář, na němž je daná sdílená položka vytvořena.	OBJ('/QNTC/server1/fshare/*') SUBTREE(*ALL)
Jenom soubory na něž se daná sdílená položka například 'fshare' odkazuje, a které odpovídají zadanému řetězci (pay*). Operační systém i5/OS neukládá adresáře ani sdílené položky.	OBJ('/QNTC/server1/fshare/pay*')
Pouze adresáře a sdílené položky (nikoli objekty) pro sdílenou položku 'fshare' a její bezprostředně podřízené položky.	OBJ('/QNTC/server1/fshare') SUBTREE(*DIR)
Adresáře, sdílené položky a soubory pro sdílenou položku 'terry' a její podstromy (nikoli adresář 'terry').	OBJ('/QNTC/server1/fdrive/terry/*') SUBTREE(*ALL)
Pouze konkrétní soubor 'myfile.exe'.	OBJ('/QNTC/server1/gdrive/myfile.exe')
Registr integrovaného serveru.	OBJ('/QNTC/server1/\$REGISTRY')

## Program Windows Backup

K zálohování prostřednictvím integrovaného Windows serveru můžete využít program Windows Backup a páskovou jednotku iSeries. Další informace najdete v tématu "Použití páskových jednotek serveru iSeries s integrovanými Windows servery" na stránce 164.

Jak spustit program Windows Backup:

1. Na konzoli integrovaného serveru klepněte na **Spustit**.
2. Vyberte **Accessories** —> **System Tools** —> **Backup**.

Informace o zálohování a obnově pomocí paměťových zařízení připojených přes LAN najdete v dokumentaci k Windows serveru od firmy Microsoft.

## Obnova NWSD a diskových jednotek integrovaného Windows serveru

Jedním ze způsobů, jak obnovit data integrovaného serveru, je obnovit popis síťového serveru (NWSD) a diskové jednotky, které jsou v systému i5/OS k tomuto serveru přiřazeny. Je to nejrychlejší metoda pro obnovu velkých objemů dat. Používáte-li zálohování na úrovni souborů, můžete obnovit i určité soubory integrovaného serveru.

Při obnově uložených objektů z operačního systému i5/OS byste měli věnovat pozornost těmto úvahám:

### Poznámky:

1. S popisem síťového serveru (NWSD), jeho předdefinovanými jednotkami (viz "Předdefinované diskové jednotky pro integrované Windows servery" na stránce 154) a veškerými s ním propojenými uživatelsky definovanými

diskovými jednotkami zacházejte jako s jedním celkem. Obnovujte je současně. Jinak integrovaný server nebude schopen obnovit některá nastavení, jako například oprávnění k systému souborů Windows serveru.

2. Chcete-li, aby operační systém i5/OS automaticky znovu propojil obnovené diskové jednotky v integrovaném systému souborů s odpovídajícím NWS, obnovte NWS až po obnovení diskových jednotek.
3. Obnovíte-li NWS ještě před obnovením předdefinovaných a uživatelsky definovaných diskových jednotek v integrovaném systému souborů, je třeba tyto jednotky znovu propojit. K tomu můžete použít příkaz ADDNWSSTGL (Připojení paměti síťového serveru) pro každou diskovou jednotku, která je přiřazena k tomuto objektu NWS:  
ADDNWSSTGL  
NWSSTG(Storage\_Name) NWS(NWS\_Name)
4. Při obnově řadiče domény zajistěte, aby databáze domény, která se udržuje na serveru, byla synchronizována s ostatními řadiči domén. Při obnově sdílených jednotek používaných klastrovým uzlem Windows může být nutné obnovit sdílené jednotky manuálně. Začněte připojením sdílené jednotky prostředku kvora. K připojení této jednotky můžete použít příkaz:

```
ADDNWSSTGL NWSSTG(Quorum_name) NWS(NWS_Name) ACCESS(*SHRUPD) DYNAMIC(*YES) DRVSEQNBR(*QR)
```

Jakmile je kvota prostředků připojena, můžete připojit i zbývající sdílené jednotky. K připojení zbývajících sdílených jednotek zadejte příkaz:

```
ADDNWSSTGL NWSSTG(Shared_name) NWS(NWS_Name) ACCESS(*SHRUPD) DYNAMIC(*YES)  
DRVSEQNBR(*CALC)
```

Použijte při tom postupy obvyklé ve Windows a v případě potřeby se podívejte do dokumentace od firmy Microsoft.

5. Obnova NWS nainstalovaného na určitém typu hardwaru na jiný typ hardwaru může být omezena. Další informace najdete v tématu “Obnova NWS u integrovaného Windows serveru” na stránce 190.

Chcete-li obnovit NWS a diskové jednotky integrovaného serveru, prostudujte níže uvedená témata:

- “Obnova předdefinovaných diskových jednotek pro integrované Windows servery”
- “Obnova uživatelsky definovaných diskových jednotek pro integrované Windows servery” na stránce 190
- “Obnova NWS u integrovaného Windows serveru” na stránce 190

## Obnova předdefinovaných diskových jednotek pro integrované Windows servery

Diskové jednotky, které obsahují operační systém a registr Windows jsou v integrovaném systému souborů. Tyto předdefinované diskové jednotky se obnovují stejně jako uživatelsky definované diskové jednotky. Chcete-li obnovit diskové jednotky v integrovaném systému souborů v i5/OS, použijte příkaz RST (Obnovit):

1. Pokud obnovujete ze záložního média, nasadte příslušné médium.
2. Nejsou-li v systému žádné paměťové prostory síťového serveru (po zadání příkazu WRKNWSSTG se žádný nezobrazí), je třeba vytvořit adresář /QFPNWSSTG před obnovením paměťových prostorů síťového serveru, které jste pod tímto adresářem uložili. Při vytváření adresáře /QFPNWSSTG postupujte takto:
  - a. Na příkazový řádek operačního systému i5/OS napište CRTNWSSTG. Vytvoří se paměťový prostor síťového serveru. Stiskněte klávesu F4.
  - b. Pojmenujte tento paměťový prostor.
  - c. Zadejte příslušné ASP; použijte minimální povolenou velikost.
  - d. Stisknutím klávesy Enter zadání potvrďte. Operační systém i5/OS vytvoří v adresáři /QFPNWSSTG paměťový prostor.
3. K obnovení paměťových prostorů napište příkaz RST a stiskněte klávesu F4.
4. Do pole Name pod Objects: zadejte '/QFPNWSSTG/stgspc' a také 'dev/QASPnn/stgspc.UDFS', kde stgspc je jméno paměťového prostoru síťového serveru a nn je číslo ASP.

**Poznámka:** Při obnově objektu .UDFS do nezávislého ASP musí být zařízení ASP logicky vypnuto. Zadejte `dev/independent ASP name/stgspc.UDFS`, kde *independent ASP name* je jméno nezávislého ASP a *stgspc* je jméno paměťového prostoru síťového serveru.

K obnovení systémové jednotky (C) použijte jméno `/QFPNWSSTG/nwsdname1`. K obnovení jednotky D použijte `/QFPNWSSTG/ nwsdname2`.

5. Dle potřeby zadejte hodnoty *i* pro další parametry a stisknutím klávesy Enter paměťový prostor obnovte.
6. Je třeba také obnovit všechny uživatelem definované diskové jednotky, které jsou k serveru přiřazeny, a obnovit objekt NWS D. Další informace najdete v tématu “Obnova uživatelsky definovaných diskových jednotek pro integrované Windows servery”. Po dokončení obnovy objektu NWS D a všech přiřazených diskových jednotek logicky zapněte integrovaný server.

**Poznámka:** Pokud byl server nainstalován v nižší verzi než V4R5, prostudujte téma `Restore predefined disk drives for integrated Windows servers created on pre-V4R5 systems` v aplikaci Information Center pro server iSeries verze V5R3.

## Obnova uživatelsky definovaných diskových jednotek pro integrované Windows servery

I když nyní umíte zálohovat jednotlivé soubory a adresáře (viz “Zálohování jednotlivých souborů a adresářů integrovaného Windows serveru” na stránce 184), nejrychlejším způsobem, jak obnovit velké objemy dat, je obnovit paměťový prostor jako celek. Jestliže zálohujete uživatelský paměťový prostor z adresáře `\QFPNWSSTG`, můžete obnovit pouze celý paměťový prostor. Další informace najdete v tématu “Zálohování uživatelem definovaných diskových jednotek u integrovaného Windows serveru” na stránce 181. Z této zálohy nelze obnovovat jednotlivé soubory.

K obnově diskových jednotek v integrovaném systému souborů použijte tento postup:

1. Pokud obnovujete ze záložního média, nasaďte příslušné médium.
2. Nejsou-li v systému žádné paměťové prostory síťového serveru (po zadání příkazu `WRKNWSSTG` se žádný nezobrazí), je třeba vytvořit adresář `/QFPNWSSTG` před obnovením paměťových prostorů síťového serveru, které jste pod tímto adresářem uložili. Při vytváření adresáře `/QFPNWSSTG` postupujte takto:
  - a. Na příkazový řádek operačního systému i5/OS napište `CRTNWSSTG`. Vytvoří se paměťový prostor síťového serveru. Stiskněte klávesu F4.
  - b. Pojmenujte tento paměťový prostor.
  - c. Zadejte příslušné ASP; použijte minimální povolenou velikost.
  - d. Stisknutím klávesy Enter zadání potvrďte. Operační systém i5/OS vytvoří v adresáři `/QFPNWSSTG` paměťový prostor.
3. K obnovení paměťových prostorů napište příkaz `RST` a stiskněte klávesu F4.
4. Do pole Name pod Objects zadejte `'/QFPNWSSTG/stgspc'` a `'dev/QASPnn/stgspc.UDFS'`, kde *stgspc* je jméno paměťového prostoru síťového serveru a *nn* je číslo ASP.

### **Poznámka:**

Při obnově objektu .UDFS do nezávislého ASP musí být zařízení ASP logicky vypnuto. Zadejte `'dev/independent ASP name/stgspc.UDFS'`, kde *independent ASP name* je jméno nezávislého ASP a *stgspc* je jméno paměťového prostoru síťového serveru.

5. Dle potřeby zadejte hodnoty *i* pro další parametry a stisknutím klávesy Enter paměťový prostor obnovte.
6. Je třeba také obnovit všechny předdefinované diskové jednotky, které jsou k serveru přiřazeny, a obnovit objekt NWS D. Další informace najdete v tématu “Obnova NWS D u integrovaného Windows serveru”. Po dokončení obnovy objektu NWS D a všech přiřazených diskových jednotek logicky zapněte integrovaný server.

## Obnova NWS D u integrovaného Windows serveru

V případě obnovy po zhroucení systému byste měli obnovit veškeré konfigurační objekty, k nimž patří i popis síťového serveru (NWS D) integrovaného Windows serveru. Zvláště v některých situacích, například při migraci na nový hardware IXS (Integrated xSeries Server), je třeba obnovit NWS D. Automatická obnova propojení diskových

jednotek v integrovaném systému souborů s obnoveným NWSD v i5/OS vyžaduje, abyste nejprve obnovili tyto diskové jednotky. K obnově NWSD slouží příkaz RSTCFG (Obnova konfigurace):

1. Na příkazový řádek operačního systému i5/OS napište RSTCFG a stiskněte klávesu F4.
2. Do pole **Objects** zadejte jméno NWSD.
3. Do pole **Device** zadejte jméno zařízení, provádíte-li obnovu z média. Provádíte-li obnovu ze souboru typu save, zadejte \*SAVF a do příslušných polí uveďte pro tento soubor jeho jméno a knihovnu.
4. Stiskněte klávesu Enter. Operační systém i5/OS obnoví NWSD.
5. Po dokončení obnovy NWSD a všech přiřazených paměťových prostorů, spusťte integrovaný server. Další informace najdete v tématu “Spuštění a zastavení integrovaného serveru” na stránce 141.

**Poznámka:** Až obnovíte NWSD, musíte také obnovit všechny objekty popisu linky a popisu zařízení, které jsou k NWSD přiřazeny. Rovněž je nutné obnovit všechny popisy linek, které měly definováno rozhraní TCP/IP.

---

## Obnova objektů NWSH integrovaných Windows serverů pro servery připojené pomocí iSCSI

V případě nápravy po havárii byste měli obnovit všechny objekty konfigurace, tedy i objekt NWSH (adaptér hostitele síťového serveru). Chcete-li objekt NWSH uložit, použijte příkaz RSTCFG (Obnova konfigurace):

1. Na příkazový řádek operačního systému i5/OS napište RSTCFG a stiskněte klávesu F4.
2. Do pole **Objects** zadejte jméno a typ NWSH.
3. Do pole **Device** zadejte jméno zařízení, provádíte-li obnovu z média. Provádíte-li obnovu ze souboru typu save, zadejte \*SAVF a do příslušných polí uveďte pro tento soubor jeho jméno a knihovnu.
4. Stiskněte klávesu Enter. Operační systém i5/OS obnoví NWSH.

### Poznámky:

1. Až obnovíte NWSH, musíte jej spustit ještě před spuštěním integrovaného serveru.

---

## Obnova objektů NWSCFG integrovaných Windows serverů pro servery připojené pomocí iSCSI

Další objekty konfigurace pro servery připojené pomocí adaptérů iSCSI HBA by měly být obnoveny do knihovny QUSRSYS. Patří mezi ně objekty konfigurace síťových serverů (typu \*NWSCFG) a objekt přiřazeného ověřovacího seznamu (typu \*VLDDL).

**Poznámka:** Objekty \*NWSCFG a \*VLDDL sdílejí stejné jméno.

K obnovení paměťových prostorů serveru slouží příkaz RSTOBJ (Obnova objektu):

1. Na příkazový řádek operačního systému i5/OS napište RSTOBJ a stiskněte klávesu F4.
2. Pokud obnovujete ze záložního média, nasadte příslušné médium.
3. Do pole **Objects** zadejte jméno konfigurace síťového serveru. (Chcete-li obnovit několik objektů NWSCFG, zadejte generická jména “nwsdname\*”. Jména objektů můžete také určit explicitně zadáním znaku plus (+) a stisknutím klávesy Enter.)
  - Chcete-li obnovit předvolenou konfiguraci síťového serveru se zabezpečeným připojením, zadejte jméno NWSD následované znaky CN.
  - Chcete-li obnovit předvolenou konfiguraci síťového serveru se servisním procesorem, zadejte jméno NWSD následované znaky SP.
  - Chcete-li obnovit předvolenou konfiguraci síťového serveru ve vzdáleném systému, zadejte jméno NWSD následované znaky RM.
4. Do pole **Save Library** zadejte jméno QUSRSYS.



- l 5. Do pole **Device** zadejte buď jméno zařízení, které obsahuje záložní médium, nebo (v případě obnovy ze souboru typu save) zadejte \*SAVF.
- l 6. Do pole **Object types** zadejte \*NWSCFG i \*VLDL.
- l 7. Provádíte-li obnovu ze souboru typu save, zadejte pro tento soubor jeho jméno a knihovnu.
- l 8. Stisknutím klávesy **Enter** obnovte konfiguraci síťového serveru a přiřazeného ověřovacího seznamu.

---

## Obnova souborů integrovaného Windows serveru

Produkt IBM iSeries Integrated Server Support podporuje zálohování a obnovu na úrovni souborů. Ze zálohy v systému i5/OS můžete obnovit vybraný soubor, aniž byste museli obnovit celou diskovou jednotku. Před použitím této metody však zvažte množství dat, která bude třeba obnovit. V případě velkých objemů dat je obnova celého objektu diskové jednotky podstatně rychlejší než obnova jednotlivých souborů z této jednotky. Při menších objemech dat však tato metoda skvěle funguje.

Měli byste obnovit nejdříve adresář, potom soubory, potom registr a nakonec znovu zavést operační systém, aby se nové záznamy v registru mohly projevit. Obnova souborů uložených touto metodou se provádí příkazem RST:

1. Ujistěte se, že integrovaný Windows server a TCP/IP jsou spuštěny.
2. Na příkazový řádek operačního systému i5/OS napište RST a stiskněte klávesu F4.
3. Do pole **Device** zadejte zařízení, kde se nacházejí požadovaná data. (Například příkaz 'QSYS.LIB/TAP01.DEVD' obnoví data z pásky.)
4. Do pole **Object** zadejte objekty, které má operační systém i5/OS obnovit, ve tvaru '/QNTC/jménoserveru/sharename'.

Může používat zástupné znaky. V tématu "Příklady: Jak adresovat součásti integrovaného Windows serveru" na stránce 187 najdete informace o tom, jak se zadávají konkrétní součásti integrovaného Windows serveru. Nepoužívejte tuto metodu k obnově systémových souborů Windows, protože obnovené soubory se mohou chovat nepředvídatelně.

5. Do pole **Name** zadejte cestu k objektu, který chcete obnovit.
6. Pomocí pole **Include or omit** můžete zahrnout nebo vynechat objekty, které odpovídají vzoru zadanému v poli **Name** u parametru **Object**.
7. V poli **New object name** ponechte nabídnuté stejné jméno objektu, nebo zadejte novou cestu. Nová cesta musí být odkazována jménem sdílené položky, která existuje na integrovaném Windows serveru.

### Poznámka:

Když ukládáte adresář, nad nímž jsou definovány sdílené položky, operační systém i5/OS uloží informace o sdílených položkách spolu s tímto adresářem. Jestliže při obnově adresáře zadáte nové jméno objektu, operační systém i5/OS již tyto sdílené položky nevytvoří.

8. Pomocí pole **Directory subtree** zadejte, zda chcete obnovit i příslušné podadresáře daného adresáře. Předvolena je obnova všech adresářů.
9. Chcete-li obnovit soubory, které byly uloženy během určitého časového intervalu, zadejte počáteční a koncové datum a čas do pole **Change period**.
10. Zadejte libovolné další informace, která má operační systém i5/OS použít při obnově souborů, a stiskněte klávesu **Enter**.
11. Po dokončení obnovy souborů znovu zaveďte operační systém integrovaného serveru, aby se mohly projevit nové záznamy v registru.

---

## Kapitola 13. Odinstalování operačního systému Windows serveru z hardwaru integrovaného serveru

K odinstalování Windows serveru ze serveru Integrated xSeries Server můžete použít příkaz DLTWNTSVR (Výmaz Windows serveru). Před spuštěním příkazu Výmaz Windows serveru ukončíte práci integrovaného Windows serveru v operačním systému i5/OS. Další informace najdete v tématu “Spuštění a zastavení integrovaného serveru” na stránce 141.

Příkaz DLTWNTSVR (Výmaz Windows serveru) vymaže popis síťového Windows serveru a asociované objekty, které byly vytvořeny příkazem INSWNTSVR (Instalace Windows serveru). K těmto objektům patří popis síťového serveru, popisy linek, rozhraní TCP/IP a systémově vytvořené paměťové prostory síťového serveru. Síťový server musí být při použití tohoto příkazu logicky vypnutý.

Pokud není možné použít příkaz DLTWNTSVR (jestliže například objekt serveru NWSD již neexistuje, ale je nezbytné vyčistit některé asociované objekty), můžete manuálně vymazat server a asociované objekty pomocí níže uvedené procedury:

1. Vypněte integrovaný server, viz “Spuštění a zastavení integrovaného serveru” na stránce 141.
2. “Odpojení diskových jednotek integrovaného Windows serveru” na stránce 160.
3. “Výmaz diskových jednotek integrovaného Windows serveru” na stránce 160.
4. “Výmaz NWSD integrovaného Windows serveru”.
5. “Výmaz popisů linek integrovaného Windows serveru” na stránce 194.
6. “Výmaz rozhraní TCP/IP asociovaných s integrovaným Windows serverem” na stránce 194.
7. “Výmaz popisů radičů integrovaného Windows serveru” na stránce 195.
8. “Výmaz popisů zařízení asociovaných s integrovaným Windows serverem” na stránce 195.
9. “Výmaz konfigurací síťového serveru asociovaných s integrovaným Windows serverem sítě iSCSI” na stránce 195

Pokud odstraníte z operačního systému i5/OS všechny Windows servery a servery Linux, které používají konkrétní objekt NWSH (Network server host adapter), a nemáte-li v úmyslu v budoucnosti instalovat žádné další servery, které by tento NWSH používaly, můžete uvedený NWSH vymazat. Další informace najdete v tématu “Výmaz objektu NWSH” na stránce 116.

Jestliže odstraníte z operačního systému i5/OS všechny Windows servery a Linux a nemáte v úmyslu je v budoucnu znovu nainstalovat, můžete vymazat produkt IBM iSeries Integrated Server Support, abyste si uvolnili paměť, kterou tento produkt využívá. Další informace najdete v tématu “Výmaz produktu IBM i5/OS Integrated Server Support, volba 29 operačního systému i5/OS (5722–SS1)” na stránce 195.

---

### Výmaz NWSD integrovaného Windows serveru

Než vymažete popis síťového serveru (NWSD), je třeba odpojit jeho diskové jednotky (viz “Odpojení diskových jednotek integrovaného Windows serveru” na stránce 160) a vymazat paměťové prostory, jež jsou s tímto NWSD asociovány (viz “Výmaz diskových jednotek integrovaného Windows serveru” na stránce 160). Potom můžete vymazat i NWSD.

1. K odpojení paměťového prostoru pro systémovou jednotku v případě NWSD vytvořeného ve verzi V4R5 (nebo vyšší) napište na příkazový řádek operačního systému i5/OS příkaz `RMVNWSSTGL NWSSTG(nwsdname1) NWSD(nwsdname)`. Stiskněte klávesu Enter.
2. K odpojení paměťového prostoru pro jednotku s instalačním zdrojem napište příkaz `RMVNWSSTGL NWSSTG(nwsdname2) NWSD(nwsdname)` a stiskněte klávesu Enter.



3. V tomto okamžiku lze odstranit i uživatelsky definované paměťové prostory, které jsou k tomuto NWSG připojeny. Použijte k tomu příkaz `RMVNWSSSTGL NWSSTG(nwsstgname) NWSG(nwsdname)` (následovaný stisknutím klávesy Enter) tolikrát, kolikrát je třeba.
4. K vymazání objektu paměťového prostoru síťového serveru pro systémovou jednotku napište příkaz `DLTNWSSSTG NWSSTG(nwsdname1)` a stiskněte klávesu Enter.
5. K vymazání objektu paměťového prostoru síťového serveru pro jednotku s instalačním zdrojem napište příkaz `DLTNWSSSTG NWSSTG(nwsdname2)` a stiskněte klávesu Enter.
6. Ostatní již nepotřebné paměťové prostory odstraní příkazem `DLTNWSSSTG NWSSTG(nwsstgname)` a stisknutím klávesy Enter.

K vymazání popisu síťového serveru (NWSG) pro integrovaný server použijte tento postup:

1. Na příkazový řádek operačního systému i5/OS napište příkaz `WRKNWSD` a stiskněte klávesu Enter.
2. Do pole **Volba** vlevo od síťového serveru napište volbu **8** a stiskněte klávesu Enter. Objeví se obrazovka **Práce se stavem konfigurace**.
3. Jestliže NWSG není ve stavu "logicky vypnutý", napište do pole **Volba** vlevo od síťového serveru volbu **2**. Jinak přejděte na další krok.
4. Stisknutím klávesy F3 se vraťte na předchozí dialogové okno.
5. Do pole **Volba** vlevo od síťového serveru napište volbu **4** a stiskněte klávesu Enter.
6. Na obrazovce **Potvrzení popisů síťového serveru** stiskněte klávesu Enter.

**Poznámka:** Pokud provádíte výmaz NWSG, který byl vytvořen před verzí V4R5, prostudujte si téma **Výmaz NWSG integrovaného Windows serveru v aplikaci iSeries Information Center verze V5R3**.

---

## Výmaz popisů linek integrovaného Windows serveru

K vymazání všech popisů linek integrovaného serveru použijte tento postup:

1. Na příkazový řádek operačního systému i5/OS napište příkaz `WRKLIND` a stiskněte klávesu Enter.
2. Pomocí klávesy PageDown vyhledejte popis linky, který chcete vymazat.

**Poznámka:**

Jméno popisu linky by se mělo skládat ze jména popisu síťového serveru (NWSG), za nímž následuje dvojice znaků 00, 01, 02, PP, V0, V1, V2, V3, V4, V5, V6, V7, V8 nebo V9 podle toho, přes jaký port je tento popis připojen.

3. Do pole **Volba** vlevo od popisu linky napište volbu **4** a stiskněte klávesu Enter. Tento krok opakujte pro všechny další popisy linek, které jsou s tímto NWSG asociovány.

**Poznámka:**

Druhý možný způsob je, že namísto kroků 1 a 2 použijete příkaz `WRKLIND nwsdname*`, kde `nwsdname` je jméno popisu asociovaného síťového serveru.

---

## Výmaz rozhraní TCP/IP asociovaných s integrovaným Windows serverem

K vymazání rozhraní TCP/IP asociovaných s integrovaným serverem použijte tento postup:

1. Z konzole operačního systému i5/OS zadejte příkaz `CFGTCP`.
2. Z menu **Konfigurace TCP/IP** vyberte volbu **1. Práce s rozhraním TCP/IP**.
3. Do pole **Volba** vedle rozhraní TCP/IP, které chcete odstranit, napište **4** a stiskněte klávesu Enter.  
Rozhraní TCP/IP, která jsou asociována s popisem síťového serveru (NWSG), poznáte podle jména připojeného popisu linky. Toto jméno se skládá z NWSG, za nímž následuje číslo.
4. Krok 3 opakujte pro každé rozhraní TCP/IP, které je s tímto NWSG asociováno.

---

## Výmaz popisů řadičů integrovaného Windows serveru

K vymazání všech popisů řadičů integrovaného serveru použijte tento postup:

1. Na příkazový řádek operačního systému i5/OS napište příkaz **WRKCTLD** a stiskněte klávesu **Enter**.
2. Pomocí klávesy **PageDown** vyhledejte popis řadiče, který chcete vymazat.

**Poznámka:**

Jméno popisu řadiče začíná prvními pěti znaky jména **NWSD**, za nimiž následuje 'NET' a dvoumístné číslo. Je-li jméno **NWSD** například **MYSERVER**, jméno řadiče by mohlo být například **MYSERVERNET01**.

3. Do pole **Volba** vlevo od popisu řadiče napište volbu **4** a stiskněte klávesu **Enter**. Tento krok opakujte pro všechny další popisy řadičů, které jsou s tímto **NWSD** asociovány.

**Poznámka:**

Druhý možný způsob je, že namísto kroků 1 a 2 použijete příkaz **WRKCTLD MYSER\***, kde **MYSER** je prvních pět znaků jména **NWSD**.

**Upozornění:** Při použití této metody si ověřte, že chcete vymazat všechny **NWSD** ve vašem systému, které začínají těmito 5 znaky.

---

## Výmaz popisů zařízení asociovaných s integrovaným Windows serverem

K vymazání všech popisů zařízení pro integrovaný server použijte tento postup:

1. Na příkazový řádek operačního systému i5/OS napište příkaz **WRKDEVD** a stiskněte klávesu **Enter**.
2. Pomocí klávesy **PageDown** vyhledejte popis zařízení, který chcete vymazat.

**Poznámka:**

Jméno popisu zařízení začíná prvními pěti znaky jména **NWSD**, za nimiž následuje 'TCP' a dvoumístné číslo. Je-li jméno **NWSD** například **MYSERVER**, jméno zařízení by mohlo být **MYSERTCP01**.

3. Do pole **Volba** vlevo od popisu zařízení napište volbu **4** a stiskněte klávesu **Enter**. Tento krok opakujte pro všechny další popisy zařízení, které jsou s tímto **NWSD** asociovány.

**Poznámka:**

V systému může být mnoho zařízení. Pomocí příkazu **WRKDEVD MYSERTCP\*** nebo **WRKDEVD \*NET** si zobrazte úplný seznam všech síťových zařízení, která je třeba vymazat.

---

## Výmaz konfigurací síťového serveru asociovaných s integrovaným Windows serverem síť iSCSI

Při vymazávání konfigurací síťového serveru asociovaných s integrovaným serverem postupujte takto:

1. Z konzole operačního systému i5/OS zadejte příkaz **WRKNWSCFG**.
2. Vyhledejte konfigurace síťového serveru asociované s **NWSD**. Běžně bývají označovány genericky jako **nwsdname\***
3. Do pole **Volba** vedle konfigurací síťového serveru, které chcete odstranit, napište **4**.
4. Stiskněte klávesu **Enter**.

---

## Výmaz produktu IBM i5/OS Integrated Server Support, volba 29 operačního systému i5/OS (5722–SS1)

Jestliže ze serveru iSeries odstraňujete všechny integrované Windows servery a všechny servery Linux, které nejsou rozdělené na logické části, a nemáte v úmyslu v budoucnu opět instalovat jiné, můžete rovněž odstranit z operačního systému i5/OS produkt IBM i5/OS Integrated Server Support, volba 29. Odstraněním tohoto programu uvolníte prostor, který v operačním systému i5/OS využíval.

**Poznámka:**

Odstraněním tohoto programu se automaticky nevymažou stávající popisy síťových serverů ani uživatelsky definované diskové jednotky. Zůstanou však nepoužitelné. Informace o výmazu popisů síťových serverů a diskových jednotek najdete v tématu Kapitola 13, “Odinstalování operačního systému Windows serveru z hardwaru integrovaného serveru”, na stránce 193.


Chcete-li vymazat produkt IBM i5/OS Integrated Server Support, postupujte takto:

1. Na příkazový řádek operačního systému i5/OS napište příkaz `GO LICPGM` a stiskněte klávesu Enter.
2. V menu **Práce s licencovanými programy** vyberte volbu **12** a stiskněte klávesu Enter.
3. Pomocí klávesy PageDown vyhledejte v seznamu licencovaných programů položku **Integrated Server Support**.
4. Do pole **Volba** vlevo od programu napište **4**. Stiskněte klávesu Enter a operační program i5/OS tuto položku vymaže.

---




## Kapitola 14. Odstraňování problémů s integrovanými Windows servery

Nepracuje-li váš integrovaný server správně, vyzkoušejte při nápravě problému tyto kroky:

1. Znovu spusťte integrovaný server. Další informace najdete v tématu “Spuštění a zastavení integrovaného serveru” na stránce 141.
2. Zobrazte si informace o NWSD a asociovaných linkách, řadičích a zařízeních. Další informace najdete v tématu “Prohlížení a změna informací o konfiguraci integrovaného Windows serveru” na stránce 144.
3. Jestliže problém přetrvává, podívejte se na údaje zapsané v protokolech. Další informace najdete v tématu “Kontrola zpráv a protokolů úloh”.
4. Konkrétní problém potom vyhledejte v tématu “Problémy s integrovaným Windows serverem v systému iSeries” na stránce 200.
5. Můžete se též podívat na Informační APAR, které obsahují nejnovější rady a servisní informace. Najdete je na webových stránkách IBM Integrated xSeries Solutions .
6. V případě poškození integrovaného serveru byste měli být schopni zachovat instalované aplikace a uživatelská data tím, že jej přeinstalujete. Další informace najdete v tématu “Přeinstalování integrovaného Windows serveru” na stránce 230.
7. Potřebujete-li shromáždit servisní údaje, které byste měli poslat pracovníkům podpory, podívejte se na téma “Shromáždění údajů pro servis u integrovaného Windows serveru” na stránce 231.

### Další možnosti, jak řešit problémy

Nenajdete-li řešení svého problému v této části publikace, existují ještě další možnosti, které vám mohou pomoci problém vyřešit.

- Prostudujte si téma Troubleshooting  na webových stránkách Integrated xSeries Solutions ([www.ibm.com/servers/eserver/series/integratedxseries/troubleshooting.html](http://www.ibm.com/servers/eserver/series/integratedxseries/troubleshooting.html)).
- V případě problémů s konkrétní aplikací se obraťte na dodavatele této aplikace.
- V případě poruch hardwaru nebo problémů s instalací serveru IXS (Integrated xSeries Server) kontaktujte služby IBM.
- U nenapravitelných chyb serveru (například typu “modrá obrazovka”) můžete získat dodatečné informace na těchto webových stránkách:
  - Support for the iSeries family  ([www.ibm.com/servers/eserver/support/series/](http://www.ibm.com/servers/eserver/support/series/)).
  - Microsoft Help and Support  (<http://support.microsoft.com>).

Potřebujete-li další pomoc, pracovníci servisního střediska vám v rámci servisní smlouvy IBM pomohou nalézt správnou cestu k řešení. Kontaktujte linku podpory IBM.

---

## Kontrola zpráv a protokolů úloh

Informace o integrovaných Windows serverech se zaznamenávají na několika místech. Tyto informace vám pomohou při zjišťování příčin problémů.

### Protokol monitorovací úlohy

Protokol monitorovací úlohy (viz “Monitorovací úloha” na stránce 199) obsahuje veškeré zprávy, od událostí běžného zpracování až po podrobné chybové zprávy. Chcete-li si prohlédnout tento protokol, postupujte takto:

1. Na příkazový řádek operačního systému i5/OS zadejte příkaz WRKACTJOB (Práce s aktivní úlohou) a vyhledejte danou úlohu v podsystému QSYSWRK pod stejným jménem jako síťový server. Jestliže jste úlohu na této obrazovce nenašli, pravděpodobně právě skončila nebo ještě nezačala.
2. Po vyhledání úlohy můžete použít volbu 5 k práci s touto úlohou nebo volbu 10 k zobrazení jejího protokolu.
3. Podrobné zprávy zobrazíte stisknutím klávesy F10.
4. Jestliže jste v protokolu našli potřebné informace, запиšte si ID úlohy (všechny části: jméno, uživatel, číslo). Potom si protokol vytiskněte. Použijte příkaz: DSPJOBLOG JOB(číslo/uživatel/jméno) OUTPUT(\*PRINT).

#### **Poznámka:**

Jestliže problém vyvolal ukončení monitorovací úlohy nebo řešíte problém, který nastal ještě před současnou monitorovací úlohou, vyhledejte soubor pro souběžné zpracování, který obsahuje informace o předchozím protokolu úlohy. Soubory pro souběžné zpracování, které se týkají vašeho síťového serveru, zobrazíte příkazem WRKSPLF SELECT(QSYS \*ALL \*ALL jméno\_nwsd).

#### **Protokol úlohy QVNAVARY**

Protokol úlohy QVNAVARY obsahuje zprávy, které se týkají logického zapnutí a vypnutí popisu serveru připojeného pomocí IXS a IXA při ukončení práce a následném restartování z Windows serveru. Chcete-li si prohlédnout tento protokol chyb při vypnutí a zapnutí, postupujte takto:

1. Na příkazový řádek operačního systému i5/OS zadejte příkaz WRKACTJOB (Práce s aktivní úlohou) a vyhledejte úlohu QVNAVARY v podsystému QSYSWRK.
2. Použijte volbu 5 k práci s touto úlohou nebo volbu 10 k zobrazení jejího protokolu.

Můžete také zadat příkaz WRKJOB JOB(QVNAVARY).

Pro servery xSeries připojené pomocí IXS nebo IXA bude zadána dávková úloha používající jméno BTnwsdname, která provede logické vypnutí a logické zapnutí nezbytné pro "opětovné zavedení operačního systému" serveru.

Označte kvalifikované jméno úlohy, která byla zadána v protokolu úlohy QVNAVARY. V protokolu úlohy naleznete úlohu zadanou pro "opětovné zavedení operačního systému" podle plně kvalifikovaného jména úlohy pomocí příkazu WRKSPLF SELECT(\*ALL) JOB(qualjobname).

Vytvořte seznam všech úloh "opětovného zavedení operačního systému" pomocí příkazu WRKSPLF SELECT(\*ALL) JOB(BTnwsdname).

#### **Protokol úlohy, která vyvolala logické zapnutí nebo vypnutí**

Jestliže nějaká dávková úloha nebo interaktivní uživatel vyvolal logické zapnutí nebo vypnutí NWSD z operačního systému i5/OS, můžete z protokolu této úlohy získat užitečné informace. Jestliže jste použili například příkaz VRYCFG nebo WRKCFGSTS, můžete se pomocí příkazu DSPJOB (Zobrazení úlohy) a volby 10 podívat na protokol této úlohy.

#### **Fronta zpráv serveru**

Jestliže jste při instalaci specifikovali pro svůj síťový server frontu zpráv, můžete v ní nalézt užitečné informace.

1. Chcete-li si ověřit, zda jste frontu zpráv uvedli, napište na příkazový řádek operačního systému i5/OS příkaz DSPNWSN NWSD(jméno\_nwsd) a stiskněte klávesu Enter. Jestliže se zobrazí hodnota \*none, budou pouze závažné zprávy odesílány do fronty zpráv QSYSOPR.
2. Byla-li fronta zpráv specifikována, můžete zprávy z ní zobrazit tímto příkazem i5/OS: DSPMSG MSGQ(knihovna/fronta)

#### **Fronta zpráv systémového operátora**

Integrovaný server odesílá do fronty zpráv systémového operátora (QSYSOPR) kromě chybových zpráv i zprávy o normálním vypnutí a spuštění. K zobrazení těchto zpráv ze znakově orientovaného rozhraní zadejte příkaz DSPMSG QSYSOPR.

## Fronta zpráv komunikací

Servery připojené pomocí iSCSI zahrnují parametr fronty zpráv komunikací. Jestliže jste během instalace specifikovali pro svůj síťový server frontu zpráv komunikací, můžete v ní nalézt užitečné informace týkající se zpráv o stavu komunikace.

1. Chcete-li si ověřit, jakou frontu zpráv jste uvedli, napište na příkazový řádek operačního systému i5/OS příkaz DSPNWSN NWSN(jméno\_nwsn) a stiskněte klávesu Enter. Pokud je fronta zpráv komunikací nastavena na \*SYSOPR, budou zprávy odesílány do fronty zpráv QSYSOPR.
2. Byla-li fronta zpráv komunikací specifikována, můžete si zprávy z ní zobrazit tímto příkazem i5/OS: DSPMSG MSGQ(knihovna/fronta)

## Protokol úlohy synchronizace profilů

Protokol úlohy synchronizace profilů obsahuje zprávy týkající se EIM a zápisu uživatelských profilů. Tento protokol si můžete prohlédnout pomocí příkazu WRKJOB QPRFSYNCH.

## Monitorovací úloha

Každý aktivní integrovaný Windows server má monitorovací úlohu, která se spouští zároveň se spuštěním serveru. Monitorovací úloha se spouští v podsystému QSYSWRK pod uživatelským profilem QSYS. Jméno úlohy je stejné jako jméno síťového serveru, který monitoruje.

Při spuštění monitorovací úlohy odešle operační systém i5/OS informativní zprávu CPIA41B do fronty zpráv QSYSOPR. Tato zpráva obsahuje ID této monitorovací úlohy. Tento ID úlohy použijte u příkazu WRKJOB (Práce s úlohou) k vyhledání protokolu monitorovací úlohy a dalších informací týkajících se této úlohy.

## Další protokoly a zprávy pro servery připojené pomocí iSCSI

### Protokol úlohy adaptéru NWSH

Adaptéry NWSH jsou přiřazeny určitým systémovým úlohám pomocí operačního systému i5/OS. Z protokolu úlohy pro systémovou úlohu asociovanou s adaptérem NWSH můžete získat užitečné informace.

1. Chcete-li určit jméno systémové úlohy, napište na příkazový řádek operačního systému i5/OS příkaz DSPDEVD DEVD(nwsname) a stiskněte klávesu Enter. Pomocí klávesy Page down odstráňte na hodnoty jmen úlohy.
2. Příkazem DSPJOB (Zobrazení úlohy) a výběrem volby 10 se podívejte na protokol úlohy označený výše.

### Fronta zpráv zařízení hostitelského systému síťového serveru

Adaptéry NWSH zahrnují parametr fronty zpráv. Tato fronta zpráv může poskytovat užitečné informace.

1. Pokud chcete určit, která fronta zpráv se používá, podívejte se na téma “Zobrazení vlastností objektu NWSH” na stránce 114. Klepněte na kartu **Komunikace** a poznamenejte si jméno fronty zpráv a knihovnu.
2. Chcete-li si zobrazit frontu zpráv pomocí produktu iSeries Navigator, postupujte takto:
  - a. Rozbalte **Základní operace** → **Zprávy**.
  - b. Klepněte pravým tlačítkem myši na **Zprávy** a vyberte **Přizpůsobit tento pohled** → **Zahrnout...**
  - c. Vyberte volbu **Fronta zpráv** a vyplňte jméno fronty zpráv a knihovnu, které se objeví na panelu vlastností adaptéru NWSH.

**Poznámka:** Jestliže je na panelu vlastností adaptéru NWSH zobrazeno “Systémový operátor”, potom uveďte jako jméno fronty zpráv QSYSOPR.

### Protokol PAL (Product Activity Log)

Některé chyby související se sítěmi typu iSCSI, jako například selhání autentizace CHAP, jsou zapsány do protokolu PAL. Při přístupu do protokolu PAL postupujte takto:



- | 1. Spusťte CL příkaz STRSST (Spuštění systémových servisních nástrojů).
- | 2. Vyberte **Spuštění SST**.
- | 3. Vyberte **Product Activity Log**.


---

## Problémy s integrovaným Windows serverem v systému iSeries

Nepracuje-li váš integrovaný Windows server správně, podívejte se, zda jej můžete zařadit do některé skupiny v tomto seznamu:




- “Chyby typu STOP nebo “modrá obrazovka”” na stránce 201
- Problémy s programem pro údržbu softwaru. Další informace najdete v tématu “Program typu snap-in IBM iSeries Integrated Server Support” na stránce 211.
- **Problémy s jednotkami**
  - “Plná systémová jednotka integrovaného serveru” na stránce 201
- **Problémy se zařízením**
  - “Problémy s optickou jednotkou” na stránce 202
  - “Problémy s páskami” na stránce 202
- **Problémy se spuštěním/ukončením**
  - “Problémy se spuštěním integrovaného Windows serveru” na stránce 204
  - “Problémy týkající se výměny za chodu mezi servery” na stránce 205
  - “Chyby v konfiguračním souboru NWSD” na stránce 207
- **Externě připojené servery xSeries**
  - “DASD na serverech připojených pomocí IXA nebo iSCSI” na stránce 208
- **Problémy se zápisem uživatelů a skupin**
  - “Problémy při zápisu uživatelů a skupin” na stránce 208
  - “Problémy s oprávněním k zápisu uživatelů” na stránce 209
  - “Problémy s heslem” na stránce 210
- | • **Servery xSeries připojené pomocí iSCSI nebo servery IBM BladeCenter**
  - | – “Problémy se servery připojenými pomocí iSCSI” na stránce 212
  - | – “Síťová analýza cesty pro zavedení systému a cesty k paměťovým prostorům” na stránce 214
  - | – “Správa certifikátů cest” na stránce 214
  - | – “Odstraňování problémů s produktem IBM Director” na stránce 215
  - | - “Problémy zjišťování” na stránce 215
  - | - “Problémy s připojeními typu SSL” na stránce 216
  - | – “Problémy virtuální sítě Ethernet se servery připojenými pomocí iSCSI” na stránce 218
- **Problémy se sítěmi**
  - “Problémy virtuální sítě Ethernet se servery připojenými pomocí IXS a IXA” na stránce 220
  - “Problémy s externími sítěmi” na stránce 223
  - “Manuální aktualizace ovladačů LAN na integrovaném Windows serveru” na stránce 223
  - “Konflikty IP adres ve dvoubodové virtuální síti Ethernet” na stránce 226
  - “Problémy s přístupem u IFS” na stránce 228
  - “Problémy s TCP/IP nad virtuální sítí Ethernet” na stránce 227
  - “Problémy s přístupem ke sdíleným položkám serveru Windows Server 2003 ze systému souborů QNTC” na stránce 228
- | • “Problémy sdílení hardwaru hostovaného systému” na stránce 206
- “Problémy s ukládáním souborů integrovaného Windows serveru” na stránce 228
- “Nečitelné zprávy ve frontě zpráv serveru” na stránce 229

- “Problémy se získáním výpisu paměti systému Windows” na stránce 230

l Pokud se výše uvedená témata netýkají zcela problému, který řešíte, podívejte se na webové stránky Integrated xSeries Solutions Troubleshooting  na adrese <http://www.ibm.com/servers/eserver/iseriess/integratedxseries/troubleshooting.html>. Tyto webové stránky jsou dalším zdrojem informací pro odstraňování problémů.

## Chyby typu STOP nebo “modrá obrazovka”

Dochází-li k chybám vyvolávajícím modrou obrazovku, zkuste pomocí následujících kroků zjistit příčinu chyb a možnost jejich nápravy:

1. Na příkazový řádek operačního systému i5/OS napište příkaz DSPMSG QSYSOPR.
2. Stiskněte klávesu Enter. Objeví se fronta zpráv QSYSOPR.
3. Podívejte se, zda mezi zprávami není něco, co by vám mohlo pomoci zjistit příčinu problému.
4. Restartujte integrovaný server z operačního systému i5/OS tak, že jej logicky vypnete a opět zapnete (viz “Spuštění a zastavení integrovaného serveru” na stránce 141).
5. Zkontrolujte protokol událostí v operačním systému Windows, typ stop kódu a další diagnostické informace.
6. Zkontrolujte záznamy protokolu PAL a VLOG.
7. Pokud problém stále přetrvává, podívejte se do databází technických informací na webových stránkách  IBM iSeries Support . Nenaleznete-li ani zde řešení, obraťte se na svého poskytovatele technické podpory.
8. V případě serverů připojených pomocí iSCSI se podívejte na téma iSCSI troubleshooting  ([www.ibm.com/servers/eserver/iseriess/integratedxseries/iscsireadme/troubleshooting.html](http://www.ibm.com/servers/eserver/iseriess/integratedxseries/iscsireadme/troubleshooting.html)).

## Plná systémová jednotka integrovaného serveru

Systémová jednotka obsahuje operační systém Windows serveru a může obsahovat i aplikace a data. Když se tato jednotka zaplní, může to vyvolávat zprávy o plné jednotce nebo chyby stránkování.

Abyste zabránili zaplnění systémové jednotky, proveďte jeden nebo více těchto kroků:



- Zvětšíte velikost systémové jednotky při instalaci Windows serveru.
- Při instalaci aplikací je instalujte do některého z uživatelsky definovaných paměťových prostorů a nikoli na systémovou jednotku, která je nabízena jako předvolba.
- Přesuňte stránkovací soubor Windows serveru do některého z uživatelsky definovaných prostorů namísto předvolené systémové jednotky. Jestliže přesunete stránkovací soubor, nebudete moci shromáždit výpis paměti v případě STOP chyby nebo modré obrazovky. Chcete-li to však udělat, postupujte takto:
  1. Klepněte pravým tlačítkem myši na ikonu **My Computer** a vyberte **Properties**.
  2. Klepněte na kartu **Advanced**.
  3. Klepněte na tlačítko **Performance**.
  4. Klepněte na tlačítko **Change** v sekci **Virtual memory**.
  5. Vyberte uživatelsky definovaný paměťový prostor, který má potřebnou velikost volného prostoru.
  6. Klepněte na **OK**.
- Přesuňte výpis paměti Windows serveru do některého z uživatelsky definovaných prostorů namísto předvolené systémové jednotky. Chcete-li to učinit, postupujte takto:
  1. Rozbalte **Start, Settings**, a potom **Control Panel**.
  2. Klepněte na kartu **Startup/Shutdown**.
  3. Vyberte pole **Write debugging information to** v sekci **Recovery**.
  4. Vyberte uživatelsky definovaný paměťový prostor, který má dostatek volného prostoru (asi o 12 MB větší než je velikost paměti RAM). V dokumentaci k Windows najdete další doporučení a požadavky na velikost stránky.

5. Klepněte na **OK**.

**Poznámka:**



Jestliže přesunete výpis paměti Windows serveru do uživatelsky definovaného prostoru, budete muset zkopírovat soubor s výpisem na pásku a zaslat ji technické podpoře.

- Pokud problém stále přetrvává, podívejte se do databázi technických informací na webových stránkách

 IBM iSeries Support  . Nenaleznete-li ani zde řešení, obraťte se na svého poskytovatele technické podpory.

## Problémy s optickou jednotkou

Jestliže optická jednotka operačního systému i5/OS nespolupracuje s integrovaným Windows serverem, vyzkoušejte následující kroky:

1. Zkontrolujte, zda je optická jednotka v operačním systému i5/OS logicky zapnutá. Návod, jak logicky zapnout optickou jednotku, najdete v tématu “Použití optických jednotek serveru iSeries s integrovanými Windows servery” na stránce 163.
2. Zkontrolujte, zda je optická jednotka alokována tomuto integrovanému serveru.
3. Zkontrolujte, zda je v jednotce vloženo optické médium.
4. Je-li váš systém rozdělen na logické části, zkontrolujte, zda je optická jednotka alokována stejné logické části jako integrovaný server.
5. Podívejte se do protokolu událostí, zda nezaznamenal chyby optické jednotky.
6. Zkontrolujte, zda se daná optická jednotka zobrazí na integrovaném Windows serveru pod složkou **My Computer**.
7. Postup obnovy optických jednotek:
  - a. Zavřete program typu snap-in IBM iSeries Integrated Server Support.
  - b. Logicky vypněte optickou jednotku na serveru iSeries.
  - c. Opět ji logicky zapněte.
  - d. Znovu přiřaďte jednotku k integrovanému serveru.
8. Pokud problém stále přetrvává, podívejte se do databázi technických informací na webových stránkách  IBM iSeries Support  .
9. Nenaleznete-li ani zde řešení, obraťte se na svého poskytovatele technické podpory.

Jestliže se integrovaný server zastaví dříve, než uvolní zámek optické jednotky, bude tato jednotka nedostupná pro operační systém i5/OS i pro ostatní integrované servery. Další informace najdete v tématu “Uzamknutá optická jednotka při selhání serveru”.

## Uzamknutá optická jednotka při selhání serveru



Jestliže se integrovaný server zastaví dříve, než uvolní zámek optické jednotky (nebo než ji logicky vypnut), bude tato jednotka nedostupná pro operační systém i5/OS i pro ostatní Windows servery. V takovém případě je třeba tuto optickou jednotku logicky vypnout pomocí příkazu WRKCFGSTS \*DEV \*OPT a znovu ji zapnout, aby se zámek uvolnil.

## Problémy s páskami

Jestliže pásková jednotka operačního systému iSeries nespolupracuje s integrovaným Windows serverem, vyzkoušejte následující kroky:

1. Zkontrolujte, zda jste tuto páskovou jednotku logicky vypnuli v operačním systému i5/OS a uzamkli ji na integrovaném serveru. Další informace najdete v tématu “Alokace páskové jednotky serveru iSeries pro integrovaný Windows server” na stránce 165. Chyba při uzamykání může nastat z těchto důvodů:
  - Pásková jednotka nebo její knihovna jsou logicky zapnuté.
  - Pro jednotku není zaveden ovladač.
  - Daná pásková jednotka není podporována.

- Při problémech s uzamknutím páskové jednotky zkontrolujte, zda je na integrovaném serveru příslušný ovladač. To se obvykle děje automaticky. Další informace najdete v tématu “Kontrola, zda byl zaveden ovladač páskové jednotky”.
  - Zkontrolujte, zda je daná pásková jednotka podporována. Další informace najdete v tématu “Podporované páskové jednotky iSeries” na stránce 167.
2. U modernějších aplikací se může stát, že uzamknou jednotku pro služby, které pokračují v činnosti i po zavření aplikačního rozhraní. To brání ostatním aplikacím v použití jednotky. Tyto služby se mohou restartovat automaticky po restartu počítače a uzamknout jednotku pro aplikaci. Chcete-li vidět služby určité aplikace (například Seagate and Computer Associates), postupujte takto:
    - a. Klepněte na **Start, Programs, Administrative Tools** a potom na **Component Services**.
    - b. Dvakrát klepněte na **Services**.
    - c. V případě potřeby můžete služby zastavit z okna **Services**.
  3. Integrovaných serverů můžete mít více. Je-li tomu tak, zkontrolujte, zda je pásková jednotka u všech serverů odemknuta s výjimkou toho, pro něž ji chcete používat. Další informace najdete v tématu “Přenos řízení páskových a optických jednotek iSeries mezi integrovanými Windows servery” na stránce 167.
  4. Má-li váš systém logické části, zkontrolujte, zda je pásková jednotka alokována též logické části jako daný integrovaný server.
  5. Ověřte si, že je páska v jednotce správně naformátovaná. Další informace najdete v tématu “Formátování pásky v i5/OS pro použití s integrovanými Windows servery” na stránce 165.
  6. Ověřte si, že daná jednotka není na seznamu zařízení, k nimž je v operačním systému i5/OS omezen přístup. Použijte k tomu příkaz DSPNWSDD (Zobrazení popisu síťového serveru).
  7. Podívejte se do protokolu událostí, zda nezaznamenal chyby páskové jednotky.
  8. Podívejte se, zda je daná pásková jednotka na seznamu zařízení.
    - a. Klepněte na **Start, Programs, Administrative Tools** a potom na **Computer Management**.
    - b. Vyberte **System Tools** a potom **Device Manager**.
    - c. Ověřte si, zda se vaše pásková jednotka nachází na seznamu zařízení.
  9. Pokud problém stále přetrvává, podívejte se do databázi technických informací na webových stránkách

 **@server** IBM iSeries Support  . Nenaleznete-li ani zde řešení, obraťte se na svého poskytovatele technické podpory.

## Kontrola, zda byl zaveden ovladač páskové jednotky

Aby mohla aplikace spuštěná na integrovaném serveru používat páskovou jednotku iSeries, musí být na integrovaném serveru zaveden ovladač páskové jednotky. To se obvykle děje automaticky. Další informace týkající se podporovaných páskových jednotek najdete v tématu “Podporované páskové jednotky iSeries” na stránce 167.

Chcete-li se přesvědčit, zda je tento ovladač zaveden, postupujte takto:

1. Na nástrojové liště Windows serveru klepněte na **Start, Programs**, a potom na **Administrative Tools**.
2. Vyberte **Computer Management, System Tools** a potom **Device Manager**.
3. Rozbalte ikonu se jménem vašeho počítače. Je-li ovladač páskové jednotky zaveden, zobrazí se ikona páskové jednotky.
4. Rozbalte ikonu páskové jednotky, abyste viděli, které ovladače páskové jednotky jsou zavedeny.

Pokud máte páskovou jednotku IBM iSeries Tape Drive, která nepožaduje ovladač jiného výrobce a manuální zavedení ovladače zařízení, proveďte na konzoli integrovaného serveru tyto kroky.

1. Klepněte na **Start**, pak na **Settings** a nakonec na **Control Panel**.
2. Klepněte na **Add/Remove Hardware**.
3. V průvodci přidáním nebo odebráním hardwaru klepněte na **Next**.
4. Vyberte **Add/Troubleshoot a device** a klepněte na **Next**.
5. V sekci **Choose a Hardware Device** v okně průvodce vyberte **Add a new device** a klepněte na **Next**.

6. V sekci **Find New Hardware** v okně průvodce vyberte "No, I want to select the hardware from a list" a klepněte na **Next**.
  7. V sekci **Hardware Type** vyhledejte položku **Tape drives**, vyberte ji a klepněte na **Next**.
  8. V seznamu výrobců v sekci **Select a Device Driver** vyberte **IBM**. V seznamu modelů vyberte **IBM iSeries Tape Drive** a klepněte na **Next**.
  9. V sekci **IBM iSeries Tape Drive** tohoto okna klepněte na **Next**.
  10. Pokud se objeví okno pro zadání souborů s označením "Files Needed", zadejte do pole "Copy files from" cestu %SystemRoot%\System32\drivers, kde C: je vaše systémová jednotka. Klepněte na **OK**.
  11. V sekci "Completing the Add/Remove Hardware" v okně průvodce klepněte na **Finish**. Tím by všechny páskové jednotky měly být zavedeny.
  12. Po restartu počítače zopakujte kroky 1 – 4, abyste se přesvědčili, že požadovaná zařízení byla zavedena.
- Informace o zavádění jiných ovladačů páskové jednotky najdete v tématu "Instalace ovladačů páskových jednotek" na stránce 165.

## Problémy se spuštěním integrovaného Windows serveru

Jestliže integrovaný server nelze spustit, zkuste pomocí následujících kroků zjistit, v čem je problém.

1. Zkontrolujte stav serveru. Aktuální stav NWSD musí být **VARRIED OFF** (Logicky vypnutý). Pokud není, vypněte tento NWSD a znovu zkuste spustit server. Další informace najdete v tématu "Spuštění a zastavení integrovaného serveru" na stránce 141. Je-li stav serveru **VARY ON PENDING** (Nevyřízené logické zapnutí) a integrovaný server se přesto nespustí, může jít o problém s ovladačem zařízení.
2. Zkuste najít chybové zprávy a možné nápravné kroky v protokolu úlohy, kde se logické zapnutí NWSD provádělo.
3. Podívejte se i do fronty zpráv QSYSOPR na chybové zprávy a možné nápravné kroky.
4. Jestliže jste vytvořili konfigurační soubor serveru, který by mohl být příčinou problémů, zkuste tento konfigurační soubor serveru opravit nebo obnovit. Další informace najdete v tématu "Chyby v konfiguračním souboru NWSD" na stránce 207.
5. Jestliže jste restart iniciovali z integrovaného serveru, proveďte tyto kroky:
  - a. V operačním systému i5/OS napište příkaz **WRKACTJOB SBS(QSYSWRK)**.
  - b. Stiskněte klávesu **Enter**.
  - c. Vyhledejte úlohu **QVNAVARY**.
  - d. Vyberte volbu 5 pro práci s úlohou.
  - e. Je-li tato úloha aktivní nebo čeká ve frontě úloh, vyberte volbu 10 pro zobrazení protokolu úlohy. Vyhledejte chybové zprávy a možné nápravné kroky.
  - f. Jestliže je úloha ukončena, zadejte příkaz **WRKSPLF SELECT(\*CURRENT \*ALL \*ALL QVNAVARY)** pro zobrazení souboru pro souběžné zpracování.
6. Zadejte příkaz **WRKPRB**, který zobrazí zaznamenané problémy.

Pro server xSeries připojený pomocí IXS nebo IXA bude zadána dávková úloha používající jméno BTnwsdname, která provede logické vypnutí a logické zapnutí nezbytné pro "opětovné zavedení operačního systému" serveru.

Označte kvalifikované jméno úlohy, která byla zadána v protokolu úlohy QVNAVARY. V protokolu úlohy naleznete úlohu zadanou pro "opětovné zavedení operačního systému" podle plně kvalifikovaného jména úlohy pomocí příkazu **WRKSPLF SELECT(\*ALL) JOB(qualjobname)**.

Vytvořte seznam všech úloh "opětovného zavedení operačního systému" pomocí příkazu **WRKSPLF SELECT(\*ALL) JOB(BTnwsdname)**.

### Oprava při nouzovém stavu

Jestliže problém přetrvává kvůli poruchám systémové jednotky, a máte-li zálohu této jednotky, zkuste tuto opravu v případě nouzového stavu. K obnově ztracených dat a návratu systému do funkčního stavu použijte tento postup:

#### **Poznámka:**

V následujících příkladech je použito jméno NWSD ERS se systémovou jednotkou ERS1.

1. Odpojte vadnou systémovou jednotku (obvykle je to jednotka C:) pomocí příkazu: `RMVNWSSTGL NWSSTG(ERS1) NWSD(ERS)`.
2. Zkopírujte vadnou systémovou jednotku na nové jméno pomocí příkazu: `CRTNWSSTG NWSSTG(ERSBKP) FROMNWSSTG(ERS1)`.
3. Proveďte obnovu z poslední zálohy systémové jednotky.
4. Obnovenou systémovou jednotku připojte pomocí příkazu: `ADDNWSSTGL NWSSTG(ERS1) NWSD(ERS)`.
5. Připojte vadnou systémovou jednotku z kroku 1 pomocí příkazu: `ADDNWSSTGL NWSSTG(ERS1BKP) NWSD(ERS)`
6. Logicky zapněte NWSD příkazem: `VRYCFG CFGOBJ(ERS) CFGTYPE(*NWS) STATUS(*ON)`.
7. Z vadné systémové jednotky zkopírujte všechny klíčové soubory, jako jsou datové soubory, které se změnily od poslední zálohy.
8. Nainstalujte případné aplikace, které jste přidali nebo převáděli na vyšší verzi od poslední zálohy.
9. Logicky vypněte NWSD příkazem: `VRYCFG CFGOBJ(ERS1) CFGTYPE(*NWS) STATUS(*OFF)`.
10. Odpojte vadnou systémovou jednotku z kroku 5 pomocí příkazu: `RMVNWSSTGL NWSSTG(ERS1BKP) ERS(ERS1)`.
11. Pokud si nejste jisti, že jste si přenesli všechna potřebná data z vadné systémové jednotky, můžete ji opět připojit a zkopírovat na obnovenou jednotku další soubory. Po přenesení všech dat z vadné systémové jednotky proveďte novou zálohu všech paměťových prostorů. Informace o zálohování paměťových prostorů najdete v tématu “Zálohování předdefinovaných diskových jednotek pro integrované Windows servery” na stránce 181. Potom vymažte vadnou jednotku příkazem: `DLTNWSSTG NWSSTG(ERS1BKP)`.

## **Problémy týkající se výměny za chodu mezi servery**

Hlavní příčinou toho, že funkce výměny za chodu mezi integrovanými servery může selhat, je otázka kompatibility hardwaru. Tyto problémy může rovněž způsobit aktivace serveru Windows Server 2003. Podrobnosti jsou uvedeny v následujících sekcích.

### **Kompatibilita hardwaru při výměně za chodu**

Přepnutí Windows serveru z jedné sady hardwaru integrovaného serveru na jiný je jako migrace systémové jednotky Windows z jednoho PC na jiný. Rozdíly v požadované vrstvě HAL (Hardware abstraction layer), úrovni BIOS (Basic input/output system) nebo v zařízení, která jsou instalována na těchto dvou PC, mohou způsobit problémy s migrací. Během výchozího zavádění operačního systému Windows na druhý PC jsou rozdíly v hardwaru odhaleny a jsou ošetřeny různými způsoby:

- Některé rozdíly v hardwaru je možné automaticky obsloužit prostřednictvím funkce “plug and play”.
- Některé rozdíly v hardwaru mohou vyžadovat manuální zásah. Může být například nutné instalovat nový ovladač zařízení.
- Pokud jsou rozdíly v hardwaru značné, mohou zabránit druhému PC v zavedení operačního systému. Tyto dva PC například požadují kompatibilní verze HAL.

Tytéž pokyny týkající se kompatibility platí při výměně za chodu mezi servery xSeries připojenými pomocí IXS a IXA, servery IBM xSeries připojenými pomocí iSCSI nebo servery BladeCenter. Aby migrace výměny za chodu proběhla úspěšně, měla by se konfigurace obou serverů co nejvíce shodovat.

### **Server IXS (Integrated xSeries Server) jako rezervní server pro výměnu za chodu**

Aby bylo možné používat výměnu za chodu mezi servery IXS, mělo by se jednat o servery kompatibilního typu, které by měly mít srovnatelnou konfiguraci adaptérů LAN atd. Konkrétní konfigurace rezervního serveru IXS pro výměnu za



chodu, které jsou podporovány, uvádí konfigurační tabulka serveru IXS (Integrated xSeries Server) na této webové stránce: [http://www.ibm.com/eserver/series/integratedxseries/ixs\\_system\\_config.html](http://www.ibm.com/eserver/series/integratedxseries/ixs_system_config.html).

### Server xSeries nebo IBM BladeCenter jako rezervní server pro výměnu za chodu

Aby bylo možné používat výměnu za chodu mezi servery xSeries připojenými pomocí IXA, servery xSeries připojenými pomocí iSCSI nebo servery IBM BladeCenter, důrazně doporučujeme, abyste používali tentýž typ serverů xSeries nebo blade serverů IBM BladeCenter. Například server xSeries model 236 může být rezervním serverem pro výměnu za chodu pro jiný server xSeries model 236. Navíc by servery xSeries měly mít podobnou konfiguraci adaptérů PCI atd.

**Poznámka:** Je možné provádět výměnu za chodu mezi dvěma modely serveru xSeries nebo modely blade serveru, které nejsou téhož typu. Mezi modely serveru xSeries a modely blade serveru ovšem existují značné rozdíly v konfiguraci. Proto byste měli otestovat konkrétní kombinaci modelů serveru xSeries nebo modelů blade serveru, které v tomto případě plánujete používat pro výměnu za chodu. Předtím, než začnete modely serverů xSeries nebo modely blade serveru používat pro zálohování s možností výměny za chodu v provozním prostředí, měli byste ověřit, že mají kompatibilní hardwarovou konfiguraci a že je možné provádět bezproblémovou migraci z jednoho serveru na druhý.

### Aktivace serveru Windows Server 2003

Pokaždé, když jsou paměťové prostory serveru Windows Server 2003 přepnuty na jiný rezervní integrovaný server pro výměnu za chodu, musí být spuštěna funkce Windows Activation. Každý licenční klíč má omezený počet bezplatných aktivací. Pokud je aktivace vyvolávána vícekrát, může dojít k situaci, že bude nezbytné zatelefonovat do firmy Microsoft, aby mohla být provedena opětovná aktivace. To může omezit rychlost, jakou lze server opětovně aktivovat. V tomto případě mohou pomoci licence na nosič softwaru Windows Server 2003, neboť zde není aktivace vyžadována.

## Problémy sdílení hardwaru hostovaného systému

Informace zabývající se problémy se sdílením hardwaru hostovaného systému najdete pod těmito odkazy:

- “Několik NWSD definovaných na stejném hardwaru hostovaného systému”
- “Speciální pokyny týkající se systémů připojených pomocí iSCSI”

### Několik NWSD definovaných na stejném hardwaru hostovaného systému

Je možné definovat několik popisů síťového serveru (NWSD) pro řízení hardwaru určitého serveru IXS (Integrated xSeries Server), systému xSeries nebo serveru IBM BladeCenter. U serverů, které nejsou připojeny pomocí iSCSI, musí být tyto NWSD ve stejné logické části iSeries. U serverů připojených pomocí iSCSI ovšem tyto NWSD mohou být definované jak ve stejné logické části systému iSeries, tak v jiné logické části téhož systému iSeries, nebo na zcela jiném serveru iSeries. Můžete mít například NWSD definovaný pro použití systému xSeries na provozní práci během běžných pracovních hodin a jiný NWSD definovaný pro použití téhož systému xSeries v jinou dobu.

V jednom okamžiku může používat konkrétní hardwarový prostředek pouze jeden NWSD. Z tohoto důvodu, pokud existuje několik definovaných NWSD, které se mají spouštět na jednom hardwaru a jeden z těchto NWSD momentálně tento hardware používá, ostatní nemají povoleno se spustit, dokud NWSD momentálně používající hardware není ukončen (logicky vypnut). To zabraňuje, aby některý NWSD neúmyslně přebíral hardware, který již používá jiný NWSD.

Pokud máte problémy se spuštěním NWSD a hardware serveru je momentálně používán jiným NWSD, potom správný způsob předání řízení hardwaru z jednoho NWSD na druhý je tento: nejprve ukončíte NWSD, který hardware momentálně používá, a potom spustíte NWSD, který potřebuje tento hardware používat dále.

### Speciální pokyny týkající se systémů připojených pomocí iSCSI

V případě serverů připojených pomocí iSCSI platí, že stav hardwaru serveru se používá k řízení přístupu k hardwaru, aby se tak zajistilo, že v jednom časovém okamžiku bude hardware používat pouze jeden NWSD. Když se spustí (logicky zapne) NWSD, konkrétní chování serveru připojeného pomocí iSCSI závisí na typu servisního procesoru, který tento server má:

- V případě serverů xSeries se servisním procesorem BMC musí být hardware na začátku ve stavu Vypnuto.
  - V případě serveru xSeries s adaptérem RSA II nebo serveru IBM BladeCenter s modulem Management Module nesmí být na hardware zaveden operační systém (například DOS nebo Windows). Je dovolen systém xSeries, který je uveden na náznaku vložení diskety, tento systém ovšem bude čekat určitý časový interval, aby si ověřil, že se žádný jiný systém nepokouší tento systém používat.
- Jinak operace spuštění selže. Po ukončení práce (logickém vypnutí) NWSD, bude hardware serveru xSeries nebo blade serveru BladeCenter tohoto NWSD ponechán ve stavu Vypnuto.

Kromě případu, kdy nějaký NWSD momentálně používá hardware serveru, existují ještě jiné možné důvody pro to, aby byl hardware serveru ve stavu Zapnuto. Hardware serveru mohl být například zapnutý kvůli provedení nastavení hardwaru, jako například zavedení firmwaru nebo změna nastavení BIOS. Jiným příkladem je, když operační systém serveru zaznamenal nenapravitelnou chybu, která vyústila v selhání serveru, ale hardware byl ponechán ve stavu Zapnuto. V těchto případech spuštění NWSD normálním způsobem selže, protože hardware serveru není ve stavu Vypnuto nebo servisní procesor indikuje, že operační systém stále pracuje.

Existuje řada způsobů, jak tuto situaci napravit:

- Pokud nějaký NWSD momentálně používá hardware, ale operační systém serveru selhal, pokuste se ukončit práci serveru. Ve většině případů se rovněž vypne hardware serveru a zpřístupní se pro tentýž nebo jiný NWSD. Jestliže ukončení práce NWSD daný problém nevyřeší, vyzkoušejte níže uvedenou metodu.
- Při spuštění NWSD je zde volba resetování systému, která přinutí hardware serveru, aby se během spuštění NWSD resetoval. Tuto volbu můžete použít ke spuštění NWSD, který používá hardware serveru, jenž je ve stavu, který by normálně způsobil selhání spuštění (logického zapnutí) serveru.

**Upozornění:** Funkci resetování systému použijte pouze tehdy, pokud jste si jisti, že hardware serveru není momentálně používán jiným NWSD. Jestliže ke spuštění NWSD použijete funkci resetování systému v případě, že zde je jiný NWSD, který je dosud spuštěný na tomto hardware, nastane selhání tohoto druhého NWSD a může dojít ke ztrátě nebo narušení dat.

Chcete-li resetovat vzdálený systém pomocí produktu iSeries Navigator, postupujte takto:

1. Rozbalte **Administrace integrovaných serverů**.
2. Rozbalte **Servery**.
3. Klepněte pravým tlačítkem myši na server v zobrazeném seznamu.
4. Vyberte **Začněte volbami...**
5. Zaškrtněte políčko **Resetovat vzdálený systém**.
6. Klepněte na **Start**. Objeví se potvrzovací panel.
7. Na potvrzovacím panelu klepněte na **Start**, aby se spustil a resetoval vzdálený systém.

Jestliže chcete použít CL příkaz, podívejte se na klíčové slovo RESETSYS (Resetování systému) příkazu VRYCFG (Logické zapnutí/vypnutí konfigurace).

## Chyby v konfiguračním souboru NWSD

Máte-li podezření, že příčinou chyby je vámi vytvořený konfigurační soubor NWSD, zkuste nastavit parametr tohoto konfiguračního souboru NWSD na \*NONE. Další informace najdete v tématu “Resetování parametru konfiguračního souboru NWSD” na stránce 208. Jestliže chyba zmizí, bude problém ve vašem konfiguračním souboru NWSD.

V případě, že konfigurační soubor NWSD vyvolává chyby, máte následující možnosti:

- Pokračovat dále, aniž byste používali tento váš konfigurační soubor NWSD.
- “Použití předchozí verze souboru integrovaného serveru” na stránce 208
- “Oprava konfiguračního souboru NWSD” na stránce 208

## Oprava konfiguračního souboru NWSD

Chcete-li opravit svůj konfigurační soubor NWSD, abyste odstranili chyby, vezměte v úvahu tyto možnosti.

1. Podívejte se do protokolů na chyby a možnosti nápravy. Další informace najdete v tématu “Kontrola zpráv a protokolů úloh” na stránce 197.
2. Upravte svůj konfigurační soubor NWSD.
3. Znovu spusťte server. Další informace najdete v tématu “Spuštění a zastavení integrovaného serveru” na stránce 141.

## Resetování parametru konfiguračního souboru NWSD

Nastavením parametru konfiguračního souboru pro daný NWSD na \*NONE, zabráníte působení změn v souboru integrovaného serveru, které vyvolávají chyby. Chcete-li zabránit operačnímu systému i5/OS, aby používal konfigurační soubor NWSD, postupujte takto:

1. Na příkazový řádek operačního systému i5/OS napište příkaz WRKNWSD pro práci s popisy síťových serverů (NWSD).
2. Na řádku s problematickým síťovým serverem vyberte volbu 2 (Změna).
3. V poli Configuration file vyberte hodnotu \*NONE.
4. Logicky zapněte síťový server a zkuste, jestli se chyba odstranila.

### Poznámka:

Všechny současné modifikace jiných souborů, které konfigurační soubor zpracovává, zůstanou beze změny. Existuje soubor .BKU, který má obsah stejný jako před poslední modifikací provedenou při logickém zapnutí serveru. Tento soubor můžete použít k nahrazení změněné verze, nebo můžete původní soubor obnovit z poslední zálohy, pokud existuje.

## Použití předchozí verze souboru integrovaného serveru

Máte-li fungující verzi souboru integrovaného serveru, můžete tento soubor vrátit do stavu této verze. Použijte tento postup:

1. Nastavením parametru konfiguračního souboru pro daný NWSD na \*NONE zabráníte působení změn v souboru integrovaného serveru, které vyvolávají chyby. Další informace najdete v tématu “Resetování parametru konfiguračního souboru NWSD”.
2. Vyberte soubor, který chcete vrátit na předchozí verzi.
3. Je-li server funkční a logicky zapnutý, přihlaste se k němu nebo spusťte z konzole i5/OS vzdálený příkaz (viz “Vzdálené spuštění příkazů integrovaného Windows serveru” na stránce 145) pro přejmenování souborů:
  - Změňte jméno souboru, který vyvolává problémy, na jiné jméno.
  - Změňte jméno předchozí verze tohoto souboru na původní jméno souboru.
4. Logicky vypněte a opět zapněte integrovaný server. Server bude nyní používat předchozí verzi souboru.

## DASD na serverech připojených pomocí IXA nebo iSCSI

Lokální jednotky pevných disků nejsou u serveru xSeries podporovány, pokud je přímo připojen k serveru iSeries pomocí adaptéru IXA. Lokální jednotky pevných disků nejsou u serveru IBM xSeries nebo BladeCenter podporovány, pokud je připojen k severu iSeries pomocí adaptéru iSCSI HBA. Ve většině případů se lokální disková jednotka nezobrazí. Pokud se tato jednotka zobrazí a použije se, může dojít k nepředvídatelným výsledkům. Používáte-li servery xSeries nebo IBM BladeCenter v režimu přímého připojení k serveru iSeries pomocí adaptéru IXA nebo iSCSI HBA, zajistěte, aby všechny jednotky pevného disku byly odstraněny.

## Problémy při zápisu uživatelů a skupin

Pokud nelze zapisovat skupiny či uživatele do prostředí Windows na serveru iSeries, zkuste pomocí následujícího postupu zjistit problém.

### Z prostředí operačního systému i5/OS:

- Podívejte se na chyby do protokolu zpráv pro tento NWS (při instalaci označeného jako QSYSOPR, uživatelsky definovaný protokol zpráv nebo protokol uživatelské úlohy). K nápravě problému použijte nápravné akce pro danou chybovou zprávu. Chybové kódy můžete najít i na obrazovce WRKNWSEN (Práce se zápisem na NWS).
- Je-li v protokolu zpráv chyba NTA0282 (chyba uživatele Admin), prostudujte si téma “Problémy s oprávněním k zápisu uživatelů”.
- Ověřte si, zda je stav serveru VARIED ON (Logicky zapnutý).
- Zkontrolujte stav zápisu (viz “Zápis jednoho uživatele operačního systému i5/OS do prostředí Windows pomocí produktu iSeries Navigator” na stránce 169) a vyhledejte chybové zprávy. Stisknutím klávesy F5 stav aktualizujte.
- Ověřte si, zda je operační systém i5/OS nastaven tak, aby uchovával hesla (parametr QRETSVRSEC je nastaven na 1). Zkontrolujte také, zda se uživatelé, kteří se pokoušejí zapsat, přihlásili do operačního systému i5/OS až po nastavení této hodnoty.
- Specifikujte a vytvořte frontu zpráv pro NWS a zkontrolujte zprávy v této frontě.
- V operačním systému i5/OS zadejte příkaz WRKACTJOB. Zkontrolujte úlohu QPRFSYNCH v podsystému QSYSWRK. Podívejte se do protokolu této úlohy - stisknutím klávesy F10 zobrazte podrobnější zprávy.
- V operačním systému i5/OS zadejte příkaz WRKJOB *nwsdname*, kde *nwsdname* je jméno NWS pro váš integrovaný server. Je-li úloha aktivní, zobrazte si její protokol (stisknutím klávesy F10 zobrazte podrobnější zprávy). Je-li úloha ukončena zobrazte si soubor pro souběžné zpracování.

## Z integrovaného Windows serveru:

Při určování problému můžete vyzkoušet také následující kroky:

- Podívejte se, zda je spuštěna služba pro administraci uživatelů.
  1. V menu **Start** na integrovaném serveru vyberte **Programs, Administrative Tools** a potom **Component Services**.
  2. Vyberte **System Tools** a potom **Services**.
  3. Podívejte se, zda je v seznamu služeb uvedena položka **iSeries User Administration**.
  4. Pokud je služba **iSeries User Administration** uvedena, ale její stav nenaznačuje, že je spuštěna, klepněte pravým tlačítkem myši na **iSeries User Administration** a z nabídky vyberte **Start**.
  5. Pokud služba **iSeries User Administration** v seznamu uvedena není, nainstalujte ji takto:
    - a. Z nabídky **Start** vyberte **Run** a napište **command**. Otevře se okno s příkazovým řádkem.
    - b. Přejděte na jednotku C: (nebo jednotku s operačním systémem Windows).
    - c. Napište `%SystemRoot%\as400wsv\admin\qvnadaem/install` a stiskněte klávesu **Enter**.
    - d. Zavřete okno **Services**.
    - e. Znovu otevřete **Services**.
    - f. Jestliže jste službu **iSeries User Administration** dosud nespustili, klepněte na **Start**.

Obdržíte-li chybovou zprávu s informací, že nebyl nalezen řadič domény Windows, může to být proto, že se pokoušíte zapsat uživatele do pracovní skupiny Windows. V sítích Windows mohou být skupiny lokálních serverů volně sdruženy do pracovních skupin Windows. Jestliže například otevřete Místa v síti a klepnete na Okolní počítače, uvidíte seznam počítačů ve stejné pracovní skupině, ve které se nacházíte. V prostředí produktu iSeries Navigator to někdy vypadá, že můžete zapisovat uživatele systému i5/OS do pracovních skupin. Pokus o tento zápis ovšem vyvolá chybu. Pro pracovní skupiny Windows neexistuje žádný seznam uživatelů, jako je tomu u domény Windows.

## Problémy s oprávněním k zápisu uživatelů

Obdržíte-li chybovou zprávu NTA0282, která indikuje nedostatečné oprávnění k vytváření a aktualizaci uživatelů integrovaného serveru, proveďte příslušnou akci.

- Pokoušíte-li se zapsat uživatele a skupiny do domény poprvé, zkontrolujte, zda jste nastavili pro ID uživatele QAS400NT potřebná oprávnění. Postup je uveden v tématu “Uživatel QAS400NT” na stránce 175. Dále si ověřte,

zda je tento uživatel nakonfigurován jako tradiční uživatel, to znamená, že musí uvádět heslo pro systém iSeries a mít povolenu správu místních hesel. Další informace najdete v tématu “Typy uživatelských konfigurací” na stránce 51.

- Jestliže jste již uživatele úspěšně zapisovali, zkontrolujte, zda neskončila platnost hesla uživatele QAS400NT v operačním systému i5/OS. Při vypršení platnosti hesla uživatele QAS400NT skončí i platnost jeho účtu na integrovaném serveru. Při nápravě této situace postupujte takto:

1. Povolte tento účet na integrovaném serveru.

#### Na řadiči domény:

- a. Rozbalte **Start** —> **Programs** —> **Administrative Tools**.
- b. Vyberte **Active Directory Users and Computers**.
- c. Klepněte pravým tlačítkem myši na **Users** a potom dvakrát klepněte na uživatele **QAS400NT**.
- d. Klepněte na kartu **Account** nahoře v okně **User Properties**.
- e. Změňte datum v poli **Account expires** na nějaké datum v budoucnosti a klepněte na **Never**.

#### Na lokálním integrovaném Windows serveru:



- a. Otevřete **Start, Programs, Administrative Tools**.
  - b. Vyberte **Computer Management**.
  - c. Rozbalte **System Tools** a potom **Local Users and Groups**.
  - d. V seznamu klepněte pravým tlačítkem myši na uživatele **QAS400NT**.
  - e. Klepněte na kartu **Account** nahoře v okně **User Properties**.
  - f. Změňte datum v poli **Account expires** na nějaké datum v budoucnosti a klepněte na **Never**.
2. V operačním systému i5/OS použijte pro uživatele QAS400NT příkaz CHGUSRPRF (Změna uživatelského profilu) nebo CHGPWD (Změna hesla).
  3. Znovu spusíte službu iSeries User Administration Service.
    - a. Klepněte na **Start, Programs, Administrative Tools** a vyberte **Component Services**.
    - b. Klepněte na **Services**.
    - c. Klepněte na **iSeries User Administration**, potom klepnutím pravým tlačítkem myši na **Stop** službu zastavte.
    - d. Klepněte na **iSeries User Administration**, potom klepnutím pravým tlačítkem myši na **Start** službu spusíte.

Při restartu této služby se systém automaticky pokusí o zápis uživatelů a skupin.

Abyste se vyhnuli podobným problémům, nezapomínejte v operačním systému i5/OS pravidelně měnit heslo uživatele QAS400NT, aby nedošlo k ukončení jeho platnosti.

Máte-li více než jeden server iSeries s více integrovanými servery, které jsou součástí domény Windows, můžete minimalizovat problémy s ukončením platnosti hesla pomocí kroků uvedených v tématu “Uživatel QAS400NT” na stránce 175.

- Pokud problém přetrvává, podívejte se do databází technických informací na webových stránkách IBM

  iSeries Support  . Nenaleznete-li ani zde řešení, obraťte se na svého poskytovatele technické podpory.

## Problémy s heslem

Dříve se v heslech operačního systému Windows mohly používat všechny znaky, které byly povolené v heslech operačního systému i5/OS. Nyní operační systém i5/OS povoluje delší hesla a více znaků, než je tomu ve Windows. Chcete-li používat zápis uživatelů, měli byste v operačním systému i5/OS používat pouze hesla, jejichž délka i použité znaky vyhovují požadavkům na hesla Windows. Více informací o zabezpečení operačního systému na úrovni hesel

najdete v tématu Plánování změn na úrovni hesel v publikaci Zabezpečení iSeries - Referenční informace  .

Jestliže platnost hesla vyprší každý den vždy po jeho změně z integrovaného Windows serveru, znamená to, že jste zapomněli, že heslo je třeba změnit v operačním systému i5/OS. Změníte-li vy heslo operačního systému i5/OS, problém se vyřeší.





Jestliže se heslo v operačním systému i5/OS a heslo na Windows serveru neshoduje, zkuste pomocí následujících kroků zjistit, proč:

1. Zkontrolujte, zda je daný uživatel nakonfigurován jako uživatel Windows. Další informace najdete v tématu “Typy uživatelských konfigurací” na stránce 51.
  - a. Na příkazový řádek operačního systému i5/OS napište příkaz `WRKUSRPRF`.
  - b. Napište správný ID uživatele.
  - c. Podívejte se, jestli je atribut `LCLPWDGMT` (Local password management) nastaven na `*NO`. Pokud ano, je uživatel nakonfigurován tak, že má heslo v operačním systému i5/OS nastaveno na `*NONE` a heslo v operačním systému i5/OS a ve Windows nebude shodné.
2. Zkontrolujte, zda je operační systém i5/OS nastaven na uchovávání hesel:
  - a. Na příkazový řádek operačního systému i5/OS napište příkaz `WRKSYSVAL SYSVAL(QRETSVRSEC)`.
  - b. Do pole **Volba** zadejte volbu 2 a stiskněte klávesu **Enter**.
  - c. Ověřte si, že volba **Retain server security data** je nastavena na hodnotu 1. Pokud není, změňte ji na 1.
3. Na integrovaném Windows serveru zkontrolujte, zda je spuštěna služba pro administraci uživatelů **User Administration Service**. Další informace najdete v tématu “Problémy při zápisu uživatelů a skupin” na stránce 208.
4. Zjistěte si, která úroveň hesla je v operačním systému i5/OS podporována.
  - a. Na příkazový řádek operačního systému i5/OS napište příkaz `WRKSYSVAL SYSVAL(QPWLVL)`.
  - b. Do pole pro volbu zadejte hodnotu 5 a stiskněte klávesu **Enter**.

Úroveň hesla v operačním systému i5/OS může být nastavena tak, že jsou povolena hesla uživatelských profilů o délce 1 - 10 znaků nebo hesla o délce 1 - 128 znaků. Úroveň hesla 0 nebo 1 znamená že operační systém i5/OS podporuje hesla o délce 1 - 10 znaků a použitá znaková sada je limitovaná. Při úrovni 0 nebo 1 operační systém i5/OS konvertuje hesla pro Windows server na malá písmena. Úroveň hesla 2 nebo 3 znamená, že operační systém i5/OS podporuje hesla o délce 1 - 128 znaků a je povoleno více znaků včetně rozlišení malých a velkých písmen. Při úrovni 2 nebo 3 operační systém i5/OS zachová rozlišování velkých a malých písmen i pro Windows server. Změna úrovně hesla v operačním systému i5/OS se projeví až po IPL.

5. Zkontrolujte stav zápisu daného uživatele. Ujistěte se, že tento uživatel již neexistoval v prostředí Windows pod jiným heslem v okamžiku, kdy jste jej se pokoušeli zapsat (viz “Zápis jednoho uživatele operačního systému i5/OS do prostředí Windows pomocí produktu iSeries Navigator” na stránce 169). Pokud tento uživatel existoval pod jiným heslem, pokus o zápis selže. Nejprve změňte heslo ve Windows tak, aby se shodovalo s heslem v operačním systému i5/OS, a potom zápis opakujte.
6. Pokud problém stále přetrvává, podívejte se do databázi technických informací na webových stránkách

 IBM iSeries Support  . Nenaleznete-li ani zde řešení, obraťte se na svého poskytovatele technické podpory.

## Program typu snap-in IBM iSeries Integrated Server Support

Při pokusu spustit program typu snap-in IBM iSeries Integrated Server Support můžete zaznamenat chybu. Program se nespustí, podává neočekávané informace nebo se chyba objeví při jeho používání.

Jestliže se obrazovka programu typu snap-in IBM iSeries Integrated Server Support vůbec neobjeví, zkuste určit problém pomocí následujících kroků.

- Zjistěte, zda již v systému není spuštěna jiná instance programu typu snap-in IBM iSeries Integrated Server Support nebo programu `Lvlsync`. U těchto programů lze spouštět současně pouze jednu instanci. Je-li již spuštěna instance některého z těchto programů, nové volání tohoto programu se vrátí. Než spustíte novou instanci, musíte stávající program ukončit.
- Zkontrolujte, zda má uživatel přístup na úrovni administrátora a zvláštní oprávnění. Programy typu snap-in IBM iSeries Integrated Server Support tato oprávnění vyžadují. Zkuste spustit program s oprávněním administrátora.
- Přesvědčte se, že je spuštěn `iSeries NetServer`. `iSeries NetServer` se v operačním systému i5/OS spustí automaticky se spuštěním podsystému `QSERVER`. Pokud operační systém i5/OS dosud `iSeries NetServer` nespustil, spusťte jej.





- Zkontrolujte, zda je na serveru iSeries NetServer povolen uživatelský profil 'guest'. Pokud ne, povolte jej, aby se uživatelé typu 'guest' mohli pod tímto profilem připojovat k serveru iSeries NetServer (viz "Vytvoření uživatelského profilu 'guest' pro iSeries NetServer" na stránce 61). Po povolení přístupu typu 'guest' nejprve zastavte a potom restartujte iSeries NetServer. Poté zkuste spustit program typu snap-in IBM iSeries Integrated Server Support.
- Podívejte se, zda systémový protokol událostí na Windows serveru neobsahuje zprávy týkající se programu typu snap-in IBM iSeries Integrated Server Support.

Obrazovka programu typu snap-in IBM iSeries Integrated Server Support se objeví, ale informace, které operační systém i5/OS zobrazí, nejsou takové, jaké byste očekávali. V takovém případě zkuste určit problém pomocí níže uvedeného postupu:

- Ověřte si, že je v operačním systému i5/OS k dispozici nejnovější servisní balík PTF a že je v aktivním stavu. K tomu slouží příkaz DSPPTF (Zobrazení PTF).
- Zkontrolujte, zda je servisní balík, který jste dle vašeho přesvědčení nainstalovali, na integrovaném serveru skutečně nainstalován.
- Podívejte se, zda systémový nebo aplikační protokol událostí na integrovaném serveru neobsahuje zprávy týkající se programu typu snap-in Integrated Server Support.

Problém se může vyskytnout také při provádění některých akcí s programem typu snap-in IBM iSeries Integrated Server Support. Následující seznam vám pomůže při řešení problémů, které mohou nastat po klepnutí na tlačítko **OK**.

- Program typu snap-in IBM iSeries Integrated Server Support potřebuje k pokračování operace písmeno jednotky. Toto písmeno jednotky je třeba mít k dispozici pouze dočasně. Jsou-li všechna písmena využita, uvolněte některé z nich pro program typu snap-in IBM iSeries Integrated Server Support a opakujte akci.
- Program typu snap-in IBM iSeries Integrated Server Support provádí zadanou operaci. Systém může nebo nemusí být restartován podle toho, jaké sady souborů se aktualizují. Než dojde k zastavení a novému spuštění, může to nějakou dobu trvat.
- Podívejte se, zda systémový nebo aplikační protokol událostí na integrovaném serveru neobsahuje zprávy týkající se programu typu snap-in IBM iSeries Integrated Server Support.
- Pokud problém stále přetrvává, podívejte se do databází technických informací na webových stránkách

 IBM iSeries Support  . Nenaleznete-li ani zde řešení, obraťte se na svého poskytovatele technické podpory.

## Problémy se servery připojenými pomocí iSCSI

- | Jestliže zaznamenáte jeden z níže uvedených problémů, můžete začít z odstraňováním problémů pomocí uvedených akcí. Tento seznam není vyčerpávající, takže některé problémy mohou vyžadovat zásahy, které zde nejsou uvedené.
- | Pokud chcete získat další informace, které by vám pomohly s odstraňováním problémů, podívejte se na téma "Kontrola zpráv a protokolů úloh" na stránce 197.

### Inicializace konfigurace servisního procesoru selhala

- | Jestliže se ve frontě zpráv systémového operátora (QSYSOPR) nebo v protokolu úlohy pro dávkovou úlohu nebo zúčastněného interaktivního uživatele objeví zprávy CPDC4xx nebo CPFC4xx, prostudujte si téma "Odstraňování problémů s produktem IBM Director" na stránce 215.

### Při instalaci nebo spuštění serveru zůstane stav NWSO logicky vypnutý (VARIED OFF)


- | • Zajistěte, aby všechny požadované adaptéry NWSH nakonfigurované pro server byly před instalací nebo spuštěním serveru logicky zapnuté. Jestliže se adaptér NWSH logicky nezapne, zkontrolujte zprávy ve frontě zpráv zařízení hostitele.
- | • Jestliže se ve frontě zpráv systémového operátora (QSYSOPR) nebo v protokolu úlohy pro dávkovou úlohu nebo zúčastněného interaktivního uživatele objeví zprávy CPDC4xx nebo CPFC4xx, prostudujte si téma "Odstraňování problémů s produktem IBM Director" na stránce 215.

## | **Pokud je hostovaný systém zapnutý, server se nespustí**

| Další informace najdete v tématu “Problémy sdílení hardwaru hostovaného systému” na stránce 206.

## | **Na konzoli hostovaného systému se zobrazuje zpráva “No iSCSI devices found” nebo výzva k zavedení diskety**


| • Adaptér iSCSI HBA konfigurovaný pro zavedení systému do hostovaného systému nebyl schopen tuto akci provést.

| • Může se jednat o problém s konfigurací iSCSI. Informace najdete v tématu iSCSI Troubleshooting   
| ([www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/troubleshooting.html](http://www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/troubleshooting.html)).

| • Pokud se v protokolu PAL vyskytuje zpráva CPPC056, je velice pravděpodobný problém s konfigurací CHAP.

| • Může existovat problém se sítí mezi iSCSI HBA hostovaného systému, který je nakonfigurovaný pro zavádění  
| systému, a mezi HBA serveru iSeries, který odpovídá cestě nakonfigurované pro paměťový prostor systémové  
| jednotky NWSA. Další informace najdete v tématu “Síťová analýza cesty pro zavedení systému a cesty  
| k paměťovým prostorům” na stránce 214.

## | **Stav NWSA je logicky zapnutý (VARIED ON), ale operační systém Windows se nezačíná zavádět**

| • Může se jednat o problém s konfigurací iSCSI. Informace najdete v tématu iSCSI Troubleshooting   
| ([www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/troubleshooting.html](http://www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/troubleshooting.html)).

| • Pokud se v protokolu PAL vyskytuje zpráva CPPC056, je velice pravděpodobný problém s konfigurací CHAP.

| • Může existovat problém se sítí mezi iSCSI HBA hostovaného systému, který je nakonfigurovaný pro zavádění  
| systému, a mezi HBA serveru iSeries, který odpovídá cestě nakonfigurované pro paměťový prostor systémové  
| jednotky NWSA. Další informace najdete v tématu “Síťová analýza cesty pro zavedení systému a cesty  
| k paměťovým prostorům” na stránce 214.

## | **Stav NWSA je DEGRADED**

| Zajistěte, aby všechny požadované adaptéry NWSH nakonfigurované pro server byly logicky zapnuté. Jestliže se  
| adaptér NWSH logicky nezapne, zkontrolujte zprávy ve frontě zpráv zařízení hostitele.

## | **Paměť používající cestu jinou než cestu pro zavedení systému se ve Windows nezobrazuje**

| • Může se vyskytovat problém mezi hostovaným systémem a iSCSI HBA na serveru iSeries, který odpovídá jiné  
| cestě než cestě pro zavádění systému. Další informace najdete v tématu “Síťová analýza cesty pro zavedení systému  
| a cesty k paměťovým prostorům” na stránce 214.


| • Pokud se v protokolu PAL vyskytuje zpráva CPPC056, jedná se o problém s protokolem CHAP. S nejvyšší  
| pravděpodobností se jedná o problém s digitálními certifikáty, když prostředí Windows na serveru iSeries potřebuje  
| provést zabezpečený přenos vlastních důvěrných dat mezi operačním systémem i5/OS a Windows. Další informace  
| najdete v tématu “Správa certifikátů cest” na stránce 214.

## | **Paměť používající cestu jinou než cestu pro zavedení systému se někdy ve Windows zobrazuje pozdě**

| • To je běžné při prvním spuštění serveru, když jste provedli určité změny v informacích konfigurace operačního  
| systému i5/OS, jako například v informacích o lokálním rozhraní SCSI v adaptéru NWSH nebo v informacích  
| CHAP v konfiguraci vzdáleného systému.

| • Je to normální i tehdy, pokud iSCSI HBA v hostovaném systému nebyl s tímto konkrétním popisem NWSA dříve  
| používán. Tento případ nastává, když je iSCSI HBA v hostovaném systému nahrazen nebo pokud se použije jiný  
| hostovaný systém jako rezervní server pro výměnu za chodu.

| • Pokud vaše aplikace zahrnuje automaticky spouštěná zařízení, která jsou odpovídají výše uvedeným situacím,

| podívejte se na webovou stránku Advanced iSCSI tasks   
| ([www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/advancedtasks.html](http://www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme/advancedtasks.html)).


## | **Zápis uživatelů nebo zadání vzdáleného příkazu selhává se zprávou NTA02BB, NTA028A, NTA028B**

- Jedná se o problém s digitálními certifikáty, když prostředí Windows na serveru iSeries potřebuje provést zabezpečený přenos vlastních důvěrných dat mezi operačním systémem i5/OS a Windows. Další informace najdete v tématu “Správa certifikátů cest”.
- V případě zpráv NTA028A a NTA028B zajistěte, aby se datum a čas v hostovaném systému výrazně nelišil od data a času na serveru iSeries, jelikož to může způsobit, že se digitální certifikáty jeví jako neplatné.

## Síťová analýza cesty pro zavedení systému a cesty k paměťovým prostorům

Další informace o těchto krocích a dodatečných procedurách odstraňování problémů najdete v tématu iSCSI

Troubleshooting  ([www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme/troubleshooting.html](http://www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme/troubleshooting.html)).

- V hostovaném systému použijte obslužný program CTRL-Q k tomu, aby zobrazil adresy iSCSI HBA MAC pro hostovaný systém. Ujistěte se, že tyto adresy odpovídají hodnotám adresy adaptéru rozhraní SCSI v konfiguraci vzdáleného serveru v operačním systému i5/OS. Tento krok je možné přeskočit, pokud jste se sem dostali kvůli selhání manuálně konfigurovaného zavedení systému.
- Pomocí obslužného programu CTRL-Q nebo zobrazení ovladače SCSI v produktu Device Manager otestujte spojení příkazem PING spuštěným na IP adresu SCSI příslušného iSCSI HBA ze serveru iSeries.
- Pokud příkaz PING selže, proveďte tyto kroky:
  - Zajistěte, aby byla fyzická síť řádně propojena a aby zařízení v síti, jako například přepínače, byly funkční.
  - Zajistěte, aby byly splněny požadavky definované v tématu “Síť iSCSI” na stránce 28.
  - Pokud je zahrnut firewall nebo podobná funkce pro filtrování paketů, zajistěte, aby tento firewall umožňoval průchod paketů ICMP (Internet Control Message Protocol). Na rozdíl od IP adres SCSI mohou být IP adresy LAN ovlivňovány softwarem firewallu, který je provozován ve Windows.
  - Jestliže váš NWSO používá pravidla zabezpečení IP (IPSec) jiná než \*NONE, podívejte se na téma iSCSI Troubleshooting  ([www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme/troubleshooting.html](http://www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme/troubleshooting.html)).
- Pokud se příkaz ping provede úspěšně, postupujte takto:
  - Je-li zahrnut firewall nebo podobná funkce pro filtrování paketů, prostudujte si téma “Konfigurace firewallu” na stránce 126. Na rozdíl od IP adres SCSI mohou být IP adresy LAN ovlivňovány softwarem firewallu, který je provozován ve Windows.
  - Jestliže zavedení DHCP selže a pokud je směrovaná síť komplikovaná, zajistěte, aby v síti existoval příslušným způsobem nakonfigurovaný agent přenosu DHCP (rovněž známý jako BOOTP relay boot).

## Správa certifikátů cest

**Poznámka:** Tato část se týká pouze systémů připojených pomocí iSCSI.

Prostředí Windows na serveru iSeries obvykle automaticky generuje digitální certifikáty, pokud potřebuje zabezpečený přenos vlastních důvěrných dat mezi operačními systémy i5/OS a Windows. Těmto digitálním certifikátům se říká certifikáty cest. Pokud máte podezření, že se jedná o problém s certifikátem cesty, můžete provést tyto akce:

- Ujistěte se, že je nainstalovaný produkt 5722-SS1, volba 34 (Digital Certificate Manager).
- Zajistěte, aby operační systémy i5/OS a Windows měly kompatibilní digitální certifikáty tím, že se při spuštění systému budou generovat nové certifikáty. To by se mělo provádět pouze v neobvyklých situacích, například tehdy, když je stará verze paměťového prostoru pro systémovou jednotku Windows obnovována, aniž by byla obnovena odpovídající paměť certifikátů systému i5/OS. Chcete-li generovat nové certifikáty cest pomocí produktu iSeries Navigator, postupujte takto:
  1. Rozbalte **Administrace integrovaných serverů**.
  2. Rozbalte **Servery**.
  3. Klepněte pravým tlačítkem myši na server v zobrazeném seznamu.
  4. Vyberte **Začněte volbami...**
  5. Zaškrtněte volbu **Regenerovat certifikáty cest**.
  6. Klepněte na **Start**.

l Jestliže chcete použít CL příkaz, podívejte se na klíčové slovo GENPTHCERT (Generování certifikátu cesty) příkazu VRYCFG (Logické zapnutí/vypnutí konfigurace).

## l **Odstraňování problémů s produktem IBM Director**

l **Poznámka:** Tato část se týká pouze systémů připojených pomocí iSCSI.

l Pokud se nemůžete připojit k produktu IBM Director (například při spouštění nebo ukončování práce systému) postupujte takto:

- l • Počkejte pět minut a zkuste provést operaci znovu.
- l • Zastavte a restartujte produkt IBM Director.
  - l – Na příkazový řádek operačního systému i5/OS zadejte příkaz `ENDTCPSVR SERVER(*DIRECTOR)`.
  - l – Zastavení serveru bude trvat několik minut, případně delší dobu. Stav procesu zastavování můžete získat spuštěním tohoto příkazu z překladače qsh: `/qibm/userdata/director/bin/twgstat`. Po několika minutách bude konečně zobrazen neaktivní stav - “inactive”.
  - l – Spusťte překladač qsh zadáním příkazu `qsh` na příkazový řádek operačního systému i5/OS.
  - l – Z překladače qsh spusťte: `/qibm/userdata/director/bin/twgstart`
- l • Ověřte soubor vlastností konfigurace produktu IBM Director.

Soubor vlastností produktu IBM Director se instaluje během instalace produktu IBM Director do umístění `/QIBM/ProdData/Director/classes/com/ibm/sysmg/app/iide/IIDETask.properties`.

Ověřte, že soubor vlastností produktu IBM Director existuje. Pokud neexistuje, přeinstalujte produkt IBM Director nebo se obraťte na servisního zástupce.
- l • Ověřte, že port v souboru vlastností produktu IBM Director je uveden port.

Tento soubor by měl také obsahovat řádek, na kterém je uvedeno “port = **xxxxx**”, kde **xxxxx** je číslo portu. Jestliže tento řádek neexistuje, postupujte takto:

  - l 1. Upravte soubor a přidejte řádek, který bude obsahovat “port = 5779”. 5779 je předvolený port používaný pro připojení i5/OS k produktu IBM Director.
  - l 2. Restartujte produkt IBM Director.
- l • Ověřte, že port používaný produktem IBM Director není používán jinou aplikací.

Po spuštění produktu IBM Director ověřte, že port uvedený v souboru vlastností produktu IBM Director nepoužívá jiná aplikace.

  - l 1. V prostředí produktu iSeries Navigator rozbalte **Síť**—>**Konfigurace TCP/IP**—>**IPv4**—>**Připojení**.
  - l 2. Klepněte pravým tlačítkem myši na záznam, který má ve sloupci **Lokální port** stejné číslo jako číslo portu uvedené v souboru vlastností produktu IBM Director, a vyberte **Úlohy**.
  - l 3. V seznamu úloh vyhledejte úlohu se jménem **Qcpmgtsvr** a uživatele **Qcpmgtdir**. To by měla být jediná úloha, která používá uvedený port.

Pokud tento port používají ještě jiné úlohy, musíte změnit port používaný produktem IBM Director. Provedete to takto:

  - l 1. V souboru vlastností produktu IBM Director změňte číslo portu uvedené v řádku “port = **xxxxx**”, kde **xxxxx** je číslo portu.
  - l 2. Restartujte produkt IBM Director.

l **Problémy zjišťování:** Jestliže je zaprotokolována zpráva, která indikuje, že vzdálený server nebo kryt nebyl nalezen, potom rozhraní produktu IBM Director nebude schopné v síti nalézt cílový servisní procesor. Další informace najdete v tématu “Zjišťování vzdálených serverů a jejich správa” na stránce 134.

l Pokud používáte servisní procesor Remote Supervisor II, ověřte, že používáte nejnovější firmware. Viz dokument

l iSCSI install read me first 

l ([www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme](http://www.ibm.com/servers/eserver/series/integratedxseries/iscsireadme))

**Pokud nepoužíváte ke zjištění servisního procesoru adresování typu unicast, proveďte tyto kroky:**

- Ověřte, že váš server iSeries má fyzické síťové připojení k servisnímu procesoru ve vzdáleném systému.
  - Viz téma Testování spojení z prostředí produktu iSeries Navigator v kolekci témat Odstraňování problémů s TCP/IP.
- Pokud server iSeries má fyzické síťové připojení k servisnímu procesoru, zkontrolujte v nastavení firewallu směrovače nebo přepínače sítě typu iSCSI. Síťové směrovače nebo přepínače mezi rozhraním iSeries LAN a servisním procesorem možná nepodporují adresování typu multicast nebo nejsou nakonfigurovány tak, aby toto adresování umožňovaly.

Síťové směrovače nebo firewally mohou blokovat pakety typu SLP multicast. Směrovače nebo firewally možná bude nutné nakonfigurovat tak, aby umožňovaly IP adresu typu SLP (Service Location Protocol) o hodnotě 239.255.255.253 nebo číslo portu 427, aby se umožnil průchod paketů typu SLP.
- Nakonfigurujte svůj servisní procesor tak, aby podporoval adresování typu unicast.

Servisní procesor musí mít nakonfigurované statické jméno hostitele nebo IP adresu. To je možné provést pomocí obslužného programu BIOS pro adaptér RSA II nebo prostřednictvím webového rozhraní servisního procesoru. Pokyny, týkající se způsobu použití webového rozhraní servisního procesoru ke konfiguraci servisního procesoru, najdete v tématu “Použití webového rozhraní modulu Management Module a adaptéru RSA II” na stránce 139.

Změňte konfiguraci servisního procesoru tak, aby se k připojení k servisnímu procesoru používalo adresování typu unicast, které využívá jméno hostitele nebo IP adresu, které byly nastaveny pro servisní procesor výše uvedeným postupem. Další informace najdete v tématu “Změna vlastností konfigurace servisního procesoru” na stránce 120.

**Pokud používáte ke zjištění servisního procesoru adresování typu unicast, proveďte tyto kroky:**

- Ověřte, zda jsou jak IP adresa, tak jméno hostitele vašeho servisního procesoru správně nakonfigurovány na servisním procesoru vzdáleného systému a v konfiguraci servisního procesoru v operačním systému i5/OS.
- Obecné procedury pro odstraňování problémů s TCP/IP uvádí téma Odstraňování problémů s TCP/IP.

**Problémy s připojeními typu SSL:** Jestliže je k servisnímu procesoru nakonfigurováno připojení typu SSL (Secure Socket Layer), může dojít k řadě různých problémů. Viz téma “Konfigurace zabezpečení SSL servisního procesoru” na stránce 125.

**Certifikát není importován do správné paměti certifikátů operačního systému i5/OS**

Pokud používáte manuální režim zabezpečení, ověřte, že kořenový vydavatel certifikátů (CA) servisního procesoru je v paměti certifikátů iSeries \*SYSTEM.

1. Připojte se k webovému rozhraní servisního procesoru.
2. Zobrazte certifikát. Poznamenejte si vydavatele certifikátů v poli certifikátu “Issued by”.
3. Připojte se k rozhraní iSeries Digital Certificate Manager (DCM), abyste určili, zda je vydavatel certifikátu (CA) uveden jako certifikát v paměti certifikátů \*SYSTEM.
  - a. Určete kořenového vydavatele certifikátů (CA) pro certifikát, který byl instalován na servisním procesoru.
    - 1) Připojte se k webovému rozhraní servisního procesoru pomocí webového prohlížeče na adrese <http://hostname> (kde *hostname* je jméno hostitele servisního procesoru) nebo na adrese <http://ipaddress> (kde *ipaddress* je IP adresa servisního procesoru).
    - 2) Řiďte se pokyny nápovědy vašeho prohlížeče a prohlédněte si certifikát zabezpečení, který ověřoval identitu webového serveru.
    - 3) Řiďte se pokyny nápovědy vašeho prohlížeče a prohlédněte si hierarchii certifikátů.
    - 4) Nejvyšší záznam v hierarchii bude kořenový certifikát vydavatele certifikátů (CA).
    - 5) Poznamenejte si jméno, které je uvedené pro kořenový certifikát vydavatele certifikátů (CA), abyste je mohli použít v dalším kroku.
  - b. Připojte se k rozhraní iSeries Digital Certificate Manager (DCM). Informace naleznete pod heslem Start DCM v tématu Digital Certificate Manager.
  - c. Klepněte na **Select Certificate Store**.
  - d. Vyberte **\*SYSTEM** a klepněte na **Continue**.



- e. Zadejte heslo paměti certifikátů pro paměť certifikátů \*SYSTEM.
- f. V levém okně klepněte na **Fast Path**.
- g. Vyberte **Work with CA certificates** a klepněte na **Continue**.
- h. Na stránce **Work with CA Certificates** vyhledejte záznam v poli Certificate Authority (CA), který odpovídá jménu kořenového certifikátu vydavatele certifikátů (CA), které jste určili v kroku a).
- i. Jestliže je v poli **Status** pro tento záznam uvedeno **Enabled**, potom je vydavatel certifikátu (CA) nakonfigurován správně.
- j. Pokud je v poli **Status** pro tento záznam uvedeno **Disabled**, potom jej musíte následujícím postupem povolit:
  - 1) Vyberte rádiové tlačítko nalevo od záznamu Certificate Authority (CA), který má být povolen.
  - 2) Vyberte tlačítko Enable v dolní části tabulky.
  - 3) Vydavatel certifikátu (CA) je nyní správně nakonfigurován.
- k. Pokud v poli Certificate Authority (CA) není žádný záznam, který by se shodoval se jménem kořenového certifikátu vydavatele certifikátů (CA), jež bylo určeno v kroku a), přidejte vydavatele certifikátu (CA) tímto postupem:
  - 1) Podívejte se na původní e-mailový dopis, který jste dostali od vydavatele certifikátu (CA). Tento dopis by měl obsahovat certifikát (který byl importován do servisního procesoru) a související certifikát z důvěryhodného zdroje.
  - 2) Pomocí FTP pošlete tento certifikát z důvěryhodného zdroje do adresáře v systému souborů IFS na serveru iSeries a poznamenejte si úplnou cestu a celé jméno souboru.
  - 3) V levém okně vyberte **Manage Certificates**, aby se zobrazil seznam úloh.
  - 4) Ze seznamu úloh vyberte **Import certificate**.
  - 5) Označte jako typ certifikátu **Certificate Authority (CA)** a klepněte na **Continue**.
  - 6) Zadejte plně kvalifikovanou cestu a jméno souboru pro soubor certifikátu vydavatele certifikátů (CA) a klepněte na **Continue**. Zobrazí se zpráva, která bude buď potvrzovat, že importovací proces proběhl úspěšně, nebo bude obsahovat informaci o chybě, pokud tento proces selhal.
  - 7) Vydavatel certifikátu (CA) je nyní správně nakonfigurován.

### Konfigurace servisního procesoru není inicializována

Pokud používáte automatický režim zabezpečení, musí být konfigurace servisního procesoru inicializována až po nakonfigurování automatického režimu zabezpečení.

Proveďte tyto kroky:

- Pokud je servisní procesor vzdáleného systému inicializován poprvé, postupujte podle procedury popsané v tématu “Inicializace servisního procesoru” na stránce 120 a proveďte inicializaci nového servisního procesoru.
- Jestliže byl servisní procesor vzdáleného systému inicializován již dříve, potom se řiďte postupem popsáním v tématu “Inicializace servisního procesoru” na stránce 120 a v konfiguraci servisního procesoru proveďte synchronizaci uživatele, hesla a certifikátu ze servisního procesoru vzdáleného systému.

### Identifikátor certifikátu servisního procesoru není rozpoznán

Pokud používáte manuální zabezpečení, ověřte, zda pole certifikátu servisního procesoru odpovídá identifikátoru certifikátu servisního procesoru v konfiguraci servisního procesoru.

1. Zobrazte konfiguraci servisního procesoru (viz “Zobrazení vlastností konfigurace servisního procesoru” na stránce 119) a klepněte na kartu **Security**. Poznamenejte si hodnoty pro komponentu identifikátoru certifikátu servisního procesoru a hodnoty porovnejte: Hodnoty komponenty se mapují na pole certifikátu tímto způsobem:
  - Common name – Issued to (Subject) Common Name (CN)
  - E-mail address – Issued to (Subject) (E)
  - Organizational unit – Issued to (Subject) Organizational Unit (OU)
2. Přistupte k webovému rozhraní servisního procesoru.



- | 3. Zobrazte certifikát zabezpečení servisního procesoru.
- | 4. Porovnejte hodnoty certifikátu se srovnatelnými hodnotami uvedenými v konfiguraci servisního procesoru.
- | 5. Jestliže se tyto hodnoty neshodují, zadejte správnou hodnotu pomocí metody popsané v tématu “Změna vlastností konfigurace servisního procesoru” na stránce 120. Potom si přečtete téma “Inicializace servisního procesoru” na stránce 120, kde získáte informace o tom, jak synchronizovat certifikát ze servisního procesoru vzdáleného systému s konfigurací servisního procesoru.

| **Poznámka:** V konfiguraci servisního procesoru můžete zadat, že nechcete používat certifikát servisního procesoru.

#### | **Servisní procesor nepodporuje SSL.**

- | • Pokud nepožadujete zabezpečené připojení, přečtete si téma “Změna vlastností konfigurace servisního procesoru” na stránce 120. Na kartě **Security** vyberte volbu **Do not use a certificate (requires physical security)** s uložte změny.
- | • Ověřte, že váš servisní procesor podporuje SSL.
  - | 1. Další informace najdete v tématu “Zjišťování vzdálených serverů a servisních procesorů” na stránce 135.
  - | 2. Pokud je váš servisní procesor schopen SSL, požádejte servisního zástupce, aby určil, zda je pro přidání podpory SSL nezbytná aktualizace firmwaru nebo hardwaru.

#### | **Problémy virtuální sítě Ethernet se servery připojenými pomocí iSCSI**

| Chcete-li si prohlédnout informace o dostupných připojení v zásobníku Windows TCP/IP, zadejte na příkazový řádek Windows příkaz **ipconfig /all**. Měly by se zobrazit informace o těchto položkách:

- | • externí síťové adaptéry
- | • rozhraní LAN pro porty adaptérů iSCSI HBA
- | • virtuální adaptéry Ethernet pro váš server iSeries

| Porovnejte výsledky příkazu ipconfig s jedním z níže uvedených případů odstraňování problémů a proveďte akce, které jsou pro uvedený případ navrženy, dokud se problém nevyřeší.

#### | **V příkazu ipconfig chybí nakonfigurovaná IP adresa LAN**

| Jedná se o případ, kdy se internetová adresa pro rozhraní LAN ve vzdálené konfiguraci i5/OS neshoduje s IP adresou, která je uvedena v příkazu ipconfig pro libovolný adaptér iSCSI HBA. Informace o zobrazení konfigurace vzdáleného systému najdete v tématu “Zobrazení vlastností konfigurace vzdáleného systému” na stránce 117.

- | • Prověřte výsledky příkazu ipconfig a vyhledejte fyzické adresy (adresy MAC) adaptérů iSCSI HBA. Pokud se fyzická adresa zobrazená příkazem ipconfig liší od adresy adaptéru pro rozhraní LAN v konfiguraci vzdáleného systému i5/OS, postupujte takto:
  - | 1. Z konzole Windows ukončete práci systému.
  - | 2. Z operačního systému i5/OS logicky vypněte NWSD. Další informace najdete v tématu “Spuštění a zastavení integrovaného serveru” na stránce 141.
  - | 3. V konfiguraci vzdáleného systému změňte adresu adaptéru pro rozhraní LAN.
  - | 4. Pomocí operačního systému i5/OS spusíte (logicky zapnete) NWSD. Další informace najdete v tématu “Spuštění a zastavení integrovaného serveru” na stránce 141.
- | • Otevřete **Control Panel**, potom **Administrative Tools** a nakonec **Services**. Ujistěte se, že **iSeries Shutdown Manager** je uveden v seznamu služeb a je ve stavu **Started**. Tato služba automaticky přiřadí informaci rozhraní LAN IP z konfigurace vzdáleného systému i5/OS portům, které mají konfigurované adresy MAC.
- | • Ve Windows vyhledejte v protokolu **Application event log** události, jejichž zdrojem je služba **iSeries Shutdown Manager**.
- | • Zavřete všechna okna s vlastnostmi sítě (Network properties), které mají karty **General**, **Authentication** a **Advanced**, jelikož tento typ oken zamyká prostředky požadované pro přiřazení IP adresy. Po zavření těchto typů oken počkejte 30 sekund, aby mohla služba iSeries Shutdown Manager přiřadit chybějící IP adresy a zadejte znovu příkaz **ipconfig /all**.

- Jestliže žádný z výsledků příkazu ipconfig nepopisuje instalovaný adaptér iSCSI HBA, otevřete ve Windows službu Device Manager a ujistěte se, že je nainstalován a povolen ovladač sítě pro iSCSI HBA. Pokud je u ovladače žlutý '!' nebo je ovladač zobrazen šedě, vyhledejte ve Windows v protokolu systémových událostí události se zdrojem QL40xx a ujistěte se, že adaptér iSCSI HBA není zablokovaný nastavovacím menu systému BIOS.

#### l **Příkaz ipconfig zobrazuje nakonfigurované připojení iSCSI HBA ve stavu "media disconnected"**

l Jedná se o situaci, kdy příkaz ipconfig zobrazuje připojení iSCSI HBA, které je ve stavu "media disconnected" a má fyzickou adresu, která se shoduje s adresou adaptéru v konfiguraci vzdáleného systému i5/OS.

- Zajistěte, aby byla fyzická síť řádně připojena a aby zařízení v síti, jako například přepínače, byly na fyzické lince k iSCSI HBA hostovaného systému funkční.

#### l **Příkaz ipconfig zobrazuje připojení "IBM iSeries Virtual Ethernet" ve stavu "media disconnected"**

l • Virtuální síť Ethernet vyžaduje fungující síť iSCSI, takže problémy týkající se adaptéru iSCSI HBA musí být vyřešeny nejdříve. Předtím, než budete pokračovat, se ujistěte, že program ipconfig zobrazuje adresy LAN v konfiguraci vzdáleného systému i5/OS.

l • Zajistěte, aby byla fyzická síť řádně připojena a aby zařízení v síti, jako například přepínače, byly na fyzické lince k iSCSI HBA hostovaného systému funkční.

l • Zajistěte, aby byly splněny požadavky definované v tématu "Síť iSCSI" na stránce 28.

l • Otevřete **Control Panel**, potom **Administrative Tools** a nakonec **Services**. Ujistěte se, že **iSeries Manager**, **iSeries Shutdown Manager** a **iSeries Virtual Ethernet Manager** jsou uvedeny v seznamu služeb a jsou ve stavu **Started**.

l • Ve Windows vyhledejte v protokolu **Application event log** události, jejich zdrojem je služba **iSeries Virtual Ethernet Manager**.

l • Pokud je zahrnut firewall nebo podobná funkce pro filtrování paketů, prostudujte si téma "Konfigurace firewallu" na stránce 126. Rozhraní LAN IP v konfiguraci vzdáleného systému i5/OS mohla být ovlivněna softwarem firewallu, který je provozován ve Windows.

l • Jestliže váš NWSD používá pravidla zabezpečení IP (IPSec) jiná než \*NONE, podívejte se na webovou stránku

l iSCSI troubleshooting 

l ([www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme/troubleshooting.html](http://www.ibm.com/servers/eserver/iseries/integratedxseries/iscsireadme/troubleshooting.html)).

#### l **Příkaz ipconfig zobrazuje připojení "IBM iSeries Virtual Ethernet" s nesprávnou IP adresou**

l • Manuálně konfiguruje tuto IP adresu ve Windows. U dvoubodové virtuální sítě Ethernet najdete informace v tématu "Konflikty IP adres ve dvoubodové virtuální síti Ethernet" na stránce 226. V případě ostatních virtuálních sítí Ethernet použijte pouze kroky 1 až 5 uvedené procedury.

#### l **V operačním systému i5/OS je nakonfigurována 'virtuální síť x Ethernet', ale v programu ipconfig chybí informace týkající se 'IBM iSeries Virtual Ethernet x'**

l • V operačním systému i5/OS ověřte, že pro virtuální síť Ethernet, která vás zajímá, existuje popis linky. U dvoubodové virtuální sítě Ethernet najdete informace v tématu "Prozkoumání dvoubodových virtuálních sítí Ethernet" na stránce 109.

l • Otevřete **Control Panel**, potom **Administrative Tools** a nakonec **Services**. Ujistěte se, že **iSeries Virtual Ethernet Manager** je uveden v seznamu služeb a je ve stavu **Started**. Tato služba automaticky vytváří a odstraňuje virtuální adaptéry Ethernet serveru IBM iSeries tak, aby se shodovaly s konfigurací popisu linky v operačním systému i5/OS.

l • Zajistěte, aby byl systém nastaven tak, aby neblokoval instalaci nepřirazených ovladačů. Podrobnosti uvádí krok 1 až v tématu "Zahájení instalace nebo aktualizace ovladače LAN" na stránce 224. Pokud změníte nastavení hodnoty **Block**, restartujte službu **iSeries Virtual Ethernet Manager**, potom počkejte 30 sekund a zadejte příkaz **ipconfig /all** znovu.

l • Ve Windows otevřete **Device Manager** a ujistěte se, že je ovladač sítě pro virtuální síť Ethernet serveru IBM iSeries, který vás zajímá, instalován a povolen. Pokud je u ovladače žlutý '!', vyhledejte v **protokolu systémových událostí** ve Windows události se zdrojem **Qvndvimp**.

## | Výsledek programu ipconfig vypadá dobře, ale velké přenosy dat selhávají

- | • Ujistěte se, že virtuální adaptéry Ethernet serveru IBM iSeries a strana 'LAN' portů iSCSI HBA nejsou konfigurovány pro použití větší maximální přenosové jednotky, než podporuje síť typu iSCSI. Například ne všechny přepínače podporují jumbo rámce o velikosti 9000 bajtů. Zkontrolujte specifikace vybavení vaší sítě. Další informace najdete v tématu "Posouzení velikosti maximální přenosové jednotky (MTU)" na stránce 131.

## Problémy virtuální sítě Ethernet se servery připojenými pomocí IXS a IXA

Pro účely této části jsou dvoubodová lokální virtuální síť Ethernet a porty virtuální sítě Ethernet 0-9 považovány za virtuální adaptéry Ethernet nebo porty virtuální sítě Ethernet.

Existují dva druhy ovladačů virtuálních zařízení typu Ethernet. Jedná se o virtuální adaptér Ethernet (VE) a datový přenos typu Ethernet (DT).

- Adaptér virtuální sítě Ethernet odpovídá ovladači, který se jeví jako "virtuální" adaptér, protože s ním není asociován žádný hardware.
- Datový přenos typu Ethernet je ovladač, který poskytuje spojení se systémovou sběrnici, která propojuje všechny virtuální sítě Ethernet.

Když port virtuální sítě Ethernet nemůže komunikovat přes systémovou sběrnici, systém hlásí, že je odpojen kabel pro tento port. To je důležitý bod pro odstraňování chyb virtuální sítě Ethernet.

Porty virtuální sítě Ethernet pod Windows se automaticky instalují a odebírají pomocí obslužného programu pro virtuální síť Ethernet (VEU). Tento program dostává prostřednictvím konfiguračního souboru signály z NWSA. Když například uživatel vytvoří pro určitý port virtuální sítě Ethernet pod NWSA popis linky, VEU nainstaluje odpovídající port virtuální sítě Ethernet. Při novém spuštění Windows serveru se nakonfiguruje i adresa portu virtuální sítě Ethernet.

Následující virtuální komponenty typu Ethernet používají uvedené ovladače.

- virtuální adaptér Ethernet: qvndvemp.sys
- virtuální datový přenos typu Ethernet: qvndvedt.sys
- obslužný program virtuální sítě Ethernet: qvndveu.exe

Odstraňování problémů s virtuální sítí Ethernet

Nefunguje-li komunikace mezi porty virtuální sítě Ethernet, je potřeba při řešení problému provést následující dva úkoly.

1. Zjistit stav portů virtuální sítě Ethernet.
2. Porovnat získané výsledky s následujícími případy, které mohou nastat při řešení problémů.

### Zjištění stavu portu virtuální sítě Ethernet

Jak zjistit stav portů virtuální sítě Ethernet:

- Z konzole iSeries určete, zda je pod NWSA vytvořen popis linky pro port virtuální sítě Ethernet.
- Z konzole operačního systému Windows otevřete složku **Network and Dial Up Connections** a zjistěte, zda je zobrazena ikona portu virtuální sítě Ethernet.

### Porovnání stavu portu se vzorovými případy při odstraňování problémů

Porovnejte zjištěné stavy portů virtuální sítě Ethernet s některým z následujících případů, které mohou nastat při odstraňování problémů.

- "Existuje popis linky i ikona" na stránce 221.
- "Existuje popis linky, ale chybí ikona" na stránce 221.
- "Popis linky chybí, ale ikona existuje" na stránce 222.

- “Chybí popis linky i ikona” na stránce 222.

V každém případě je třeba nejprve prověřit problém ze strany operačního systému i5/OS, a potom ze strany Windows. Při zkoumání ze strany Windows je třeba otevřít protokol událostí (Event Log) a nástroj Device Manager.

- Chcete-li otevřít protokol událostí ve Windows, rozbalte nabídku **Start**, vyberte **Programs**, potom **Administrative Tools** a nakonec **Event Viewer**.
- Správce úloh (Device Manager) otevřete tak, že rozbalíte nabídku **Start**, vyberete **Settings**, potom **Control Panel**, potom **Administrative Tools**, potom **Computer Management** a nakonec **Device Manager**.

## Existuje popis linky i ikona

### Prověření problému ze strany i5/OS

Zkontrolujte popis linky. Je-li popis linky ve stavu FAIL (selhání), proveďte tyto kroky:

1. Shromážděte záznamy protokolu PAL a VLOG.
2. Kontaktujte podporu.
3. Prověřte stranu Windows.

Je-li popis linky ve stavu VARY-ON PENDING (nevyřízené logické zapnutí), VARY-ON (logicky zapnutá) nebo RCYPND, prověřte stranu Windows.

### Prověření problému ze strany Windows

Otevřete okno **Network and Dialup Connections** a podívejte se, zda se v něm nachází ikona portu virtuální sítě Ethernet.

- Je-li ikona v pořádku a popis linky je ve stavu VARY-ON (logicky zapnutá), zkontrolujte, zda jsou správně nakonfigurovány IP adresy. Pokud problém přetrvává, kontaktujte podporu.
- Je-li ikona v pořádku a popis linky je ve stavu VARY-ON PENDING (nevyřízené logické zapnutí) nebo RCYPND, zkontrolujte záznamy v protokolu PAL a kontaktujte podporu.
- Je-li u ikony portu virtuální sítě Ethernet červené X (odpojený kabel), otevřete protokol událostí a vyhledejte záznamy týkající se ovladače qvndvemp.sys.
  - Najdete-li záznamy pro qvndvemp.sys, poznamenejte si je a kontaktujte podporu. Pravděpodobně selhala inicializace ovladače a k určení problému bude třeba výpis paměti z IOP.
  - Jestliže jste nenašli žádné záznamy pro qvndvemp.sys, kontaktujte podporu a uveďte stav popisu linky. Problém bude pravděpodobně souviset s interním kódem LIC operačního systému i5/OS.

## Existuje popis linky, ale chybí ikona

### Prověření problému ze strany i5/OS

Zkontrolujte popis linky. Je-li popis linky ve stavu FAIL (selhání), proveďte tyto kroky:

1. Shromážděte záznamy protokolu PAL a VLOG.
2. Kontaktujte podporu.
3. Prověřte stranu Windows.

Je-li popis linky ve stavu VARY-ON PENDING (nevyřízené logické zapnutí), VARY-ON (logicky zapnutá) nebo RCYPND, prověřte stranu Windows.

### Prověření problému ze strany Windows

Otevřete **Device Manager**, klepněte na **Network Adapters** a v zobrazeném seznamu vyhledejte záznam pro port virtuální sítě Ethernet.

- Pokud je vedle portu virtuální sítě Ethernet vykřičník (!), proveďte tyto kroky:
  1. Otevřete protokol událostí, vyhledejte záznamy týkající se ovladače qvndvemp.sys a poznamenejte si je.

2. Kontaktujte podporu. V případě selhání inicializace ovladače potřebujete pomoci se stanovením příčiny.
- Je-li u portu virtuální sítě Ethernet červené X, proveďte tyto kroky:
    1. Klepněte pravým tlačítkem myši na port virtuální sítě Ethernet a vyberte **Enable**.
    2. Otevřete okno **Network and Dialup Connections** a vyhledejte ikonu portu virtuální sítě Ethernet.
    3. Jestliže ikona portu virtuální sítě Ethernet chybí nebo je šedivá, otevřete **Event Log**.
    4. Vyhledejte záznamy týkající se ovladače qvndvemp.sys, pokud existují, poznamenejte si je a kontaktujte podporu. Selhalo zavedení nebo zapnutí portu virtuální sítě Ethernet.

## Popis linky chybí, ale ikona existuje

### Prověření problému ze strany i5/OS

Ověřte si, že v současné době neexistuje pod daným NWSD žádný popis linky pro port virtuální sítě Ethernet. Potom prověřte stranu Windows.

### Prověření problému ze strany Windows

Otevřete okno **Network and Dialup Connections** a podívejte se, zda se v něm nachází ikona portu virtuální sítě Ethernet. Jestliže program VEU nedokázal odstranit port virtuální sítě Ethernet, znovu zaveďte integrovaný server, aby se tato skutečnost napravila. Pokud problém přetrvává, proveďte tyto kroky:

1. Pomocí programu VEU ručně odstraňte port virtuální sítě Ethernet. Použijte tento příkaz:

```
qvndveu -a -R -x [port_id]
```

kde [port\_id] je buď desítkové číslo (0-9), které odpovídá odstraňovanému portu, nebo hodnota p u dvoubodové virtuální sítě Ethernet.
2. Pokud se po provedení příkazu ikona portu virtuální sítě Ethernet ztratí, je proces dokončen. Pokud však program VEU při odstraňování portu virtuální sítě Ethernet selže, pokračujte těmito kroky:
3. Shromážděte soubor protokolu VEU (D:\as400nt\qvndveu.log).
4. Otevřete **protokol událostí**, vyhledejte záznamy týkající se ovladače qvndvemp.sys a poznamenejte si je.
5. Kontaktujte podporu. Měli byste mít po ruce tyto informace.
  - Všechny záznamy o ovladači qvndvemp.sys, které jste si poznamenali.
  - Soubor protokolu VEU, který jste shromáždili.

## Chybí popis linky i ikona

### Prověření problému ze strany i5/OS

Pro port virtuální sítě Ethernet, který se má instalovat, je třeba mít v NWSD popis linky. K vytvoření popisu linky použijte pokyny z části “Konfigurace virtuálních sítí Ethernet” na stránce 107.

#### Poznámka:

Při přidávání popisu linky musí být NWSD logicky vypnutý. Po vytvoření popisu linky a znovuzavedení integrovaného Windows serveru program VEU automaticky vytvoří pod operačním systémem Windows port virtuální sítě Ethernet.

Pokud problém s portem virtuální sítě Ethernet přetrvává i po úspěšném vytvoření popisu linky a znovuzavedení integrovaného serveru, vraťte se do této části pro odstraňování závad a postupujte podle pokynů uvedených u nového příslušného případu selhání.

### Prověření problému ze strany Windows

Neexistuje-li v operačním systému i5/OS popis linky, neměl by se ve Windows zobrazovat port virtuální sítě Ethernet. Nainstalujte popis linky tak, jak je uvedeno v tématu “Konfigurace virtuálních sítí Ethernet” na stránce 107 a restartujte integrovaný server, abyste zjistili, zda se problém vyřešil.



## Problémy s externími sítěmi

Máte-li problém s externí sítí integrovaného serveru:

- Podívejte se do protokolu událostí integrovaného Windows serveru na případné chyby komunikace nebo chyby ovladače. K tomu slouží **Event Viewer** na Windows serveru. Protokoly událostí, které jsou asociované s externími adaptéry podporovaným servery IXS 2890, 2892 a 4812, mohou mít v poli Source hodnoty: IBMTRP, PCNET, ALTND5, E100B nebo E1000. Nemůžete-li v protokolu událostí nalézt text pro službu IBMTRP Token-ring, je třeba provést změny v registru Windows.

### Poznámka:

Neumíte-li dělat změny v registru Windows, obraťte se na servisního zástupce.



Jestliže proces změn v registru Windows znáte, použijte ke zviditelnění textu v protokolu událostí tento postup:

1. Z nabídky **Start** operačního systému Windows vyberte volbu **Run**.
  2. Napište **regedit**.
  3. V programu Registry Editor přejděte na větev  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\System\IBMTRP.
  4. Vyberte **EventMessageFile**.
  5. Z menu **Edit** programu Registry Editor vyberte volbu **Modify**.
  6. Napište %SystemRoot%\System32\netevent.dll;%SystemRoot%\System32\ibmsgnet.dll
  7. Zavřete program Registry Editor a restartujte integrovaný server.
- U adaptéru Ethernet se přesvědčte, zda je uveden ovladač, který má ve jménu **iSeries** nebo **AMD PCNET Family Ethernet Adapter (PCI)**, a zda má stav **started** (spuštěno).
    1. Klepněte na **Start - Administrative Tools - Computer Management - System Tools - Device Manager** a **Network Adapters**.
    2. Přesvědčte se, zda je uveden ovladač, který má ve jménu **iSeries** nebo **AMD PCNET Family Ethernet Adapter (PCI)**, a zda má stav **started** (spuštěno).
  - U sítí typu Token-ring se v okně **Device Manager** přesvědčte, že jste spustili **IBM High-Speed 100/16/4 Token-Ring PCI Adapter** nebo **IBM PCI Token-Ring Adapter**.

### Poznámka:

Při spuštění musí být nastavena volba **povolit**.


- U sítí Token-ring zkontrolujte, zda je nastavení rychlosti přenosu dat v síti vhodné pro vaši síť.
- U sítí Ethernet zkontrolujte, zda je nastavení rychlosti linky a duplexu vhodné pro váš přepínač nebo rozbočovač (hub). Pokud se váš server 4812 nebo 5701 nepřipojí s rychlostí vyšší než 100 milionů bitů za sekundu, zkontrolujte, zda jsou specifikace přepínače v souladu s normami IEEE 802.3ab. Ovladače Windows LAN pro porty typu Gigabit Ethernet serverů 4812 nebo 5701 mohou být omezeny na 100 milionů bitů za sekundu, když jsou připojeny k některým dřívějším nevyhovujícím přepínačům.
- Port sítě Ethernet o rychlosti 10/100 Mbps instalovaný na serveru IXS 2892 nepodporuje přímé připojení k určitým rozbočovačům a směrovačům o rychlosti 10 Mbps, které postrádají možnost **automatické úpravy polarity**. Máte-li problém s rozběhnutím portu 2892 10/100 pro rozbočovač nebo směrovač o rychlosti 10 MB/s, podívejte se do jeho specifikace na podporu **automatické úpravy polarity**. Rovněž se podívejte, zda tento port 2892 10/100 funguje pro jiná zařízení.
- Pokud problém stále přetrvává, podívejte se do databází technických informací na webových stránkách

 IBM iSeries Support  . Nenaleznete-li ani zde řešení, obraťte se na svého poskytovatele technické podpory.

## Manuální aktualizace ovladačů LAN na integrovaném Windows serveru

Windows 2000 Server a Windows Server 2003 obecně instalují příslušné ovladače LAN pro existující adaptéry a porty automaticky. V určité situaci však můžete ovladač LAN nainstalovat nebo aktualizovat manuálně.



Chcete-li na externě připojeném serveru Netfinity nebo xSeries manuálně instalovat nebo aktualizovat ovladač LAN pro jiný adaptér, než pro virtuální síť Ethernet, navštivte webové stránky IBM Personal computing support  a vyberte **Servers** a potom **Device driver file matrix**.

Při manuální instalaci nebo aktualizaci ovladače LAN pro adaptér nebo port na serveru IXS nebo pro virtuální síť Ethernet postupujte takto:

1. “Zahájení instalace nebo aktualizace ovladače LAN”.
2. “Výběr adaptéru, který se bude instalovat nebo aktualizovat”.
3. “Dokončení instalace nebo aktualizace ovladače LAN”.

### Zahájení instalace nebo aktualizace ovladače LAN

Při spuštění manuální instalace nebo aktualizace ovladače LAN pro adaptér nebo port na serveru IXS (Integrated xSeries Server) nebo pro virtuální síť Ethernet postupujte takto:

1. Z nabídky **Start** operačního systému Windows vyberte **Settings** a potom **Control Panel**.
2. Dvakrát klepněte na **System**.
3. V okně **System Properties** vyberte kartu **Hardware**.
4. Jestliže nový ovladač LAN nemá digitální podpis nebo si tím nejste jisti, ověřte si, zda je metoda pro podpisy ovladačů nastavena na Ignore.
  - a. V okně **System Properties** klepněte na tlačítko **Driver Signing**.
  - b. Zapamatujte si aktuální nastavení a vyberte **Ignore**. Potom klepněte na **OK**.
5. Klepněte na **Device Manager**.
6. “Výběr adaptéru, který se bude instalovat nebo aktualizovat”.

### Výběr adaptéru, který se bude instalovat nebo aktualizovat

Po úspěšném spuštění instalace nebo aktualizace (viz “Zahájení instalace nebo aktualizace ovladače LAN”) ovladače LAN pro adaptér nebo port na serveru IXS (Integrated xSeries Server) nebo pro virtuální síť je třeba vybrat požadovaný adaptér.

Při výběru adaptéru, který chcete instalovat nebo aktualizovat, postupujte takto:

1. V okně **Device Manager** otevřete **Network Adapters**.
2. Pod **Network Adapters** klepněte pravým tlačítkem myši na adaptér, který chcete aktualizovat, a vyberte **Properties**.
3. V oknech **Properties** pro tento adaptér klepněte na kartu **Driver**.
4. Klepněte na tlačítko **Update Driver** nebo **Install Driver** (vždy se zobrazí pouze jedna možnost).
5. V dialogovém okně **Update Device Driver Wizard** klepněte na **Next**.
6. “Dokončení instalace nebo aktualizace ovladače LAN”.

### Dokončení instalace nebo aktualizace ovladače LAN

Je třeba, abyste měli provedeny oba předchozí úkoly vyžadované při manuální instalaci nebo aktualizaci ovladače pro adaptér nebo port LAN na serveru IXS (Integrated xSeries Server) nebo pro virtuální síť Ethernet.

- “Zahájení instalace nebo aktualizace ovladače LAN”.
- “Výběr adaptéru, který se bude instalovat nebo aktualizovat”.

K dokončení instalace nebo aktualizace ovladače nebo portu LAN použijte jeden z uvedených postupů, podle toho, o který z následujících případů se jedná.

- Používáte Windows 2000 Server nebo jste dostali pokyn k instalaci ovladače LAN z konkrétní složky pro Windows Server 2003.
- Používáte Windows Server 2003 a nedostali jste pokyn k instalaci ovladače LAN z konkrétního umístění.

## Používáte Windows 2000 Server, nebo jste dostali pokyn k instalaci ovladače LAN z konkrétní složky pro Windows Server 2003.

K dokončení instalace nebo aktualizace ovladač LAN použijte tento postup:

1. Vyberte **Display a list of the known drivers for this device so that I can choose a specific driver** a klepněte na **Next**.
2. Klepněte na **Have Disk**. Otevře se dialogové okno **Install From Disk**, kam zadáte umístění ovladače.
  - Jestliže jste byli instruováni k instalaci z určité jednotky a složky, klepněte na **Browse** a vyhledejte toto umístění. Potom klepněte na **Open**.
  - Jinak klepněte na **Browse** a vyhledejte na systémové jednotce (obvykle C:) umístění ovladače, který odpovídá adaptéru, který instalujete nebo aktualizujete. Při vyhledávání složky, která obsahuje ovladač pro daný hardware použijte následující seznam.
    - \wsv\ibm pro hardware typu 2744
    - \wsv\alt pro hardware typu 2743 a 2760
    - \wsv pro virtuální síť Ethernet
    - \wsv\amd pro hardware typu 2838 v systému Windows 2000
    - \windows\inf pro hardware typu 2723 a 2838 ve Windows serveru
    - \wsv\itl pro hardware typu 2892 v systému Windows 2000
    - \wsv pro hardware typu 2892 v systému Windows Server 2003
    - \wsv\alt pro hardware typu 4812, 5700 a 5701 v systému Windows 2000
    - \wsv\itg pro hardware typu 4812, 5700 a 5701 v systému Windows Server 2003
3. Klepněte na **OK**.
4. V dialogovém okně **Update Device Driver Wizard** vyberte ze seznamu příslušný ovladač, pokud již není zvýrazněn, a klepněte na **Next**.
5. Znovu klepněte na **Next**.
6. Jestliže se při dokončení procedury aktualizace ovladače objeví Ret Code 22, může být ovladač zablokovaný. V takovém případě k aktivaci adaptéru použijte okno **Device Manager**, ve kterém klepněte na nepřístupný adaptér a vyberte **Enable**.
7. Chcete-li nainstalovat nebo aktualizovat více adaptérů, přečtěte si téma “Výběr adaptéru, který se bude instalovat nebo aktualizovat” na stránce 224.

### Poznámka:

Pokud operační systém Windows po každé aktualizaci ovladače hlásí, že je třeba restartovat počítač, odložte to až do chvíle, kdy již nechcete aktualizovat žádné další ovladače.

8. Jestliže jste při zahájení instalace nebo aktualizace změnili metodu podpisu ovladače (viz “Zahájení instalace nebo aktualizace ovladače LAN” na stránce 224), nastavte znovu původní metodu.

## Používáte Windows Server 2003 a nedostali jste pokyn k instalaci ovladače LAN z konkrétního umístění.

K dokončení instalace nebo aktualizace ovladač LAN použijte tento postup:

1. Vyberte **Search for a suitable driver for my device** a klepněte na **Next**.
2. Opět klepněte na **Next**. Zobrazí se kompatibilní hardware.
3. Zrušte výběr všech **Optional search locations**, klepněte na **Next**, a potom opět klepněte na **Next**.
4. Jestliže se při dokončení procedury aktualizace ovladače objeví Ret Code 22, může být ovladač zablokovaný. V takovém případě k aktivaci adaptéru použijte okno **Device Manager**, ve kterém klepněte na nepřístupný adaptér a vyberte **Enable**.
5. Chcete-li nainstalovat nebo aktualizovat více adaptérů, přečtěte si téma “Výběr adaptéru, který se bude instalovat nebo aktualizovat” na stránce 224.

**Poznámka:**

Pokud operační systém Windows po každé aktualizaci ovladače hlásí, že je třeba restartovat počítač, odložte to až do chvíle, kdy již nechcete aktualizovat žádné další ovladače.

6. Jestliže jste při zahájení instalace nebo aktualizace ovladače změnili metodu podpisu ovladače (viz "Zahájení instalace nebo aktualizace ovladače LAN" na stránce 224), nastavte znovu původní metodu.

## Konflikty IP adres ve dvoubodové virtuální síti Ethernet

Produkt IBM iSeries Integrated Server Support používá pro dvoubodovou síť Ethernet IP adresy v rozsahu 192.168.x.y. Standardně se adresy vybírají pomocí i5/OS příkazu INSWNTSVR (Instalace Windows serveru). Podrobnosti a příklady najdete v tématu "Přidělování IP adres ve dvoubodové virtuální síti Ethernet" na stránce 227. V závislosti na síti mohou nastat konflikty s již používanými adresami. Abyste se vyhnuli potenciálním konfliktům, můžete pro server připojený pomocí IXS nebo IXA použít parametr VRTPTPPORT.

Jestliže si konflikt vyžádá změnu adres, musíte se postarat o to, aby dvoubodová virtuální síť Ethernet měla v operačním systému i5/OS svoji vlastní podsít. Používaná maska podsítě je 255.255.255.0. Abyste zajistili, že dvoubodová virtuální síť Ethernet bude mít svoji vlastní podsít, použijte IP adresy ve tvaru a.b.x.y, kde a.b.x bude mít na obou stranách dvoubodové virtuální síť Ethernet stejnou hodnotu. Zkontrolujte také, zda hodnota a.b.x je ve vaší síti jedinečná.

Při změně adres ve dvoubodové virtuální síti Ethernet z důvodu konfliktu postupujte takto:

1. Z konzole operačního systému i5/OS zadejte příkaz `DSPNWSD NWSD(name) OPTION (*PORTS)`.  
Poznamenejte si připojenou linku pro číslo portu `*VRTETHPTP`, tzv. popis linky.
2. Pomocí příkazu `CFGTCP` (Konfigurace TCP/IP) a volby 1 si zobrazte rozhraní TCP. Poznamenejte si IP adresu a masku podsítě, které jsou asociovány s popisem linky z kroku 1.

**Poznámka:**

IP adresa zadaná u dvoubodové virtuální sítě Ethernet z konzole Windows přepíše hodnotu portu `*VRTETHPTP` nastavenou v `NWSD` v parametru `TCPPRTCFG`.

1. Klepněte na **Start** → **Settings** → **Control Panel**, a potom na **Network and Dial-up Connections**.
2. Klepněte pravým tlačítkem myši na **Local Area Connection**, které odpovídá dvoubodové virtuální síti Ethernet, a z menu vyberte **Properties**.
3. V seznamu instalovaných protokolů vyberte **TCP/IP Protocol** a stiskněte tlačítko **Properties**. Zobrazí se vlastnosti TCP/IP.
4. Změňte IP adresu pro novou hodnotu, kterou jste vybrali.
5. Klepněte na **OK** potom klepnutím na **Close** zavřete aplikaci.
6. Vypněte integrovaný Windows server, aniž byste prováděli restart.
7. V operačním systému i5/OS logicky vypněte příslušný NWSD.
8. Zadejte příkaz `RMVTCPIFC` (Odstranění rozhraní TCP/IP) a použijte adresu z kroku 2.
9. Pomocí příkazu `ADDDCPIFC` (Přidání rozhraní TCP/IP) přidejte nové rozhraní. Použijte IP adresu, kterou jste vybrali pro stranu i5/OS dvoubodové virtuální sítě Ethernet. Je rovněž třeba zadat masku podsítě a popis linky z kroku 1 a 2.
10. Na příkazový řádek operačního systému i5/OS napište příkaz `CHGNWSD NWSD(jméno)` a stiskněte klávesu F4.
  - a. Nalistujte sekci označenou `TCP/IP port configuration`.
  - b. V poli `Internet address` změňte IP adresu pro port `*VRTETHPTP` na hodnotu, kterou jste použili v kroku 3. Stiskněte klávesu Enter, aby se změna projevila.
  - c. Logicky zapněte NWSD.

**Poznámka:**

Jestliže instalujete více serverů, raději sami přidělte IP adresy dvoubodové virtuální síti Ethernet (viz "Přidělování IP adres ve dvoubodové virtuální síti Ethernet" na stránce 227), než abyste je nechali

generovat příkazem INSWNTSVR. Vyhněte se tak možným konfliktům. Parametr Virtual PTP Ethernet port umožňuje zadat IP adresy, o nichž víte, že jsou v systému jedinečné.

## Přidělování IP adres ve dvoubodové virtuální síti Ethernet

Příkaz INSWNTSVR (Instalace Windows serveru) standardně přiděluje IP adresy dvoubodové virtuální síti Ethernet ve tvaru 192.168.x.y. Chcete-li se vyhnout konfliktům, použijte tento příkaz s parametrem VRTPTPPORT, kterým můžete přidělit IP adresy o nichž víte, že jsou v systému jedinečné.

Jestliže necháte nastavit adresy příkazem automaticky a dojde ke konfliktu, můžete IP adresy změnit. U serverů připojených pomocí IXS a IXA tento příkaz přiděluje za x hodnotu, která je založena na čísle prostředku serveru IXS (Integrated xSeries Server). Příkaz hledá dvojici hodnot y a y+1 (počínaje y=1) s adresami, které nejsou v daném operačním systému i5/OS použity. Příkaz přidělí nižší číslo ve dvojici straně operačního systému i5/OS a vyšší číslo straně Windows serveru ve dvoubodové virtuální síti Ethernet.

Předpokládejme například, že máte server IXS 2892 se jménem prostředku LIN03. Po provedení příkazu INSWNTSVR (Instalace Windows serveru) mohou být pro dvoubodovou virtuální síť Ethernet nastaveny tyto adresy:

192.168.3.1 (na straně i5/OS)  
192.168.3.2 (na straně Windows serveru)

V případě konfliktu na instalovaném serveru se ujistěte, že konkrétní náhradní hodnota (například 192.168.17) není v síti použita, a změňte IP adresu na tuto hodnotu.

192.168.17.1 (na straně i5/OS)  
192.168.17.2 (na straně Windows serveru)

Pamatujte si, že IP adresa zadaná pro dvoubodovou virtuální síť Ethernet z konzole Windows přepíše hodnotu portu \*VRTETHPTP nastavenou v NWSD v parametru TCPPORTCFG.

Pokud problém stále přetrvává, podívejte se do databázi technických informací na webových stránkách

 IBM iSeries Support  . Nenaleznete-li ani zde řešení, obraťte se na svého poskytovatele technické podpory. Jestliže problém přetrvává, kontaktujte servis IBM.

## Problémy s TCP/IP nad virtuální síť Ethernet

Ověřte, že konfigurace TCP/IP u dvoubodové virtuální síti Ethernet je správná. Jestliže je konfigurace TCP/IP na straně i5/OS nová nebo pokud byla změněna, pomocí níže uvedeného postupu ověřte, že konfigurace TCP/IP ve Windows je správná.

1. Klepněte na **Start** → **Control Panel** → **Network Connections** nebo **Start** → **Settings** → **Network and Dial up Connections**.
2. Klepněte pravým tlačítkem myši na **Network Connections** nebo **Network and Dial-up Connections**, aby se zobrazila rozbalovací nabídka a vyberte **Open**.
3. Dvakrát klepněte na **IBM iSeries Virtual Ethernet point to point Connection**.
4. Klepněte na tlačítko **Properties**.
5. Vyberte Internet Protocol (TCP/IP)
6. Klepněte na tlačítko **Properties**. Jestliže je vybrána volba **Use the Following IP Address** a zobrazuje se IP adresa z konzole operačního systému i5/OS, nemusíte již pokračovat. Je-li vybrána volba **Obtain an IP address automatically**, pokračujte dalším krokem.
7. Klepněte na přepínač **Use the Following IP Address**.
8. Na příkazový řádek operačního systému i5/OS napište následující příkaz, kde 'nwsd' je jméno NWSD pro váš server a stiskněte klávesu Enter: `DSPNWSD NWSD(nwsd) OPTION(*TCPIP)`
  - V dialogovém okně DSPNWSD vyhledejte port s označením \*VRTETHPTP. Zde je zobrazena IP adresa a maska podsítě pro danou dvoubodovou virtuální síť Ethernet .
  - Z konzole integrovaného serveru zadejte hodnoty IP adresy dvoubodové virtuální síti Ethernet a masky podsítě, které jste získali z příkazu DSPNWSD.

- | 9. Klepněte na OK.
- | 10. Klepněte na OK.
- | 11. Klepněte na Zavřít.

| Informace o ověření konfigurace TCP/IP v operačním systému i5/OS a Windows najdete v tématu “Prozkoumání dvoubodových virtuálních sítí Ethernet” na stránce 109.

| Dvoubodová virtuální síť Ethernet používaná každým aktivním serverem musí používat zřetelnou podsíť IP. Chcete-li se dozvědět více o požadavcích na podsíť nebo změnit konfiguraci TCP/IP, přečtěte si téma “Konflikty IP adres ve dvoubodové virtuální síti Ethernet” na stránce 226.

| **Ověřte, že jsou virtuální adaptéry Ethernet serveru iSeries konfigurovány správně a že pracují.**

| Při odstraňování problémů s virtuálním adaptérem Ethernet se podívejte na jedno z těchto témat:

- | • “Problémy virtuální sítě Ethernet se servery připojenými pomocí iSCSI” na stránce 218.
- | • “Problémy virtuální sítě Ethernet se servery připojenými pomocí IXS a IXA” na stránce 220

| Chcete-li ověřit, že je popis linky pro virtuální adaptér Ethernet nakonfigurován správně, podívejte se na téma Kapitola 6, “Správa virtuálních sítí Ethernet a externích sítí”, na stránce 107.

| **Zajistěte, aby firewall nerušil provoz.**

| Pokud je zahrnut firewall, jako například firewall provozovaný v operačním systému Windows, musí být nakonfigurován tak, aby umožňoval požadovaný provoz.

- | • V případě IP adresy dvoubodového virtuálního připojení typu Ethernet serveru IBM iSeries povolte dynamické porty, aby zabránily selhání aplikací administrace serveru. Nepoužívejte funkci NAT (Network Address Translation).
- | • V případě IP adresy dvoubodového virtuálního připojení typu Ethernet serveru IBM iSeries povolte protokoly a porty požadované vašimi aplikacemi.
- | • V případě IP adresy připojení typu iSCSI HBA si prostudujte téma “Konfigurace firewallu” na stránce 126.

## **Problémy s přístupem ke sdíleným položkám serveru Windows Server 2003 ze systému souborů QNTC**

Pokud nelze k přístupu ke sdíleným položkám na serveru Windows Server 2003, který má nainstalovaný adresář Active Directory (například je v ovladači domény), použít systém souborů QNTC operačního systému i5/OS, potom možná bude nutné provést některá dodatečná nastavení. Další informace najdete v tématu “Použití služby Kerberos se serverem Windows Server 2003 Active Directory Server” na stránce 100.

## **Problémy s přístupem u IFS**

Když se z integrovaného Windows serveru pokoušíte o přístup k systému souborů (IFS) operačního systému i5/OS prostřednictvím serveru iSeries NetServer, může v následujících situacích přístup selhat.

- | • Používáte jméno UNC (Universal Naming Convention), které obsahuje IP adresu.
- | • Mezi integrovaným Windows serverem a operačním systémem i5/OS existuje cesta pro dvoubodovou virtuální síť Ethernet i externí síť LAN.

Buď změňte jméno UNC tak, aby se místo něho použilo jméno serveru iSeries NetServer, nebo zablokujte cestu pro externí síť LAN a zopakujte operaci, která selhala.

## **Problémy s ukládáním souborů integrovaného Windows serveru**

Máte-li u integrovaného Windows serveru problémy se zálohováním na úrovni souborů, podívejte se pod Windows na zprávy v protokolu událostí a pod i5/OS do fronty zpráv QSYSOPR.

- | • Zobrazí-li se vám chybový kód CPDB050 (chyba inicializace relace) CPDB055 (chyba komunikace relace), postupujte takto.



1. Zkontrolujte, zda se server i5/OS NetServer nachází v téže doméně (viz “Zajištění stejné domény pro server iSeries NetServer a integrovaný Windows server” na stránce 187) jako integrovaný server, jehož soubory chcete zálohovat.
  2. Přesvědčte se, že jste provedli kroky z části “Vytvoření sdílených položek na integrovaných Windows serverech” na stránce 186 a z části “Přidání členů do souboru QAZLCSAVL” na stránce 186.
  3. Ověřte si, že je spuštěn podsystém QSERVER.
  4. Zkontrolujte, zda je protokol TCP/IP aktivní:
    - a. V příkazu CFGTCP zadejte volbu 1.
    - b. Stisknutím klávesy F11 zobrazte stav rozhraní.
    - c. U příslušné síťové služby napište číslo 9, abyste spustili rozhraní TCP/IP.
    - d. Stisknutím klávesy F5 aktualizujte údaje. Vybraná služba TCP/IP by nyní měla být aktivní.
  5. Potom pokus o uložení souborů opakujte.
- Obdržíte-li chybovou zprávu, která indikuje problém s výměnou informací (CPDB053) nebo s přihlašováním k serveru (NTA02AE), postupujte takto:
    1. Přesvědčte se, zda jste na integrovaném serveru zapsán jako člen skupiny Administrators.
    2. Zkontrolujte, zda máte stejné heslo v operačním systému i5/OS jako na integrovaném serveru.
    3. Potom pokus o uložení souborů opakujte.
  - Obdržíte-li chybovou zprávu CPDB058, která indikuje problém se zpracováním sdíleného členu souboru, zkontrolujte správnost nastavení souboru QAZLCSAVL.
    1. Přesvědčte se, že jste provedli tento krok “Vytvoření sdílených položek na integrovaných Windows serverech” na stránce 186.
    2. A rovněž krok “Přidání členů do souboru QAZLCSAVL” na stránce 186. Dále musíte mít v tomto souboru uvedenou sdílenou položku, kterou jste zadali v příkazu SAV (Uložení).
  - Obdržíte-li chybovou zprávu NTA02A3, která indikuje problém komunikace s NTSAV, zkontrolujte, zda je spuštěna služba vzdáleného volání procedur (Remote Procedure Call).
    1. V programové liště integrovaného serveru klepněte na **Start** → **Programs** → **Administrative Tools**.
    2. Dvakrát klepněte na **Services**.
    3. Zkontrolujte, zda je spuštěna služba pro vzdálené příkazy (Remote Command Service).
  - Při zadání příkazu SAV se mohou vyskytnout tyto chyby:
    - CPFA09C Nemáte oprávnění k objektu
    - CPD3730 Nelze uložit adresář /qntc/(server)/(share)/System Volume Information

Tyto chyby indikují, že se neuložil adresář s informacemi o systémovém svazku (**System Volume Information**). Jedná se o skrytý systémový adresář, který je přístupný pouze přes účet Windows SYSTEM. Budete-li tuto zprávu ignorovat, tento adresář ani jeho obsah se nezazálohuje (obsahuje pomocné soubory protokolů používané při kódování souborů). Jinak můžete také přidat povolení k tomuto adresáři pro uživatele, který spouští příkaz SAV. Chcete-li udělit povolení, je třeba tento adresář zviditelnit (zobrazovat skryté soubory a neskrývat chráněné soubory systému). Informace o tom, jak nastavit povolení pro složku, najdete v nápovědě k serveru Windows 2000 Server resp. Windows Server 2003.

Chyba CPFA09C se může objevit i v případě, že spouštíte zálohování na úrovni souborů pod uživatelským profilem QSECOFR, ať už je uživatel QSECOFR na serveru zapsán, nebo ne. Použijte jiný uživatelský profil, který má na integrovaném serveru oprávnění k zálohování.

## Nečitelné zprávy ve frontě zpráv serveru



Zprávy z protokolu událostí ve Windows se nezobrazují správně, jestliže je identifikátor kódové sady znaků (CCSID) pro frontu zpráv nastaven na \*HEX (65535). Obsahuje-li fronta zpráv serveru (v NWSD je udána parametrem MSGQ) nečitelné zprávy, postupujte takto.

1. Z konzole i5/OS zadejte příkaz CHGMSGQ, kterým změníte CCSID pro frontu zpráv serveru na jinou hodnotu než \*HEX (65535), například na \*MSG.



Například pro frontu zpráv MYSVRQ v knihovně MYLIB použijte ke změně CCSID tento příkaz systému i5/OS: CHGMSGQ MSGQ(MYLIB/MYSVRQ) CCSID(\*MSG).

2. Pokud problém stále přetrvává, podívejte se do databází technických informací na webových stránkách

 IBM iSeries Support  . Nenaleznete-li ani zde řešení, obraťte se na svého poskytovatele technické podpory.

## Problémy se získáním výpisu paměti systému Windows

Je-li v systémové jednotce dostatek prostoru, je integrovaný Windows server nastaven tak, že automaticky shromáždí výpis systémové paměti v případě chyby STOP nebo modré obrazovky. Jestliže se výpis systémové paměti nevytvoří, postupujte takto:

1. Vyberte **Start, Programs**, a potom **Administrative Tools**.
2. Klepněte na **Computer Management**.
3. V nabídce **Action** klepněte na **Properties**.
4. Vyberte kartu **Advanced**.
5. Klepněte na tlačítko **Startup/Recovery**.
6. Zaškrtněte políčko **Write debugging information to**. Předvolená cesta k souboru memory.dmp, který se vytvoří při modré obrazovce, je %SystemRoot%, což je C:\WINNT pro Windows 2000 Server a C:\WINDOWS pro Windows Server 2003.



Další problémy, které brání vytvoření výpisu systémové paměti, jsou následující.

- Je nastavena nedostatečná velikost stránkovacího souboru. Velikost stránkovacího souboru musí být dostatečná na to, aby obsáhla veškerou fyzickou paměť RAM, plus 12 MB. Chcete-li zjistit velikost fyzické paměti RAM v počítači, postupujte takto:

1. Vyberte **Start, Settings**, a **Control Panel**.
2. Dvakrát klepněte na **System**. Hodnota uvedená pod nadpisem **Computer** na kartě **General** udává velikost fyzické paměti RAM, kterou máte v systému.

Chcete-li zkontrolovat nebo změnit velikost stránkovacího souboru, postupujte takto:

1. Vyberte kartu **Advanced** a klepněte na tlačítko **Performance Options** v sekci **Virtual Memory**. Pod nadpisem **Virtual Memory** je uvedena aktuální velikost stránkovacího souboru.
  2. Potřebujete-li změnit velikost stránkovacího souboru, klepněte na tlačítko **Change**.
- Stránkovací soubor se nenachází na systémové jednotce. Výpis systémové paměti se nevytvoří, pokud se stránkovací soubor nenachází na systémové jednotce. Systémová jednotka je jednotka C:. Chcete-li změnit jednotku pro stránkovací soubor, postupujte takto:
    1. Vyberte kartu **Advanced** a klepněte na tlačítko **Performance Options** v sekci **Virtual Memory**.
  - Na jednotce, kterou jste uvedli jako cestu k souboru memory.dmp, není dostatek prostoru. Předvolená cesta k souboru memory.dmp je systémová jednotka, ale můžete ji změnit na jinou jednotku. Ověřte si, zda je na systémové jednotce nebo na vámi zvolené jednotce dostatek prostoru. Potřebný volný prostor se rovná velikosti fyzické paměti RAM plus 12 MB.
  - Pokud problém stále přetrvává, podívejte se do databází technických informací na webových stránkách

 IBM iSeries Support  . Nenaleznete-li ani zde řešení, obraťte se na svého poskytovatele technické podpory.

---

## Přeinstalování integrovaného Windows serveru

V případě poškození integrovaného serveru byste měli být schopni zachovat instalované aplikace a uživatelská data tím, že jej přeinstalujete. Zkuste se buď přihlásit, nebo spustit operační systém DOS ze zaváděcího menu programu NTLDR (NT Loader). (To je možné pouze v případě, že zaváděcí jednotka je naformátovaná jako FAT.) Potom můžete přeinstalovat Windows server. Tím se systém vrátí na základní úroveň kódu Windows serveru, který byl původně nainstalován. Je tedy nutné znovu aplikovat všechny servisní balíky Microsoft, které jste měli nainstalovány. Měli byste také přeinstalovat nejnovější servisní balík pro produkt IBM iSeries Integrated Server Support.

Chcete-li přeinstalovat Windows server, použijte tento postup:

1. Zastavte integrovaný server. Viz téma “Spuštění a zastavení integrovaného serveru” na stránce 141.
2. Ze zaváděcího menu vyberte zavést PC-DOS nebo Windows server podle toho, co funguje.
3. Jestliže jste zvolili Windows server, otevřete okno MS-DOS.
- 4.

• V případě Windows 2000 zadejte `winnt /s:D:\i386 /u:D:\unattend.txt`

• V případě serveru Windows Server 2003 zadejte `winnt /b /t:C:/s:D:\i386 /u:D:\unattend.txt`

5. V okně MS-DOS zadejte:

```
D:  
cd \i386  
winnt /s:D:\i386 /u:D:\unattend.txt
```

6. Stiskněte klávesu Enter.

#### **Poznámka:**

Síťové jednotky mohou být tak poškozeny, že se nebudete moci přihlásit na integrovaný Windows server ani spustit operační systém DOS. V takovém případě zkuste obnovit všechny předdefinované i uživatelsky definované paměťové prostory z funkční zálohy. Další informace najdete v tématu “Zálohování předdefinovaných diskových jednotek pro integrované Windows servery” na stránce 181 a v tématu “Zálohování uživatelem definovaných diskových jednotek u integrovaného Windows serveru” na stránce 181.

Systémy Windows 2000 Server a Windows Server 2003 rovněž nabízejí konzoli pro obnovu systému (Windows Recovery Console), což je konzole příkazového řádku, která poskytuje omezený přístup k systému a tak umožňuje provádět řadu administračních úkolů nebo opravit systém. Více informací najdete v dokumentaci k serveru Windows 2000 Server nebo Windows Server 2003.

Může se stát, že bude nutné provést přeinstalaci od samého začátku pomocí tohoto postupu uvedeného v tématu “Spuštění instalace z konzole i5/OS” na stránce 87.

---

## **Shromáždění údajů pro servis u integrovaného Windows serveru**

Je-li třeba poskytnout pracovníkům podpory servisní údaje, podívejte se nejprve do protokolů operačního systému i5/OS (viz “Kontrola zpráv a protokolů úloh” na stránce 197) a do protokolu událostí ve Windows. Můžete si také v operačním systému i5/OS vytvořit kopii protokolů událostí ve Windows (viz “Protokolování zpráv” na stránce 144) a vytvářet výpisy paměti Windows serveru, které umožní odstraňování problémů vzdáleným způsobem. V tomto tématu se dozvíte, jak vytvářet výpisy a shromažďovat další údaje pro diagnostiku.

1. “Vytvoření výpisu paměti integrovaného Windows serveru v operačním systému i5/OS”.
2. V tématu “Použití nástroje operačního systému i5/OS pro výpis paměti popisu síťového serveru (NWSD)” na stránce 232 se dozvíte, jak lze z výpisu paměti zjistit, které konfigurační soubory a protokoly by měly být prohlédnuty nejdříve.

## **Vytvoření výpisu paměti integrovaného Windows serveru v operačním systému i5/OS**

Vytvoření výpisu paměti operačního systému Windows v operačním systému i5/OS vám může pomoci vyřešit problémy na integrovaném serveru. Je-li Windows server instalován na serveru iSeries, výpis se standardně vytváří v systémové jednotce. Cesta je následující:

- %SystemRoot%\Memory.Dmp pro Windows Server 2003.
- %SystemRoot%\Memory.Dmp pro Windows 2000 servery.

#### **Poznámka:**

Aby mohl operační systém Windows úspěšně vytvořit kompletní výpis paměti, musí se stránkovací soubor nacházet na systémové jednotce a mít velikost nejméně stejnou jako velikost paměti plus 12 MB. Při vytváření výpisu paměti se obsah paměti zapisuje do stránkovacího souboru. To je první krok procesu výpisu paměti. Při druhém kroku se data ze stránkovacího souboru zapisují do skutečného souboru s výpisem paměti.

K tomuto kroku dochází, když je systém po výpisu paměti znovu zaveden. Na jednotce, která obsahuje soubor s výpisem paměti (standardně je to soubor memory.dmp), musí být alespoň tolik volného prostoru, jaký je objem nainstalované paměti.

Výpis paměti je standardně povolen, jestliže je v systémové jednotce dostatek prostoru pro stránkovací soubor. Chcete-li zjistit, zda je povolen výpis paměti, nebo zapsat soubor memory.dmp na jinou jednotku, postupujte takto:

1. Rozbalte **Start, Settings**, a potom **Control Panel**.
2. Otevřete **System**.
  - Klepněte na kartu **Advanced** a potom na tlačítko **Startup and Recovery**.
3. Zaškrtněte volbu **Write Debugging Information To**.
4. V případě potřeby změňte umístění souboru s výpisem paměti.
5. Jestliže chcete, aby systém tento soubor přepsal pokaždé, když se vyskytne chyba Kernel STOP Error, zaškrtněte volbu **Overwrite any Existing File**.
6. Vyberte příslušný typ výpisu paměti (Small Memory Dump, Kernel Memory Dump nebo Complete Memory Dump) podle toho, jaká je velikost stránkovacího souboru a kolik je volného prostoru v systémové jednotce.
7. Klepněte na **OK**.

## Použití nástroje operačního systému i5/OS pro výpis paměti popisu síťového serveru (NWSD)

Nástroj pro výpis paměti NWSD se nazývá QFPDMPLS a slouží k vytvoření výpisu různých konfiguračních souborů a protokolů, které se používají na integrovaném Windows serveru. K práci s tímto nástrojem potřebujete zvláštní oprávnění ALLOBJ.

Postupujte takto:

1. Logicky vypněte NWSD (viz “Spuštění a zastavení integrovaného serveru” na stránce 141).
2. Na příkazový řádek operačního systému i5/OS napište:

```
CALL QFPDMPLS PARM(nwsdname)
```

kde nwsdname je jméno popisu síťového serveru.

Program vytvoří databázový soubor QGPL/QFPNWSMDMP s více členy. Jméno každého členu databázového souboru se skládá ze jména NWSD, za nímž následují dvě číslice v rozmezí 01 - 99. Bude-li mít například NWSD jméno MYSERVER, může se první člen jmenovat MYSERVER01.
3. Zobrazte si tento člen, abyste viděli obsah různých souborů asociovaných s popisem vašeho serveru. Některé z těchto souborů jsou důležité pro analýzu problémů, která závisí na tom, který krok instalace působí problémy.
4. V následující tabulce se můžete podívat, jaký význam má každý soubor v konkrétním kroku instalace. Je-li soubor označen 1, odkazujte se na něj při analýze problému jako na první, 2 druhý, 3 poslední. Neoznačené soubory nejsou pro instalaci důležité ale mohou být důležité v jiných situacích. Některé členy se vytvoří až ve fázi po instalaci.

### Poznámka:

Nástroj QFPDMPLS nelze použít k načtení souborů v systémové jednotce, jestliže jednotku převeďte na systém souborů NTFS.

Na některých serverech nemusíte najít všechny soubory, které jsou uvedeny v tabulce. Není-li určitý potřebný soubor nalezen, nebude jej rozhraní QFPDMPLS API moci načíst a odpovídající databázový člen se nevytvoří.

### Konfigurační soubory a soubory protokolů NWSD

Jméno členu	Typ dat	Jméno souboru	Adresář Windows	Instalace	Po instalaci
nwsdname01	Txt	CONFIG.SYS	C:\	3	3
nwsdname02	Txt	AUTOEXEC.BAT	C:\	2	2
nwsdname03	Txt	BOOT.INI	C:\		

Jméno členu	Typ dat	Jméno souboru	Adresář Windows	Instalace	Po instalaci
nwsdname04	Txt	HOSTS	C:\ nebo D:\		3
nwsdname05	Txt	QVNI.CFG	C:\ nebo D:\		
nwsdname06	Txt	QVNACFG.TXT	C:\ nebo D:\		
nwsdname07	Txt	QVNADAEM.LOG	C:\ nebo D:\		
nwsdname08	Txt	DUMPFIL.E.C01	C:\		
nwsdname09	Bin	DUMPFIL.E.C01	C:\		
nwsdname10	Txt	DUMPFIL.E.C02	C:\		
nwsdname11	Bin	DUMPFIL.E.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.E.D01	D:\		
nwsdname29	Bin	DUMPFIL.E.D01	D:\		
nwsdname30	Txt	DUMPFIL.E.D02	D:\		
nwsdname31	Bin	DUMPFIL.E.D02	D:\		
nwsdname32	Txt	HOSTS	%SystemRoot%\SYSTEM32\DRIVERS\ETC		3
nwsdname33	Txt	LMHOSTS	%SystemRoot%\SYSTEM32\DRIVERS\ETC		3
nwsdname34	Bin	MEMORY.DMP	C:\WINNT		
nwsdname35	Txt	VRMFLOG.TXT	E:\PROGRA~1\IBM\AS400NT\SERVICE\VRM		
nwsdname36	Txt	PTFLOG.TXT	E:\PROGRA~1\IBM\AS400NT\SERVICE\PTF		
nwsdname37	Txt	PTFUNIN.TXT	E:\PROGRA~1\IBM\AS400NT\SERVICE\PTF		
nwsdname38	Txt	A4EXCEPT.LOG	D:\		
nwsdname39	Txt	DUMPFIL.E.E01	E:\		
nwsdname40	Bin	DUMPFIL.E.E01	E:\		
nwsdname41	Txt	DUMPFIL.E.E02	E:\		
nwsdname42	Bin	DUMPFIL.E.E02	E:\		
nwsdname43	Txt	CMDLINES.TXT	D:\386\SOEMS	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	SETUPAPL.LOG	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		

Jméno členu	Typ dat	Jméno souboru	Adresář Windows	Instalace	Po instalaci
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	QVNDSDMR.LOG	D:\AS400NT		
nwsdname66	Txt	QVNDSDMC.LOG	D:\AS400NT		
nwsdname67	Txt	QVNILMGR.LOG	D:\AS400NT		

---

## Kapitola 15. Konfigurační soubory popisu síťového serveru

Integrované Windows servery můžete přizpůsobit svým potřebám vytvořením vlastních konfiguračních souborů. Můžete například změnit rozlišení obrazovky nebo potlačit instalaci protokolu IPX. Postup se skládá ze dvou částí:

1. Vytvořte konfigurační soubor NWSD. Další informace najdete v tématu “Popisy síťového serveru” na stránce 65.
2. Při instalaci serveru nebo při vytváření či změně popisu síťového serveru uveďte tento soubor v parametru Konfigurační soubor.

Pokaždé, když se spustí síťový server, operační systém i5/OS pomocí tohoto konfiguračního souboru změni zadaný soubor integrovaného serveru, který se nachází na jednotce C nebo D serveru.

Když příkaz INSWNTSVR (Instalace Windows serveru) aktivuje integrovaný server, vygeneruje se soubor s instalačním skriptem pro neobsluhovanou instalaci (UNATTEND.TXT). Když uvedete u příkazu INSWNTSVR svůj konfigurační soubor, můžete jej při instalaci použít k modifikaci souboru UNATTEND.TXT.

**Upozornění:** Dejte pozor na to, co chcete konfiguračním souborem změnit. Vyhněte se například odstraňování ovladačů zařízení ze souboru UNATTEND.TXT nebo modifikaci sekce OEM nebo sekce, která pro instalaci TCP. Takovéto změny by mohly zabránit serveru ve spuštění. Jestliže vytváříte konfigurační soubor za účelem modifikace již instalovaného serveru, vytvořte si záložní kopii všech souborů, které chcete měnit.

- Chcete-li zjistit, jak je formátovaná vaše systémová jednotka, použijte příkaz WRKNWSSTG (Práce s paměťovými prostory síťového serveru).
- Než začnete vytvářet konfigurační soubor, přečtěte si téma “Formát konfiguračního souboru NWSD”. V ní se dozvíte, jak používat jednotlivé typy záznamů.
- Měli byste si rovněž přečíst téma “Použití substitučních proměnných pro hodnoty klíčových slov” na stránce 246, kde se dozvíte, které proměnné máte k dispozici a jak si můžete vytvořit vlastní seznam.
- Můžete si přečíst i téma “Příklad: Konfigurační soubor NWSD” na stránce 236.
- Tím budete připraveni k provedení procedury “Vytvoření konfiguračního souboru NWSD” na stránce 236.

Budete-li mít po vytvoření konfiguračního souboru problém se spuštěním serveru, podívejte se na téma “Chyby v konfiguračním souboru NWSD” na stránce 207.

---

### Formát konfiguračního souboru NWSD

Konfigurační soubor NWSD se skládá z více různých **typů záznamů**, z nichž každý má svoji vlastní funkci. Typy záznamů jsou uvedeny v těchto tématech:

**“Odstranění řádků z existujícího souboru integrovaného serveru pomocí typu záznamu CLEARCONFIG” na stránce 237**

Tento typ záznamu použijte, chcete-li ze souboru integrovaného serveru odstranit všechny řádky.

**“Změna souboru integrovaného serveru pomocí typu záznamu ADDCONFIG” na stránce 238**

Tento typ záznamu použijte, k přidávání, nahrazování nebo odstraňování řádků v souboru integrovaného serveru.

**“Změna souboru integrovaného Windows serveru pomocí typu záznamu UPDATECONFIG” na stránce 242**

Tento typ záznamu slouží k přidání nebo odstranění řetězců v řádcích souboru integrovaného serveru.

**“Nastavení konfiguračních předvoleb pomocí typu záznamu SETDEFAULTS” na stránce 244**

Tento typ záznamu použijte k nastavení předvoleb pro určitá klíčová slova. Operační systém i5/OS používá tyto předvolby pouze při zpracování záznamů ADDCONFIG a UPDATECONFIG v aktuálním členu souboru.



Termín **záznam** znamená jeden výskyt typu záznamu. Každý záznam obsahuje řadu klíčových slov, za nimiž následuje rovnítko (=) a hodnoty pro tato klíčová slova.

### Základní pravidla formátování

- Délka záznamu zdrojového fyzického souboru musí být 92 bajtů.
- Řádek může obsahovat pouze jeden záznam, ale záznam může obsahovat více řádků.
- Mezery můžete používat mezi typem záznamu a klíčovým slovem, kolem rovnítka a za čárkami.
- Prázdné řádky můžete používat mezi záznamy a mezi klíčovými slovy.

#### Klíčová slova

- Klíčová slova můžete do záznamu psát v libovolném pořadí.
- Hodnoty klíčových slov oddělujte čárkami; za poslední hodnotou se již čárka nepíše.
- Jestliže hodnoty klíčových slov obsahují čárky, mezery, hvězdičky, rovnítka nebo uvozovky, musí být ohraničeny jednoduchými uvozovkami.
- Obsahují-li hodnoty klíčových slov jednoduché uvozovky, použijte vždy pro vyjádření jedné jednoduché uvozovky uvnitř hodnoty klíčového slova dvě jednoduché uvozovky.
- Hodnoty klíčových slov mohou mít délku řetězce maximálně 1024 znaků.
- Hodnoty klíčových slov mohou přesahovat více řádků, v tom případě však hodnota musí být ohraničena jednoduchými uvozovkami. Taková hodnota má v každém řádku počáteční a koncové mezery.

#### Komentáře

- Na začátku komentáře pište hvězdičku (\*).
- Komentář můžete napsat jak na samostatný řádek, tak i na řádek, který obsahuje text, jenž není součástí komentáře.

---

## Vytvoření konfiguračního souboru NWSD

Než začnete vytvářet konfigurační soubor, přečtěte si téma “Formát konfiguračního souboru NWSD” na stránce 235 a téma “Použití substitučních proměnných pro hodnoty klíčových slov” na stránce 246. Můžete si přečíst i téma “Příklad: Konfigurační soubor NWSD”.

Při vytváření konfiguračního souboru postupujte takto:

1. Vytvořte zdrojový fyzický soubor.
  - a. Na příkazový řádek operačního systému i5/OS napište CRTSRCPF a stiskněte klávesu F4.
  - b. Zadejte jméno souboru, libovolný text popisu a jméno členu. Stisknutím klávesy Enter se tento soubor vytvoří.
2. Pomocí libovolného editoru, který máte k dispozici, přidejte do tohoto fyzického souboru záznamy pro NWSD. Další informace najdete v tématu “Formát konfiguračního souboru NWSD” na stránce 235. Můžete použít například příkaz WRKMBRPDM (Práce s členy pomocí PDM):
  - a. Na příkazový řádek operačního systému i5/OS napište WRKMBRPDM file(*jméno\_vašeho\_souboru*) mbr(*jméno\_členu*) a stiskněte klávesu Enter.
  - b. U souboru, který chcete upravit, napište volbu 2.

---

## Příklad: Konfigurační soubor NWSD

Tento vzorový konfigurační soubor:

- Nastaví předvolenou cestu k souboru.
- Vymaže časové pásmo a nastaví je podle zadané proměnné.
- Nastaví předvolené hodnoty pro vyhledávání, které způsobí, že před sekci UserData přidají řádky s konfigurací.
- Přidá řádky, které nastavují zobrazení.

```
+-----+
| ***** Začátek dat *****
| *****
```

```

* Aktualizace D:\UNATTEND.TXT
*****
*
*=====
* Nastavení hodnot adresáře a jména souboru.
*=====
SETDEFAULTS TARGETDIR = 'D:\', TARGETFILE = 'UNATTEND.TXT'
*
*=====
* Vymazání časového pásma a jeho nahrazení hodnotou proměnné.
*=====
ADDCONFIG VAR = 'TimeZone', ADDWHEN = 'NEVER', DELETEWHEN = 'ALWAYS'
ADDCONFIG ADDSTR = 'TimeZone="%TIMEZONE%"',
FILESEARCHSTR = '%FPA_L_BRACKET%GuiUnattended%FPA_R_BRACKET%'
*
* Přidání řádků pro konfiguraci zobrazení.
*=====
* Nastavení předvoleb pro vyhledávání pro přidávání nových
* příkazů před záhlaví sekce UserData.
SETDEFAULTS FILESEARCHSTR = '%FPA_L_BRACKET%UserData%FPA_R_BRACKET%',
FILESEARCHPOS = 'BEFORE'
*
* Přidání příkazů pro zobrazení.
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'
*

```

## Odstranění řádků z existujícího souboru integrovaného serveru pomocí typu záznamu CLEARCONFIG

Typ záznamu CLEARCONFIG slouží k odstranění všech řádků z existujícího souboru integrovaného serveru.

**Upozornění:** Odstranění všech řádek ze souboru integrovaného serveru může způsobit, že nebudete moci síťový server logicky zapnout. Nastanou-li problémy, přečtěte si téma “Chyby v konfiguračním souboru NWSD” na stránce 207.

Chcete-li vyčistit soubor integrovaného serveru, vytvořte konfigurační soubor NWSD, který bude obsahovat typ záznamu CLEARCONFIG.

```

CLEARCONFIG
LINECOMMENT = '<"REM "|<řetězec_komentáře>>', (volitelné)
TARGETDIR = '<BOOT|path>', (volitelné)
TARGETFILE = '<jméno_souboru>' (povinné)

```

Podrobné vysvětlení klíčových slov v záznamu CLEARCONFIG najdete pod následujícími odkazy. Můžete se také vrátit na téma “Formát konfiguračního souboru NWSD” na stránce 235 nebo na téma “Změna souboru integrovaného serveru pomocí typu záznamu ADDCONFIG” na stránce 238.

- “Klíčové slovo LINECOMMENT” na stránce 240
- “Klíčové slovo TARGETDIR”
- “Klíčové slovo TARGETFILE” na stránce 238

### Klíčové slovo TARGETDIR

TARGETDIR slouží ke specifikaci cesty k souboru integrovaného serveru, který chcete vyčistit.

### Poznámka:

Když měníte soubor, operační systém i5/OS použije pouze první adresář uvedený pro tento soubor. Veškeré další záznamy, které uvádějí jiný adresář, jsou ignorovány.

## Klíčové slovo TARGETFILE

TARGETFILE slouží ke specifikaci souboru integrovaného serveru, který chcete vyčistit.

---

## Změna souboru integrovaného serveru pomocí typu záznamu ADDCONFIG

Pomocí typu záznamu ADDCONFIG můžete měnit soubor integrovaného Windows serveru následujícími způsoby:

- Přidat řádek na začátek nebo na konec souboru.
- Přidat nový řádek před nebo za řádek, který obsahuje určitý řetězec.
- Odstranit řádek ze souboru.
- Nahradit první, poslední nebo všechny výskyty určitého řádku v souboru.
- Specifikovat adresář souboru, který se má změnit.

Chcete-li změnit soubor integrovaného serveru, vytvořte konfigurační soubor NWSD, který bude obsahovat typ záznamu ADDCONFIG, takto:

```
ADDCONFIG
VAR                = '<jméno_proměnné>',          (podmíněně vyžadováno)
ADDSTR             = '<řádek ke zpracování>',      (volitelné)
ADDWHEN           = '<ALWAYS|NEVER|<výraz>>',      (volitelné)
DELETEWHEN        = '<NEVER|ALWAYS|<výraz>>',      (volitelné)
LINECOMMENT        = '<"REM "|<řetězec_komentáře>>', (volitelné)
LOCATION            = '<END|BEGIN>',                (volitelné)
FILESEARCHPOS      = '<AFTER|BEFORE>',            (volitelné)
FILESEARCHSTR      = '<vyhledávací_řetězec>',      (podmíněně vyžadováno)
FILESEARCHSTROCC  = '<LAST|FIRST>',              (volitelné)
REPLACEOCC         = '<LAST|FIRST|ALL>',          (volitelné)
TARGETDIR          = '<BOOT|path>',              (volitelné)
TARGETFILE         = '<CONFIG.SYS|<jméno_souboru>>', (volitelné)
UNIQUE            = '<NO|YES>'                   (volitelné)
```

Podrobné vysvětlení klíčových slov v záznamu ADDCONFIG najdete pod následujícími odkazy. Můžete se také vrátit na téma “Formát konfiguračního souboru NWSD” na stránce 235 nebo na téma “Změna souboru integrovaného Windows serveru pomocí typu záznamu UPDATECONFIG” na stránce 242.

- “Klíčové slovo VAR” na stránce 239
- “Klíčové slovo ADDSTR” na stránce 239
- “Klíčové slovo ADDWHEN” na stránce 239
- “Klíčové slovo DELETEWHEN” na stránce 240
- “Klíčové slovo LINECOMMENT” na stránce 240
- “Klíčové slovo LOCATION” na stránce 240
- “Klíčové slovo FILESEARCHPOS (typ záznamu ADDCONFIG)” na stránce 241
- “Klíčové slovo FILESEARCHSTR” na stránce 241
- “Klíčové slovo FILESEARCHSTROCC” na stránce 241
- “Klíčové slovo REPLACEOCC” na stránce 241
- “Klíčové slovo TARGETDIR” na stránce 241
- “Klíčové slovo TARGETFILE” na stránce 242
- “Klíčové slovo UNIQUE” na stránce 242

## Klíčové slovo VAR

VAR udává hodnotu na levé straně rovnítko, podle níž se identifikuje řádek, který chcete přidat nebo ze souboru odebrat. Například:

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

Operační systém i5/OS vyžaduje toto klíčové slovo, jestliže v konfiguračním souboru neuvedete klíčové slovo REPLACEOCC.

## Klíčové slovo ADDSTR

ADDSTR slouží ke specifikaci řetězce, který chcete přidat do souboru integrovaného serveru. Například:

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

## Klíčové slovo ADDWHEN

ADDWHEN určuje, ve kterém okamžiku zpracování má operační systém i5/OS přidat do souboru integrovaného Windows serveru nový řádek nebo řetězec.

Můžete zadat:

- ALWAYS - jestliže chcete, aby operační systém i5/OS přidal tento řádek nebo řetězec pokaždé, když zpracovává konfigurační soubor. (ALWAYS je předvolená hodnota, pokud jste nenastavili jinou předvolbu pomocí záznamu SETDEFAULTS v tomto členu.)
- NEVER - jestliže chcete, aby operační systém i5/OS nikdy nepřidal tento řádek nebo řetězec.
- Výraz, na jehož základě operační systém i5/OS přidá řádek nebo řetězec při splnění (=TRUE) zadané podmínky. Výrazy se skládají z operátorů a operandů (viz “Operátory ve výrazech používané u klíčových slov ADDWHEN a DELETEWHEN”) a musí vracet hodnotu TRUE nebo FALSE.

### Poznámka:

Jestliže nechcete, aby operační systém i5/OS interpretoval některý výraz (například výraz obsahující hvězdičku (\*)) jako matematickou operaci, ohraničte tento výraz uvozovkami. Například k přidání řádku u NWSD typu \*WINDOWSNT můžete napsat:

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

## Operátory ve výrazech používané u klíčových slov ADDWHEN a DELETEWHEN

Ve výrazech můžete používat tyto operátory:

Operátor	Popis
==	Vrací TRUE, když se operandy rovnají; FALSE, když se nerovnají.
!=	Vrací FALSE, když se operandy rovnají; TRUE, když se nerovnají.
>	Vrací TRUE, když je operand vlevo větší než operand vpravo; FALSE, když tomu tak není. Jsou-li operandy řetězce, porovnávají se hodnoty ASCII.
<	Vrací TRUE, když je operand vlevo menší než operand vpravo; FALSE, když tomu tak není. Jsou-li operandy řetězce, porovnávají se hodnoty ASCII.
>=	Vrací TRUE, když je operand vlevo větší nebo roven operandu vpravo; FALSE, když tomu tak není. Jsou-li operandy řetězce, porovnávají se hodnoty ASCII.
<=	Vrací TRUE, když je operand vlevo menší nebo roven operandu vpravo; FALSE, když tomu tak není. Jsou-li operandy řetězce, porovnávají se hodnoty ASCII.
&&	Logické AND. Vrací TRUE, když oba operandy mají hodnotu různou od nuly (0). Operandů musí být celá čísla.
	Logické OR. Vrací TRUE, když jeden z operandů má hodnotu různou od nuly (0). Operandů musí být celá čísla.
+	Jsou-li oba operandy celá čísla, výsledkem je součet těchto čísel. Jsou-li oba operandy řetězce, výsledkem je jejich zřetězení.

Operátor	Popis
-	Odečítá celá čísla.
*	Násobí celá čísla.
/	Dělí celá čísla.
()	Závorky mění pořadí vyhodnocení.
!	Logické NOT. Vrací TRUE, když je hodnota jediného operandu 0. Vrací FALSE, pokud to není 0.
ALWAYS	Vždy vrací TRUE.
NEVER	Vždy vrací FALSE.

## Klíčové slovo DELETEWHEN

DELETEWHEN určuje, ve kterém okamžiku zpracování má operační systém i5/OS vymazat ze souboru řádek nebo řetězec. Můžete zadat:

- ALWAYS - jestliže chcete, aby operační systém i5/OS vymazal tento řádek nebo řetězec pokaždé, když zpracovává konfigurační soubor.
- NEVER - jestliže chcete, aby operační systém i5/OS nikdy nemazal tento řádek nebo řetězec. (NEVER je předvolená hodnota, pokud jste nenastavili jinou předvolbu pomocí záznamu SETDEFAULTS v tomto členu.)
- Výraz, na jehož základě operační systém i5/OS vymaže řádek nebo řetězec při splnění (=TRUE) zadané podmínky. Výrazy se skládají z operátorů a operandů (viz "Operátory ve výrazech používané u klíčových slov ADDWHEN a DELETEWHEN" na stránce 239) a musí vracet hodnotu TRUE nebo FALSE.

### Poznámka:

Jestliže nechcete, aby operační systém i5/OS interpretoval některý výraz (například výraz obsahující hvězdičku (\*)) jako matematickou operaci, ohraničte tento výraz uvozovkami. Například k odstranění řádku u NWSD typu \*WINDOWSNT můžete napsat:

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

## Klíčové slovo LINECOMMENT

LINECOMMENT udává řetězec, který se v souboru použije jako předpona označující komentáře. Chcete-li používat předponu 'REM', ponechte u klíčového slova LINECOMMENT předvolenou hodnotu. Můžete však definovat i jinou hodnotu. Chcete-li například v souboru označovat komentáře středníkem, zadejte LINECOMMENT = ';' do **prvního** záznamu, který se na tento soubor odkazuje. (V každém jiném záznamu operační systém i5/OS klíčové slovo LINECOMMENT ignoruje.)

## Klíčové slovo LOCATION

LOCATION určuje, kam se má do souboru přidat nový řádek. Předvolená hodnota END znamená, že operační systém i5/OS přidá řádek na konec souboru. Pokud chcete, aby operační systém i5/OS přidal řádek na začátek souboru, zadejte hodnotu BEGIN.

## Klíčové slovo LINESEARCHPOS

LINESEARCHPOS určuje, zda se má řetězec zadaný v klíčovém slově ADDSTR přidat za (AFTER - předvolba) nebo před (BEFORE).

## Klíčové slovo LINESEARCHSTR

Udává řetězec, který se má vyhledávat v řádcích.

### Poznámka:

Hodnota klíčového slova LINESEARCHSTR se vyhledává pouze v části napravo od rovnítko.

## Klíčové slovo LINELOCATION

LINELOCATION určuje, kam se má do řádku přidat řetězec, zadaný v klíčovém slově ADDSTR.

Předvolená hodnota END znamená, že operační systém i5/OS přidá řetězec na konec řádku. Chcete-li, aby operační systém i5/OS přidal řetězec na začátek řádku, zadejte hodnotu BEGIN.

## Klíčové slovo FILESEARCHPOS (typ záznamu ADDCONFIG)

Nastavte předvolbu pro určení, kam se má umístit řádek ve vztahu k vyhledanému řetězci. Můžete zadat:

- AFTER - jestliže chcete, aby operační systém i5/OS přidal tento řádek za řádek, který obsahuje hledaný řetězec. (AFTER je předvolená hodnota, pokud jste nenastavili jinou předvolbu pomocí záznamu SETDEFAULTS v tomto členu.)
- BEFORE - jestliže chcete, aby operační systém i5/OS přidal tento řádek před řádek, který obsahuje hledaný řetězec.

## Klíčové slovo FILESEARCHSTR

FILESEARCHSTR ve spojení s klíčovým slovem REPLACEOCC určuje, který řádek se má nahradit. Jako hodnotu musíte uvést celý řádek.

Jestliže přidáváte nový řádek, můžete jako hodnotu FILESEARCHSTR zadat libovolnou část řádku, kterou chcete vyhledat.

Toto klíčové slovo nemá předvolenou hodnotu, pokud jste předvolbu nenastavili pomocí záznamu SETDEFAULTS v tomto členu.

## Klíčové slovo FILESEARCHSTROCC

FILESEARCHSTROCC určuje, který výskyt řetězce, jenž se v souboru vyskytuje vícekrát, se má použít při umístění nového řádku.

Předvolená hodnota LAST znamená poslední výskyt hledaného řetězce. Pokud chcete, aby operační systém i5/OS použil první výskyt řetězce, zadejte hodnotu FIRST.

## Klíčové slovo REPLACEOCC

REPLACEOCC určuje, který výskyt řádku se má nahradit.

- Zadáte-li hodnotu LAST, operační systém i5/OS nahradí poslední výskyt hledaného řetězce.
- Zadáte-li ALL, operační systém i5/OS nahradí všechny výskyty hledaného řetězce.
- Při zadání FIRST operační systém i5/OS nahradí první výskyt hledaného řetězce.

Pomocí klíčového slova FILESEARCHSTR specifikujte celý řádek, který chcete nahradit.

Operační systém i5/OS vymaže ze souboru řádek, který se shoduje s hledaným řetězcem (FILESEARCHSTR) a namísto něho přidá hodnoty klíčových slov VAR a ADDSTR.

### Poznámka:

REPLACEOCC má přednost před LOCATION a FILESEARCHPOS. Jestliže operační systém i5/OS nenajde řetězec uvedený v klíčovém slově FILESEARCHSTR ve spojení s REPLACEOCC, přidá nový řádek na základě hodnoty klíčového slova LOCATION, ale nenahradí žádný jiný řádek.

## Klíčové slovo TARGETDIR

TARGETDIR slouží ke specifikaci cesty k souboru integrovaného serveru, který chcete změnit.

Pokud jste nezměnili předvolbu pro toto klíčové slovo pomocí záznamu SETDEFAULTS, musíte zadat cestu k souboru UNATTEND.TXT nebo ke svému vlastním souboru integrovaného serveru. (Toto klíčové slovo má předvolbu BOOT, která určuje, že operační systém i5/OS má změnit soubor v kořenovém adresáři jednotky C.)

### Poznámky:



1. Podporu konfiguračních souborů NWSD mají pouze předdefinované diskové jednotky formátované jako FAT. Paměťové soubory, které byly převedeny na systém souborů NTFS, nejsou pro konfigurační soubory dostupné. Další informace najdete v tématu “Předdefinované diskové jednotky pro integrované Windows servery” na stránce 154.
2. Když měníte soubor, operační systém i5/OS použije pouze první adresář uvedený pro tento soubor. Veškeré další záznamy, které uvádějí jiný adresář, jsou ignorovány.

## Klíčové slovo TARGETFILE

TARGETFILE slouží ke specifikaci souboru integrovaného serveru, který chcete změnit. Hodnota UNATTEND.TXT určuje, že operační systém i5/OS změní soubor se skriptem pro neobsluhovanou instalaci integrovaného serveru.

Pokud jste nezměnili předvolbu pro toto klíčové slovo pomocí záznamu SETDEFAULTS, musíte zadat soubor UNATTEND.TXT nebo svůj vlastní soubor integrovaného serveru. (Toto klíčové slovo má předvolbu CONFIG.SYS.)

## Klíčové slovo UNIQUE

Zadejte YES, pokud chcete povolit pouze jeden výskyt řádku v souboru.

Předvolená hodnota NO určuje, že je povoleno více výskytů řádku v souboru.

## Klíčové slovo VAROCC

VAROCC určuje, který výskyt dané proměnné chcete změnit.

Chcete-li změnit poslední výskyt této proměnné, můžete ponechat předvolenou hodnotu. Chcete-li změnit první výskyt, zadejte FIRST.

## Klíčové slovo VARVALUE

VARVALUE použijte, jestliže chcete, aby se řádek změnil pouze tehdy, obsahuje-li tuto konkrétní vámi zadanou hodnotu proměnné.

Můžete zadat celý řetězec nebo jeho část z pravé strany výrazu, který chcete změnit.

---

## Změna souboru integrovaného Windows serveru pomocí typu záznamu UPDATECONFIG

Pomocí typu záznamu UPDATECONFIG můžete měnit soubor integrovaného Windows serveru následujícími způsoby:

- Přidat řetězce do řádků v souboru.
- Přidat nové řetězce před nebo za určitý řetězec.
- Odstranit řetězce z řádků v souboru.
- Specifikovat cestu k souboru, která se má změnit.

Chcete-li změnit soubor integrovaného serveru, vytvořte konfigurační soubor NWSD, který bude obsahovat typ záznamu UPDATECONFIG, takto:

```
UPDATECONFIG
VAR                = '<jméno_proměnné>',          (povinné)
ADDSTR             = '<řádek_ke_zpracování>',     (povinné)
ADDWHEN           = '<ALWAYS|NEVER|<výraz>>',    (volitelné)
DELETEWHEN       = '<NEVER|ALWAYS|<výraz>>',    (volitelné)
LINECOMMENT       = '<"REM "|<řetězec_komentáře>>', (volitelné)
LINELOCATION       = '<END|BEGIN>',               (volitelné)
LINESEARCHPOS    = '<AFTER|BEFORE>',            (volitelné)
LINESEARCHSTR     = '<řetězec_v_řádku>',        (volitelné)
FILESEARCHPOS    = '<AFTER|BEFORE>',            (volitelné)
FILESEARCHSTR     = '<vyhledávací_řetězec>',     (volitelné)
```

```

FILESEARCHSTROCC = '<LAST|FIRST>', (volitelně)
TARGETDIR        = '<BOOT|<cesta>>', (volitelně)
TARGETFILE       = '<CONFIG.SYS|<jméno_souboru>>', (volitelně)
VAROCC           = '<LAST|FIRST>', (volitelně)
VARVALUE         = '<hodnota_proměnné>' (volitelně)

```

Podrobný popis klíčových slov u UPDATECONFIG najdete pod následujícími odkazy. Můžete se také vrátit na téma “Formát konfiguračního souboru NWS D” na stránce 235 nebo na téma “Nastavení konfiguračních předvoleb pomocí typu záznamu SETDEFAULTS” na stránce 244.

- “Klíčové slovo VAR” na stránce 239
- “Klíčové slovo ADDSTR” na stránce 239
- “Klíčové slovo ADDWHEN” na stránce 239
- “Klíčové slovo DELETEWHEN” na stránce 240
- “Klíčové slovo LINECOMMENT” na stránce 240
- “Klíčové slovo LINELOCATION” na stránce 240
- “Klíčové slovo LINESEARCHPOS” na stránce 240
- “Klíčové slovo LINESEARCHSTR” na stránce 240
- “Klíčové slovo FILESEARCHPOS (typ záznamu UPDATECONFIG)”
- “Klíčové slovo FILESEARCHSTR (typ záznamu UPDATECONFIG)”
- “Klíčové slovo FILESEARCHSTROCC (typ záznamu UPDATECONFIG)”
- “Klíčové slovo TARGETDIR” na stránce 241
- “Klíčové slovo TARGETFILE” na stránce 242
- “Klíčové slovo VAROCC” na stránce 242
- “Klíčové slovo VARVALUE” na stránce 242

## Klíčové slovo FILESEARCHPOS (typ záznamu UPDATECONFIG)

FILESEARCHPOS udává, který výskyt proměnné má operační systém i5/OS vyhledat ve vztahu k řádku, který obsahuje hledaný řetězec. Použijte hodnoty:

- AFTER - jestliže chcete, aby operační systém i5/OS vyhledal první výskyt proměnné v řádku, který obsahuje hledaný řetězec, nebo za tímto řádkem. (AFTER je předvolená hodnota, pokud jste nenastavili jinou předvolbu pomocí záznamu SETDEFAULTS v tomto členu.)
- BEFORE - jestliže chcete, aby operační systém i5/OS vyhledal první výskyt proměnné v řádku, který obsahuje hledaný řetězec, nebo před tímto řádkem.

### Poznámka:

Pokud operační systém i5/OS nenajde hledaný řetězec, určí řádek, který se má změnit, podle klíčového slova VAROCC.

## Klíčové slovo FILESEARCHSTR (typ záznamu UPDATECONFIG)

FILESEARCHSTR slouží ke specifikaci vyhledávacího řetězce, který má operační systém i5/OS použít při hledání místa výskytu proměnné, kterou chcete nahradit.

Toto klíčové slovo nemá předvolenou hodnotu, pokud jste předvolbu nenastavili pomocí záznamu SETDEFAULTS v tomto členu.

## Klíčové slovo FILESEARCHSTROCC (typ záznamu UPDATECONFIG)

FILESEARCHSTROCC určuje, který výskyt řetězce, jenž se v souboru vyskytuje vícekrát, se má použít při vyhledávání řádků, které se mají změnit.

Zadáte-li hodnotu LAST, operační systém i5/OS použije poslední výskyt hledaného řetězce. Chcete-li, aby operační systém i5/OS použil

---

## Nastavení konfiguračních předvoleb pomocí typu záznamu SETDEFAULTS

Pro určitá klíčová slova u typu záznamů ADDCONFIG a UPDATECONFIG můžete nastavit předvolené hodnoty pomocí typu záznamu SETDEFAULTS. Předvolby je možné nastavit pro následující operace:

- Přidávání a mazání řádků.
- Vyhledávání řádků.
- Určení jména a cesty souboru, který se má změnit.

Chcete-li definovat předvolené hodnoty, vytvořte konfigurační soubor NWSD, který bude obsahovat typ záznamu SETDEFAULTS, takto:

```
SETDEFAULTS
ADDWHEN      = '<ALWAYS|NEVER|<výraz>>',      (volitelně)
DELETEWHEN   = '<NEVER|ALWAYS|<výraz>>',      (volitelně)
FILESEARCHPOS = '<AFTER|BEFORE>',              (volitelně)
FILESEARCHSTR = '<vyhledávací_řetězec>',         (volitelně)
TARGETDIR     = '<cesta>',                      (volitelně)
TARGETFILE    = '<jméno_souboru>'              (volitelně)
```

Podrobné vysvětlení klíčových slov v záznamu SETDEFAULTS najdete v níže uvedených částech:

- “ADDWHEN”
- “DELETEWHEN”
- “Klíčové slovo FILESEARCHPOS (typ záznamu SETDEFAULTS)” na stránce 245
- “Klíčové slovo FILESEARCHSTR (typ záznamu SETDEFAULTS)” na stránce 245
- “TARGETDIR” na stránce 245
- “TARGETFILE” na stránce 245

### ADDWHEN

ADDWHEN ve spojení s typem záznamu SETDEFAULTS nastavuje předvolenou hodnotu pro klíčové slovo ADDWHEN u typů záznamů ADDCONFIG a UPDATECONFIG.

Nastavte předvolbu pro určení, ve kterém okamžiku zpracování má operační systém i5/OS přidat do souboru nový řádek nebo řetězec. Můžete zadat:

- ALWAYS - jestliže chcete, aby operační systém i5/OS přidal tento řádek nebo řetězec pokaždé, když zpracovává konfigurační soubor. (ALWAYS je předvolená hodnota, pokud nezádáte jinou předvolbu.)
- NEVER - jestliže chcete, aby operační systém i5/OS nikdy nepřidal tento řádek nebo řetězec.
- Výraz, na jehož základě operační systém i5/OS přidá řádek nebo řetězec při splnění (=TRUE) zadané podmínky. Výrazy se skládají z operátorů a operandů (viz “Operátory ve výrazech používané u klíčových slov ADDWHEN a DELETEWHEN” na stránce 239) a musí vracet hodnotu TRUE nebo FALSE.

#### Poznámka:

Jestliže nechcete, aby operační systém i5/OS interpretoval některý výraz (například výraz obsahující hvězdičku (\*)) jako matematickou operaci, ohraničte tento výraz uvozovkami. Například k přidání řádku u NWSD typu \*WINDOWSNT můžete napsat:

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

### DELETEWHEN

DELETEWHEN ve spojení s typem záznamu SETDEFAULTS nastavuje předvolenou hodnotu pro klíčové slovo DELETEWHEN u typů záznamů ADDCONFIG a UPDATECONFIG.

Nastavte předvolbu pro určení, ve kterém okamžiku zpracování má operační systém i5/OS vymazat ze souboru řádek nebo řetězec.

Můžete zadat:

- ALWAYS - jestliže chcete, aby operační systém i5/OS vymazal tento řádek nebo řetězec pokaždé, když zpracovává konfigurační soubor.
- NEVER - jestliže chcete, aby operační systém i5/OS nikdy nemazal tento řádek nebo řetězec. (NEVER je předvolená hodnota, pokud nezádáte jinou předvolbu.)
- Výraz, na jehož základě operační systém i5/OS vymaže řádek nebo řetězec při splnění (=TRUE) zadané podmínky. Výrazy se skládají z operátorů a operandů (viz "Operátory ve výrazech používané u klíčových slov ADDWHEN a DELETEWHEN" na stránce 239) a musí vracet hodnotu TRUE nebo FALSE.

**Poznámka:**

Jestliže nechcete, aby operační systém i5/OS interpretoval některý výraz (například výraz obsahující hvězdičku (\*)) jako matematickou operaci, ohraničte tento výraz uvozovkami. Například k odstranění řádku u NWSN typu \*WINDOWSNT můžete napsat:

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

## Klíčové slovo FILESEARCHPOS (typ záznamu SETDEFAULTS)

FILESEARCHPOS ve spojení s typem záznamu SETDEFAULTS nastavuje předvolenou hodnotu pro klíčové slovo FILESEARCHPOS u typů záznamů ADDCONFIG a UPDATECONFIG.

Nastavte předvolbu pro určení, kam se má umístit řádek ve vztahu k vyhledanému řetězci. Můžete zadat:

- AFTER - jestliže chcete, aby byl daný řádek umístěn za řádek, který obsahuje hledaný řetězec. (AFTER je předvolená hodnota, pokud nezádáte jinou předvolbu.)
- BEFORE - jestliže chcete, aby operační systém i5/OS přidal tento řádek před řádek, který obsahuje hledaný řetězec.

## Klíčové slovo FILESEARCHSTR (typ záznamu SETDEFAULTS)

FILESEARCHSTR ve spojení s typem záznamu SETDEFAULTS nastavuje předvolenou hodnotu pro klíčové slovo FILESEARCHSTR u typů záznamů ADDCONFIG a UPDATECONFIG.

Jako hodnotu FILESEARCHSTR můžete zadat libovolnou část řádku, kterou chcete vyhledat.

## TARGETDIR

TARGETDIR ve spojení s typem záznamu SETDEFAULTS nastavuje předvolenou hodnotu pro klíčové slovo TARGETDIR u typů záznamů ADDCONFIG a UPDATECONFIG.

Cesta udává adresář, ve kterém se nachází soubor, který se má zpracovávat.

Chcete-li například nastavit jako předvolbu pro TARGETDIR soubor na jednotce D, napište tento záznam:

```
SETDEFAULTS TARGETDIR = 'D:\'
```

## TARGETFILE

TARGETFILE ve spojení s typem záznamu SETDEFAULTS nastavuje předvolenou hodnotu pro klíčové slovo TARGETFILE u typů záznamů ADDCONFIG a UPDATECONFIG.

Jméno udává soubor, který se má zpracovávat.

Chcete-li například nastavit jako předvolbu pro TARGETFILE soubor UNATTEND.TXT na jednotce D, napište tento záznam:

```
SETDEFAULTS  
TARGETDIR = 'D:\',  
TARGETFILE = 'UNATTEND.TXT'
```

## Použití substitučních proměnných pro hodnoty klíčových slov

Pro hodnoty klíčových slov můžete použít substituční proměnné. Konfigurační soubor NWSD nahradí tyto proměnné správnými hodnotami. Tyto substituční proměnné se konfiguruji na základě hodnot uložených v NWSD nebo hardwaru, který je detekován u NWSD.

Operační systém i5/OS dodává tyto proměnné:

Substituční proměnná	Popis
%FPAIPADDRPP%	TCP/IP adresa (NWSD Port *VRTETHPTP) *
%FPAIPADDR01%	TCP/IP adresa (NWSD Port 1) *
%FPAIPADDR02%	TCP/IP adresa (NWSD Port 2) *
%FPAIPADDR03%	TCP/IP adresa (NWSD Port 3) *
%FPASUBNETPP%	TCP/IP adresa podsítě (NWSD Port *VRTETHPTP) *
%FPASUBNET01%	TCP/IP adresa podsítě (NWSD Port 1) *
%FPASUBNET02%	TCP/IP adresa podsítě (NWSD Port 2) *
%FPASUBNET03%	TCP/IP adresa podsítě (NWSD Port 3) *
%FPATCPHOSTNAME%	Hostitelské jméno TCP/IP
%FPATCPDOMAIN%	Jméno domény TCP/IP
%FPATCPDNSS%	DNS TCP/IP, oddělené čárkami
%FPATCPDNS01%	Server jmen domény TCP/IP 1
%FPATCPDNS02%	Server jmen domény TCP/IP 2
%FPATCPDNS03%	Server jmen domény TCP/IP 3
%FPANWSDTYPE%	Typ NWSD, který logicky zapínáte
%FPANWSDNAME%	Jméno NWSD, který logicky zapínáte
%FPACARDTYPE%	Prostředek NWSD, který logicky zapínáte (2890, 2892, 4812, 2689, iSCSI)
%FPAINSMEM%	Zjištěná velikost instalované paměti
%FPAUSEMEM%	Zjištěná velikost využitelné paměti
%FPACODEPAGE%	Kódová stránka ASCII, použitá k překladu z EBCDIC
%FPALANGVERS%	Jazyková verze operačního systému i5/OS použitá pro NWSD
%FPASYSDDRIVE%	Písmeno jednotky používané jako systémová (C, nebo E - u systému instalovaného ve verzi V4R4 nebo starší)
%FPA_CARET%	Symbol stříška (^)
%FPA_L_BRACKET%	Symbol levá lomená závorka ([)
%FPA_R_BRACKET%	Symbol pravá lomená závorka
%FPA_PERCENT%	Symbol procento (%) Poznámka: Vzhledem k tomu, že symbol procenta slouží u substitučních proměnných jako oddělovač, měla by být tato substituční proměnná použita, když řetězec obsahuje symbol procenta, který by NEMĚL být interpretován jako oddělovač.
%FPABOOTDRIVE%	Toto je vždy jednotka E pro server IXS (Integrated xSeries Server)
%FPACFGFILE%	Jméno zpracovávaného konfiguračního souboru NWSD
%FPACFGLIB%	Knihovna, která obsahuje zpracovávaný konfigurační soubor NWSD
%FPACFGMBR%	Jméno zpracovávaného členu konfiguračního souboru NWSD
<b>* Hodnoty se načítají z NWSD</b>	

Můžete definovat i další substituční proměnné - vytvořte soubor v knihovně QUSRSYS a pojmenujte jej jménem NWSDD, k němuž přidáte příponu 'VA'. Tento soubor musíte vytvořit jako zdrojový fyzický soubor s minimální délkou věty 16 a maximální délkou věty 271.

Na příkazový řádek operačního systému i5/OS můžete například napsat:

```
CRTSRCPF FILE(QUSRSYS/nwsddnameVA) RCDLEN(271)
      MBR(nwsddname) MAXMBRS(1)
      TEXT('Configuration file variables')
```

Člen 'nwsddname' obsahuje data ve sloupcích s pevně stanoveným formátem:

- Ve sloupci 1-15 - jméno proměnné doplněné mezerami a
- Ve sloupci 16 - začíná hodnota

Například:

```
Sloupcy:
1234567890123456789012345678901234567890... myaddr          9.5.9.1
```

V tomto příkladu se do seznamu substitučních proměnných přidá proměnná %myaddr%, která má hodnotu "9.5.9.1".







---

## Kapitola 16. Související informace

Níže jsou uvedeny publikace týkající se serveru iSeries a Červené knihy IBM Redbooks (ve formátu PDF), webové servery a témata z aplikace Information Center, která souvisejí s tématem Prostředí Windows na serveru iSeries. Kterýkoli z těchto souborů PDF si můžete zobrazit nebo vytisknout.

### Publikace







- iSeries Performance Capabilities Reference 
- Zálohování a obnova 
- Pokyny pro instalaci hardwaru. Viz téma “Instalace komponent iSeries”.

### Červené knihy (www.redbooks.ibm.com)

Microsoft Windows Server 2003 Integration with iSeries, SG24-6959 

| IBM xSeries and BladeCenter Server Management, SG24-6495 

### Webové stránky

- | • Nejnovější informace o produktech a službách: 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).



---

## Dodatek. Poznámky

Tyto informace platí pro produkty a služby nabízené v USA.

IBM nemusí nabízet produkty, služby nebo vlastnosti zmiňované v tomto dokumentu v jiných zemích. Informace o produktech a službách, které jsou momentálně ve vaší zemi dostupné, můžete získat od zástupce IBM pro vaši zemi. Žádný odkaz na produkt, program nebo službu IBM není zamýšlen jako prohlášení nebo naznačení toho, že smí být používán pouze tento produkt, program nebo služba IBM. Místo toho je možné použít jakýkoliv z hlediska funkčnosti ekvivalentní produkt, program nebo službu, které neporušují žádné z práv IBM na duševní vlastnictví. Za vyhodnocení a ověření činnosti libovolného produktu, programu či služby jiného výrobce než IBM však odpovídá uživatel.

IBM může mít patenty nebo podané žádosti o patent, které zahrnují předmět tohoto dokumentu. Vlastnictví tohoto dokumentu vám nedává žádná práva k těmto patentům. Písemné dotazy ohledně licencí můžete zaslat na adresu:

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

Pokud máte zájem o licenci v zemi s dvoubajtovou znakovou sadou (DBCS), kontaktujte oddělení IBM Intellectual Property Department ve Vaší zemi, nebo se obraťte písemně na adresu:

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

**Následující odstavec se netýká Velké Británie nebo kterékoliv jiné země, kde taková opatření odporují místním zákonům:** SPOLEČNOST INTERNATIONAL BUSINESS MACHINES CORPORATION TUTO PUBLIKACI POSKYTUJE TAKOVOU, "JAKÁ JE", BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK NEPORUŠENÍ PRÁV TŘETÍCH STRAN, ZÁRUKY PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Právní řady některých zemí nepřipouštějí vyloučení vyjádřených nebo odvozených záruk v určitých transakcích a proto se na vás výše uvedené omezení nemusí vztahovat.

Tato publikace může obsahovat technické nepřesnosti nebo typografické chyby. Informace zde uváděné jsou pravidelně aktualizovány a v příštích vydáních této publikace již budou tyto změny zahrnuty. IBM má právo kdykoliv bez upozornění zdokonalovat nebo měnit produkty a programy popsané v této publikaci.

Jakékoliv odkazy v této publikaci na webové stránky jiných společností než IBM jsou poskytovány pouze pro pohodlí uživatele a nemohou být žádným způsobem vykládány jako doporučení těchto webových stránek ze strany IBM. Materiály obsažené na takovýchto webových stránkách nejsou součástí materiálů k tomuto produktu IBM a tyto webové stránky mohou být používány pouze na vlastní nebezpečí.

IBM může použít nebo distribuovat jakékoliv informace, které jí sdělíte, libovolným způsobem, který IBM považuje za odpovídající, aniž by tím vznikl jakýkoliv závazek IBM vůči vám.

Držitelé licence na tento program, kteří si přejí mít přístup i k informacím o programu za účelem (i) výměny informací mezi nezávisle vytvořenými programy a jinými programy (včetně tohoto) a (ii) vzájemného použití sdílených informací, mohou kontaktovat:

IBM Corporation  
Software Interoperability Coordinator, Department YBWA  
3605 Highway 52 N

Rochester, MN 55901  
U.S.A.

Informace tohoto typu mohou být dostupné za určitých podmínek. V některých případech připadá v úvahu zaplacení poplatku.

- | Licencovaný program popsany v těchto informacích a veškeré dostupné licencované materiály poskytuje IBM na
- | základě podmínek uvedených ve smlouvách ICA (IBM Customer Agreement), IPLA (IBM International Program
- | License Agreement), ILAMC (IBM License Agreement for Machine Code) nebo v jiné ekvivalentní smlouvě.

Všechna zde obsažená data týkající se výkonu byla zjištěna v řízeném prostředí. Výsledky získané v jiných provozních prostředích se proto mohou výrazně lišit. Některá měření mohla být prováděna v systémech na úrovni vývoje a nelze tedy zaručit, že tato měření budou ve všeobecně dostupných systémech stejná. Kromě toho mohla být některá měření odhadnuta prostřednictvím extrapolace. Skutečné výsledky se mohou lišit. Uživatelé tohoto dokumentu by si měli ověřit použitelnost dat pro svoje specifické prostředí.

Veškerá prohlášení týkající se budoucích trendů nebo strategií IBM podléhají změnám bez předchozího upozornění a představují pouze cíle a záměry.

Pokud si tyto informace prohlížíte ve formátu softcopy, fotografie a barevné ilustrace se nemusí zobrazit.

---

## Ochranné známky

Níže uvedené výrazy jsou ochrannými známkami společnosti International Business Machines Corporation ve Spojených státech anebo jiných zemích.

AIX  
AS/400  
BladeCenter  
DB2  
IBM  
iSeries  
Netfinity  
NetServer  
OS/400  
i5/OS  
PAL  
Redbooks  
ServerGuide  
Virtualization Engine  
xSeries

Pentium je ochranná známka nebo registrovaná ochranná známka společnosti Intel Corporation ve Spojených státech a případně v dalších jiných zemích.

- | Linux je ochranná známka, jejímž majitelem je Linus Torvalds, ve Spojených státech a případně v dalších jiných
- | zemích.

Microsoft, Windows, Windows NT a logo Windows jsou ochranné známky společnosti Microsoft Corporation ve Spojených státech a případně v dalších jiných zemích.

Ostatní jména společností, produktů a služeb mohou být ochrannými známkami nebo servisními značkami jiných firem.

---

## Ustanovení a podmínky

Oprávnění k užívání těchto publikací je uděleno na základě následujících ustanovení a podmínek.

**Osobní použití:** Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat pro své osobní nekomerční použití. Tyto publikace ani jakékoli jejich části nesmíte bez výslovného souhlasu IBM distribuovat, prezentovat ani z nich vytvářet odvozená díla.

**Komerční použití:** Pokud zachováte všechny výhrady týkající se vlastnických práv, můžete tyto publikace kopírovat, distribuovat a prezentovat výhradně uvnitř svého podniku. Bez výslovného souhlasu IBM nesmíte z těchto publikací vytvářet odvozená díla ani je (nebo jejich části) nesmíte kopírovat, distribuovat či prezentovat mimo rámec svého podniku.

Kromě oprávnění, která jsou zde výslovně udělena, se na publikace nebo jakékoli informace, data, software a další duševní vlastnictví obsažené v těchto publikacích nevztahují žádná další vyjádřená ani odvozená oprávnění, povolení či práva.

IBM si vyhrazuje právo odvolat oprávnění zde udělená, kdykoli usoudí, že používání publikací poškozuje jeho zájmy nebo že výše uvedené pokyny nejsou řádně dodržovány.

Tyto informace můžete stahovat, exportovat či reexportovat pouze při dodržení všech příslušných zákonů a nařízení včetně veškerých vývozních zákonů a nařízení USA.

IBM NEPOSKYTUJE ŽÁDNOU ZÁRUKU, POKUD JDE O OBSAH TĚCHTO PUBLIKACÍ. TYTO PUBLIKACE JSOU POSKYTOVÁNY NA BÁZI "JAK JSOU" (AS-IS), BEZ JAKÝCHKOLIV ZÁRUK, VYJÁDŘENÝCH NEBO ODVOZENÝCH VČETNĚ, BEZ OMEZENÍ, ODVOZENÝCH ZÁRUK PRODEJNOSTI, NEPORUŠENÍ PRÁV TŘETÍCH STRAN NEBO ZÁRUKY VHODNOSTI PRO URČITÝ ÚČEL.









Vytištěno v Dánsku společností IBM Danmark A/S.