IBM

eserver

iSeries

Rady a nástroje pro zabezpečení serveru iSeries

Verze 5

SC09-3653-07

IBM

@server

iSeries

Rady a nástroje pro zabezpečení serveru iSeries

Verze 5

SC09-3653-07

Poznámka

Dříve, než použijete tyto informace a produkt, který podporují, si nezapomeňte přečíst online informace uvedené v tématu “Poznámky” na stránce 153.

Osmé vydání (Duben 2004)

Toto vydání se týká verze 5, vydání 3, modifikace 0 licenčního programu IBM Operating System/400 (produkt 5722-SS1) a všech následujících vydání a modifikací, dokud nebude v nových vydáních uvedeno jinak. Tato verze nefunguje na všech modelech počítačů RISC (reduced instruction set computer) ani na modelech CISC models.

Toto vydání nahrazuje SC09-3653-06.

Obsah

Obrázky vii

Tabulky ix

Rady a nástroje pro zabezpečení serveru iSeries (SC09-3653-07) xi

Kdo by měl číst tuto knihu xi
Jak používat tyto informace xii
Nezbytné předchozí a související informace xii
Jak posílat připomínky xiii

Část 1. Základní zabezpečení serveru iSeries 1

Kapitola 1. Základní prvky zabezpečení serveru iSeries 3

Úrovně zabezpečení 3
Globální nastavení 4
Uživatelské profily 4
Skupinové profily 5
Zabezpečení na úrovni prostředků 5
Omezený přístup k funkci programů 5
Monitorování zabezpečení 7
Příklad: sestava atributů zabezpečení systému 7

Kapitola 2. Programy iSeries Security Wizard a eServer Security Planner . . . 11

Security Wizard 11
eServer Security Planner 13

Kapitola 3. Řízení interaktivního přihlášení 15

Stanovení pravidel pro hesla 15
Úrovně hesla 16
Plánování změn úrovně hesla 16
Změna známých hesel 20
Nastavení hodnot pro přihlášení 22
Změna chybových zpráv pro přihlášení 22
Plánování dostupnosti uživatelských profilů 23
Odstranění neaktivních uživatelských profilů 24
Automatická deaktivace uživatelských profilů . . . 24
Automatické odstranění uživatelských profilů . . . 24
Jak zabránit používání předvolených hesel 25
Monitorování aktivit souvisejících s přihlašováním a hesly 26
Uložení informací o heslech 26

Kapitola 4. Jak nakonfigurovat server iSeries, aby používal nástroje zabezpečení 27

Bezpečné ovládání nástrojů zabezpečení 27
Jak předejít konfliktům mezi soubory 27
Uložení nástrojů zabezpečení 28
Příkazy a menu pro nástroje zabezpečení 28
Volby menu Security Tools 28
Použití menu Security Batch 30
Příkazy pro přizpůsobení zabezpečení 35
Hodnoty nastavované příkazem konfigurace zabezpečení systému 35
Funkce příkazu Vyvolání obecného oprávnění . . . 37

Část 2. Rozšířené zabezpečení serveru iSeries 39

Kapitola 5. Ochrana informačních hodnot prostřednictvím oprávnění k objektům 41

Prosazení oprávnění k objektu 41
Zabezpečení na úrovni menu 41
Omezení řízení přístupu prostřednictvím menu . . . 42
Zdokonalení řízení přístupu prostřednictvím menu pomocí zabezpečení na úrovni objektů 42
Příklad: nastavení přechodného prostředí 43
Použití zabezpečení na úrovni knihoven jako doplňku k zabezpečení na úrovni menu 44
Konfigurování vlastnictví objektů 45
Oprávnění k objektu pro systémové příkazy a programy 45
Monitorování funkcí zabezpečení 45
Analýza uživatelských profilů 46
Analýza oprávnění k objektům 48
Kontrola změněných objektů 48
Analýza programů, které přebírají oprávnění 49
Správa monitorovacího žurnálu a příjemců žurnálu . . 49

Kapitola 6. Správa oprávnění 51

Monitorování veřejného oprávnění k objektům 51
Správa oprávnění pro nové objekty 52
Monitorování seznamů oprávnění 52
Použití seznamů oprávnění 53
Metody přístupu v prostředí produktu iSeries Navigator 54
Monitorování soukromých oprávnění k objektům . . . 55
Monitorování přístupu k výstupním frontám a k frontám úloh 55
Monitorování zvláštních oprávnění 56
Monitorování uživatelských prostředí 57
Správa servisních nástrojů 58

Kapitola 7. Použití zabezpečení logických částí (LPAR) 61

Správa zabezpečení pro logické části 62

Kapitola 8. Produkt iSeries Operations Console 63

Přehled zabezpečení produktu Operations Console . . . 64

Autentizace zařízení konzole 64
Autentizace uživatele 64
Utajení dat 64
Integrita dat 64
Použití produktu Operations Console s připojitelností přes LAN 65
Ochrana produktu Operations Console s připojitelností přes LAN 65
Použití průvodce nastavením produktu Operations Console 65

Kapitola 9. Detekce podezřelých programů 67
Ochrana proti počítačovým virům 67
Monitorování použití adoptovaného oprávnění 68
Omezení použití adoptovaného oprávnění 69
Jak předejít tomu, aby nové programy používaly adoptované oprávnění 70
Monitorování použití triggerů 71
Kontrola skrytých programů 72
Ohodnocení registrovaných ukončovacích programů . . 74
Kontrola naplánovaných programů 74
Omezení schopnosti provádět uložení a obnovu 75
Kontrola uživatelských objektů v chráněných knihovnách 75

Kapitola 10. Prevence a detekce pirátských pokusů 77
Fyzické zabezpečení 77
Monitorování aktivity uživatelského profilu 77
Podepisování objektů 78
Monitorování popisů podsystémů 79
Záznamy automaticky spuštěných úloh 79
Jména a typy pracovních stanic 79
Záznamy front úloh 80
Záznamy směrování 80
Záznamy komunikací a jména vzdálených systémů . . . 80
Záznamy předspuštěných úloh 81
Úlohy a popisy úloh 81
Jména TPN architektury 82
Požadavky na jména TPN architektury 82
Metody monitorování událostí týkajících se zabezpečení 84

Část 3. Aplikace a síťové komunikace 85

Kapitola 11. Použití integrovaného systému souborů k zabezpečení souborů 87
Přístup k zabezpečení z hlediska integrovaného systému souborů 87
Systémy souborů root (/), QOpenSys a uživatelem definované systémy souborů 89
Jak funguje oprávnění 89
Příkaz PRTPVTAUT (Tisk soukromých oprávnění k objektům) 91
Příkaz PRTPUBAUT (Tisk veřejně oprávněných objektů) 92
Omezení přístupu k systému souborů QSYS.LIB 93
Zabezpečení adresářů 94
Zabezpečení pro nové objekty 94
Použití příkazu Vytvoření adresáře 94
Vytvoření adresáře pomocí rozhraní API 95
Vytvoření proudového souboru pomocí rozhraní open() nebo creat() API 95
Vytvoření objektu pomocí rozhraní PC 95
Systém souborů QFileSvr.400 95
Síťový systém souborů 96

Kapitola 12. Zabezpečení komunikace APPC 99
Terminologie APPC 99
Základní prvky komunikace APPC 99
Příklad: základní relace APPC 100
Omezení relací APPC 100
Přístup uživatelů APPC k cílovému systému 101
Systémové metody pro posílání informací o uživateli 101
Možnosti rozdělení odpovědnosti za zabezpečení sítě 102
Přiřazení uživatelských profilů pro úlohy prováděné cílovým systémem 103
Volby přímého průchodu na obrazovkovou stanici . . . 104
Jak se vyvarovat neočekávaných přiřazení zařízení . . . 105
Řízení vzdálených příkazů a dávkových úloh 105
Ohodnocení vaší konfigurace APPC 106
Důležité parametry pro zařízení APPC 106
Parametry pro řadiče APPC 108
Parametry pro popisy linky 109

Kapitola 13. Zabezpečení komunikace TCP/IP 111
Jak zabránit zpracování TCP/IP 111
Komponenty zabezpečení TCP/IP 111
Použití pravidel paketu pro zabezpečení provozu TCP/IP 112
HTTP proxy server 112
Vytváření virtuálních soukromých sítí (VPN) . . . 112
SSL 113
Zabezpečení vašeho prostředí TCP/IP 113
Jak určit, které servery TCP/IP se mají spouštět automaticky 114
Pokyny k zabezpečení při používání SLIP 115
Řízení spojení příchozích hovorů po komutované lince s využitím SLIP 116
Řízení odchozích relací 117
Pokyny k zabezpečení pro protokol PPP 119
Pokyny k zabezpečení při používání serveru Bootstrap Protocol 120
Jak zabránit v přístupu BOOTP 120
Zabezpečení serveru BOOTP 121
Pokyny k zabezpečení při používání serveru DHCP . . 121
Jak zabránit v přístupu DHCP 121
Zabezpečení serveru DHCP 122
Pokyny k zabezpečení při používání serveru TFTP . . 123
Jak zabránit v přístupu TFTP 123
Zabezpečení serveru TFTP 123
Pokyny k zabezpečení při používání serveru REXEC 124
Jak zabránit v přístupu REXEC 124
Zabezpečení serveru REXEC 125
Pokyny k zabezpečení při používání serveru RouteD . . 125
Pokyny k zabezpečení při používání serveru DNS . . . 126
Jak zabránit v přístupu DNS 126
Zabezpečení serveru DNS 126

Pokyny k zabezpečení při používání serveru HTTP Server for iSeries 127
Jak zabránit v přístupu HTTP 127
Řízení přístupu k serveru HTTP 128
Pokyny k zabezpečení při používání SSL se serverem IBM HTTP Server for iSeries 132
Pokyny k zabezpečení pro LDAP 133
Pokyny k zabezpečení pro LPD 133
Jak zabránit v přístupu LPD 133
Řízení přístupu LPD 134
Pokyny k zabezpečení pro SNMP 134
Jak zabránit v přístupu SNMP 134
Řízení přístupu SNMP 135
Pokyny k zabezpečení pro server INETD 136
Pokyny k zabezpečení pro omezení průchodů TCP/IP 137

Kapitola 14. Zabezpečení přístupu prostřednictvím pracovní stanice . . . 139
Prevence virů z pracovních stanic. 139
Zabezpečení přístupu k datům pracovní stanice . . . 139
Oprávnění k objektu a přístup prostřednictvím pracovní stanice 140
Administrativa aplikací 141
Použití SSL s produktem iSeries Access for Windows 142
Zabezpečení produktu iSeries Navigator 142
Jak zabránit v přístupu ODBC. 143
Pokyny k zabezpečení pro hesla pracovních stanic. . . . 143
Ochrana serveru před vzdálenými příkazy a procedurami 144
Ochrana pracovních stanic před vzdálenými příkazy a procedurami 145
Gateway servery 145
Komunikace přes bezdrátovou síť LAN 146

Kapitola 15. Bezpečnostní ukončovací programy 147

Kapitola 16. Pokyny k zabezpečení pro webové prohlížeče 149
Riziko: poškození pracovní stanice 149
Riziko: přístup k adresářům serveru iSeries prostřednictvím mapovaných jednotek 149
Riziko: důvěryhodné podepsané applety 150

Kapitola 17. Související informace . . 151

Poznámky 153
Ochranné známky 155

Rejstřík 157

Obrázky

1. Příklad sestavy atributů zabezpečení systému . . . 8
2. Obrazovka Schedule Profile Activation – příklad 23
3. Sestava soukromých oprávnění pro seznamy oprávnění 52
4. Sestava zobrazení objektů seznamu oprávnění 53
5. Sestava informací o uživateli: 1. příklad 56
6. Sestava informací o uživateli: 2. příklad 57
7. Tisk uživatelského profilu - příklad uživatelského prostředí 58
8. Příklad sestavy Work with Registration Information 74
9. Popis zařízení APPC - ukázková sestava 106
10. Sestava konfiguračního seznamu - příklad 107
11. Popisy řadiče APPC - ukázková sestava 109
12. Popisy linky APPC - ukázková sestava 110
13. Systém iSeries s gateway serverem 145

Tabulky

1. Systémové hodnoty pro hesla. 15
2. Hesla pro profily dodávané společností IBM 21
3. Hesla pro DST 21
4. Systémové hodnoty pro přihlášení 22
5. Chybové zprávy pro přihlášení 23
6. Příkazy nástrojů pro uživatelské profily 28
7. Příkazy nástrojů pro monitorování zabezpečení 30
8. Příkazy pro sestavy o zabezpečení 31
9. Příkazy pro přizpůsobení systému 35
10. Hodnoty nastavené příkazem CFGSYSSEC 36
11. Příkazy, jejichž veřejné oprávnění se nastavuje pomocí příkazu RVKPUBAUT 38
12. Programy, jejichž veřejné oprávnění se nastavuje pomocí příkazu RVKPUBAUT 38
13. Výsledky šifrování 63
14. Příklad použití adoptovaného oprávnění (USEADPAUT) 70
15. Systémem dodávané ukončovací programy . . . 73
16. Výstupní body pro aktivitu uživatelského profilu 77
17. Programy a uživatelé pro požadavky TPN. 82
18. Hodnoty zabezpečení v architektuře 101
19. Jak spolu fungují hodnota zabezpečení architektury a hodnota SECURELOC 102
20. Možné hodnoty pro parametr předvoleného uživatele 103
21. Ukázky požadavků na přihlášení přímým průchodem 104
22. Jak příkazy TCP/IP určují, které servery se spustí 114
23. Hodnota automatického spuštění pro servery TCP/IP 115
24. Zdroje vzorových ukončovacích programů 147

Rady a nástroje pro zabezpečení serveru iSeries (SC09-3653-07)

Úloha počítačů v organizacích se rychle mění. Správci informačních technologií, dodavatelé softwaru, administrátoři systému i revizoři se nyní musí dívat jiným pohledem na řadu oblastí, které dříve považovali za samozřejmé. V tomto výčtu by nemělo chybět ani zabezpečení serveru iSeries.

Systémy nyní poskytují mnoho nových funkcí, které se nesmírně liší od tradičních účetních aplikací. Uživatelé se dostávají do systémů novými způsoby: prostřednictvím LAN, komutovaných linek (vytáčeného připojení), bezdrátově a pomocí sítí všech možných typů. Uživatelům se často nikdy nezobrazí přihlašovací obrazovka. Velké množství organizací expanduje a rozšiřuje své pole působnosti buď vytvořením soukromých sítí, nebo pomocí Internetu.

Rázem se zdá, jako by systémy měly celou řadu nových dveří a oken. Správci a administrátoři systému mají odůvodněný zájem o to, jak chránit informační zdroje v tomto tak rychle se měnícím prostředí.

Tato publikace poskytuje množinu praktických podnětů pro používání funkcí zabezpečení serveru iSeries a pro vytvoření provozních procedur, které zohledňují zabezpečení. Doporučení v této knize platí pro instalaci s průměrnými požadavky na zabezpečení a průměrným stupněm rizika. Zde uvedené informace neposkytují vyčerpávající popis dostupných funkcí zabezpečení serveru iSeries. Pokud byste si chtěli přečíst informace o dalších volbách nebo potřebujete podrobnější informace, mohou vám být dobrým zdrojem publikace, které popisuje Kapitola 17, “Související informace”, na stránce 151.

Tyto informace také popisují, jak nastavit a používat nástroje pro zabezpečení ochrany dat, které jsou součástí operačního systému OS/400. Referenční informace týkající se nástrojů pro zabezpečení ochrany dat najdete v částech Kapitola 4, “Jak nakonfigurovat server iSeries, aby používal nástroje zabezpečení”, na stránce 27 a “Příkazy a menu pro nástroje zabezpečení” na stránce 28. Najdete zde příklady použití těchto nástrojů.

Kdo by měl číst tuto knihu

Za zabezpečení ochrany dat v systému je odpovědný **správce systému** nebo **administrátor systému**. Tato odpovědnost obvykle zahrnuje následující činnosti:

- Nastavení a správu uživatelských profilů.
- Nastavení hodnot, které ovlivňují zabezpečení ochrany dat, pro celý systém.
- Administraci oprávnění k objektům.
- Prosazování a monitorování metod zabezpečení ochrany dat.

Jestliže jste odpovědní za administraci zabezpečení ochrany dat pro jeden či více systémů iSeries, jsou tyto informace určeny právě vám. Pokyny v těchto informacích předpokládají toto:

- Znáte základy obsluhy serveru iSeries, jako je např. přihlášení nebo používání příkazů.
- Znáte základní prvky zabezpečení ochrany dat serveru iSeries: úrovně zabezpečení, systémové hodnoty zabezpečení, uživatelské profily a zabezpečení objektů.

  Poznámka: Přehled těchto prvků obsahuje Kapitola 1, “Základní prvky zabezpečení serveru iSeries”, na stránce 3. Jestliže jsou pro vás tyto základní prvky nové,

přečtěte si téma *Základní zabezpečení systému a plánování* v rámci aplikace iSeries Information Center. Další podrobnosti najdete v části "Nezbytné předchozí a související informace".

- Zabezpečení ochrany dat ve vašem systému jste aktivovali nastavením systémové hodnoty úrovně zabezpečení (QSECURITY) alespoň na hodnotu 30.

Společnost IBM nepřetržitě rozvíjí možnosti zabezpečení serveru iSeries. Chcete-li využít přínosů těchto vylepšení, měli byste pravidelně aplikovat kumulativní PTF (opravy), která jsou v současné době k dispozici pro vaše vydání. Zjistěte, zda neobsahují opravy, které jsou významné z hlediska zabezpečení ochrany dat.

Jak používat tyto informace

Pokud jste váš systém nenastavili, aby používal nástroje pro zabezpečení ochrany dat, nebo pokud máte produkt Security ToolKit for OS/400 nainstalován pro nižší vydání, postupujte takto:

1. Začněte částí Kapitola 2, "Programy iSeries Security Wizard a eServer Security Planner", na stránce 11. Zde najdete popis, jak používat tyto funkce při výběru, jaké nástroje pro zabezpečení ochrany dat jsou doporučovány a jak se s nimi naučit pracovat.
2. Základnější informace o zabezpečení ochrany dat najdete v referenčních informacích pro zabezpečení v rámci aplikace iSeries Information Center.

Poznámka

Tato publikace obsahuje *mnoho* rad týkajících se zabezpečení serveru iSeries. Váš systém může vyžadovat ochranu jen v některých oblastech. Tyto informace by vás měly seznámit s možnými bezpečnostními riziky a jejich eliminací. Potom se zaměřte na oblasti, které jsou nejkritičtější pro váš systém.

Nezbytné předchozí a související informace

Výchozím bodem pro vyhledání technických informací k serveru iSeries by pro vás měla být aplikace iSeries Information Center.

K aplikaci Information Center se můžete dostat dvěma způsoby:

- Z těchto webových stránek

  `http://www.ibm.com/eserver/iseries/infocenter`
- Z CD-ROM *iSeries Information Center*, SK3T-7436-04. Tento CD-ROM je dodáván společně s novým hardwarem iSeries nebo při objednávce vyšší verze softwaru IBM Operating System/400. Tento CD-ROM si také můžete objednat na webových stránkách IBM Publications Center:

  `http://www.ibm.com/shop/publications/order`

Aplikace iSeries Information Center obsahuje nejnovější aktualizované informace iSeries, jako jsou např. instalace softwaru a hardwaru, Linux, WebSphere, Java, vysoká dostupnost, databáze, logické části, CL příkazy a rozhraní API (application programming interfaces). Dále zde najdete pomocné programy a vyhledávače, které vám pomohou při plánování, odstraňování problémů a konfiguraci vašeho hardwaru a softwaru iSeries.

S každou novou objednávkou hardwaru dostanete *CD-ROM Nastavení a provoz serverů iSeries*, SK3T-7439-02. Tento CD-ROM obsahuje produkty IBM @server IBM e(logo)server iSeries Access for Windows a průvodce EZ-Setup. Produkt iSeries Access Family nabízí

účinnou sadu klientských a serverových funkcí pro připojení PC k serverům iSeries. Průvodce EZ-Setup automatizuje řadu úloh spojených s nastavením serveru iSeries.

Jak posílat připomínky

Vaše ohlasy jsou pro nás velmi důležité, neboť nám pomáhají poskytovat přesnější a vysoce kvalitní informace. Máte-li nějaké připomínky k této knize nebo k jiné dokumentaci týkající se systému iSeries, vyplňte formulář pro připomínky čtenářů, který je uveden na konci této knihy.

- Chcete-li poslat své připomínky poštou, použijte formulář pro připomínky čtenářů, který má na rubu vytištěny adresy. Posíláte-li připomínky z jiné země než ze Spojených států amerických, můžete formulář předat místní pobočce IBM nebo zástupci IBM, který jej odešle v rámci paušalizovaného poštovného.
- Chcete-li poslat své připomínky faxem, použijte některé z těchto čísel:
  - Spojené Státy, Kanada a Portorico: 1-800-937-3430
  - Česká republika: +420 2 7213 1505, ostatní země: 1-507-253-5192
- Chcete-li poslat své připomínky raději elektronickou cestou, použijte některou z těchto e-mailových adres:
  - Připomínky ke knihám:

    RCHCLERK@us.ibm.com
  - Připomínky k aplikaci iSeries Information Center:

    RCHINFOC@us.ibm.com

Do svých připomínek nezapomeňte zahrnout tyto údaje:

- Jméno knihy nebo téma iSeries Information Center.
- Publikační číslo knihy.
- Číslo stránky nebo téma knihy, ke které se vaše připomínka vztahuje.

Část 1. Základní zabezpečení serveru iSeries

Kapitola 1. Základní prvky zabezpečení serveru iSeries

Toto téma obsahuje stručný přehled základních prvků, které společně zajišťují zabezpečení serveru iSeries. V ostatních částech této publikace se k těmto základním prvkům vyjadřujeme podrobněji a uvádíme rady pro jejich použití, které vám mohou pomoci uspokojit potřeby vaší organizace.

Úrovně zabezpečení

Požadovaný rozsah zabezpečení systému můžete zajistit nastavením systémového hodnoty QSECURITY (úroveň zabezpečení). Systém nabízí pět úrovní zabezpečení:

Úroveň 10:

Systém nevynucuje žádné zabezpečení ochrany dat. Není potřeba žádné heslo. Jestliže se někdo přihlásí pomocí uživatelského profilu, který v systému neexistuje, systém tento uživatelský profil vytvoří.

UPOZORNĚNÍ:

Počínaje verzí V4R3 nelze nastavit systémovou hodnotu QSECURITY na hodnotu 10. Jestliže se váš systém nachází v současné době na úrovni zabezpečení 10, zůstane na této úrovni i po nainstalování verze V4R3. Pokud změníte úroveň zabezpečení na nějakou jinou hodnotu, nebudete ji moci změnit zpět na 10. Jelikož úroveň 10 neposkytuje žádné zabezpečení ochrany dat, společnost IBM úroveň 10 nedoporučuje. Společnost **IBM nebude poskytovat žádnou podporu při odstraňování problémů, které se vyskytnou na úrovni zabezpečení 10, ledaže by se tyto problémy mohly vyskytnout i na vyšších úrovních zabezpečení.**

Úroveň 20:

Systém vyžaduje pro přihlášení uživatelské ID a heslo. Úroveň zabezpečení 20 je často označována jako **zabezpečení na úrovni přihlášení**.Standardně mají všichni uživatelé přístup ke všem objektům, neboť všichni mají zvláštní oprávnění *ALLOBJ.

Úroveň 30:

Systém vyžaduje pro přihlášení uživatelské ID a heslo. Uživatelé musí mít oprávnění k používání objektů, neboť standardně nemají uživatelé žádná oprávnění. Tato úroveň se nazývá **zabezpečení na úrovni prostředků**.

Úroveň 40:

Systém vyžaduje pro přihlášení uživatelské ID a heslo. Kromě zabezpečení na úrovni prostředků systém zajišťuje funkce pro **ochranu integrity**. Funkce ochrany integrity, jako např. ověření parametrů pro rozhraní k operačnímu systému, slouží k ochraně jak systému, tak objektů v něm uložených před nedovolenou manipulací prováděnou zkušenými uživateli systému. Pro většinu instalací se doporučuje právě úroveň zabezpečení 40. Když dostanete nový systém iSeries s verzí V4R5 či vyšší, je úroveň zabezpečení nastavena na hodnotu 40.

Úroveň 50:

Systém vyžaduje pro přihlášení uživatelské ID a heslo. Systém vyžaduje jak zabezpečení na úrovni prostředků, tak ochranu integrity na úrovni 40,kromě toho ale přidává **rozšířenou ochranu integrity**, jako je omezení zpracování zpráv mezi

systémovými stavovými programy a uživatelskými stavovými programy. Úroveň zabezpečení 50 je určena pro systémy iSeries s vysokými požadavky na zabezpečení ochrany dat.

Poznámka: Úroveň 50 je povinnou úrovní pro certifikaci C2 (a certifikaci FIPS-140).

Ve 2. kapitole publikace *Zabezpečení iSeries - referenční informace Reference* jsou popsány úrovně zabezpečení a způsoby přechodu z jedné úrovně na druhou.

Globální nastavení

Váš systém má globální nastavení, které má vliv na způsob zadávání práce systému a na způsob, jakým se systém jeví uživatelům jiných systémů. Tato nastavení zahrnují:

Systémové hodnoty zabezpečení:
Systémové hodnoty zabezpečení se používají k ovládání zabezpečení ve vašem systému. Tyto hodnoty se dělí na čtyři skupiny:
- Hlavní systémové hodnoty zabezpečení.
- Jiné systémové hodnoty týkající se zabezpečení.
- Systémové hodnoty, které řídí hesla.
- Systémové hodnoty, které řídí monitorování.

Několik témat v této publikaci pojednává o důsledcích konkrétních systémových hodnot na zabezpečení. Všechny systémové hodnoty vztahující se k zabezpečení popisuje 3. kapitola v publikaci *Zabezpečení iSeries - referenční informace Reference*.

Atributy sítě:
Atributy sítě řídí, jak se váš systém zapojuje (nebo nezapojuje) do komunikace s ostatními systémy v síti. Další informace o atributech sítě najdete v publikaci *Work Management*.

Popisy podsystémů a další prvky funkce Work Management:
Prvky funkce Work Management určují, jakým způsobem vstupují úkoly do systému a v jakém prostředí jsou tyto úkoly zpracovávány. Několik témat v této publikaci pojednává o důsledcích některých hodnot funkce Work Management na zabezpečení. Podrobné informace najdete v publikaci *Work Management*.

Konfigurace komunikací:
Rovněž vaše konfigurace komunikací má vliv na způsob, jakým vstupuje práce do vašeho systému. Několik témat v této publikaci obsahuje návrhy týkající se ochrany vašeho systému, když je zapojen v síti.

Uživatelské profily

Každý uživatel systému **musí** mít uživatelský profil. Dříve, než se může uživatel přihlásit, musíte uživatelský profil vytvořit. Uživatelské profily lze také použít k řízení přístupu k servisním nástrojům, jako je DASD a výpisy hlavní paměti. Další informace uvádí část “Správa servisních nástrojů” na stránce 58.

Uživatelský profil je účinný a flexibilní nástroj. Řídí, co může uživatel dělat, a upravuje vzezření systému vůči uživateli. Všechny parametry obsažené v uživatelském profilu popisuje publikace *Zabezpečení iSeries - referenční informace Reference*.

Skupinové profily

Skupinový profil je speciální typ uživatelského profilu. Skupinový profil můžete použít k definici oprávnění pro skupinu uživatelů namísto toho, abyste přidělovali oprávnění jednomu uživateli po druhém. Skupinový profil slouží také jako vzor, když vytváříte individuální uživatelské profily pomocí funkce kopírování profilu nebo když použijete produkt iSeries Navigator. K editaci uživatelských oprávnění můžete použít menu pro strategii zabezpečení ochrany dat.

Další informace o plánování a použití skupinových profilů obsahují 5. a 7. kapitola publikace *Zabezpečení iSeries - referenční informace Reference*.

Zabezpečení na úrovni prostředků

Zabezpečení na úrovni prostředků v systému umožňuje definovat, kdo a jakým způsobem může používat objekty. Schopnost přístupu k objektu se nazývá **oprávnění**. Když nastavujete oprávnění k objektu, budete muset být opatrní, abyste svým uživatelům přidělili dostatečné oprávnění pro jejich práci, aniž byste jim dali oprávnění prohlížet a měnit systém. Oprávnění k objektu dává uživateli práva k určitému objektu a může určovat, co může uživatel s daným objektem provádět. Prostředek objektu může být omezen prostřednictvím konkrétních podrobných oprávnění uživatele, např. přidávání záznamů nebo změnu záznamů. Systémové prostředky můžete použít, chcete-li uživateli umožnit přístup k určité systémem definované podmnožině oprávnění: *ALL, *CHANGE, *USE a *EXCLUDE.

Nejběžnějšími systémovými objekty, které vyžadují zabezpečení na úrovni prostředků, jsou soubory, programy, knihovny a adresáře. Vy však můžete určit oprávnění pro libovolný objekt v systému.

Kapitola 5, “Ochrana informačních hodnot prostřednictvím oprávnění k objektům” pojednává o významu nastavení oprávnění k objektům ve vašem systému. Volby pro nastavení zabezpečení na úrovni prostředků jsou popsány v 5. kapitole publikace *Zabezpečení iSeries - referenční informace Reference*.

Omezený přístup k funkci programů

Pokud pro program nemáte objekt iSeries, který by bylo možné zabezpečit, můžete zabezpečení zajistit omezením přístupu k funkci programu. Předtím, než byla ve verzi V4R3 zavedena podpora omezeného přístupu k funkci programů, jste toho mohli dosáhnout vytvořením seznamu oprávnění nebo jiného objektu a kontrolou oprávnění k objektu za účelem řízení přístupu k funkci programů. Nyní můžete využít omezeného přístupu k funkci programů, který umožňuje snadnější řízení přístupu k aplikaci, částem aplikace a funkcím v rámci programu.

Existují dvě metody, které můžete použít k řízení uživatelského přístupu k funkcím aplikace prostřednictvím produktu iSeries Navigator. První z nich používá podporu Administrativy aplikací:

1. Pravým tlačítkem myši klepněte na systém, který obsahuje funkci, u níž chcete změnit nastavení přístupu.
2. Vyberte volbu **Administrativa aplikací**.
3. Pokud jste v administrativním systému, vyberte volbu **Lokální nastavení**. Jinak pokračujte dalším krokem.
4. Vyberte funkci, kterou lze administrovat.
5. Je-li to možné, vyberte volbu **Předvolený přístup**. Vybráním této volby umožníte standardně všem uživatelům přístup k dané funkci.

6. Je-li to možné, vyberte volbu **Přístup ke všem objektům**. Vybráním této volby umožníte všem uživatelům se systémovým oprávněním ke všem objektům, aby měli přístup k této funkci.
7. Je-li to možné, vyberte volbu **Přizpůsobit**. K přidání nebo odstranění uživatelů či skupin v seznamech **Povolený přístup** a **Odepřený přístup** v dialogu **Přizpůsobení přístupu** použijte tlačítka **Přidat** a **Odstranit**.
8. Je-li to možné, vyberte volbu **Odstranit přizpůsobení**. Vybráním této volby vymažete veškeré upravené přístupy pro zvolenou funkci.
9. Klepnutím na **OK** uzavřete dialog **Administrativa aplikací**.

Druhá metoda řízení uživatelského přístupu zahrnuje podporu uživatelů a skupin produktu iSeries Navigator.

1. V prostředí produktu iSeries rozbalte položku **Uživatelé a skupiny**.
2. Vyberte volbu **Všichni uživatelé**, **Skupiny** nebo **Uživatelé, kteří nejsou ve skupině**. Zobrazí se seznam uživatelů nebo skupin.
3. Pravým tlačítkem myši klepněte na uživatele nebo skupinu a vyberte volbu **Vlastnosti**.
4. Klepněte na volbu **Schopnosti**.
5. Klepněte na ouško **Aplikace**.
6. Na této stránce změňte nastavení přístupu pro uživatele nebo skupinu.
7. Dvojím klepnutím na **OK** uzavřete dialog **Vlastnosti**.

Další informace o problematice zabezpečení v produktu iSeries Navigator najdete v části "Zabezpečení produktu iSeries Navigator" na stránce 142.

Jestliže vytváříte aplikace, můžete využít rozhraní API pro omezení přístupu k funkci programu pro tyto činnosti:

- Registrace funkce.
- Načtení informací o dané funkci.
- Definování, kdo může a kdo nemůže používat danou funkci.
- Kontrola, zda je uživateli dovoleno používat danou funkci.

Poznámka: Tato podpora **nenahrazuje** zabezpečení na úrovni prostředků. Omezený přístup k funkci programu nezabraňuje uživateli získat přístup k prostředku (např. souboru nebo programu) z jiného rozhraní.

Aby bylo možné tuto podporu používat v rámci nějaké aplikace, musí dodavatel aplikace zaregistrovat funkce při instalaci aplikace. Registrovaná funkce odpovídá kódovému bloku pro určité funkce v aplikaci. Když uživatel spustí aplikaci, zavolá aplikace nejdříve rozhraní API a teprve pak zavolá kódový blok. Rozhraní API volají API pro kontrolu použití, aby zjistila, zda má uživatel dovoleno používat danou funkci. Pokud je uživateli dovoleno používat požadovanou funkci, kódový blok se spustí. Jestliže ji nemá dovoleno používat, je uživateli znemožněno spustit kódový blok.

Poznámka: Rozhraní API zahrnují registraci 30znakového ID funkce v registrační databázi (WRKREGINF). Ačkoliv neexistují žádné výstupní body související s ID funkcí, které používají API pro omezení přístupu k funkci, je povinné mít výstupní body. Při registraci čehokoliv v registru **musíte** zadat jméno formátu výstupního bodu. Za tím účelem API pro registraci funkce vytvoří fiktivní jméno formátu a použije ho pro všechny funkce, které jsou registrovány. Jelikož se jedná o fiktivní jméno formátu, není nikdy volán žádný program výstupního bodu.

Administrátor systému určuje, komu je dovolen nebo odepřen přístup k funkci. Administrátor může k řízení přístupu k funkci programu používat buď rozhraní API, nebo grafické uživatelské rozhraní (GUI) Administrativa aplikací produktu iSeries Navigator. Informace o rozhraních API pro omezení přístupu k funkci programu obsahuje publikace *iSeries server API Reference*. Další informace o řízení přístupu k funkcím najdete v části "Zabezpečení produktu iSeries Navigator" na stránce 142.

Monitorování zabezpečení

Lidé prověřují zabezpečení systému z několika důvodů:

- Aby ohodnotili, zda je plán pro zabezpečení ochrany dat úplný.
- Aby se ujistili, že plánované ovládací prvky zabezpečení jsou vhodné a fungují. Tento typ monitorování obvykle provádí správce systému jako součást každodenní administrace zabezpečení. Také ho provádějí (někdy v podrobnějším měřítku) interní nebo externí revizoři jako součást pravidelné revize zabezpečení.
- Aby se přesvědčili, že zabezpečení systému udržuje krok se změnami systémového prostředí. Příkladem změn, které ovlivňují zabezpečení, jsou:
  - Nové objekty vytvořené uživateli systému.
  - Noví uživatelé přijatí do systému.
  - Změna vlastnictví objektů (oprávnění nebylo přizpůsobeno).
  - Změna odpovědnosti (změnila se skupina uživatelů).
  - Dočasné oprávnění (které se nezruší na základě času).
  - Nainstalované nové produkty.
- Aby se připravili na budoucí události, jako je instalace nové aplikace, přechod na vyšší úroveň zabezpečení nebo nastavení komunikační sítě.

Metody, které jsou zde popsány, jsou určeny pro všechny tyto situace. To, které věci budete monitorovat a jak často, závisí na velikosti vaší organizace a na jejích potřebách v oblasti zabezpečení ochrany dat.

Monitorování zabezpečení zahrnuje použití příkazů ve vašem systému a přístup k informacím v protokolech a žurnálech. Pro člověka, který má na starosti monitorování zabezpečení vašeho systému, můžete vytvořit speciální profil. Profil revizora musí mít zvláštní oprávnění *AUDIT, které umožňuje měnit charakteristiky monitorování systému. Některé z úloh monitorování navržených v této kapitole vyžadují uživatelský profil se zvláštním oprávněním *ALLOBJ a *SECADM. Po skončení období monitorování nastavte heslo pro profil revizora na hodnotu *NONE.

Další podrobnosti o monitorování zabezpečení uvádí 9. kapitola publikace *Security Reference*.

Příklad: sestava atributů zabezpečení systému

Obrázek 1 na stránce 8 představuje příklad výstupu z příkazu PRTSYSSECA (Tisk atributů zabezpečení systému). Ze sestavy je zřejmé nastavení systémových hodnot a atributů sítě souvisejících se zabezpečením, které jsou doporučeny pro systémy s normálními požadavky na zabezpečení. Sestava také ukazuje aktuální nastavení vašeho systému.

Poznámka: Ve sloupci *Aktuální hodnota* v sestavě je uvedeno aktuální nastavení v systému. Porovnáním těchto hodnot s doporučenou hodnotou zjistíte, kde mohou existovat nějaká bezpečnostní rizika.

```
Atributy zabezpečení systému

Jméno
syst. hodnoty    Aktuální hodnota       Doporučená hodnota
QALWOBJRST       *NONE                  *NONE
QALWUSRDMN       *ALL                   QTEMP
QATNPGM          QEZMAIN   QSYS         *NONE
QAUDENDACN       *NOTIFY                *NOTIFY
QAUDFRCLVL       *SYS                   *SYS
QAUDCTL          *AUDLVL                *AUDLVL   *OBJAUD
QAUDLVL          *SECURITY              *AUTFAIL  *CREATE
                                        *DELETE   *SECURITY
                                        *SAVRST   *NOQTEMP
```

Obrázek 1. Příklad sestavy atributů zabezpečení systému (Část 1 ze 4)

```
QAUTOCFG         0                      0
QAUTORMT         1                      0
QAUTOVRT         9999                   0
QCMNRCYLMT       0 0                    0 0
QCRTAUT          *CHANGE                Řízení na úrovni knihovny.
QCRTOBJAUD       *NONE                  Řízení na úrovni knihovny.
QDEVRCYACN       *DSCMSG                *DSCMSG
QDSCJOBITV       120                    120
QDSPSGNINF       1                      1
QINACTITV        60                     60
QINACTMSGQ       *ENDJOB                *ENDJOB
QLMTDEVSSN       0                      1
QLMTSECOFR       0                      1
QMAXSGNACN       2                      3
QMAXSIGN         3                      3
```

Obrázek 1. Příklad sestavy atributů zabezpečení systému (Část 2 ze 4)

```
QPWDEXPITV       60                     60
QPWDLMTAJC       1                      1
QPWDLMTCHR       *NONE                  AEIOU@$#
QPWDLMTREP       1                      2
QPWDLVL          0
QPWDMAXLEN       8                      8
QPWDMINLEN       6                      6
QPWDPOSDIF       1                      1
QPWDRQDDGT       1                      1
QPWDRQDDIF       0                      1
QPWDVLDPGM       *NONE                  *NONE
QRETSVRSEC       0                      0
QRMTIPL          0                      0
QRMTSIGN         *FRCSIGNON             *FRCSIGNON
QSECURITY        50                     50
QSHRMEMCTL       1                      0
QSRVDMP          *DMPUSRJOB             *NONE
QUSEADPAUT       *NONE                  CRTAUTL AUTL(QUSEADPAUT) AUT(*EXCLUDE)
                                        CHGOBJOWN OBJ(QUSEADPAUT) OBJTYPE(*AUTL)
                                        CHGSYSVAL SYSVAL(QUSEADPAUT) VALUE(QUSEADPAUT)
QVFYOBJRST       1                      3
```

Obrázek 1. Příklad sestavy atributů zabezpečení systému (Část 3 ze 4)

```
Atributy zabezpečení systému

Jméno
atributu sítě    Aktuální hodnota       Doporučená hodnota
DDMACC           *OBJAUT                *REJECT
JOBACN           *FILE                  *REJECT
PCSACC           *OBJAUT                *REJECT
```

Obrázek 1. Příklad sestavy atributů zabezpečení systému (Část 4 ze 4)

Kapitola 2. Programy iSeries Security Wizard a eServer Security Planner

Programy iSeries Security Wizard a eServer Security Planner vám mohou pomoci při rozhodování, jaké hodnoty zabezpečení uplatnit na vašem serveru iSeries. S využitím programu iSeries Security Wizard v prostředí produktu iSeries Navigator můžete vytvořit sestavy, které na základě zvolených odpovědí budou odrážet vaše potřeby v oblasti zabezpečení. Tyto sestavy pak můžete využít ke konfiguraci zabezpečení systému.

Programy iSeries Security Wizard a eServer Security Planner vám pomůže naplánovat a následně implementovat základní strategii zabezpečení ochrany dat pro servery iSeries. Cílem obou nástrojů je usnadnit implementaci a správu zabezpečení ve vašich systémech. Průvodce, který je k dispozici jako součást operačního systému OS/400, vám položí několik otázek na vyšší úrovni týkajících se prostředí vašeho serveru a na základě vašich odpovědí vám poskytne množinu doporučení, které je průvodce schopný přímo aplikovat na systém.

Program eServer Security Planner je online verzí programu Security Wizard. Umožňuje vám vybírat si volby na základě vašich potřeb v oblasi zabezpečení a poté vám poskytne sestavu s návrhy, jaké funkce jsou potřebné pro zabezpečení vašeho serveru.

Program eServer Security Planner je webovou verzí programu Securiy Wizard. Poskytuje doporučení pro implementaci zabezpečení ve vašem systému, stejně tak jako průvodce. Program Security Wizard však není schopný tato doporučení aplikovat. Místo toho vám na základě vašich odpovědí na otázky vytiskne seznam hodnot a jiných atributů pro zabezpečení systému, které byste měli v systému aplikovat.

Security Wizard

Rozhodování, které systémové hodnoty zabezpečení serveru iSeries byste měli použít ve vaší organizaci, může být komplikované. Jestliže nemáte zkušenosti s implementací zabezpečení ochrany dat na serverech iSeries nebo pokud se prostředí, v němž server iSeries provozujete, v poslední době změnilo, může vám při rozhodování pomoci nástroj Security Wizard (průvodce zabezpečením).

Co je průvodce?

- Průvodce je nástroj navržený pro uživatele - nováčky, který slouží k instalaci nebo konfiguraci něčeho v systému.
- Průvodce vyzývá uživatele k zadávání informací tím, že mu pokládá otázky. Odpověď na každou otázku určuje, jaká otázka bude následovat.
- Když průvodce položí všechny otázky, zobrazí se uživateli závěrečný dialog. Uživatel pak stiskne tlačítko **Dokončit**, které zahájí instalaci a konfiguraci dané položky.

Cíle průvodce zabezpečením

Cílem průvodce zabezpečením je nakonfigurovat na základě odpovědí uživatele následující položky:

- Systémové hodnoty a atributy sítí související se zabezpečením.
- Vykazování pro monitorování systému související se zabezpečením.
- Vygenerování sestavy administrátorských informací nazvané Administrator Information Report a sestavy uživatelských informací nazvané User Information Report:

- Sestava Administrator Information Report obsahuje doporučená nastavení zabezpečení ochrany dat a procedury, podle nichž by se mělo postupovat před uplatněním doporučení.
- Sestava User Information Report obsahuje informace, které lze použít pro firemní strategii zabezpečení ochrany dat. V této sestavě jsou například zahrnuta pravidla pro vytváření hesel.

• Zajištění doporučených nastavení pro nejrůznější systémové položky související se zabezpečením.

Úkoly průvodce zabezpečením

• Průvodce zabezpečením má tyto úkoly:
  - Na základě odpovědí uživatele na otázky průvodce určit, jaká by měla být nastavení zabezpečení systému, a potom odpovídajícím způsobem tato nastavení implementovat.
  - Průvodce vytváří podrobné sestavy, mezi něž patří:
    - Sestava vysvětlující doporučení průvodce.
    - Sestava upřesňující procedury, podle nichž by se mělo postupovat před implementací.
    - Sestava uvádějící důležité informace, které je třeba sdělit uživatelům systému.
• Tyto položky představují základní metody zabezpečení ochrany dat ve vašem systému.
• Průvodce doporučuje, abyste si naplánovali pravidelné spouštění sestav monitorovacího žurnálu. Pokud jsou naplánovány, pomáhají tyto sestavy:
  - Zajistit, aby byly dodržovány metody zabezpečení ochrany dat.
  - Zajistit, aby změny metod zabezpečení ochrany dat byly prováděny pouze s vaším souhlasem.
  - Plánovat sestavy pro monitorování událostí ve vašem systému, které souvisejí se zabezpečením.
• Průvodce vám umožňuje doporučení uložit nebo můžete některá či všechna doporučení aplikovat ve vašem systému.

Poznámka: Průvodce zabezpečením lze ve stejném systému použít vícekrát, aby si mohli uživatelé se starší instalací prohlédnout své aktuální nastavení. Průvodce zabezpečením je možné používat v systémech počínaje verzí V3R7 (kdy byl uveden produkt iSeries Navigator).

Chcete-li používat produkt iSeries Navigator, musíte mít nainstalovaný produkt IBM iSeries Access for Windows na PC s Windows 95/NT a z tohoto PC musíte mít připojení na server iSeries. Uživatel průvodce musí být připojen k serveru iSeries. Uživatel musí mít uživatelské ID se zvláštním oprávněním *ALLOBJ, *SECADM, *AUDIT a *IOSYSCFG. Užitečné informace o připojení vašeho PC Windows 95/NT k systému iSeries obsahuje téma IBM iSeries Access for Windows v rámci aplikace Information Center (podrobnosti viz část “Nezbytné předchozí a související informace” na stránce xii).

Chcete-li spustit průvodce zabezpečením, postupujte takto:

1. V prostředí produktu iSeries Navigator rozbalte položku vašeho serveru.
2. Pravým tlačítkem myši klepněte na volbu **Zabezpečení** a vyberte volbu **Konfigurovat**.
   - Když uživatel spustí volbu **Zabezpečení** produktu iSeries Navigator, odešle se serveru iSeries požadavek na kontrolu zvláštního oprávnění uživatele.
   - V případě, že uživatel nemá všechna požadovaná zvláštní oprávnění (*ALLOBJ, *AUDIT, *IOSYSCFG, *SECADM), nezobrazí se mu volba **Konfigurovat** a nemá umožněn přístup k průvodci zabezpečením.
3. Za předpokladu, že uživatel má potřebné oprávnění:
   - Načtou se předchozí odpovědi průvodce.
   - Načtou se aktuální nastavení zabezpečení.

Průvodce zabezpečením zobrazí jednu ze tří uvítacích obrazovek. To, kterou obrazovku uvidíte, závisí na splnění následujících podmínek:

- Průvodce nebyl nikdy spuštěn na cílovém serveru iSeries.
- Průvodce byl již dříve spuštěn a změny v zabezpečení byly odloženy.
- Průvodce byl již dříve spuštěn a změny v zabezpečení byly realizovány.

Jestliže nepoužíváte produkt iSeries Navigator, máte i tak možnost získat podporu při plánování vašich potřeb v oblasti zabezpečení. Produkt eServer Security Planner (poradce pro zabezpečení) je online verzí průvodce zabezpečením s jedním rozdílem. Poradce vám automaticky nenakonfiguruje systém. Na základě vašich odpovědí vám však vygeneruje sestavu doporučených voleb zabezpečení. Chcete-li získat přístup k produktu eServer Security Planner, přejděte do aplikace eServer Information Center:

`http://publib.boulder.ibm.com/eserver/`

eServer Security Planner

Produkt eServer Security Planner (poradce pro zabezpečení) je online verzí produktu Security Wizard (průvodce zabezpečením). Pokládá stejné otázky jako průvodce zabezpečením a na základě odpovědí vygeneruje stejná doporučení. Základní rozdíly mezi těmito dvěma nástroji spočívají v tom, že:

- Program eServer Security Planner —
  - Nevytváří sestavy.
  - Neporovnává aktuální nastavení s doporučenými nastaveními.
  - Nenastavuje automaticky žádné systémové hodnoty.
- Z programu eServer Security Planner nelze aplikovat doporučení.

Program eServer Security Planner generuje CL program, který můžete vystřihnout a vložit a následně upravit pro vlastní použití, což vám umožní automatizovat konfiguraci zabezpečení. Z programu eServer Security Planner se můžete také přímo připojit k dokumentaci serveru iSeries. V ní najdete informace o systémové hodnotě nebo sestavě, které vám pomohou určit, zda je toto nastavení vhodné pro vaše prostředí.

Program eServer Security Planner najdete pod vaším internetovým prohlížečem na této adrese:

`http://publib.boulder.ibm.com/eserver/`

Kapitola 3. Řízení interaktivního přihlášení

Když přemýšlíte o omezení přístupu do vašeho systému, začněte s tím, co je nejviditelnější, s přihlašovací obrazovkou. Následující volby můžete použít k tomu, abyste někomu zkomplikovali přihlášení do vašeho systému prostřednictvím přihlašovací obrazovky.

Stanovení pravidel pro hesla

Chcete-li zabezpečit přihlášení do vašeho systému, postupujte takto:
- Zaveďte strategii, která stanoví, že hesla nesmí být triviální a sdílená.
- Nastavte systémové hodnoty, které vám pomohou zajistit tuto strategii. Tabulka 1 ukazuje doporučené nastavení systémových hodnot.

Kombinace hodnot, které obsahuje Tabulka 1, je poměrně omezující a jejím cílem je výrazné snížení pravděpodobnosti triviálních hesel. Vašim uživatelům však může působit jisté potíže zvolit heslo, které by splňovalo všechna tato omezení.

Zvažte, zda byste uživatelům neměli poskytnout:
1. Seznam kritérií pro hesla.
2. Příklady platných a neplatných hesel.
3. Návrhy, jak vymyslet dobré heslo.

Spusťte příkaz CFGSYSSEC (Konfigurace zabezpečení systému), abyste mohli nastavit tyto hodnoty. Pomocí příkazu PRTSYSSECA (Tisk atributů zabezpečení systému) vytiskněte aktuální nastavení pro tyto systémové hodnoty.

3. kapitola publikace *Zabezpečení iSeries - referenční informace Reference*. Další informace o příkazu CFGSYSSEC uvádí část “Hodnoty nastavované příkazem konfigurace zabezpečení systému” na stránce 35.

Tabulka 1. Systémové hodnoty pro hesla

Jméno systémové hodnoty	Popis	Doporučená hodnota
QPWDEXPITV	Jak často musí uživatelé systému měnit svá hesla. Pro jednotlivé uživatele můžete v uživatelském profilu určit odlišné hodnoty.	60 (dní)
QPWDLMTAJC	Zda systém zamezuje použití dvou stejných znaků vedle sebe.	1 (ano)
QPWDLMTCHR	Které znaky nesmí být použity v heslech.[2]	AEIOU#$@
QPWDLMTREP	Zda systém brání tomu, aby se jeden znak vyskytoval v hesle vícekrát.	2 (nejsou dovoleny za sebou)
QPWDLVL	Zda jsou hesla uživatelských profilů omezena na 10 znaků nebo maximálně na 128 znaků.	0[3]
QPWDMAXLEN	Maximální počet znaků v hesle.	8
QPWDMINLEN	Minimální počet znaků v hesle.	6
QPWDPOSDIF	Zda se každý znak v hesle musí lišit od znaku na stejné pozici v předešlém hesle.	1 (ano)
QPWDRQDDGT	Zda heslo musí obsahovat alespoň jeden numerický znak.	1 (ano)
QPWDRQDDIF	Jak dlouho musí uživatel čekat, než může znovu použít stejné heslo.[2]	5 nebo méně (intervalů ukončení platnosti)[1]
QPWDVLDPGM	Který ukončovací program se volá za účelem ověření nově přiřazeného hesla.	*NONE

Tabulka 1. Systémové hodnoty pro hesla (pokračování)

Jméno systémové hodnoty	Popis	Doporučená hodnota

Poznámky:

1. Systémová hodnota QPWDEXPITV určuje, jak často musíte změnit své heslo, např. každých 60 dní. Toto je **interval ukončení platnosti**. Systémová hodnota QPWDRQDDIF určuje, kolik intervalů ukončení platnosti musí uběhnout, než budete moci znovu použít stejné heslo. Další informace o těchto systémových hodnotách a jejich vzájemném působení obsahuje 3. kapitola publikace *Zabezpečení iSeries - referenční informace Reference*.
2. Systémová hodnota QPWDLMTCHR není vynucována na úrovni hesla 2 nebo 3. Další podrobnosti najdete v části "Úrovně hesla".
3. Chcete-li zjistit úroveň hesla, která nejlépe odpovídá vašim potřebám, přečtěte si část "Plánování změn úrovně hesla".

Úrovně hesla

Počínaje verzí V5R1 operačního systému nabízí systémová hodnota QPWDLVL větší zabezpečení na úrovni hesla. V předešlých vydáních byly uživatelé omezeni na hesla, jejichž délka byla maximálně 10 znaků a která byla tvořena z omezeného rozsahu znaků. Nyní si uživatelé mohou zvolit heslo (nebo frázi hesla) dlouhé až 128 znaků v závislosti na úrovni hesla, na kterou je systém nastaven. Existují tyto úrovně hesla:

- **Úroveň 0:** S touto úrovní je systém dodáván. Při úrovni 0 mají hesla maximálně 10 znaků, obsahují pouze znaky A-Z, 0–9, #, @, $ a _. Hesla na úrovni 0 jsou méně bezpečná, než hesla na vyšších úrovních.
- **Úroveň 1:** Platí stejná pravidla jako pro heslo úrovně 0, ale hesla pro produkt iSeries Support for Windows Network Neighborhood (dále jen iSeries NetServer) se neukládají.
- **Úroveň 2:** Na této úrovni jsou hesla zabezpečená. Tuto úroveň lze využít pro testovací účely. Hesla se pro uživatele ukládají na úrovni 0 nebo 1, pokud mají délku 10 znaků či méně a používají sadu znaků pro hesla úrovně 0 nebo 1. Hesla (fráze hesla) na této úrovni mají následující charakteristiky:
  - Mají délku až 128 znaků.
  - Jsou složeny z libovolných dostupných znaků na klávesnici.
  - Nemohou být složeny pouze z mezer. Mezery se odstraňují z konce hesla.
  - Rozlišují velká a malá písmena.
- **Úroveň 3:** Hesla na této úrovni jsou nejvíce bezpečná a využívají nejpokročilejší šifrovací algoritmus, který je dostupný. Hesla na této úrovni mají stejné charakteristiky jako na úrovni 2. Hesla pro produkt iSeries NetServer se na této úrovni neukládají.

Pokud každý systém ve vaší síti splňuje následující kritéria, měli byste používat pouze úrovně hesla 2 a 3:

- Operační systém je verze V5R1 nebo vyšší.
- Úroveň hesla je nastavena na 2 nebo 3.

Obdobně se všichni uživatelé musí přihlašovat s využitím stejné úrovně hesla. Úrovně hesla jsou globální. Uživatelé si nemohou zvolit úroveň, na níž chtějí své heslo zabezpečit.

Plánování změn úrovně hesla

Změny úrovní hesla je třeba dobře naplánovat. Jestliže změny úrovní hesla nenaplánujete odpovídajícím způsobem, může dojít k selhání operací s jinými systémy nebo mohou mít uživatelé problémy s přihlášením do systému. Před změnou systémové hodnoty QPWDLVL se ujistěte, že jste uložili svá zabezpečovací data pomocí příkazu SAVSECDTA nebo SAVSYS. Pokud máte aktuální zálohu, budete schopni znovu nastavit původní hodnoty hesel pro všechny uživatelské profily v případě, že byste se potřebovali vrátit na nižší úroveň hesla.

U produktů, které používáte v systému nebo na klientech, s kterými systém komunikuje, mohou nastat problémy, když je systémová hodnota QPWDLVL (úroveň hesla) nastavena na hodnotu 2 nebo 3. Libovolný produkt nebo klient, jenž posílá hesla do systému v zašifrované formě, namísto prostého textu, který uživatel zadá na přihlašovací obrazovce, musí být aktualizován, aby byl schopný pracovat s novými pravidly pro šifrování hesel při QPWDLVL s hodnotou 2 nebo 3. Odesílání zašifrovaného hesla se nazývá **substituce hesla**.

Substituce hesla se používá proto, aby se zabránilo sejmutí hesla během přenosu po síti. Substituce hesla vygenerované staršími klienty, kteří nepodporují nový algoritmus pro hodnotu QPWDLVL 2 nebo 3, nebudou akceptovány, i když budou specifické znaky správné. To platí i pro libovolný přístup server iSeries - server iSeries typu peer, který využívá zašifrovaných hodnot k autentizaci z jednoho systému do druhého.

Problém spočívá ve skutečnosti, že některé produkty, kterých se to týká (např. Java Toolbox), jsou dodávány jako middleware. Produkt třetí strany, který začleňuje nižší verzi jednoho z těchto produktů, nebude správně fungovat, dokud nebude znovu vytvořen s aktualizovanou verzí middlewaru.

Z tohoto i dalších scénářů je zřejmé, proč je nezbytné změnu systémové hodnoty QPWDLVL dobře naplánovat.

Pokyny pro změnu QPWDLVL z hodnoty 0 na hodnotu 1

Úroveň hesla 1 umožňuje systému, který nepotřebuje komunikovat s produktem Windows 95/98/ME AS/400 Client Support for Windows Network Neighborhood (iSeries NetServer), eliminovat ze systému hesla pro produkt iSeries NetServer. Vyloučení zbytečných zašifrovaných hesel ze systému zvyšuje celkovou bezpečnost systému.

Při hodnotě QPWDLVL 1 budou nadále fungovat všechny aktuální mechanismy substituce a autentizace hesla před verzí V5R1. Existuje jen nepatrná možnost poruchy s výjimkou funkcí a služeb, které vyžadují heslo iSeries NetServer.

Pokyny pro změnu QPWDLVL z hodnoty 0 nebo 1 na hodnotu 2

Úroveň hesla 2 zavádí použití hesel, která rozlišují velká a malá písmena a jsou až 128 znaků dlouhá (také nazývaná fráze hesla), a poskytuje maximální schopnost vrátit se zpět k hodnotě QPWDLVL 0 nebo 1.

Bez ohledu na úroveň hesla systému se hesla úrovně 2 a 3 vytvoří vždy, když je heslo změněno nebo když se uživatel přihlásí do systému. To, že jsou v systému vytvořena hesla na úrovni 2 a 3, zatímco systém je nadále na úrovni hesla 0 nebo 1, pomáhá při přípravě na přechod na úroveň hesla 2 nebo 3.

Před změněním systémové hodnoty QPWDLVL na hodnotu 2 byste měli použít příkazy DSPAUTUSR nebo PRTUSRPRF TYPE(*PWDINFO) k vyhledání všech uživatelských profilů, které nemají heslo použitelné na úrovni hesla 2. V závislosti na tom, které profily se prostřednictvím zmíněných příkazů vyhledají, možná budete chtít použít jeden z následujících mechanismů sloužících k doplnění hesla úrovně 2 nebo 3 pro tyto profily.

- Pomocí CL příkazu CHGUSRPRF nebo CHGPWD nebo rozhraní QSYCHGPW API změňte heslo pro daný uživatelský profil. Na základě toho systém změní heslo, které je použitelné na úrovni hesla 0 nebo 1. Systém rovněž vytvoří dvě ekvivalentní hesla rozlišující velká a malá písmena, která jsou použitelná na úrovních hesla 2 a 3. Pro použití na úrovni hesla 2 nebo 3 se vytvoří dvě verze hesla - jedna psána samými velkými písmeny a druhá samými malými písmeny.

  Například změna hesla na C4D2RB4Y povede k tomu, že systém vygeneruje hesla C4D2RB4Y a c4d2rb4y na úrovni hesla 2.
- Přihlaste se do systému prostřednictvím mechanismu, který předkládá heslo ve formě prostého textu (nepoužívá substituci hesla). Pokud je heslo platné a uživatelský profil

nemá heslo, které by bylo použitelné na úrovni hesla 2 nebo 3, vytvoří systém dvě ekvivalentní hesla rozlišující velká a malá písmena, která jsou použitelná na úrovních hesla 2 a 3. Pro použití na úrovni hesla 2 nebo 3 se vytvoří dvě verze hesla - jedna psána samými velkými písmeny a druhá samými malými písmeny.

Neexistence hesla, které je použitelné na úrovni hesla 2 nebo 3, může způsobit problémy vždy, když uživatelský profil také nemá heslo použitelné na úrovních hesla 0 a 1 nebo když se uživatel pokouší přihlásit prostřednictvím produktu, který používá substituci hesla. V těchto případech nebude uživatel schopný se přihlásit, když se úroveň hesla změní na 2.

Jestliže uživatelský profil nemá heslo použitelné na úrovních hesla 2 a 3 a pokud má uživatelský profil heslo použitelné na úrovních hesla 0 a 1 a uživatel se přihlásí prostřednictvím produktu, který posílá hesla ve formě prostého textu, pak systém ověří uživatele vůči heslu úrovně 0 a pro daný uživatelský profil vytvoří dvě hesla úrovně 2 (jak bylo popsáno výše). Následná přihlášení budou ověřována vůči heslům úrovně 2.

Klienti/služby, které používají substituci hesla, nebudou správně fungovat při hodnotě QPWDLVL rovné 2, pokud tito klienti /služby nebyli aktualizováni tak, aby používali nové schéma substituce hesla (frází hesla). Administrátor by měl zkontrolovat, zda jsou klienti/služby, kteří nebyli aktualizováni na nové schéma substituce hesla, požadováni.

Mezi klienti/služby, kteří používají substituci hesla, patří:

- TELNET
- iSeries Access
- iSeries Host Servers
- QFileSrv.400
- podpora tisku iSeries NetServer
- DDM
- DRDA
- SNA LU6.2

Před změnou na QPWDLVL 2 vám rozhodně doporučujeme uložit všechny zabezpečovací data. Usnadní to případný přechod zpět na hodnotu QPWDLVL 0 nebo 1, pokud bude nezbytný.

Doporučujeme, abyste neprováděli změny ostatních systémových hodnot týkajících se hesel, jako např. QPWDMINLEN a QPWDMAXLEN, dokud neprovedete otestování QPWDLVL 2. Usnadníte si tak případný přechod zpět na hodnotu QPWDLVL 1 nebo 0, pokud bude nezbytný. Systémová hodnota QPWDVLDPGM však musí uvádět buď hodnotu *REGFAC, nebo *NONE, aby systém dovolil změnu QPWDLVL na hodnotu 2. Pokud používáte program pro ověření platnosti hesla, budete z toho důvodu možná chtít napsat nový program, který lze registrovat pro výstupní bod QIBM_QSY_VLD_PASSWRD pomocí příkazu ADDEXITPGM.

Hesla produktu iSeries NetServer jsou nadále podporována na úrovni QPWDLVL 2, proto by měly všechny funkce/služby, které vyžadují hesla produktu iSeries NetServer, i nadále správně fungovat.

Když je administrátor už zvyklý na provoz systému na úrovni QPWDLVL 2, může začít měnit systémové hodnoty týkající se hesel za účelem využití delších hesel. Administrátor by si však měl být vědom toho, že delší hesla budou mít tyto důsledky:

- Jestliže bude zadáno heslo delší než 10 znaků, vymaže se heslo úrovně 0 a 1. Tento uživatelský profil nebude schopný se přihlásit, pokud se systém vrátí na úroveň hesla 0 nebo 1.

- Pokud heslo obsahuje speciální znaky nebo nedodržuje pravidla pro vytváření jmen jednotlivých objektů (kromě rozlišování velkých a malých písmen), vymaže se heslo úrovně 0 a 1.
- Jestliže bude zadáno heslo delší než 14 znaků, vymaže se pro daný profil heslo produktu iSeries NetServer.
- Systémové hodnoty týkající se hesel platí pouze pro novou hodnotu na úrovni hesla 2 a nevztahují se na hodnotu systémem vygenerovaného hesla na úrovni 0 a 1, ani na hodnotu hesla produktu iSeries NetServer (je-li vygenerováno).

Pokyny pro změnu QPWDLVL z hodnoty 2 na hodnotu 3

Poté, co bude systém po nějakou dobu provozován na úrovni QPWDLVL 2, se může administrátor rozhodnout pro přechod na hodnotu QPWDLVL 3, aby maximalizoval zabezpečení na úrovni hesla.

Na úrovni QPWDLVL 3 jsou všechna hesla produktu iSeries NetServer vymazána, proto by systém neměl být převáděn na hodnotu QPWDLVL 3, ledaže byste nepotřebovali používat hesla produktu iSeries NetServer.

Na úrovni QPWDLVL 3 jsou vymazána všechna hesla úrovně 0 a 1. Administrátor může použít příkazy DSPAUTUSR nebo PRTUSRPRF k vyhledání uživatelských profilů, s nimiž nejsou asociována žádná hesla úrovně 2 nebo 3.

Změna na nižší úroveň hesla

Návrat zpět k nižší hodnotě QPWDLVL, pokud je možný, bohužel není zcela bezbolestný proces. Obecně se dá říci, že by měl panovat názor, že se jedná pouze o jednosměrný proces přechodu z nižších hodnot QPWDLVL na vyšší hodnoty QPWDLVL. Mohou však nastat případy, kdy je třeba znovu nastavit nižší hodnotu QPWDLVL.

V následujících částech se pojednává o činnostech, které je nutné provést při přechodu zpět na nižší úroveň hesla.

Pokyny pro změnu QPWDLVL z hodnoty 3 na hodnotu 2: Tato změna je relativně jednoduchá. Když je QPWDLVL nastavena na hodnotu 2, potřebuje administrátor zjistit, zda některé uživatelské profily musí obsahovat hesla produktu iSeries NetServer nebo hesla úrovně 0 nebo 1, a pokud takové profily existují, změnit jejich heslo na přípustnou hodnotu.

Kromě toho může být nutné změnit systémové hodnoty týkající se hesel zpět na hodnoty kompatibilní s produktem iSeries NetServer a hesly úrovně 0 nebo 1, pokud jsou tato hesla potřebná.

Pokyny pro změnu QPWDLVL z hodnoty 3 na hodnotu 1 nebo 0: Kvůli velmi vysoké pravděpodobnosti vzniku problémů v systému (např. toho typu, že se nikdo nemůže přihlásit z toho důvodu, že byla vymazána všechna hesla úrovně 0 a 1) tato volba není podporována přímo. Má-li se provést změna QPWDLVL 3 na QPWDLVL 1 nebo 0, musí systém nejdříve provést mezikrok, a to změnu na QPWDLVL 2.

Pokyny pro změnu QPWDLVL z hodnoty 2 na hodnotu 1: Před změnou QPWDLVL na hodnotu 1 by měl administrátor pomocí příkazu DSPAUTUSR nebo PRTUSRPRF TYPE(*PWDINFO) vyhledat uživatelské profily, které nemají heslo úrovně 0 nebo 1. Pokud uživatelský profil bude vyžadovat heslo po změně QPWDLVL, měl by administrátor zajistit, aby bylo pro daný profil vytvořeno heslo úrovně 0 a 1 s využitím následujících mechanismů:

- Pomocí CL příkazu CHGUSRPRF nebo CHGPWD nebo rozhraní QSYCHGPW API změňte heslo pro daný uživatelský profil. Na základě toho systém změní heslo, které je použitelné na úrovni hesla 2 nebo 3. Systém rovněž vytvoří ekvivalentní heslo obsahující samá velká písmena, které je použitelné na úrovních hesla 0 a 1. Systém je schopný vytvořit heslo na úrovních hesla 0 a 1 pouze za těchto předpokladů:

– Heslo má délku maximálně 10 znaků.
– Heslo lze převést na velká písmena EBCDIC A-Z, 0-9, @, #, $ a podtržítko.
– Heslo nezačíná číslicí ani podtržítkem.

Například změna hesla na hodnotu RainyDay by vedla k tomu, že by systém vygeneroval heslo na úrovni 0 a 1 s hodnotou RAINYDAY. Avšak změna hodnoty hesla na Rainy Days In April by způsobila, že by systém vymazal heslo úrovně 0 a 1 (neboť je heslo příliš dlouhé a obsahuje mezery).

O tom, že nelze vytvořit heslo úrovně 0 nebo 1, není vytvářena žádná zpráva ani indikace.

- Přihlaste se do systému prostřednictvím mechanismu, který předkládá heslo ve formě prostého textu (nepoužívá substituci hesla). Jestliže je heslo platné a uživatelský profil nemá žádné heslo použitelné na úrovni 0 a 1, vytvoří systém ekvivalentní heslo obsahující samá velká písmena, které je použitelné na úrovních hesla 0 a 1. Systém je schopný vytvořit heslo na úrovních hesla 0 a 1 pouze za výše uvedených předpokladů.

Administrátor potom může změnit QPWDLVL na hodnotu 1. Když tato změna nabyde platnosti (při příštím IPL), vymažou se všechna hesla produktu iSeries NetServer.

Pokyny pro změnu QPWDLVL z hodnoty 2 na hodnotu 0: Platí stejné pokyny jako při změně z hodnoty QPWDLVL 2 na 1 s tím rozdílem, že všechna hesla produktu iSeries NetServer zůstanou zachována, když změna nabyde platnosti.

Pokyny pro změnu QPWDLVL z hodnoty 1 na hodnotu 0: Po změně QPWDLVL na hodnotu 0 by měl administrátor pomocí příkazu DSPAUTUSR nebo PRTUSRPRF vyhledat uživatelské profily, které nemají heslo produktu iSeries NetServer. Pokud uživatelský profil vyžaduje heslo produktu iSeries NetServer, lze ho vytvořit změnou uživatelského hesla nebo přihlášením pomocí mechanismu, který předkládá heslo ve formě prostého textu.

Administrátor pak může změnit QPWDLVL na hodnotu 0.

Změna známých hesel

Chcete-li uzavřít některé známé přístupy na server iSeries, které mohou existovat ve vašem systému, postupujte takto:

__ Krok 1. Ujistěte se, že žádný z uživatelských profilů už nemá předvolené heslo (shodné se jménem uživatelského profilu). Můžete použít příkaz ANZDFTPWD (Analýza předvolených hesel). (Viz část “Jak zabránit používání předvolených hesel” na stránce 25.)

__ Krok 2. Pokuste se přihlásit do vašeho systému pomocí kombinace uživatelských profilů a hesel, které uvádí Tabulka 2 na stránce 21. Tato hesla jsou veřejná a představují první volbu, když se bude někdo pokoušet dostat se do vašeho systému. Pokud se vám podaří přihlásit, změňte pomocí příkazu CHGUSRPRF (Změna uživatelského profilu) heslo na doporučenou hodnotu.

__ Krok 3. Spusťte DST (Dedicated Service Tools) a pokuste se přihlásit pomocí hesel, které uvádí Tabulka 2 na stránce 21. Další informace najdete v rámci aplikace iSeries Information Center—>Zabezpečení—>Servisní nástroje. Informace o tom, jak spustit aplikaci iSeries Information Center najdete v části “Nezbytné předchozí a související informace” na stránce xii.

__ Krok 4. Jestliže se vám podaří přihlásit k DST pomocí některého z těchto hesel, měli byste hesla změnit. Podrobný postup změny ID a hesel uživatelů DST najdete v rámci aplikace iSeries Information Center—>Zabezpečení—>Servisní nástroje. Informace o přístupu k aplikaci iSeries Information Center najdete v části “Nezbytné předchozí a související informace” na stránce xii.

__ Krok 5. Nakonec se ujistěte, že se nemůžete přihlásit pouhým stisknutím klávesy Enter na přihlašovací obrazovce, aniž byste zadali uživatelské ID a heslo. Otestujte několik různých obrazovek. Pokud se vám podaří přihlásit se, aniž byste na přihlašovací obrazovce zadali informace, proveďte jednu z následujících možností:

- Změňte úroveň zabezpečení na 40 nebo 50 (systémová hodnota QSECURITY).

  Poznámka: Vaše aplikace mohou vykazovat určité rozdíly ve zpracování, když úroveň zabezpečení zvýšíte na hodnotu 40 nebo 50.

- Změňte všechny záznamy pracovní stanice pro interaktivní podsystémy, aby se odkazovaly na popisy úlohy, které uvádějí USER(*RQD).

Tabulka 2. Hesla pro profily dodávané společností IBM

ID uživatele	Heslo	Doporučená hodnota
QSECOFR	QSECOFR[1]	Hodnota, která není běžná a která je známá pouze administrátorovi systému. **Zapište si zvolené heslo a uložte je na bezpečném místě.**
QSYSOPR	QSYSOPR	*NONE[2]
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2, 3]
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

Poznámky:

1. Systém je dodáván s hodnotou *Nastavení hesla na ukončenou platnost* pro profil QSECOFR nastavenou na *YES. Když se poprvé přihlásíte do nového systému, musíte změnit heslo QSECOFR.
2. Systém tyto uživatelské profily potřebuje pro systémové funkce, ale vy byste neměli dovolit uživatelům, aby se přihlašovali pomocí těchto profilů. Pro nové systémy počínaje verzí V3R1 je toto heslo dodáváno jako *NONE.

   Když spustíte příkaz CFGSYSSEC, nastaví systém tato hesla na hodnotu *NONE.
3. Pro spouštění produktu iSeries Access for Windows pomocí TCP/IP musí být aktivován uživatelský profil QUSER.

Tabulka 3. Hesla pro DST

Úroveň DST	ID uživatele[1]	Heslo	Doporučená hodnota
Základní schopnost	11111111	11111111	Hodnota, která není běžná a která je známá pouze administrátorovi systému.[2]
Všechny schopnosti	22222222	22222222[3]	Hodnota, která není běžná a která je známá pouze administrátorovi systému.[2]
Schopnost zabezpečení	QSECOFR	QSECOFR[3]	Hodnota, která není běžná a která je známá pouze administrátorovi systému.[2]
Schopnost služeb	QSRV	QSRV[3]	Hodnota, která není běžná a která je známá pouze administrátorovi systému.[2]

Poznámky:

1. ID uživatele je požadováno pouze pro vydání PowerPC AS (RISC) operačního systému.
2. Jestliže se váš servisní zástupce HW potřebuje přihlásit pomocí tohoto ID uživatele a hesla, změňte po je odchodu heslo na novou hodnotu.
3. Platnost uživatelského profilu pro servisní nástroje skončí po jeho prvním použití.

Poznámka: Hesla DST lze měnit pouze pomocí autentizovaného zařízení. To platí i pro všechna hesla a jim odpovídající uživatelská ID, která jsou identická. Další informace o autentizovaných zařízeních obsahuje téma Nastavení produktu Operations Console v rámci aplikace iSeries Information Center.

Nastavení hodnot pro přihlášení

Tabulka 4 ukazuje několik hodnot, které můžete nastavit, abyste znesnadnili neautorizovaným osobám přihlásit se do vašeho systému. Pokud spustíte příkaz CFGSYSSEC, nastaví se tyto systémové hodnoty na doporučené hodnoty. Podrobné informace o těchto systémových hodnotách najdete ve 3. kapitole publikace *Zabezpečení iSeries - referenční informace Reference*.

Tabulka 4. Systémové hodnoty pro přihlášení

Jméno systémové hodnoty	Popis	Doporučené nastavení
QAUTOCFG	Zda systém automaticky konfiguruje nové zařízení.	0 (ne)
QAUTOVRT	Počet popisů virtuálních zařízení, které systém automaticky vytvoří, pokud není k dispozici žádné zařízení.	0
QDEVRCYACN	Co systém provede, když se zařízení znovu připojí po chybě. [1]	*DSCMSG
QDSCJOBITV	Jak dlouho systém čeká, než ukončí odpojenou úlohu.	120
QDSPSGNINF	Zda systém při přihlášení zobrazuje informace o předešlém přihlášení.	1 (ano)
QINACTITV	Jak dlouho systém čeká, než převezme činnost, když je interaktivní úloha neaktivní.	60
QINACTMSGQ	Co systém provede, když se dosáhne doby QINACTITV.	*ENDJOB
QLMTDEVSSN	Zda systém brání uživateli přihlásit se na více pracovních stanicích najednou.	1 (ano)
QLMTSECOFR	Zda se uživatelé se zvláštním oprávněním *ALLOBJ nebo *SERVICE mohou přihlásit pouze na určitých pracovních stanicích.	1 (ano)[2]
QMAXSIGN	Maximální počet po sobě jdoucích neúspěšných pokusů o přihlášení (je nesprávný uživatelský profil nebo heslo).	3
QMAXSGNACN	Co systém provede, když se dosáhne limitu QMAXSIGN.	3 (zablokuje uživatelský profil i zařízení)

Poznámky:

1. Systém může odpojit a znovu připojit relace TELNET, když je explicitně přiřazen popis zařízení pro relaci.
2. Pokud nastavíte tuto systémovou hodnotu na 1 (ano), budete muset uživatelům explicitně poskytnout zvláštní oprávnění *ALLOBJ nebo *SERVICE k zařízením. Nejjednodušším způsobem, jak to provést, je poskytnout ke konkrétním zařízením oprávnění *CHANGE uživatelského profilu QSECOFR.

Změna chybových zpráv pro přihlášení

Hackeři mají rádi přehled, jak se jim daří při získávání přístupu do systému. Když chybová zpráva na přihlašovací obrazovce sděluje Heslo není správné, může hacker předpokládat, že uživatelské ID je správné. Hackera můžete znechutit tím, že pomocí příkazu CHGMSGD (Změna popisu zprávy) změníte text pro dvě chybové zprávy týkající se přihlášení. Tabulka 5 na stránce 23 obsahuje doporučený text.

Tabulka 5. Chybové zprávy pro přihlášení

ID zprávy	Dodaný text	Doporučený text
CPF1107	CPF1107 – Password not correct for user profile. (Heslo pro uživatelský profil není správné.)	Informace pro přihlášení nejsou správné. **Poznámka:** Do textu zprávy nevkládejte ID zprávy.
CPF1120	CPF1120 – User XXXXX does not exist. (Uživatel XXXX neexistuje.)	Informace pro přihlášení nejsou správné. **Poznámka:** Do textu zprávy nevkládejte ID zprávy.

Plánování dostupnosti uživatelských profilů

Možná budete chtít, aby některé uživatelské profily byly dostupné pro přihlášení pouze v určitou dobu v rámci dne nebo v určité dny v týdnu. Pokud například máte nastaven profil pro revizora zabezpečení, můžete chtít aktivovat tento uživatelský profil pouze během hodin, kdy je plánována práce revizora. Možná budete také chtít po dobu průměrného provozu deaktivovat uživatelské profily se zvláštním oprávněním *ALLOBJ (včetně uživatelského profilu QSECOFR).

K nastavení automatické aktivace a deaktivace uživatelských profilů můžete použít příkaz CHGACTSCDE (Změna záznamu plánu aktivace). Pro každý uživatelský profil, který chcete naplánovat, vytvoříte záznam, jenž definuje plán uživatelského profilu.

Jestliže například chcete, aby byl profil QSECOFR dostupný pouze mezi 7. hodinou ranní a 10. hodinou večerní, zadali byste na obrazovce CHGACTSCDE toto:

```
              Change Activation Scd Entry (CHGACTSCDE)

Type choices, press Enter.

User profile . . . . . . . . . . > QSECOFR       Name
Enable time  . . . . . . . . . . > '7:00'        Time, *NONE
Disable time . . . . . . . . . . > '22:00'       Time, *NONE
Days . . . . . . . . . . . . . . > *MON          *ALL, *MON, *TUE, *WED...
                                 > *TUE
                                 > *WED
                                 > *THU
               + for more values > *FRI
```

Obrázek 2. Obrazovka Schedule Profile Activation – příklad

Ve skutečnosti můžete chtít mít profil QSECOFR dostupný pouze po velmi malý počet hodin každý den. Za účelem provádění většiny systémových funkcí můžete používat jiný uživatelský profil s třídou *SECOFR. Tak nebudete vystavovat známý uživatelský profil pokusům ze strany hackerů.

Můžete pravidelně používat příkaz DSPAUDJRNE (Zobrazení záznamů monitorovacího žurnálu), který slouží k vytištění záznamů monitorovacího žurnálu CP (Change Profile neboli změna profilu). Tyto záznamy použijte k ověření, že systém aktivuje a deaktivuje uživatelské profily v souladu s vámi naplánovaným rozvrhem.

Další metodou ověření, že jsou uživatelské profily deaktivovány podle vašeho plánu, je použití příkazu PRTUSRPRF (Tisk uživatelského profilu). Když pro typ sestavy zadáte hodnotu *PWDINFO, bude sestava zahrnovat stav jednotlivých zvolených uživatelských

profilů. Pokud například pravidelně deaktivujete všechny uživatelské profily se zvláštním oprávněním *ALLOBJ, můžete naplánovat, aby se okamžitě po deaktivaci těchto profilů spustil tento příkaz:

```
PRTUSRPRF TYPE(*PWDINFO) SELECT(*SPCAUT) SPCAUT(*ALLOBJ)
```

Odstranění neaktivních uživatelských profilů

Váš systém by měl obsahovat pouze uživatelské profily, které jsou nezbytné. Pokud už uživatelský profil nepotřebujete, protože uživatel odešel nebo nastoupil na jinou práci ve vaší organizaci, odstraňte tento uživatelský profil. Jestliže někdo opustí vaši organizaci na delší období, deaktivujte jeho uživatelský profil. Zbytečný uživatelský profil může poskytnout neautorizovaný přístup do vašeho systému.

Automatická deaktivace uživatelských profilů

Můžete použít příkaz ANZPRFACT (Analýza aktivity profilu) za účelem pravidelné deaktivace uživatelský profilů, které byly neaktivní po určitý počet dní. Při použití příkazu ANZPRFACT zadáváte počet neaktivních dní, který má systém vyhledat. Systém se podívá na datum posledního použití, datum obnovy a datum vytvoření uživatelského profilu.

Když zadáte hodnotu pro příkaz ANZPRFACT, systém naplánuje spouštění úlohy každý týden v 1 hodinu v noci (počínaje dnem, kdy jste prvně zadali hodnotu). Úloha prověří všechny profily a deaktivuje neaktivní profily. Příkaz ANZPRFACT nemusíte znovu použít, dokud nebudete chtít změnit počet neaktivních dní.

Pomocí příkazu CHGACTPRFL (Změna seznamu aktivních profilů) můžete některé profily vyloučit ze zpracování příkazu ANZPRFACT. Příkaz CHGACTPRFL vytvoří seznam uživatelských profilů, které příkaz ANZPRFACT nedeaktivuje bez ohledu na to, jak dlouho byly tyto profily neaktivní.

Když systém spouští příkaz ANZPRFACT, zapisuje záznamy CP do monitorovacího žurnálu pro každý uživatelský profil, který je deaktivovaný. Chcete-li vypsat všechny uživatelské profily, které jsou nově deaktivovány, můžete použít příkaz DSPAUDJRNE.

Poznámka: Systém zapíše záznamy monitorování pouze tehdy, když hodnota QAUDCTL specifikuje *AUDLVL a systémová hodnota QAUDLVL uvádí hodnotu *SECURITY.

Další metodou ověření, že jsou uživatelské profily deaktivovány podle vašeho plánu, je použití příkazu PRTUSRPRF (Tisk uživatelského profilu). Když pro typ sestavy zadáte hodnotu *PWDINFO, bude sestava zahrnovat stav jednotlivých zvolených uživatelských profilů.

Automatické odstranění uživatelských profilů

K řízení odstraňování nebo deaktivování uživatelských profilů můžete použít příkaz CHGEXPSCDE (Změna záznamu o plánovaném ukončení platnosti). Pokud víte, že se uživatel chystá opustit své pracoviště na delší období, můžete naplánovat jeho uživatelský profil tak, aby se odstranil nebo deaktivoval.

Při prvním použití příkaz CHGEXPSCDE vytvoří záznam plánu úlohy, který se spustí každý den jednu minutu po půlnoci. Úloha se podívá do souboru QASECEXP a na jeho základě určí, zda je na tento den naplánováno odstranění nějakých uživatelských profilů.

Pomocí příkazu CHGEXPSCDE můžete uživatelský profil buď deaktivovat, nebo vymazat. Pokud se rozhodnete uživatelský profil vymazat, musíte určit, co má systém provést s objekty, které daný uživatel vlastní. Dříve, než naplánujete výmaz uživatelského profilu,

musíte prozkoumat objekty, které uživatel vlastní. Jestliže například uživatel vlastní programy, které přebírají oprávnění, chcete, aby tyto programy převzaly vlastnictví nového vlastníka? Nebo má nový vlastník více oprávnění, než je nezbytné (např. zvláštní oprávnění)? Možná budete muset vytvořit nový uživatelský profil s určitými oprávněními, který by vlastnil programy, jež potřebují přebírat oprávnění.

Měli byste také zjistit, zda se po vymazání uživatelského profilu nevyskytnou nějaké problémy s aplikacemi. Například, uvádějí některé popisy úlohy daný uživatelský profil jako předvoleného uživatele?

Chcete-li zobrazit seznam uživatelských profilů, které mají být podle plánu deaktivovány nebo odstraněny, můžete použít příkaz DSPEXPSCD (Zobrazení plánu expirace).

K vypsání všech uživatelských profilů ve vašem systému můžete použít příkaz DSPAUTUSR (Zobrazení oprávněných uživatelů). Pokud chcete vymazat prošlé profily, použijte příkaz DLTUSRPRF (Výmaz uživatelského profilu).

Bezpečnostní poznámka: Uživatelský profil deaktivujete tím, že jeho stav nastavíte na hodnotu *DISABLED. Když deaktivujete uživatelský profil, není pak k dispozici pro interaktivní použití. Pomocí deaktivovaného uživatelského profilu se nemůžete přihlásit ani na něj nemůžete změnit svou úlohu. Pod deaktivovaným uživatelský profilem je možné spouštět dávkové úlohy.

Jak zabránit používání předvolených hesel

Když vytváříte nový uživatelský profil, nastaví se heslo standardně na stejnou hodnotu, jako má jméno uživatelského profilu. Tím vzniká příležitost pro ty, kteří se chtějí dostat do vašeho systému, pokud znají vaši strategii pro přiřazování jmen profilů a vědí, že do vaší organizace nastoupil nový člověk.

Když vytváříte nové uživatelské profily, zvažte, zda místo předvoleného hesla nepřiřadit jedinečné heslo, které není triviální. Heslo sdělte novému uživateli důvěrně, například v dopise “Welcome to the System”, který nastiňuje vaši strategii zabezpečení ochrany dat. Přimějte uživatele ke změně hesla hned, jak se prvně přihlásí, tím způsobem, že nastavíte uživatelský profil na PWDEXP(*YES).

Chcete-li zkontrolovat, zda uživatelské profily ve vašem systému nemají předvolená hesla, použijte příkaz ANZDFTPWD (Analýza předvolených hesel). Když tisknete sestavu, můžete specifikovat, že má systém provést nějakou akci (např. deaktivovat uživatelský profil), pokud se heslo shoduje se jménem uživatelského profilu. Příkaz ANZDFTPWD vytiskne seznam profilů, které nalezl, a všechny akce, které provedl.

Poznámka: Hesla jsou v systému uložena v jednosměrně kódované formě. Nelze je dešifrovat. Systém zašifruje zadané heslo a porovná ho s uloženým heslem stejným způsobem, jako když kontroluje heslo při vašem přihlášení do systému. Pokud prověřujete selhání oprávnění (*AUTFAIL), zapíše systém záznam monitorovacího žurnálu PW pro každý uživatelský profil, který *nemá* předvolené heslo (pro systémy verze V4R1 nebo nižší). Počínaje verzí V4R2 už systém nezapisuje záznamy monitorovacího žurnálu PW, když spustíte příkaz ANZDFTPWD.

Monitorování aktivit souvisejících s přihlašováním a hesly

Pokud se obáváte neoprávněných pokusů o přístup k vašemu systému, můžete využít příkaz PRTUSRPRF k monitorování aktivit souvisejících s přihlašováním a hesly.

Dále je uvedeno několik návrhů pro práci s touto sestavou:

- Zjistěte, zda interval ukončení platnosti hesla pro některé uživatelské profily není delší, než systémová hodnota, a zda je tento delší interval odůvodněný. Například uživatelský profil USERY má v sestavě hodnotu pro interval ukončení platnosti hesla rovnou 120 dnům.
- Tuto sestavu spouštějte pravidelně a sledujte v ní neúspěšné pokusy o přihlášení. Někdo, kdo se snaží získat přístup do vašeho systému, si může uvědomovat, že systém provede nějakou akci po určitém počtu neúspěšných pokusů. Proto se tento potenciální vetřelec může snažit o přístup méněkrát, než je hodnota QMAXSIGN, aby vás jeho pokusy zbytečně nevyplašily. Pokud však spustíte tuto sestavu každý den brzy ráno a všimnete si, že určité profily mají často neúspěšné pokusy o přihlášení, můžete tušit problém.
- Identifikujte uživatelské profily, které nebyly dlouhou dobu používány nebo jejichž hesla nebyla dlouho změněna.

Uložení informací o heslech

Za účelem podpory některých síťových funkcí a požadavků na komunikace poskytují servery iSeries metodu zabezpečení pro uložení hesel, která by mohla být dešifrována. Systém tato hesla využívá například k navázání připojení SLIP v jiným systémem. (Použití uložených hesel popisuje část “Zabezpečení odchozích relací” na stránce 118.)

Servery iSeries ukládají tato speciální hesla do zabezpečené oblasti, která není přístupná žádným uživatelským programům ani rozhraním. Tato hesla mohou nastavovat a načítat pouze explicitně autorizované systémové funkce.

Pokud například používáte uložené heslo pro odchozí připojení SLIP, nastavujete toto heslo pomocí systémového příkazu, který vytváří konfigurační profil (WRKTCPPTP). K použití příkazu musíte mít oprávnění *IOSYSCFG. Během procedury vytáčení se heslo načte pomocí speciálního kódovaného skriptu pro spojení, který heslo dešifruje. Dešifrované heslo není pro uživatele ani žádné protokoly úlohy viditelné.

Jako administrátor systému se musíte rozhodnout, zda dovolíte, aby hesla, která je možné dešifrovat, byla uložena ve vašem systému. Toto určuje systémová hodnota QRETSVRSEC (zachycení dat zabezpečení serveru). Předvolenou hodnotou je 0 (ne). Proto váš systém nebude ukládat hesla, která je možné dešifrovat, pokud tuto systémovou hodnotu explicitně nenastavíte.

Pokud vaše síťové zpracování nebo komunikace vyžadují uložená hesla, měli byste zavést vhodnou strategii a seznámit se se strategiemi a praktikami vašich partnerů, se kterými komunikujete. Pokud například používáte SLIP ke komunikaci s jiným serverem iSeries, mělo by se u obou systémů zvážit, zda pro navazování relací nezaložit zvláštní uživatelské profily. Tyto zvláštní profily by měly mít omezené oprávnění v systému. Tím omezíte negativní dopad případného prozrazení uloženého hesla v partnerském systému.

Kapitola 4. Jak nakonfigurovat server iSeries, aby používal nástroje zabezpečení

Tyto informace popisují, jak nastavit váš systém, aby používal nástroje zabezpečení, které jsou součástí operačního systému OS/400. Když nainstalujete operační systém OS/400, jsou nástroje zabezpečení připraveny pro použití. Následující témata předkládají návrhy pro práci s procedurami pomocí nástrojů zabezpečení.

Bezpečné ovládání nástrojů zabezpečení

Když nainstalujete operační systému OS/400, jsou objekty, které jsou asociovány s nástroji zabezpečení, zabezpečené. Chcete-li s nástroji zabezpečení pracovat bezpečně, vyvarujte se jakýchkoliv změn v oprávněních k objektům nástrojů zabezpečení.

Dále jsou uvedena nastavení zabezpečení a požadavky pro objekty nástrojů zabezpečení:

- Programy a příkazy nástrojů zabezpečení jsou uloženy v knihovně produktů QSYS. Tyto příkazy a programy jsou dodávány s veřejným oprávněním *EXCLUDE. Mnoho z příkazů nástrojů zabezpečení vytváří soubory v knihovně QUSRSYS. Když systém vytvoří tyto soubory, má veřejné oprávnění pro soubory hodnotu *EXCLUDE.

  Soubory, které obsahují informace pro vytváření sestav změn, mají jména začínající na QSEC. Soubory, které obsahují informace pro správu uživatelských profilů, mají jména začínající na QASEC. Tyto soubory obsahují důvěrné informace o vašem systému. Proto byste k uvedeným souborům neměli měnit veřejné oprávnění.
- Nástroje zabezpečení používají běžné nastavení vašeho systému pro směrování tištěného výstupu. Tyto sestavy obsahují důvěrné informace o vašem systému. Chcete-li výstup směrovat do chráněné výstupní fronty, proveďte odpovídající změny v uživatelském profilu nebo popisu úlohy pro ty uživatele, kteří budou spouštět nástroje zabezpečení.
- Jelikož příkazy nástrojů zabezpečení používají své funkce zabezpečení a pracují s řadou objektů v systému, vyžadují zvláštní oprávnění *ALLOBJ. Některé z příkazů také vyžadují zvláštní oprávnění *SECADM, *AUDIT nebo *IOSYSCFG. Abyste měli jistotu, že příkazy budou fungovat správně, měli byste se přihlašovat jako správce systému, když používáte nástroje zabezpečení. Proto byste neměli udělovat soukromé oprávnění k žádnému z příkazů nástrojů zabezpečení.

Jak předejít konfliktům mezi soubory

Mnoho z příkazů pro práci se sestavami nástrojů zabezpečení vytváří databázový soubor, který můžete použít k vytištění změněné verze sestavy. V části ″“Příkazy a menu pro nástroje zabezpečení” na stránce 28″ jsou uvedena jména souborů pro jednotlivé příkazy. Příkaz můžete v jeden okamžik spouštět vždy jen z jedné úlohy. Řada příkazů má již nyní kontroly, které toto vynucují. Pokud spustíte nějaký příkaz ve chvíli, kdy jej ještě jiná úloha nedokončila, dostanete chybovou zprávu.

Mnoho tiskových úloh je časově náročných. Když posíláte sestavy do dávky nebo je přidáváte do plánovače úloh, musíte být opatrní, abyste nezpůsobili konflikty mezi soubory. Například můžete chtít vytisknout dvě verze sestavy PRTUSRPRF s různými kritérii výběru. Jestliže předáváte sestavy do dávky, měli byste použít frontu úloh, která v určitý okamžik zpracovává vždy jen jednu úlohu, abyste měli jistotu, že se úlohy sestav zpracují postupně.

Pokud používáte plánovač úloh, je třeba naplánovat tyto dvě úlohy s dostatečným odstupem, aby se první verze stihla dokončit předtím, než se spustí druhá úloha.

Uložení nástrojů zabezpečení

Programy nástrojů zabezpečení se uloží vždy, když spustíte příkaz SAVSYS (Uložení systému) nebo volbu z menu Uložení, která spouští příkaz SAVSYS.

Soubory nástrojů zabezpečení jsou uloženy v knihovně QUSRSYS. Tuto knihovnu byste už měli ukládat v rámci vašich běžných provozních postupů. Knihovna QUSRSYS obsahuje data pro mnoho licencovaných programů ve vašem systému. Další informace o příkazech a volbách, které slouží k uložení knihovny QUSRSYS, najdete v rámci aplikace Information Center.

Příkazy a menu pro nástroje zabezpečení

Tato část popisuje příkazy a menu pro nástroje zabezpečení. V rámci těchto informací najdete příklady použití příkazů.

Pro nástroje zabezpečení jsou k dispozici dvě menu:

- Menu SECTOOLS (Security Tools) pro interaktivní spouštění příkazů.
- Menu SECBATCH (Submit or Schedule Security Reports to Batch) pro spouštění pro práci se sestavami v dávce. Menu SECBATCH má dvě části. První část používá příkaz SBMJOB (Zadání úlohy) pro předání sestav k okamžitému zpracování v dávce.

  Druhá část menu používá příkaz ADDJOBSCDE (Přidání záznamu plánu úlohy). Ten slouží k naplánování toho, aby se sestavy o zabezpečení spouštěly pravidelně v určitý den a čas.

Volby menu Security Tools

Tabulka 6 popisuje následující volby menu a k nim přiřazené příkazy:

Tabulka 6. Příkazy nástrojů pro uživatelské profily

Volba menu[1]	Jméno příkazu	Popis	Použitý databázový soubor
1	ANZDFTPWD	Příkaz Analýza předvolených hesel slouží k vytvoření sestav a provedení určité akce pro ty uživatelské profily, jejichž heslo je shodné se jménem uživatelského profilu.	QASECPWD[2]
2	DSPACTPRFL	Příkaz Zobrazení seznamu aktivních profilů slouží k zobrazení nebo vytištění seznamu uživatelských profilů, které jsou vyloučeny ze zpracování ANZPRFACT.	QASECIDL[2]
3	CHGACTPRFL	Příkaz Změna seznamu aktivních profilů slouží k přidání nebo odstranění uživatelských profilů ze seznamu výjimek pro příkaz ANZPRFACT. Uživatelský profil, který je uveden v seznamu aktivních profilů, je trvale aktivní (dokud jej neodstraníte ze seznamu). Příkaz ANZPRFACT neprovede deaktivaci profilu, který je v seznamu aktivních profilů, bez ohledu na to, jak dlouho byl profil neaktivní.	QASECIDL[2]
4	ANZPRFACT	Příkaz Analýza aktivity profilu slouží k deaktivaci uživatelských profilů, které nebyly použity po určitý počet dní. Poté, co v příkazu ANZPRFACT zadáte počet dní, systém v noci spustí úlohu ANZPRFACT. Chcete-li vyloučit některé uživatelské profily, aby nedošlo k jejich deaktivaci, použijte příkaz CHGACTPRFL.	QASECIDL[2]

Tabulka 6. Příkazy nástrojů pro uživatelské profily (pokračování)

Volba menu[1]	Jméno příkazu	Popis	Použitý databázový soubor
5	DSPACTSCD	Příkaz Zobrazení plánu aktivace profilů slouží k zobrazení nebo vytištění informací o plánu aktivace a deaktivace určitých uživatelských profilů. Tento plán vytvoříte pomocí příkazu CHGACTSCDE.	QASECACT[2]
6	CHGACTSCDE	Příkaz Změna záznamu plánu aktivace slouží k tomu, aby se uživatelský profil zpřístupnil pro přihlášení pouze v určitou dobu dne nebo týdne. Pro každý uživatelský profil, který plánujete, systém vytvoří záznam plánu úlohy pro dobu aktivace a deaktivace.	QASECACT[2]
7	DSPEXPSCD	Příkaz Zobrazení plánu expirace slouží k zobrazení nebo vytištění seznamu uživatelských profilů, pro něž je v budoucnosti naplánována deaktivace nebo odstranění. K nastavení ukončení platnosti uživatelského profilu se používá příkaz CHGEXPSCDE.	QASECEXP[2]
8	CHGEXPSCDE	Příkaz Změna záznamu o plánovaném ukončení platnosti slouží k plánování odstranění uživatelského profilu. Uživatelský profil můžete odstranit dočasně (jeho deaktivací) nebo jej můžete vymazat ze systému. Tento příkaz používá záznam plánu úlohy, který se spouští každý den v 00:01 (minutu po půlnoci). Úloha se podívá do souboru QASECEXP a určí z něj, zda je u některých uživatelských profilů na daný den nastaveno ukončení platnosti. K zobrazení uživatelských profilů, které mají naplánováno ukončení platnosti, použijte příkaz DSPEXPSCD.	QASECEXP[2]
9	PRTPRFINT	Příkaz Tisk vnitřních informací profilu slouží k vytištění sestavy obsahující informace o počtu záznamů v uživatelském profilu. Počet záznamů určuje velikost uživatelského profilu.	

Poznámky:

1. Jedná se o volby z menu SECTOOLS.
2. Tento soubor se nachází v knihovně QUSRSYS.

Stisknutím klávesy Page Down v menu zobrazíte další volby. Tabulka 7 na stránce 30 popisuje volby menu a jim přiřazené příkazy pro monitorování zabezpečení:

Tabulka 7. Příkazy nástrojů pro monitorování zabezpečení

Volba menu[1]	Jméno příkazu	Popis	Použitý databázový soubor
10	CHGSECAUD	Příkaz Změna monitorování zabezpečení slouží k nastavení monitorování zabezpečení a ke změně systémových hodnot, které řídí monitorování zabezpečení. Když spustíte příkaz CHGSECAUD, vytvoří systém žurnál monitorování zabezpečení (QAUDJRN), pokud ještě neexistuje. Příkaz CHGSECAUD poskytuje volby, které usnadňují nastavení systémové hodnoty QAUDLVL (úroveň monitorování). Chcete-li aktivovat všechna možná nastavení úrovní monitorování, zadejte *ALL. Nebo můžete zadat hodnotu *DFTSET a aktivuje se většina běžně používaných nastavení (*AUTFAIL, *CREATE, *DELETE, *SECURITY a *SAVRST). **Poznámka:** Jestliže k nastavení monitorování používáte nástroje zabezpečení, nezapomeňte naplánovat správu vašich příjemců monitorovacího žurnálu. Jinak byste mohli brzy narazit na problémy s využitím disků.	
11	DSPSECAUD	Příkaz Zobrazení monitorování zabezpečení slouží k zobrazení informací o žurnálu monitorování zabezpečení a systémových hodnotách, které řídí monitorování zabezpečení.	

Poznámky:

1. Jedná se o volby z menu SECTOOLS.

Použití menu Security Batch

Níže je uvedena první část menu SECBATCH:

```
SECBATCH         Submit or Schedule Security Reports To Batch
                                                                  System:
Select one of the following:

  Submit Reports to Batch
     1. Adopting objects
     2. Audit journal entries
     3. Authorization list authorities
     4. Command authority
     5. Command private authorities
     6. Communications security
     7. Directory authority
     8. Directory private authority
     9. Document authority
    10. Document private authority
    11. File authority
    12. File private authority
    13. Folder authority
```

Když vyberete nějakou volbu z tohoto menu, objeví se obrazovka SBMJOB (Submit Job). Jestliže chcete změnit předvolené volby pro příkaz, můžete stisknout klávesu F4 (Náznak) na řádce *Command to run*.

Abyste se dostali na volbu Schedule Batch Reports, použijte v menu SECBATCH klávesu Page Down. Pomocí voleb v této části menu můžete například nastavit váš systém tak, aby

pravidelně spouštěl změněné verze sestav. Další volby menu se zobrazí, když použijete klávesu Page Down. Když vyberete volbu z této části menu, objeví se obrazovka ADDJOBSCDE (Add Job Schedule Entry).

Jestliže chcete pro sestavu zvolit odlišné nastavení, můžete kurzor nastavit na řádku *Command to run* a stisknout klávesu F4 (Náznak). Úloze byste měli přiřadit smysluplné jméno, abyste ji rozpoznali, když si zobrazíte záznamy plánu úloh.

Volby menu Security Batch

Tabulka 8 popisuje volby menu a jim přiřazené příkazy pro sestavy o zabezpečení:

Když spustíte sestavy o zabezpečení, vytiskne systém pouze informace, které splňují jak vámi zadaná kritéria výběru, tak kritéria výběru pro daný nástroj. Například popisy úloh, které uvádějí jméno uživatelského profilu, jsou významné z hlediska zabezpečení. Proto sestava popisů úloh (PRTJOBDAUT) vytiskne popisy úloh v zadané knihovně pouze za předpokladu, že veřejné oprávnění pro daný popis úlohy není *EXCLUDE *a* že popis úlohy uvádí v parametru USER jméno uživatelského profilu.

Podobně, když tisknete informace o podsystému (příkaz PRTSBSDAUT), vytiskne systém informace o podsystému pouze tehdy, když popis podsystému má záznam komunikace, který specifikuje nějaký uživatelský profil.

Jestliže určitá sestava vytiskne méně informací, než jste očekávali, podívejte se do informací online nápovědy a zjistěte kritéria výběru pro danou sestavu.

Tabulka 8. Příkazy pro sestavy o zabezpečení

Volba menu[1]	Jméno příkazu	Popis	Použitý databázový soubor
1, 40	PRTADPOBJ	Příkaz Tisk adoptovaných objektů slouží k vytištění seznamu objektů, které přebírají oprávnění určeného uživatelského profilu. Můžete zadat jediný profil, generické jméno profilu (např. všechny profily, které začínají na Q) nebo všechny uživatelské profily v systému. Tato sestava má dvě verze. Plná verze obsahuje všechny adoptované objekty, které splňují kritéria výběru. Sestava změn uvádí rozdíly mezi adoptovanými objekty, které jsou v danou chvíli v systému, a adoptovanými objekty, které byly v systému, když jste naposled spouštěli sestavu.	QSECADPOLD[2]
2, 41	DSPAUDJRNE	Příkaz Zobrazení záznamů monitorovacího žurnálu slouží k zobrazení nebo vytištění informací o záznamech v žurnálu monitorování zabezpečení. Můžete zvolit určitý typ záznamů, určité uživatele a dobu.	QASYxxJ4[3]

Tabulka 8. Příkazy pro sestavy o zabezpečení (pokračování)

Volba menu[1]	Jméno příkazu	Popis	Použitý databázový soubor
3, 42	PRTPVTAUT *AUTL	Když použijete příkaz Tisk soukromých oprávnění pro objekty *AUTL, dostanete seznam všech seznamů oprávnění v systému. Sestava zahrnuje uživatele, kteří mají oprávnění k jednotlivým seznamům, a oprávnění, které mají tito uživatelé k danému seznamu. Tyto informace slouží k analýze zdrojů oprávnění k objektům ve vašem systému. Tato sestava má tři verze. Plná verze obsahuje seznam všech seznamů oprávnění v systému. Sestava změn uvádí seznam doplnění a změn v oprávněních, ke kterým došlo od posledního spuštění sestavy. Sestava výmazů obsahuje seznam uživatelů, jejichž oprávnění k seznamu oprávnění bylo od posledního spuštění sestavy vymazáno. Když tisknete plnou sestavu, máte možnost vytisknout seznam objektů, které jsou chráněny jednotlivými seznamy oprávnění. Systém vytvoří zvláštní sestavu pro každý seznam oprávnění.	QSECATLOLD[2]
6, 45	PRTCMNSEC	Příkaz Tisk zabezpečení komunikací slouží k vytištění nastavení souvisejících se zabezpečením pro objekty, které mají vliv na komunikace v systému. Tato nastavení ovlivňují způsob, jakým mohou uživatelé a úlohy vstupovat do vašeho systému. Tento příkaz vytváří dvě sestavy: sestavu, která zobrazuje nastavení pro konfigurační seznamy v systému, a sestavu, která zobrazuje parametry související se zabezpečením pro popis linky, řadiče a popisy zařízení. Každá z těchto sestav má svoji plnou a změněnou verzi.	QSECCMNOLD[2]
15, 54	PRTJOBDAUT	Příkaz Tisk oprávnění k popisu úlohy slouží k vytištění seznamu popisů úloh, které specifikují uživatelský profil a mají veřejné oprávnění, jež není *EXCLUDE. Sestava ukazuje zvláštní oprávnění pro uživatelský profil, který je uveden v popisu úlohy. Tato sestava má dvě verze. Plná verze uvádí všechny objekty popisů úloh, které splňují kritéria výběru. Sestava změn uvádí rozdíly mezi objekty popisů úloh, které jsou v danou chvíli v systému, a objekty popisů úloh, které byly v systému, když jste naposled spouštěli sestavu.	QSECJBDOLD[2]

Tabulka 8. Příkazy pro sestavy o zabezpečení (pokračování)

Volba menu[1]	Jméno příkazu	Popis	Použitý databázový soubor
Viz poznámka 4.	PRTPUBAUT	Příkaz Tisk veřejně oprávněných objektů slouží k vytištění seznamu objektů, jejichž veřejné oprávnění není *EXCLUDE. Při spuštění příkazu zadáváte pro sestavu typ objektu a knihovnu(y). Příkaz PRTPUBAUT můžete použít k vytištění informací o objektech, k nimž má přístup každý uživatel v systému. Tato sestava má dvě verze. Plná verze uvádí všechny objekty, které splňují kritéria výběru. Sestava změn uvádí rozdíly mezi zadanými objekty, které jsou v danou chvíli v systému, a objekty (stejného typu a ve stejné knihovně), které byly v systému, když jste naposled spouštěli sestavu.	QPBxxxxxx[5]
Viz poznámka 5.	PRTPVTAUT	Příkaz Tisk soukromých oprávnění slouží k vytištění seznamu soukromých oprávnění k objektům určitého typu v zadané knihovně. Tato sestava vám pomůže určit zdroje oprávnění k objektům. Tato sestava má tři verze. Plná verze uvádí všechny objekty, které splňují kritéria výběru. Sestava změn uvádí rozdíly mezi zadanými objekty, které jsou v danou chvíli v systému, a objekty (stejného typu a ve stejné knihovně), které byly v systému, když jste naposled spouštěli sestavu. Sestava výmazů obsahuje seznam uživatelů, jejichž oprávnění k objektu bylo od posledního spuštění sestavy vymazáno.	QPVxxxxxx[5]
24, 63	PRTQAUT	Příkaz Tisk oprávnění k frontě slouží k vytištění nastavení zabezpečení pro výstupní fronty a fronty úloh v systému. Tato nastavení řídí, kdo může prohlížet a měnit záznamy ve výstupní frontě a frontě úloh. Tato sestava má dvě verze. Plná verze uvádí všechny objekty výstupních front a front úloh, které splňují kritéria výběru. Sestava změn uvádí rozdíly mezi objekty výstupních front a front úloh, které jsou v danou chvíli v systému, a objekty výstupních front a front úloh, které byly v systému, když jste naposled spouštěli sestavu.	QSECQOLD[2]
25, 64	PRTSBSDAUT	Příkaz Tisk popisu podsystému slouží k vytištění záznamů komunikací souvisejících se zabezpečením pro popisy podsystému ve vašem systému. Tato nastavení řídí, jak může práce vstupovat do systému a jak jsou úlohy zpracovávány. Sestava vytiskne popis podsystému pouze tehdy, když existují záznamy komunikací, které uvádějí jméno uživatelského profilu. Tato sestava má dvě verze. Plná verze uvádí všechny objekty popisů podsystémů, které splňují kritéria výběru. Sestava změn uvádí rozdíly mezi objekty popisů podsystémů, které jsou v danou chvíli v systému, a objekty popisů podsystémů, které byly v systému, když jste naposled spouštěli sestavu.	QSECSBDOLD[2]

Tabulka 8. Příkazy pro sestavy o zabezpečení (pokračování)

Volba menu[1]	Jméno příkazu	Popis	Použitý databázový soubor
26, 65	PRTSYSSECA	Příkaz Tisk atributů zabezpečení systému slouží k vytištění seznamu systémových hodnot a atributů sítí souvisejících se zabezpečením. Sestava uvádí aktuální hodnotu a doporučenou hodnotu.	
27, 66	PRTTRGPGM	Příkaz Tisk triggerů slouží k vytištění seznamu triggerů, které jsou asociovány s databázovými soubory v systému. Tato sestava má dvě verze. Plná verze uvádí každý spouštěcí impuls, který je přiřazen a splňuje vaše kritéria výběru. Sestava změn obsahuje triggery, které byly přiřazeny od té doby, kdy jste naposled spustili tuto sestavu.	QSECTRGOLD[2]
28, 67	PRTUSROBJ	Příkaz Tisk uživatelských objektů slouží k vytištění seznamu uživatelských objektů (objektů, které nebyly dodány společností IBM), které jsou v knihovně. Tuto sestavu můžete použít k vytištění seznamu uživatelských objektů, které jsou uloženy v nějaké knihovně (např. QSYS), jež se nachází v systémové části seznamu knihoven. Tato sestava má dvě verze. Plná verze uvádí všechny uživatelské objekty, které splňují kritéria výběru. Sestava změn uvádí rozdíly mezi uživatelskými objekty, které jsou v danou chvíli v systému, a uživatelskými objekty, které byly v systému, když jste naposled spouštěli sestavu.	QSECPUOLD[2]
29, 68	PRTUSRPRF	Příkaz Tisk uživatelského profilu slouží k analýze uživatelských profilů, které splňují zadaná kritéria. Uživatelské profily můžete vybírat na základě zvláštních oprávnění, třídy uživatele nebo podle kombinace zvláštních oprávnění a třídy uživatele. Můžete si vytisknout informace o oprávněních, o prostředí, o hesle a jeho úrovni.	
30, 69	PRTPRFINT	Příkaz Tisk vnitřních informací profilu slouží k vytištění sestavy obsahující informace o počtu záznamů.	
31, 70	CHKOBJITG	Příkaz Kontrola integrity objektu slouží k určení, zda objekty, s nimiž lze operovat (např. programy), byly změněny bez použití kompilátoru. Tento příkaz vám může pomoci při zjišťování pokusů o zavedení viru do vašeho systému nebo o změnu programu za účelem provádění neoprávněných instrukcí. Další informace o příkazu CHKOBJITG obsahuje publikace *Zabezpečení iSeries - referenční informace Reference*.	

Tabulka 8. Příkazy pro sestavy o zabezpečení (pokračování)

Volba menu[1]	Jméno příkazu	Popis	Použitý databázový soubor
Poznámky: 1. Jedná se o volby z menu SECBATCH. 2. Tento soubor se nachází v knihovně QUSRSYS. 3. xx je dvouznakový typ záznamu žurnálu. Například modelový výstupní soubor pro záznamy žurnálu AE je QSYS/QASYAEJ4. Modelové výstupní soubory jsou popsány v dodatku F publikace *Zabezpečení iSeries - referenční informace Reference*. 4. Menu SECBATCH obsahuje volby pro typy objektů, které jsou předmětem zájmu administrátora systému. Například můžete použít volby 11 nebo 50, chcete-li příkaz PRTPUBAUT spustit vůči objektům *FILE. K zadání typu objektu použijte obecné volby (18 a 57). 5. Menu SECBATCH obsahuje volby pro typy objektů, které jsou předmětem zájmu administrátora systému. Například volby 12 nebo 51 spouštějí příkaz PRTPVTAUT vůči objektům *FILE. K zadání typu objektu použijte obecné volby (19 a 58). 6. xxxxxx ve jménu souboru je typ objektu. Například soubor pro objekty typu program se nazývá QPBPGM pro veřejná oprávnění a QPVPGM pro soukromá oprávnění. Soubory jsou uloženy v knihovně QUSRSYS. Soubor obsahuje člen pro každou knihovnu, pro niž jste vytiskli sestavu. Jméno členu je shodné se jménem knihovny.			

Příkazy pro přizpůsobení zabezpečení

Tabulka 9 popisuje příkazy, které můžete použít k přizpůsobení zabezpečení ochrany dat ve vašem systému. Tyto příkazy se nacházejí v menu SECTOOLS.

Tabulka 9. Příkazy pro přizpůsobení systému

Volba menu[1]	Jméno příkazu	Popis	Použitý databázový soubor
60	CFGSYSSEC	Příkaz Konfigurace zabezpečení systému slouží k nastavení systémových hodnot souvisejících se zabezpečením na jejich doporučené nastavení. Příkaz také nastaví monitorování zabezpečení v systému. V části "Hodnoty nastavované příkazem konfigurace zabezpečení systému" je popsáno, co příkaz provádí. **Poznámka:** Chcete-li získat doporučení týkající se zabezpečení, která odpovídají vaší situaci, spusťte místo tohoto příkazu program iSeries Security Wizard nebo iSeries Security Advisor. Další informace o těchto nástrojích uvádí Kapitola 2, "Programy iSeries Security Wizard a eServer Security Planner", na stránce 11.	
61	RVKPUBAUT	Příkaz Vyvolání obecného oprávnění slouží k nastavení veřejného oprávnění na hodnotu *EXCLUDE pro sadu příkazů souvisejících se zabezpečením v systému. Činnosti, které provádí příkaz RVKPUBAUT, popisuje část "Funkce příkazu Vyvolání obecného oprávnění" na stránce 37.	
Poznámky: 1. Jedná se o volby z menu SECTOOLS.			

Hodnoty nastavované příkazem konfigurace zabezpečení systému

Tabulka 10 na stránce 36 uvádí seznam systémových hodnot, které se nastaví, když spustíte příkaz CFGSYSSEC. Příkaz CFGSYSSEC spouští program s názvem QSYS/QSECCFGS.

Tabulka 10. Hodnoty nastavené příkazem CFGSYSSEC

Jméno systémové hodnoty	Nastavení	Popis systémové hodnoty
QALWOBJRST	*NONE	Zda lze obnovit systémové stavové programy a programy, které přebírají oprávnění.
QAUTOCFG	0 (ne)	Automatická konfigurace nových zařízení.
QAUTOVRT	0	Počet popisů virtuálních zařízení, které systém automaticky vytvoří, pokud není k dispozici žádné zařízení.
QDEVRCYACN	*DSCMSG (odpojit se zprávou)	Akce systému, když se znovu navazuje komunikace.
QDSCJOBITV	120	Doba, po kterou systém čeká, než provede nějakou akci pro odpojenou úlohu.
QDSPSGNINF	1 (ano)	Zda se uživatelům zobrazuje obrazovka s informacemi o přihlášení.
QINACTITV	60	Doba, po kterou systém čeká, než provede nějakou akci pro neaktivní interaktivní úlohu.
QINACTMSGQ	*ENDJOB	Akce, kterou systém provede pro neaktivní úlohu.
QLMTDEVSSN	1 (ano)	Zda jsou uživatelé omezeni v tom směru, že se v daném okamžiku mohou přihlásit pouze k jednomu zařízení.
QLMTSECOFR	1 (ano)	Zda jsou uživatelé *ALLOBJ a *SERVICE omezeni pouze na určitá zařízení.
QMAXSIGN	3	Kolik po sobě jdoucích neúspěšných pokusů o přihlášení je povoleno.
QMAXSGNACN	3 (oba)	Zda systém při dosažení limitu QMAXSIGN zablokuje pracovní stanici nebo uživatelský profil.
QRMTSIGN	*FRCSIGNON	Jak systém zpracovává pokusy o vzdálené připojení (ovládat nebo TELNET).
QRMTSVRATR	0 (vypnuto)	Umožňuje, aby byl systém analyzován vzdáleně.
QSECURITY [1 na stránce 37]	50	Úroveň zabezpečení, která je vynucená.
QVFYOBJRST	3 (ověřovat podpisy při obnově)	Ověřovat objekty při obnově.
QPWDEXPITV	60	Jak často musí uživatelé měnit svá hesla.
QPWDMINLEN	6	Minimální délka hesel.
QPWDMAXLEN	8	Maximální délka hesel.
QPWDPOSDIF	1 (ano)	Zda se každá pozice v novém hesle musí lišit od stejné pozice v předešlém hesle.
QPWDLMTCHR	Viz poznámka 2 na stránce 37.	Znaky, které nejsou dovoleny v heslech.
QPWDLMTAJC	1 (ano)	Zda jsou v heslech zakázána sousedící čísla.
QPWDLMTREP	2 (nelze je opakovat vedle sebe)	Zda jsou v heslech zakázány opakující se znaky.
QPWDRQDDGT	1 (ano)	Zda heslo musí obsahovat alespoň jedno číslo.
QPWDRQDDIF	1 (32 jedinečných hesel)	Kolik jedinečných hesel je požadováno, než je možné zopakovat nějaké heslo.
QPWDVLDPGM	*NONE	Uživatelský ukončovací program, který systém volá za účelem ověření hesel.

Tabulka 10. Hodnoty nastavené příkazem CFGSYSSEC (pokračování)

Jméno systémové hodnoty	Nastavení	Popis systémové hodnoty

Poznámky:

1. Pokud v současnosti máte systémovou hodnotu QSECURITY nastavenu na hodnotu 40 nebo nižší, přečtěte si informace ve 2. kapitole publikace *Zabezpečení iSeries - referenční informace Reference* dříve, než provedete změnu na vyšší úroveň zabezpečení.
2. Vyhrazené znaky jsou uloženy v ID zprávy CPXB302 v souboru zpráv QSYS/QCPFMSG. Jsou dodávány jako AEIOU@$#. Ke změně vyhrazených znaků můžete použít příkaz CHGMSGD (Změna popisu zprávy). Systémová hodnota QPWDLMTCHR je vynucována na úrovni hesla 2 nebo 3.

Příkaz CFGSYSSEC také nastaví heslo na hodnotu *NONE pro níže uvedené uživatelské profily dodávané IBM:

QSYSOPR

QPGMR

QUSER

QSRV

QSRVBAS

Nakonec příkaz CFGSYSSEC nastaví monitorování zabezpečení pomocí příkazu CHGSECAUD (Změna monitorování zabezpečení). Příkaz CFGSYSSEC zapne monitorování akcí a objektů a také specifikuje předvolenou sadu akcí, které se mají v příkazu CHGSECAUD monitorovat.

Přizpůsobení programu

Jestliže některá z těchto nastavení neodpovídají vaší instalaci, můžete si vytvořit svou vlastní verzi programu, který zpracovává tento příkaz. Postupujte takto:

__ Krok 1. Pomocí příkazu RTVCLSRC (Načtení CL zdroje) zkopírujte zdroj pro program, který se spouští, když použijete příkaz CFGSYSSEC. Jedná se o program QSYS/QSECCFGS. Když jej načtete, dejte mu *odlišné jméno*.

__ Krok 2. Upravte program podle potřeby. Pak jej zkompilujte. Při kompilaci se ujistěte, že *nenahrazujete* program QSYS/QSECCFGS dodaný IBM. Váš program by měl mít jiné jméno.

__ Krok 3. Pomocí příkazu CHGCMD (Změna příkazu) změňte parametr PGM (program pro zpracování příkazu) pro příkaz CFGSYSSEC. Hodnotu PGM nastavte na jméno vašeho programu. Pokud jste například vytvořili program v knihovně QGPL, který se jmenuje MYSECCFG, zadali byste toto:

```
CHGCMD CMD(QSYS/CFGSYSSEC) PGM(QGPL/MYSECCFG)
```

Poznámka: Jestliže změníte program QSYS/QSECCFGS, neručí společnost IBM za jeho spolehlivost, funkčnost nebo výkon. Odvozené záruky na prodejnost a způsobilost pro určitý účel se výslovně zamítají.

Funkce příkazu Vyvolání obecného oprávnění

Příkaz RVKPUBAUT (Vyvolání obecného oprávnění) můžete použít k nastavení veřejného oprávnění na hodnotu *EXCLUDE pro sadu příkazů a programů. Příkaz RVKPUBAUT spouští program s názvem QSYS/QSECRVKP. Program QSECRVKP je dodáván tak, že vyvolává veřejné oprávnění (nastavením veřejného oprávnění na hodnotu *EXCLUDE) pro příkazy, které uvádí Tabulka 11 na stránce 38, a pro rozhraní API, která uvádí Tabulka 12 na stránce 38. Když obdržíte systém, mají tyto příkazy a API nastaveno veřejné oprávnění na hodnotu *USE.

Příkazy, které obsahuje Tabulka 11, a rozhraní API, jež uvádí Tabulka 12, provádějí funkce v systému, které mohou poskytovat příležitost pro vznik nežádoucích situací. Administrátor systému by měl uživatelům poskytnout oprávnění k těmto příkazům a programům explicitně, nikoliv je zpřístupnit všem uživatelům systému.

Když spouštíte příkaz RVKPUBAUT, zadáváte knihovnu, která obsahuje příkazy. Předvolenou knihovnou je QSYS. Pokud máte v systému několik národních jazyků, je nutné spustit tento příkaz pro každou knihovnu QSYSxxx.

Tabulka 11. Příkazy, jejichž veřejné oprávnění se nastavuje pomocí příkazu RVKPUBAUT

ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGE
ADDPJE	CHGWSE	RMVWSE
ADDRTGE	CPYCFGL	RSTLIB
ADDWSE	CRTCFGL	RSTOBJ
CHGAJE	CRTCTLAPPC	RSTS36F
CHGCFGL	CRTDEVAPPC	RSTS36FLR
CHGCFGLE	CRTSBSD	RSTS36LIBM
CHGCMNE	ENDRMTSPT	STRRMTSPT
CHGCTLAPPC	RMVAJE	STRSBS
CHGDEVAPPC	RMVCFGLE	WRKCFGL

Všechna dále uvedená rozhraní API se nacházejí v knihovně QSYS:

Tabulka 12. Programy, jejichž veřejné oprávnění se nastavuje pomocí příkazu RVKPUBAUT

QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

Když spustíte příkaz RVKPUBAUT, nastaví systém veřejné oprávnění pro kořenový adresář na hodnotu *USE (pokud již není *USE nebo nižší).

Přizpůsobení programu

Jestliže některá z těchto nastavení neodpovídají vaší instalaci, můžete si vytvořit svou vlastní verzi programu, který zpracovává tento příkaz. Postupujte takto:

__ Krok 1. Pomocí příkazu RTVCLSRC (Načtení CL zdroje) zkopírujte zdroj pro program, který se spouští, když použijete příkaz RVKPUBAUT. Jedná se o program QSYS/QSECRVKP. Když jej načtete, dejte mu *odlišné jméno*.

__ Krok 2. Upravte program podle potřeby. Pak jej zkompilujte. Při kompilaci se ujistěte, že *nenahrazujete* program QSYS/QSECRVKP dodaný IBM. Váš program by měl mít jiné jméno.

__ Krok 3. Pomocí příkazu CHGCMD (Změna příkazu) změňte parametr PGM (program pro zpracování příkazu) pro příkaz RVKPUBAUT. Hodnotu PGM nastavte na jméno vašeho programu. Pokud jste například vytvořili program v knihovně QGPL, který se jmenuje MYRVKPGM, zadali byste toto:

```
CHGCMD CMD(QSYS/RVKPUBAUT) PGM(QGPL/MYRVKPGM)
```

Poznámka: Jestliže změníte program QSYS/QSECRVKP, neručí společnost IBM za jeho spolehlivost, funkčnost nebo výkon. Odvozené záruky na prodejnost a způsobilost pro určitý účel se výslovně zamítají.

Část 2. Rozšířené zabezpečení serveru iSeries

Kapitola 5. Ochrana informačních hodnot prostřednictvím oprávnění k objektům

Jako administrátor systému máte za úkol chránit informační hodnoty vaší organizace, aniž byste nějakým způsobem znepříjemňovali práci uživatelům systému. Musíte se ujistit, že mají uživatelé dostatečné oprávnění k provádění své práce, ale na druhou stranu nemají tak velké oprávnění, aby mohli procházet systémem a provádět neautorizované změny.

Tip na zabezpečení

Oprávnění, které je příliš svazující, může mít opačný účinek. Uživatelé někdy na příliš omezená oprávnění reagují tak, že vzájemně sdílejí hesla.

Operační systém OS/400 poskytuje integrované zabezpečení objektů. Uživatelé musí za účelem přístupu k objektům používat rozhraní poskytované systémem. Pokud například chcete získat přístup k databázovému souboru, musíte použít příkazy nebo programy, které jsou určeny pro přístup k databázovým souborům. Nemůžete použít příkaz určený pro přístup k frontě zpráv nebo protokolu úlohy.

Kdykoliv použijete systémové rozhraní za účelem přístupu k objektu, ověří systém, že máte k tomuto objektu oprávnění, které je požadováno daným rozhraním. Oprávnění k objektu je účinným a pružným nástrojem ochrany zdrojů v systému. Jako administrátor systému musíte stanovit efektivní schéma zabezpečení objektů, které můžete řídit a spravovat.

Prosazení oprávnění k objektu

Kdykoliv se snažíte získat přístup k objektu, operační systém kontroluje vaše oprávnění k tomuto objektu. Pokud je však úroveň zabezpečení ve vašem systému (systémová hodnota QSECURITY) nastavena na hodnotu 10 nebo 20, má každý uživatel automaticky oprávnění pro přístup ke všem objektům, neboť všechny uživatelské profily mají zvláštní oprávnění *ALLOBJ.

Rada pro oprávnění k objektu: Pokud si nejste jisti, zda používáte oprávnění k objektu, zkontrolujte systémovou hodnotu QSECURITY (úroveň zabezpečení). Jestliže má QSECURITY hodnotu 10 nebo 20, pak zabezpečení na úrovni objektů nepoužíváte.

Než se rozhodnete pro změnu úrovně zabezpečení na hodnotu 30 či vyšší, je nutné provést řádné plánování a přípravu. Jinak by mohlo dojít k situaci, kdy by vaši uživatelé neměli přístup k informacím, které potřebují.

Popis metod pro analýzu vašich aplikací a rozhodování, jak nastavit zabezpečení na úrovni objektů, obsahuje téma **Základní zabezpečení systému a plánování** v rámci aplikace Information Center. Toto téma vám pomůže s prvními kroky, pokud ještě nepoužíváte zabezpečení objektů nebo je vaše schéma zabezpečení objektů již zastaralé a příliš spletité.

Zabezpečení na úrovni menu

Server iSeries byl původně navržen jako produkt navazující na systémy S/36 a S/38. Řada instalací serveru iSeries byla kdysi instalací systému S/36 nebo S/38. K určování, co mohli uživatelé dělat, často administrátoři těchto dřívějších systémů používali metody označované jako **zabezpečení na úrovni menu** nebo **řízení přístupu prostřednictvím menu**.

Řízení přístupu prostřednictvím menu znamená, že po přihlášení se uživateli zobrazí nějaké menu. Uživatel může provádět pouze ty funkce, které jsou v daném menu. Uživatel se nemůže dostat na příkazovou řádku, aby z ní prováděl funkce, které nejsou v menu. Administrátor systému se teoreticky nemusí zabývat oprávněními k objektům, neboť to, co mohou uživatelé dělat, je zcela řízeno menu a programy.

Server iSeries poskytuje několik voleb pro uživatelské profily, které pomáhají při řízení přístupu prostřednictvím menu. Můžete použít:

- Parametr **INLMNU** (počáteční menu), který určuje, jaké menu uživatel uvidí jako první po přihlášení.
- Parametr **INLPGM** (počáteční program), který slouží ke spuštění programu nastavení, než se uživateli zobrazí menu. Parametr INLPGM můžete také použít k omezení uživatele na spouštění jediného programu.
- Parametr **LMTCPB** (omezení možností), který dává uživateli k dispozici omezenou sadu příkazů. Zároveň zabraňuje tomu, aby uživatel uvedl na přihlašovací obrazovce jiný počáteční program nebo menu. (Parametr LMTCPB omezuje pouze ty příkazy, které se zadávají z příkazové řádky.)

Omezení řízení přístupu prostřednictvím menu

Počítače i jejich uživatelé prošly během několika posledních let obrovskou změnou. Nyní je k dispozici řada nástrojů, jako jsou např. dotazovací programy a tabulkové kalkulátory, které uživatelům umožňují provádět drobné programování nezávisle na oddělení informačních systémů. Některé nástroje, např. SQL nebo ODBC, poskytují schopnost informace prohlížet a měnit. Zprovoznit takové nástroje v rámci struktury na bázi menu je velmi složité.

Pracovní stanice s pevnými funkcemi (“zelené obrazovky”) jsou rychle nahrazovány osobními počítači a počítačovými sítěmi. Jestliže je váš systém zapojen v síti, mohou do něj uživatelé vstupovat, aniž by se jim kdy zobrazila přihlašovací obrazovka nebo menu.

Jako administrátor systému, který se snaží prosadit řízení přístupu prostřednictvím menu, máte před sebou dva základní problémy:

- Pokud se vám podaří omezit uživatele na menu, budou vaši uživatelé pravděpodobně nespokojení, neboť nebudou moci v plné míře využívat moderních nástrojů.
- Jestliže se vám to nepodaří, mohli byste vydat všanc důležité a důvěrné informace, které měly být chráněny na bázi řízení přístupu prostřednictvím menu. Když je váš systém zapojen v síti, vaše šance prosadit řízení přístupu prostřednictvím menu se snižuje. Například parametr LMTCPB se vztahuje pouze na příkazy zadávané z příkazové řádky v interaktivní relaci. Parametr LMTCPB nemá žádný vliv na požadavky z komunikačních relací, jako je přenos PC souboru, FTP nebo vzdálené příkazy.

Zdokonalení řízení přístupu prostřednictvím menu pomocí zabezpečení na úrovni objektů

S tím, jak přibývá nových možností pro připojování k systémům, nemůže životaschopné schéma zabezpečení serveru iSeries spoléhat pouze na řízení přístupu prostřednictvím menu. Toto téma poskytuje návrhy, jak vaše řízení přístupu prostřednictvím menu rozšířit o prostředí zabezpečení na úrovni objektů.

Metody pro analýzu oprávnění k objektům, která musí uživatelé mít, aby mohli spouštět stávající aplikace, popisuje téma *Základní zabezpečení systému a plánování* v rámci aplikace Information Center. Potom rozdělíte uživatele do skupin a těmto skupinám přidělíte odpovídající oprávnění. Tento přístup je rozumný a logický. Pokud však byl váš systém v provozu po mnoho let a má velké množství aplikací, bude se otázka analýzy aplikací a nastavení oprávnění k objektům pravděpodobně zdát nezvladatelná.

Rada pro oprávnění k objektům: Dobrým přechodem od řízení přístupu prostřednictvím menu mohou být vaše menu v kombinaci s programy, které přebírají oprávnění od vlastníků programu. Zajistěte, aby byly chráněny jak programy přebírající oprávnění, tak uživatelské profily, které je vlastní.

Možná budete schopni použít svá stávající menu pro nastavení přechodného prostředí, zatímco byste postupně analyzovali své aplikace a objekty. Dále uvádíme příklad, který používá menu OEMENU (Zadání objednávek) a přiřazené soubory a programy.

Příklad: nastavení přechodného prostředí

Tento příklad vychází z následujících předpokladů a požadavků:

- Všechny soubory jsou v knihovně ORDERLIB.
- Neznáte jména všech souborů. Rovněž nevíte, jaké oprávnění vyžadují volby menu pro různé soubory.
- Menu a všechny programy, které volá, jsou uloženy v knihovně ORDERPGM.
- Chcete, aby všichni, kdo se mohou přihlásit do vašeho systému, byli schopni si prohlížet informace ve všech souborech objednávek, souborech zákazníků a souborech zboží (např. pomocí dotazů nebo tabulkových kalkulátorů).
- Pouze uživatelé, jejichž aktuální přihlašovací menu je OEMENU, by měli být schopni měnit soubory. K tomu musí používat programy v daném menu.
- Systémoví uživatelé, kteří nejsou administrátoři systému, nemají zvláštní oprávnění *ALLOBJ ani *SECADM.

Podle následujícího postupu změníte toto prostředí řízení přístupu prostřednictvím menu tak, aby bylo schopné splnit potřeby týkající se dotazů:

__ Krok 1. Vytvořte seznam uživatelů, jejichž počáteční menu je OEMENU.

K vytvoření přehledu prostředí pro každý uživatelský profil ve vašem systému můžete použít příkaz PRTUSRPRF *ENVINFO (Tisk uživatelského profilu). Sestava zahrnuje počáteční menu, počáteční program a aktuální knihovnu. Obrázek 7 na stránce 58 je příkladem takové sestavy.

__ Krok 2. Ujistěte se, že objekt OEMENU (může se jednat o objekt *PGM nebo *MENU) vlastní uživatelský profil, který se nepoužívá pro přihlášení. Uživatelský profil by měl být deaktivován nebo by měl mít heslo *NONE. Například předpokládejme, že OEOWNER vlastní objekt OEMENU typu program.

__ Krok 3. Ujistěte se, že uživatelský profil, který vlastní objekt OEMENU typu program, není skupinovým profilem. Můžete použít tento příkaz:

```
DSPUSRPRF USRPRF(OEOWNER) TYPE(*GRPMBR)
```

__ Krok 4. Změňte program OEMENU tak, aby přebíral oprávnění od uživatelského profilu OEOWNER. (Pomocí příkazu CHGPGM změňte parametr USRPRF na hodnotu *OWNER.)

Poznámka: Objekty typu *MENU nemohou přebírat oprávnění. Pokud je OEMENU objekt typu *MENU, můžete tento příklad přizpůsobit jedním z těchto způsobů:

- Vytvořte program pro zobrazení menu.
- Pro programy, které se spustí, když uživatel vybere volby z menu OEMENU, použijte adoptované oprávnění.

__ Krok 5. Vůči všem souborům v knihovně ORDERLIB nastavte veřejné oprávnění na hodnotu *USE pomocí těchto dvou příkazů:

```
RVKOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
     AUT(*ALL)
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
     AUT(*USE)
```

Uvědomte si, že pokud vyberete oprávnění *USE, mohou uživatelé kopírovat soubor pomocí přenosu PC souboru nebo FTP.

__ Krok 6. Profilu, který vlastní program menu, přidělte oprávnění *ALL k souborům, a to tímto způsobem:

```
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(OEOWNER)
     AUT(*ALL)
```

Pro většinu aplikací je dostačující oprávnění *CHANGE k souborům. Vaše aplikace však mohou provádět funkce, např. mazání členů fyzických souborů, které vyžadují vyšší oprávnění než *CHANGE. Případně byste měli vaše aplikace zanalyzovat a poskytnout jim co nejnižší oprávnění, které je nezbytné. Během přechodového období se však díky převzetí oprávnění *ALL vyhnete selhávání aplikací způsobenému nedostatečným oprávněním.

__ Krok 7. Omezte oprávnění k programům v knihovně objednávek následujícím způsobem:

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(*PUBLIC)
     AUT(*EXCLUDE)
```

__ Krok 8. Profilu OEOWNER přidělte oprávnění k programům v dané knihovně tímto příkazem:

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(OEOWNER)
     AUT(*USE)
```

__ Krok 9. Uživatelům, které jste určili v kroku 1, poskytněte oprávnění k programu menu tak, že pro každého uživatele napíšete tento příkaz:

```
GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM)
     USER(jméno-uživatelského-profilu) AUT(*USE)
```

Když dokončíte tyto kroky, budou všichni uživatelé systému, kteří nebudou explicitně vyloučeni, mít přístup k souborům (ale nebudou je moci měnit) v knihovně ORDERLIB. Uživatelé, kteří mají oprávnění k programu OEMENU, budou schopni používat programy v menu k aktualizaci souborů v knihovně ORDERLIB. Pouze ti uživatelé, kteří mají oprávnění k programu OEMENU, budou schopni měnit soubory v této knihovně. Kombinace zabezpečení na úrovni objektů a řízení přístupu prostřednictvím menu chrání soubory.

Když podobné kroky dokončíte pro všechny knihovny, které obsahují uživatelská data, vytvořili jste jednoduché schéma pro řízení aktualizací databází. Tato metoda zabraňuje uživatelům systému aktualizovat databázové soubory s výjimkou toho, kdy používají schválená menu a programy. Zároveň jste uživatelům zpřístupnili databázové soubory za účelem prohlížení, analyzování a kopírování pomocí nástrojů pro podporu rozhodování nebo pomocí spojení z jiného systému nebo PC.

Rada pro oprávnění k objektu: Když je váš systém zapojen v síti, může oprávnění *USE poskytovat vyšší oprávnění, než byste očekávali. Například, máte-li k souboru oprávnění *USE, můžete pomocí FTP vytvořit kopii souboru v jiném systému (včetně PC).

Použití zabezpečení na úrovni knihoven jako doplňku k zabezpečení na úrovni menu

Abyste měli přístup k objektu v knihovně, musíte mít oprávnění jak k danému objektu, tak ke knihovně. Většina operací vyžaduje pro knihovnu buď oprávnění *EXECUTE, nebo *USE.

V závislosti na vaší situaci můžete oprávnění ke knihovně používat jako jednoduchý prostředek pro zabezpečení objektů. Například předpokládejme, že kdokoliv, kdo má oprávnění k menu pro zadávání objednávek, může používat všechny programy v knihovně ORDERPGM. Místo, abyste zabezpečovali jednotlivé programy, můžete veřejné oprávnění ke knihovně ORDERPGM nastavit na hodnotu *EXCLUDE. Potom můžete poskytnout oprávnění *USE k této knihovně určitým uživatelským profilům, což jim umožní používat programy v uvedené knihovně. (Předpokladem je, že veřejné oprávnění k programům je *USE nebo vyšší.)

Oprávnění ke knihovně představuje jednoduchou a účinnou metodu správy oprávnění k objektu. Musíte však mít jistotu, že znáte obsah knihoven, které takto zabezpečujete, abyste nechtěně neposkytli přístup k nějakým objektům.

Konfigurování vlastnictví objektů

Vlastnictví objektů ve vašem systému je důležitou součástí schématu oprávnění k objektům. Standardně má vlastník objektu oprávnění *ALL k tomuto objektu. Doporučení a příklady pro plánování vlastnictví objektů obsahuje 5. kapitola v publikaci *Zabezpečení iSeries - referenční informace Reference*. Několik rad uvádíme níže:

- Obecně platí, že by skupinové profily neměly vlastnit objekty. Pokud skupinový profil vlastní objekt, mají k tomuto objektu všichni členové skupiny oprávnění *ALL, pokud ovšem není nějaký člen skupiny výslovně vyloučen.
- Pokud používáte adoptované oprávnění, zvažte, zda by měly uživatelské profily, které vlastní programy, vlastnit také aplikační objekty, jako např. soubory. Možná nebudete chtít, aby uživatelé, kteří spouštějí programy, jež přejímají oprávnění, měli oprávnění *ALL k souborům.

Jestliže používáte produkt iSeries Navigator, můžete toho dosáhnout provedením změn prostřednictvím funkce **metod** zabezpečení ochrany dat. Další informace najdete v rámci aplikace iSeries Information Center (podrobnosti najdete v části “Nezbytné předchozí a související informace” na stránce xii).

Oprávnění k objektu pro systémové příkazy a programy

Dále je uvedeno několik návrhů pro omezení oprávnění k objektům dodaným společností IBM:

- Když máte v systému více než jeden národní jazyk, má systém více než jednu systémovou knihovnu (QSYS). Systém obsahuje knihovnu QSYSxxxx pro každý národní jazyk v systému. Pokud používáte oprávnění k objektu za účelem řízení přístupu k systémovým příkazům, uvědomte si, že je třeba zabezpečit příkazy v knihovně QSYS a v každé knihovně QSYSxxx v systému.
- Knihovna systému System/38 někdy poskytuje příkaz s funkcí, která odpovídá příkazům, které chcete omezit. Nezapomeňte omezit odpovídající příkaz v knihovně QSYS38.
- Jestliže máte prostředí systému System/36, budete možná muset omezit další programy. Například program QY2FTML zajišťuje přenos souborů v systému System/36.

Monitorování funkcí zabezpečení

Tato kapitola popisuje techniky monitorování efektivnosti zabezpečení ve vašem systému. Lidé prověřují zabezpečení systému z několika důvodů:

- Aby ohodnotili, zda je plán pro zabezpečení ochrany dat úplný.
- Aby se ujistili, že plánované ovládací prvky zabezpečení jsou vhodné a fungují. Tento typ monitorování obvykle provádí správce systému jako součást každodenní administrace

zabezpečení. Také ho provádějí (někdy v podrobnějším měřítku) interní nebo externí revizoři jako součást pravidelné revize zabezpečení.

- Aby se přesvědčili, že zabezpečení systému udržuje krok se změnami systémového prostředí. Příkladem změn, které ovlivňují zabezpečení, jsou:
  - Nové objekty vytvořené uživateli systému.
  - Noví uživatelé přijatí do systému.
  - Změna vlastnictví objektů (oprávnění nebylo přizpůsobeno).
  - Změna odpovědnosti (změnila se skupina uživatelů).
  - Dočasné oprávnění (které se nezruší na základě času).
  - Nainstalované nové produkty.
- Aby se připravili na budoucí události, jako je instalace nové aplikace, přechod na vyšší úroveň zabezpečení nebo nastavení komunikační sítě.

Metody, které jsou popsány v této kapitole, jsou určeny pro všechny tyto situace. To, které věci budete monitorovat a jak často, závisí na velikosti vaší organizace a na jejích potřebách v oblasti zabezpečení ochrany dat. Tato kapitola si neklade za cíl poskytnout návod pro frekvenci monitorování. Jejím smyslem je rozebrat, jaké informace jsou k dispozici, jak je získat a proč jsou potřebné.

Kapitolu tvoří tři části:

- Kontrolní seznam pro položky zabezpečení, které lze naplánovat a monitorovat.
- Informace o nastavení a použití monitorovacího žurnálu poskytované systémem.
- Další metody získávání informací o zabezpečení v systému.

Monitorování zabezpečení zahrnuje použití příkazů v systému iSeries a prohlížení informací v protokolech a žurnálech v systému. Pro člověka, který má na starosti monitorování zabezpečení vašeho systému, budete možná chtít vytvořit speciální profil. Tento profil bude vyžadovat zvláštní oprávnění *AUDIT, aby bylo možné měnit charakteristiky monitorování systému. Některé z úloh monitorování navržených v této kapitole vyžadují uživatelský profil se zvláštním oprávněním *ALLOBJ a *SECADM. Po skončení období monitorování zajistěte, aby se heslo pro profil revizora nastavilo na hodnotu *NONE.

Další podrobnosti o monitorování zabezpečení uvádí 9. kapitola publikace *Security Reference*.

Analýza uživatelských profilů

Pomocí příkazu DSPAUTUSR (Zobrazení oprávněných uživatelů) si můžete zobrazit nebo vytisknout seznam všech uživatelů ve vašem systému. Seznam může být seřazen podle jména profilu nebo podle jména skupinového profilu. Dále je uveden příklad řazení podle skupinového profilu:

```
                          Display Authorized Users

                      Password
Group       User      Last         No
Profile     Profile   Changed   Password  Text
DPTSM
            ANDERSOR  08/04/0x            Roger Anders
            VINCENTM  09/15/0x            Mark Vincent
DPTWH
            ANDERSOR  08/04/0x            Roger Anders
            WAGNERR   09/06/0x            Rose Wagner
QSECOFR
            JONESS    09/20/0x            Sharon Jones
            HARRISOK  08/29/0x            Ken Harrison
*NO GROUP
            DPTSM     09/05/0x    X       Sales and Marketing
            DPTWH     08/13/0x    X       Warehouse
            RICHARDS  09/05/0x            Janet Richards
            SMITHJ    09/18/0x            John Smith
```

Tisk zvolených uživatelských profilů

Pomocí příkazu DSPUSRPRF (Zobrazení uživatelského profilu) můžete vytvořit výstupní soubor, který lze dále zpracovat pomocí dotazovacího nástroje.

```
DSPUSRPRF USRPRF(*ALL) +
          TYPE(*BASIC) OUTPUT(*OUTFILE)
```

Dotazovací nástroj můžete použít k vytvoření široké škály analytických sestav z výstupního souboru, jako např.:

- Seznam všech uživatelů, kteří mají zvláštní oprávnění *ALLOBJ i *SPLCTL.
- Seznam všech uživatelů seřazený podle pole uživatelského profilu, např. počáteční program nebo třída uživatele.

Také si můžete vytvořit dotazovací programy, které by z vašeho výstupního souboru vytvářely různé sestavy. Například:

- Seznam všech uživatelských profilů, které mají libovolné zvláštní oprávnění, na základě výběru těch záznamů, u nichž se pole UPSPAU nerovná hodnotě *NONE.
- Seznam všech uživatelů, kteří mají dovoleno zadávat příkazy, na základě výběru těch záznamů, u nichž se pole *Omezení možností* (UPLTCP v modelovém databázovém výstupním souboru) rovná hodnotě *NO nebo *PARTIAL.
- Seznam všech uživatelů, kteří mají určité počáteční menu nebo počáteční program.
- Seznam neaktivních uživatelů na základě kontroly pole s datem posledního přihlášení.

Prozkoumání velkých uživatelských profilů

Uživatelské profily s velkým počtem oprávnění, které budí dojem, že jsou rozprostřeny skoro přes celý systém, mohou odrážet nedostatečné plánování zabezpečení. Dále uvádíme jednu z metod, kterou je možné vyhledat velké uživatelské profily a zhodnotit je:

1. Pomocí příkazu DSPOBJD (Zobrazení popisu objektu) vytvořte výstupní soubor obsahující informace o všech uživatelských profilech v systému:

   ```
   DSPOBJD OBJ(*ALL) OBJTYPE(*USRPRF) +
           DETAIL(*BASIC) OUTPUT(*OUTFILE)
   ```

2. Vytvořte dotazovací program, který vygeneruje seznam jmen a velikostí všech uživatelských profilů v sestupném řazení podle velikosti.

3. Vytiskněte si podrobné informace o největších uživatelských profilech a vyhodnoťte oprávnění a vlastněné objekty z hlediska jejich smysluplnosti:

```
DSPUSRPRF USRPRF(jméno-uživatelského-profilu) +
          TYPE(*OBJAUT) OUTPUT(*PRINT)
DSPUSRPRF USRPRF(jméno-uživatelského-profilu) +
          TYPE(*OBJOWN) OUTPUT(*PRINT)
```

Některé uživatelské profily dodávané IBM jsou velmi velké kvůli počtu objektů, které vlastní. Jejich výpis a analýza nebývá obvykle nutná. Měli byste však zkontrolovat programy přejímající oprávnění z těchto uživatelských profilů dodávaných IBM, které mají zvláštní oprávnění *ALLOBJ, např. QSECOFR a QSYS.

Další podrobnosti o monitorování zabezpečení uvádí 9. kapitola publikace *Security Reference*.

Analýza oprávnění k objektům

Následující metodu můžete použít ke zjištění, kdo má oprávnění ke knihovnám v systému:

1. K vypsání všech knihoven v systému použijte příkaz DSPOBJD:

```
DSPOBJD OBJ(QSYS/*ALL) OBJTYPE(*LIB) ASPDEV(*ALLAVL) OUTPUT(*PRINT)
```

Poznámka: Knihovny v nezávislých ASP (společná paměťová oblast), které nejsou ve stavu AVAILABLE, se tímto příkazem nezobrazí.

2. K zobrazení seznamu oprávnění ke konkrétní knihovně použijte příkaz DSPOBJAUT (Zobrazení oprávnění k objektu):

```
DSPOBJAUT OBJ(QSYS/jméno-knihovny) OBJTYPE(*LIB) +
          ASPDEV(jméno-zařízení-asp) OUTPUT(*PRINT)
```

3. K zobrazení objektů v knihovně použijte příkaz DSPLIB (Zobrazení knihovny):

```
DSPLIB LIB(QSYS/jméno-knihovny) ASPDEV(jméno-zařízení-asp) OUTPUT(*PRINT)
```

Na základě těchto sestav můžete určit, co knihovna obsahuje a kdo k ní má přístup. V případě nutnosti můžete příkaz DSPOBJAUT použít také k zobrazení oprávnění pro vybrané objekty v knihovně.

Kontrola změněných objektů

Chcete-li vyhledat objekty, které byly nějak upraveny, můžete použít příkaz CHKOBJITG (Kontrola integrity objektu). Změněný objekt je obvykle signálem, že se někdo pokouší vměšovat do vašeho systému. Tento příkaz možná budete chtít spustit poté, co někdo:

- Provedl obnovu programů ve vašem systému.
- Použil DST.

Když spustíte tento příkaz, vytvoří systém databázový soubor obsahující informace o možných problémech s integritou. Můžete zkontrolovat objekty vlastněné jedním profilem, několika různými profily nebo všemi profily. Lze vyhledat objekty, jejichž doména byla pozměněna. Rovněž můžete přepočítat hodnoty ověření platnosti programů a zjistit tak objekty typu *PGM, *SRVPGM, *MODULE a *SQLPKG, které byly nějak upraveny.

Ke spuštění programu CHKOBJITG je požadováno zvláštní oprávnění *AUDIT. Z důvodu prováděných snímání a výpočtů může zpracování příkazu trvat poměrně dlouho. Proto byste jej měli spouštět v době, kdy není váš systém příliš vytížený.

Poznámka: Profily, které vlastní mnoho objektů s velkým množstvím soukromých oprávnění, se mohou stát dosti velkými. Velikost profilu vlastníka ovlivňuje výkon, když se zobrazuje nebo nějak zpracovává oprávnění k vlastněným objektům a když se profil ukládá nebo obnovuje. Jistý dopad se může projevit

také u systémových operací. Chcete-li předejít těmto negativním důsledkům jak u výkonu, tak u systémových operací, rozložte vlastnictví objektů na více profilů. **Nepřiřazujete všechny (nebo téměř všechny) objekty pouze jednomu profilu vlastníka.**

Analýza programů, které přebírají oprávnění

Programy, které přebírají (adoptují) oprávnění od uživatele se zvláštním oprávněním *ALLOBJ, představují bezpečnostní riziko. K vyhledání a prozkoumání těchto programů může sloužit následující metoda:

1. Pro každého uživatele se zvláštním oprávněním *ALLOBJ vypište pomocí příkazu DSPPGMADP (Zobrazení programů, které adoptují oprávnění) seznam programů, které přebírají oprávnění uživatele:

   ```
   DSPPGMADP USRPRF(jméno-uživatelského-profilu) +
             OUTPUT(*PRINT)
   ```

   Poznámka: V části “Tisk zvolených uživatelských profilů” na stránce 47 je popsáno, jak vypsat uživatele s oprávněním *ALLOBJ.

2. Pomocí příkazu DSPOBJAUT určete, kdo má oprávnění k použití jednotlivých přebírajících programů a jaké je veřejné oprávnění k programu:

   ```
   DSPOBJAUT OBJ(jméno-knihovny/jméno-programu) +
             OBJTYPE(*PGM) ASPDEV(jméno-knihovny/jméno-programu) +
             OUTPUT(*PRINT)
   ```

3. Prozkoumejte zdrojový kód a popis programu a na základě zjištěných informací určete:
   - Zda je uživateli programu zabráněno používat pro něj nadbytečné funkce, jako např. použití příkazové řádky, když je spuštěn pod adoptovaným profilem.
   - Zda program přebírá minimální nezbytnou úroveň oprávnění pro požadovanou funkci. Aplikace, které používají selhání programu, mohou být navrženy pomocí stejného profilu vlastníka pro objekty i programy. Když se převezme oprávnění vlastníka programu, má uživatel oprávnění *ALL k aplikačním objektům. V řadě případů profil vlastníka nevyžaduje žádné zvláštní oprávnění.

4. Pomocí příkazu DSPOBJD ověřte, kdy byl program naposledy změněn:

   ```
   DSPOBJD OBJ(jméno-knihovny/jméno-programu) +
           OBJTYPE(*PGM) ASPDEV(jméno-knihovny/jméno-programu) +
           DETAIL(*FULL)
   ```

Správa monitorovacího žurnálu a příjemců žurnálu

Monitorovací žurnál, QSYS/QAUDJRN, je určen výhradně pro monitorování zabezpečení. Objekty by neměly být zapisovány do monitorovacího žurnálu. Monitorovací žurnál by neměl být používán v rámci vázaného zpracování. Do tohoto žurnálu by neměly být posílány uživatelské záznamy pomocí příkazu SNDJRNE (Odeslání záznamu žurnálu) nebo rozhraní QJOSJRNE API.

Za účelem zajištění, aby systém mohl zapisovat monitorovací záznamy do monitorovacího žurnálu se používá zvláštní ochrana zamknutí. Když je aktivní monitorování (systémová hodnota QAUDCTL není *NONE), zadrží systémová arbitrážní úloha (QSYSARB) na žurnálu QSYS/QAUDJRN zámek. Když je monitorování aktivní, nelze s monitorovacím žurnálem provádět určité operace, jako např.:

- příkaz DLTJRN
- příkaz ENDJRNxxx
- příkaz APYJRNCHG
- příkaz RMVJRNCHG
- příkaz DMPOBJ nebo DMPSYSOBJ

- přesun žurnálu
- obnova žurnálu
- operace, které pracují s oprávněním, jako např. příkaz GRTOBJAUT
- příkaz WRKJRN

Informace zapisované do zabezpečovacích záznamů žurnálu jsou popsány v publikaci *Security Reference*. Všechny zabezpečovací záznamy v monitorovacím žurnálu mají kód žurnálu T. V žurnálu QAUDJRN se kromě záznamu o zabezpečení vyskytují systémové záznamy. Jsou to záznamy s kódem žurnálu J, které se vztahují k IPL a obecným operacím prováděným v příjemcích žurnálu (např. uložení příjemce).

Pokud dojde k poškození žurnálu nebo jeho aktuálního příjemce v takové míře, že není možné zapisovat monitorovací záznamy, určuje systémová hodnota QAUDENDACN, jakou akci systém provede. Obnova poškozeného žurnálu nebo příjemce žurnálu je stejná jako u ostatních žurnálů.

Možná budete chtít, aby změnu příjemců žurnálu řídil systém. Když vytváříte žurnál QAUDJRN, zadejte hodnotu MNGRCV(*SYSTEM). Jestliže už máte žurnál vytvořený, změňte jej na tuto hodnotu. Jestliže zadáte hodnotu MNGRCV(*SYSTEM), systém automaticky odpojí příjemce v okamžiku, kdy dosáhne své prahové velikosti, a vytvoří a připojí příjemce žurnálu. To je označováno jako **systémem řízená změna žurnálu**. Další informace naleznete v rámci aplikace iSeries Information Center —>Správa systému–> Správa žurnálů–>Správa lokálních žurnálů–>Správa žurnálů. Informace o přístupu k aplikaci iSeries Information Center najdete v části “Nezbytné předchozí a související informace” na stránce xii.

Kapitola 6. Správa oprávnění

K udržení přehledu o nastavení oprávnění ve vašem systému je vám k dispozici sada sestav o zabezpečení. Když tyto sestavy spustíte poprvé, můžete si vytisknout veškeré informace (např. oprávnění pro všechny soubory nebo pro všechny programy).

Když si již vytvoříte svou informační základnu, můžete pravidelně spouštět změněné verze těchto sestav. Změněné verze vám pomáhají určit změny v systému týkající se zabezpečení, které si zasluhují vaši pozornost. Například můžete spustit sestavu, která každý týden zobrazí veřejné oprávnění k souborům. Můžete si vyžádat pouze změněnou verzi sestavy. V sestavě budou uvedeny jak nové soubory v systému, které jsou dostupné komukoliv, tak stávající soubory, jejichž veřejné oprávnění se od posledního spouštění sestavy změnilo.

Ke spuštění nástrojů zabezpečení je možné použít dvě menu:

- Menu SECTOOLS použijte, chcete-li spouštět programy interaktivně.
- Menu SECBATCH použijte, pokud chcete spouštět programy dávkově. Menu SECBATCH má dvě části: jednu pro okamžité zadávání úloh do fronty úloh a druhou pro umístění úloh do plánovače úloh.

Jestliže používáte produkt iSeries Navigator, postupujte při spouštění nástrojů zabezpečení takto:

1. V prostředí produktu iSeries Navigator rozbalte váš server—>**Zabezpečení**.
2. Pravým tlačítkem myši klepněte na volbu **Metody** a vyberte volbu **Prozkoumat**. Zobrazí se seznam metod, které můžete vytvořit a řídit.

Monitorování veřejného oprávnění k objektům

Kvůli jednoduchosti a zajištění výkonnosti je převážná část systémů nastavena tak, že většina objektů je dostupná většině uživatelů. Uživatelům je výslovně odepřen přístup k určitým důvěrným objektům citlivým na utajení místo toho, aby byli explicitně opravňováni k použití každého objektu. Jen málo systémů s velmi vysokými požadavky na zabezpečení volí opačný přístup a poskytuje oprávnění k objektům na základě momentální potřeby. V těchto systémech je většina objektů vytvořena s veřejným oprávněním nastaveným na hodnotu *EXCLUDE.

Server iSeries je systém na bázi objektů s mnoha různými typy objektů. Většina typů objektů neobsahuje citlivé informace a neprovádí funkce související se zabezpečením. Jako administrátor systému iSeries s typickými potřebami v oblasti zabezpečení se budete pravděpodobně chtít zaměřit na objekty, které vyžadují ochranu, jako jsou např. databázové soubory a programy. U ostatních typů objektů stačí jen nastavit veřejné oprávnění, které je dostatečné pro vaše aplikace, což je ve většině případů oprávnění *USE.

K vytištění informací o objektech, k nimž mají přístup obecní uživatelé, můžete použít příkaz PRTPUBAUT (Tisk obecného oprávnění). (**Obecný uživatel** je kdokoliv s oprávněním k přihlášení, kdo nemá explicitní oprávnění k objektu.) Při použití příkazu PRTPUBAUT můžete uvést typy objektů a knihovny nebo adresáře, které chcete prozkoumat. V menu SECBATCH a SECTOOLS najdete volby pro vytištění sestavy objektů s veřejným oprávněním pro ty typy objektů, které jsou všeobecně svázány se zabezpečením ochrany dat. Můžete si pravidelně tisknout změněnou verzi této sestavy, abyste měli přehled, které objekty by si zasluhovaly vaši pozornost.

Správa oprávnění pro nové objekty

Operační systém OS/400 poskytuje funkce, které pomáhají spravovat oprávnění a vlastnictví nových objektů v systému. Když uživatel vytvoří nový objekt, určí systém toto:

- Kdo bude vlastnit objekt.
- Jaké je veřejné oprávnění k objektu.
- Zda má objekt nějaká soukromá oprávnění.
- Kam se má objekt uložit (do jaké knihovny nebo adresáře).
- Zda se bude monitorovat přístup k objektu.

Systém za tím účelem používá systémové hodnoty, parametry knihoven a uživatelských profilů. Několik příkladů dostupných voleb uvádí část "Assigning Authority and Ownership to New Objects " v 5. kapitole publikace *Zabezpečení iSeries - referenční informace Reference*.

K vytištění parametrů uživatelského profilu, které mají vliv na vlastnictví a oprávnění k novým objektům, můžete použít příkaz PRTUSRPRF. Příklad takové sestavy uvádí Obrázek 5 na stránce 56.

Monitorování seznamů oprávnění

Objekty s podobnými požadavky na zabezpečení můžete seskupit pomocí seznamu oprávnění. Koncepčně seznam oprávnění obsahuje seznam uživatelů a oprávnění, která mají uživatelé k objektům chráněným tímto seznamem. Seznamy oprávnění představují účinný způsob správy oprávnění k podobným objektům v systému. V některých případech však bývá složité udržet přehled o oprávněních k objektům.

K vytištění informací o oprávněních seznamu oprávnění můžete použít příkaz PRTPVTAUT (Tisk soukromých oprávnění). Obrázek 3 je příkladem takové sestavy.

```
                        Private Authorities (Full Report)
SYSTEM4
Authorization                Primary                              List  ----------Object----------  ------------Data------------
List          Owner          Group          User          Authority  Mgt   Opr  Mgt  Exist  Alter  Ref  Read  Add  Upd  Dlt  Execute
LIST1         QSECOFR        *NONE          *PUBLIC       *EXCLUDE
LIST2         BUDNIKR        *NONE          BUDNIKR       *ALL        X     X    X     X      X     X    X     X    X    X      X
                                            *PUBLIC       *CHANGE           X                              X     X    X    X      X
LIST3         QSECOFR        *NONE          *PUBLIC       *EXCLUDE
LIST4         CJWLDR         *NONE          CJWLDR        *ALL        X     X    X     X      X     X    X     X    X    X      X
                                            GROUP1        *ALL              X    X     X      X     X    X     X    X    X      X
                                            *PUBLIC                  *EXCLUDE
```

Obrázek 3. Sestava soukromých oprávnění pro seznamy oprávnění

Tato sestava ukazuje stejné informace, které vidíte na obrazovce Editace seznamu oprávnění (EDTAUTL). Předností této sestavy je to, že poskytuje informace o všech seznamech oprávnění zároveň. Pokud nastavujete zabezpečení např. pro novou skupinu objektů, můžete si v rychlosti vytisknout tuto sestavu, abyste zjistili, zda stávající seznam oprávnění splňuje potřeby těchto objektů.

Můžete si vytisknout změněnou verzi sestavy, z níž je patrné, které seznamy oprávnění jsou nové a které byly změněny od posledního vytištění této sestavy. Rovněž máte možnost vytisknout si seznam objektů, které jsou chráněny jednotlivými seznamy oprávnění. Obrázek 4 na stránce 53 znázorňuje příklad sestavy pro jeden seznam oprávnění:

```
                    Display Authorization List Objects
Authorization list . . . . . :   CUSTAUTL
Library  . . . . . :     QSYS
Owner  . . . . . :   AROWNER
Primary group  . . . . . :   *NONE

                                                      Primary
Object         Library        Type         Owner     group          Text
CUSTMAS        CUSTLIB        *FILE        AROWNER   *NONE
CUSTORD        CUSTORD        *FILE        OEOWNER   *NONE
```

Obrázek 4. Sestava zobrazení objektů seznamu oprávnění

Tuto sestavu můžete využít například pro vyjasnění dopadu přidání nového uživatele do seznamu oprávnění (jaká oprávnění tento uživatel získá).

Použití seznamů oprávnění

Produkt iSeries Navigator poskytuje funkce zabezpečení navržené tak, aby vám usnadnily vývoj plánu a strategie zabezpečení a konfiguraci systému dle potřeb vaší organizace. Jednou z dostupných funkcí je použití seznamů oprávnění.

Seznamy oprávnění mají tyto rysy:
- Seznam oprávnění seskupuje objekty s podobnými požadavky na zabezpečení ochrany dat.
- Seznam oprávnění koncepčně obsahuje seznam uživatelů a skupin a oprávnění, která existují vůči objektům chráněným tímto seznamem.
- Každý uživatel a skupina může mít různá oprávnění k množině objektů, které jsou chráněny tímto seznamem.
- Oprávnění lze poskytovat prostřednictvím seznamu, což je preferováno před poskytováním oprávnění jednotlivým uživatelům nebo skupinám.

S využitím seznamů oprávnění můžete provádět tyto úlohy:
- Vytvořit seznam oprávnění.
- Změnit seznam oprávnění.
- Přidat uživatele a skupiny.
- Změnit povolení uživatelů.
- Zobrazit chráněné objekty.

Chcete-li použít tuto funkci, postupujte takto:
1. V prostředí produktu iSeries Navigator rozbalte váš server—>Zabezpečení. Zobrazí se **Seznamy oprávnění** a **Metody**.
2. Pravým tlačítkem myši klepněte na volbu **Seznamy oprávnění** a vyberte volbu **Nový seznam oprávnění**. Volba **Nový seznam oprávnění** vám umožní provést následující činnosti.
   - **Use (použití):** Umožní přístup k atributům objektu a použití objektu. Obecní uživatelé si mohou objekty prohlížet, ale nemohou je měnit.
   - **Change (změna):** Umožní měnit obsah objektů (s určitými výjimkami).
   - **All (vše):** Umožní všechny operace s objektem kromě těch, které jsou vyhrazeny pro vlastníka. Uživatel nebo skupina může ovládat existenci objektu, zadávat zabezpečení pro objekt, měnit objekt a provádět s objektem základní funkce. Uživatel nebo skupina může rovněž měnit vlastnictví objektu.
   - **Exclude (vyloučení):** Všechny operace s objektem jsou zakázány. Uživatelům a skupinám s tímto povolením není dovolen přístup k objektu ani operace s ním. Uvádí, že obecným uživatelům není dovoleno objekt používat.

Při práci se seznamy oprávnění budete zřejmě chtít udělit povolení jak k objektům, tak k datům. Níže jsou uvedena povolení k objektům, pro která se můžete rozhodnout.

- **Operational** (operační): Poskytuje povolení prohlížet si popis objektu a používat objekt tak, jak to určuje povolení k datům, které má uživatel nebo skupina k danému objektu.
- **Management** (správa): Poskytuje povolení specifikovat zabezpečení pro objekt, přesouvat nebo přejmenovávat objekt a přidávat členy do databázových souborů.
- **Existence:** Poskytuje povolení řídit existenci a vlastnictví objektu. Uživatel nebo skupina může objekt vymazat, uvolnit paměť, kterou objekt zabírá, provádět s objektem operace uložení a obnovy a převádět vlastnictví objektu. Pokud má uživatel nebo skupina zvláštní povolení pro ukládání, nepotřebuje uživatel nebo skupina povolení k existenci objektu.
- **Alter** (úpravy) (používá se pouze pro databázové soubory a balíky programů SQL): Poskytuje povolení potřebné pro úpravy atributů objektu. Jestliže má uživatel nebo skupina toto povolení k databázovému souboru, může uživatel nebo skupina přidávat nebo odstraňovat triggery, přidávat nebo odstraňovat referenční a jedinečné omezující podmínky a měnit atributy databázového souboru. Pokud má uživatel nebo skupina toto povolení k balíku programů SQL, může uživatel nebo skupina měnit atributy balíku programů SQL. Toto povolení se v současné době používá pouze pro databázové soubory a balíky programů SQL.
- **Reference** (používá se pouze pro databázové soubory a balíky programů SQL): Poskytuje povolení potřebné pro odkazování na objekt z jiného objektu, např. operace s tímto objektem mohou být omezeny jiným objektem. Jestliže má uživatel nebo skupina toto povolení k fyzickému souboru, může uživatel nebo skupina přidávat referenční omezující podmínky, v nichž je daný fyzický soubor nadřazeným (rodičem). Toto povolení se v současné době používá pouze pro databázové soubory.

Níže jsou uvedena povolení k datům, pro která se můžete rozhodnout.

- **Read** (čtení): Poskytuje povolení potřebné pro získání a zobrazení obsahu objektů, např. pro prohlížení záznamů v souboru.
- **Add** (přidávání): Poskytuje povolení pro přidávání záznamů do objektu, např. přidání zpráv do fronty zpráv nebo přidání záznamů do souboru.
- **Update** (aktualizace): Poskytuje oprávnění měnit záznamy v objektu, např. měnit záznamy v souboru.
- **Delete** (výmaz): Poskytuje povolení pro odstranění záznamů z objektu, např. odstranění zpráv z fronty zpráv nebo výmaz záznamů ze souboru.
- **Execute** (provádění): Poskytuje povolení potřebné pro spouštění programu, servisního programu nebo balíku programů SQL. Uživatel může také vyhledat objekt v knihovně nebo adresáři.

Další informace o jednotlivých procesech při vytváření a editaci seznamů oprávnění najdete v online nápovědě v rámci produktu iSeries Navigator.

Metody přístupu v prostředí produktu iSeries Navigator

Produkt iSeries Navigator můžete použít k prohlížení a správě metod pro váš server iSeries. Produkt iSeries Navigator pracuje s metodami v pěti oblastech:

- **Metoda monitorování**
  Tato metoda umožňuje nastavit monitorování pro určité akce a přístup k určitým prostředkům systému.
- **Metoda zabezpečení**
  Tato metoda umožňuje určit úroveň zabezpečení a další volby, které se vztahují k zabezpečení systému.
- **Metoda hesel**
  Tato metoda umožňuje stanovit úroveň hesla pro systém.
- **Metoda obnovy**
  Tato metoda vám umožňuje určit, jak se obnovují určité objekty v systému.

- **Metoda přihlašování**
  Tato metoda umožňuje stanovit, jak se mohou uživatelé přihlašovat do systému.

Chcete-li si prohlédnout nebo změnit uvedené metody pomocí produktu iSeries Navigator, proveďte následující kroky:

1. V prostředí produktu iSeries Navigator rozbalte váš server—>**Zabezpečení**.
2. Pravým tlačítkem myši klepněte na volbu **Metody** a vyberte volbu **Prozkoumat**. Zobrazí se seznam metod, které můžete vytvořit a řídit. Specifika těchto metod obsahuje nápověda produktu iSeries Navigator.

Monitorování soukromých oprávnění k objektům

Volby menu SECBATCH:
12 *pro okamžité spuštění*, **41** *pro použití plánovače úloh*

K vytištění seznamu všech soukromých oprávnění k objektům určitého typu v určité knihovně můžete použít příkaz PRTPVTAUT (Tisk soukromých oprávnění).

Tato sestava vám pomůže určit nová oprávnění k objektům. Rovněž vám pomůže udržovat vaše schéma soukromých oprávnění v takovém stavu, kdy je přehledné a zvladatelné.

Monitorování přístupu k výstupním frontám a k frontám úloh

Někdy administrátor systému skvělým způsobem zajistí ochranu přístupu k souborům, ale na druhou stranu zapomene na to, co se stane, když se obsah souboru vytiskne. Servery iSeries poskytují funkce, kterými je možné zabezpečit citlivé výstupní fronty a fronty úloh. Výstupní fronta je chráněna tak, že neoprávnění uživatelé nemohou například prohlížet nebo kopírovat soubory pro souběžný tisk, které čekají na vytištění. Fronty úloh se chrání tak, že neoprávnění uživatelé nemohou přesměrovat důvěrnou úlohu do nedůvěrné výstupní fronty ani nemohou úlohu zcela zrušit.

Volby menu SECBATCH:
24 pro okamžité spuštění , **63** *pro použití plánovače úloh*

Způsob ochrany výstupních front a front úloh popisuje téma *Základní zabezpečení systému a plánování* v rámci aplikace Information Center a v publikaci *Zabezpečení iSeries - referenční informace Reference*.

Příkaz PRTQAT (Tisk oprávnění k frontě) můžete použít k vytištění nastavení zabezpečení pro fronty úloh a výstupní fronty v systému. Potom můžete prověřit tiskové úlohy, které tisknou důvěrné informace, a ujistit se, že směřují do výstupních front a front úloh, které jsou chráněné.

U výstupních front a front úloh, které považujete za citlivé na utajení, můžete porovnat nastavení zabezpečení s informacemi v dodatku D publikace *Zabezpečení iSeries - referenční informace Reference*. Tabulky v tomto dodatku uvádějí, jaká nastavení jsou nezbytná pro provádění různých funkcí výstupní fronty a fronty úloh.

Monitorování zvláštních oprávnění

Když uživatelé vašeho systému mají zbytečná zvláštní oprávnění, může být vaše snaha vyvinout dobré schéma oprávnění k objektům marná. Oprávnění k objektu ztrácí smysl v okamžiku, kdy má uživatelský profil zvláštní oprávnění *ALLOBJ. Uživatel se zvláštním oprávněním *SPLCTL si může prohlížet libovolné soubory pro souběžný tisk v systému bez ohledu na to, jaké úsilí jste vynaložili na zabezpečení vašich výstupních front. Uživatel se zvláštním oprávněním *JOBCTL může ovlivňovat činnost systému a přesměrovávat úlohy. Uživatel se zvláštním oprávněním *SERVICE je schopný používat servisní nástroje za účelem přístupu k datům, aniž by musel jít přes operační systém.

Volby menu SECBATCH:
29 pro okamžité spuštění, 68 *pro použití plánovače úloh*

K vytištění informací o zvláštních oprávněních a třídách uživatelů pro uživatelské profily ve vašem systému můžete použít příkaz PRTUSRPRF (Tisk uživatelského profilu). Když spouštíte tuto sestavu, máte několik možností, co vytisknout:
- Všechny uživatelské profily.
- Uživatelské profily s určitými zvláštními oprávněními.
- Uživatelské profily, které mají určité třídy uživatele.
- Uživatelské profily s nesrovnalostmi mezi třídou uživatele a zvláštními oprávněními.

Obrázek 5 představuje příklad sestavy, která uvádí zvláštní oprávnění pro všechny uživatelské profily:

```
                                    User Profile Information
  Report type  . . . . . . . . . . :   *AUTINFO
  Select by  . . . . . . . . . . . :   *SPCAUT
  Special authorities  . . . . . . :   *ALL
                   -------------Special Authorities-------------
                                *IO                                                    Group
User      Group     *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  User       Owner     Group      Authority   Limited
Profile   Profiles   OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  Class      Owner     Authority  Type        Capability
USERA     *NONE      X     X     X    X     X     X     X     X    *SECOFR    *USRPRF   *NONE      *PRIVATE    *NO
USERB     *NONE                      X     X                       *PGMR      *USRPRF   *NONE      *PRIVATE    *NO
USERC     *NONE      X     X     X    X     X     X     X     X    *SECOFR    *USRPRF   *NONE      *PRIVATE    *NO
USERD     *NONE                                                    *USER      *USRPRF   *NONE      *PRIVATE    *NO
```

Obrázek 5. Sestava informací o uživateli: 1. příklad

Kromě zvláštních oprávnění v sestavě najdete tyto informace:
- Zda má uživatelský profil omezené schopnosti.
- Zda uživatel nebo skupina uživatele vlastní nové objekty, které uživatel vytvořil.
- Jaké oprávnění skupina uživatele automaticky obdrží k novým objektům, které uživatel vytvoří.

Obrázek 6 na stránce 57 představuje příklad sestavy, která uvádí nesrovnalosti mezi zvláštními oprávněními a třídami uživatele:

```
User Profile Information
Report type  . . . . . :   *AUTINFO
Select by  . . . . . :   *MISMATCH
-------------------------------Special Authorities-------------
                               *IO                                                    Group
User      Group     *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  User               Group      Authority   Limited
Profile   Profiles   OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  Class      Owner    Authority  Type        Capability
USERX     *NONE       X                X     X                 X    *SYSOPR    *USRPRF  *NONE       *PRIVATE    *NO
USERY     *NONE                                    X               *USER      *USRPRF  *NONE       *PRIVATE    *NO
USERZ                                              X               *USER      *USRPRF  *NONE       *PRIVATE    *NO
          QPGMR                          X     X
```

Obrázek 6. Sestava informací o uživateli: 2. příklad

U informací, které obsahuje Obrázek 6, si všimněte těchto skutečností:

- USERX má třídu uživatele *SYSOPR (systémový operátor), ale zároveň má zvláštní oprávnění *ALLOBJ a *SPLCTL.
- USERY má třídu uživatele *USER (uživatel), ale zároveň má zvláštní oprávnění *SECADM.
- USERZ má také třídu uživatele *USER (uživatel) a zvláštní oprávnění *SECADM. Také si všimněte, že USERZ je členem skupiny QPGMR, která má zvláštní oprávnění *JOBCTL a *SAVSYS.

Tyto sestavy můžete spouštět pravidelně, což vám pomůže monitorovat správu uživatelských profilů.

Monitorování uživatelských prostředí

Jedním z úkolů uživatelského profilu je definovat prostředí pro uživatele, včetně výstupní fronty, počátečního menu a popisu úlohy. Prostředí uživatele má vliv na to, jak se uživateli jeví systém, a do určité míry i na to, co je uživateli dovoleno provádět. Uživatel musí mít oprávnění k objektům, které jsou uvedeny v uživatelském profilu. Pokud se však vaše schéma oprávnění ještě vyvíjí nebo není příliš omezující, může uživatelské prostředí definované v uživatelském profilu vést k výsledkům, které jste neočekávali. Zde je několik příkladů:

Volby menu SECBATCH:

29 *pro okamžité spuštění,* **68** *pro použití plánovače úloh*

- Popis úlohy uživatele může specifikovat uživatelský profil, který má více oprávnění než uživatel.
- Uživatel může mít počáteční menu, které nemá příkazovou řádku. Příkazovou řádku však může poskytnout program klávesy Attention daného uživatele.
- Uživatel může mít oprávnění ke spouštění důvěrných sestav. Výstupy uživatele však mohou být směrovány do výstupní fronty dostupné uživatelům, kteří by sestavy neměli vidět.

Při monitorování prostředí, která jsou definována pro uživatele systému, vám pomůže volba *ENVINFO příkazu PRTUSRPRF (Tisk uživatelského profilu). Obrázek 7 na stránce 58 znázorňuje příklad takové sestavy:

```
                                        User Profile Information
  Report type  . . . . . :   *ENVINFO
  Select by  . . . . . :   *USRCLS
                          Initial        Initial          Job          Message        Output         Attention
User            Current   Menu/          Program/      Description/    Queue/         Queue/         Program/
Profile         Library   Library        Library         Library       Library        Library        Library
+AUDSECOFR       AUDITOR    MAIN           *NONE          QDFTJOBD       QSYSOPR        *WRKSTN        *SYSVAL
                          *LIBL                         QGPL            QSYS
USERA           *CRTDFT   OEMENU          *NONE          QDFTJOBD       USERA          *WRKSTN        *SYSVAL
                          *LIBL                         QGPL            QUSRSYS
USERB           *CRTDFT   INVMENU         *NONE          QDFTJOBD       USERB          *WRKSTN        *SYSVAL
                          *LIBL                         QGPL            QUSRSYS
USERC           *CRTDFT   PAYROLL         *NONE          QDFTJOBD       USERC          PAYROLL        *SYSVAL
                          *LIBL                         QGPL            QUSRSYS         PRPGMLIB
```

Obrázek 7. Tisk uživatelského profilu - příklad uživatelského prostředí

Správa servisních nástrojů

Servisní nástroje slouží ke konfiguraci, správě a obsluze serveru. Existují dva přístupy k servisním nástrojům: z DST (Dedicated Service Tools) nebo z SST (System Service Tools). Pro přístup k DST a SST a k použití funkcí produktu iSeries Navigator pro správu LPAR (logical partition) a správu diskových jednotek jsou požadována uživatelská ID servisních nástrojů.

DST jsou dostupné, když je spuštěn interní kód LIC, i kdyby ještě nebyl zaveden operační systém OS/400. SST jsou dostupné z operačního systému OS/400. V následující tabulce jsou nastíněny základní rozdíly mezi DST a SST.

Charakteristika	DST	SST
Způsob přístupu	Fyzický přístup přes konzoli během ručního IPL nebo vybráním volby 21 na ovládacím panelu.	Přístup přes interaktivní úlohu s možností přihlásit se s QSRV nebo s následujícími oprávněními: • Oprávnění pro CL příkaz STRSST (Spuštění SST). • Zvláštní oprávnění *SERVICE nebo zvláštní oprávnění *ALLOBJ. • Funkční právo používat SST.
Kdy je k dispozici	Dostupné, i když má server omezené schopnosti. K přístupu k DST není vyžadován operační systém OS/400.	Dostupné po spuštění operačního systému OS/400. Pro přístup k SST je vyžadován operační systém OS/400.
Způsob autentizace	Vyžaduje ID a heslo uživatele servisních nástrojů.	Vyžaduje ID a heslo uživatele servisních nástrojů.

Prostudujte si téma v rámci aplikace iSeries Information Center—>Zabezpečení—>Servisní nástroje, kde naleznete informace o použití servisních nástrojů k provádění následujících činností:

- Přístup k servisním nástrojům prostřednictvím DST.
- Přístup k servisním nástrojům prostřednictvím SST.
- Přístup k servisním nástrojům prostřednictvím produktu iSeries Navigator.
- Vytvoření ID uživatele servisních nástrojů.

- Změna funkčních práv pro ID uživatele servisních nástrojů.
- Změna popisu pro ID uživatele servisních nástrojů.
- Zobrazení ID uživatele servisních nástrojů.
- Aktivace a deaktivace ID uživatele servisních nástrojů.
- Výmaz ID uživatele servisních nástrojů.
- Změna ID a hesel uživatele servisních nástrojů pomocí SST nebo DST.
- Změna vašeho hesla uživatele servisních nástrojů pomocí STRSST.
- Změna ID a hesel uživatele servisních nástrojů.
- Změna rozhraní QSYCHGDS API (Change Service Tools User ID).
- Nastavení hesla uživatelského profilu QSECOFR operačního systému OS/400 na původní hodnotu.
- Nastavení ID a hesla uživatele servisních nástrojů QSECOFR na původní hodnotu.
- Uložení a obnova zabezpečovacích dat servisních nástrojů.
- Vytvoření vlastní verze ID uživatele servisních nástrojů pro QSECOFR.
- Konfigurování serveru servisních nástrojů pro DST.
- Konfigurování serveru servisních nástrojů pro operační systém OS/400.
- Monitorování použití servisních funkcí pomocí DST.
- Monitorování použití servisních nástrojů prostřednictvím protokolu pro monitorování zabezpečení operačního systému OS/400.

Informace o tom, jak spustit aplikaci iSeries Information Center najdete v části “Nezbytné předchozí a související informace” na stránce xii.

Kapitola 7. Použití zabezpečení logických částí (LPAR)

Použití několika logických částí systému na jednom serveru iSeries může být přínosné v následujících situacích.

- **Údržba nezávislých systémů**: Vyhrazením části zdrojů (disková paměťová jednotka, procesory a I/O zařízení) pro logickou část se dosáhne logické izolace softwaru. Pokud jsou logické části dobře nakonfigurovány, jsou schopny tolerovat určitá selhání hardwaru. Interaktivní a dávkové zpracování, která spolu nemusí správně fungovat na jednom počítači, lze oddělit a efektivně spouštět v samostatných logických částech.
- **Konsolidace**: Systém rozdělený na logické části může vést ke snížení počtu serverů iSeries potřebných v rámci organizace. Několik systémů můžete konsolidovat do jediného systému rozděleného na logické části. Díky tomu nebudete potřebovat další vybavení a s ním spojené výdaje. Podle toho, jak se budou měnit vaše potřeby, můžete zdroje odejmout jedné logické části a přidělit je jiné.
- **Vytvoření kombinovaného provozního a testovacího prostředí:** Máte možnost vytvořit kombinaci provozního a testovacího prostředí. V primární logické části můžete vytvořit jednu provozní část. Chcete-li vytvořit více provozních části, přečtěte si níže uvedený odstavec *Vytvoření prostředí s několika provozními částmi*.

  Logická část je buď testovací, nebo provozní. V provozní části jsou zpracovávány vaše hlavní komerční aplikace. Selhání v provozní části by mohlo výrazně zkomplikovat podnikové operace, což by vás zřejmě stálo čas i peníze. Testovací část testuje software. Selhání v testovací části nenaruší běžné podnikové operace (pokud to není nezbytně naplánováno).
- **Vytvoření prostředí s několika provozními částmi:** Více provozních částí byste měli vytvářet pouze ve vašich sekundárních částech. V této situaci vyhradíte primární logickou část pro správu logických částí.
- **Pohotové zálohování:** Když se sekundární logická část replikuje na jinou logickou část v rámci stejného systému, způsobilo by přepnutí na zálohu během selhání logické části minimální potíže. Tato konfigurace rovněž minimalizuje negativní dopad dlouhých ukládacích oken. Záložní logickou část můžete logicky vypnout a uložit, zatímco jiná logická část pokračuje v provádění běžné provozní činnosti. Pokud budete chtít použít tuto strategii pohotového zálohování, budete potřebovat speciální software.
- **Integrovaný klastr:** Při použití produktu OptiConnect/400, aplikačního softwaru s vysokou dostupností, může být váš systém rozdělený na logické části spouštěn jako integrovaný klastr. Integrovaný klastr můžete použít k ochraně vašeho systému před většinou neplánovaných selhání v rámci sekundární logické části.

Poznámka: Při nastavování sekundární logické části je třeba zavést další opatření pro umístění karet. Pokud I/O procesor (IOP), který jste zvolili pro konzoli, má také kartu LAN a tato karta LAN není určena pro použití s produktem Operations Console, aktivuje se pro použití konzolí a vy ji možná nebudete schopni použít pro zamýšlené účely. Další informace o práci s produktem Operations Console uvádí Kapitola 8, “Produkt iSeries Operations Console”, na stránce 63.

Podrobné informace o tomto tématu obsahuje téma ″Logické části″ v rámci aplikace iSeries Information Center.

Správa zabezpečení pro logické části

Úlohy související se zabezpečením, které provádíte v systému rozděleném na logické části, jsou stejné jako úlohy v systému bez logických částí. Když však vytvoříte logické části, budete pracovat s více než jedním nezávislým systémem. Proto budete muset provádět stejné úlohy v každé logické části a nikoliv jen v jednom systému, jak by tomu bylo v případě systému bez logických částí.

Pokud se snažíte zabezpečit systém s logickými částmi, měli byste brát na zřetel některá základní pravidla:

- Uživatele přidávejte do systému v jednom okamžiku vždy jen do jedné logické oblasti. Uživatele musíte přidat do každé logické oblasti, k níž mají mít přístup.
- Omezte počet lidí, kteří mají oprávnění pro přístup k DST a SST v primární logické části. Další informace o DST a SST uvádí téma ″Správa logických částí prostřednictvím iSeries Navigator, DST a SST″ v rámci aplikace iSeries Information Center. Informace o použití uživatelských profilů servisních nástrojů pro řízení přístupu k činnostem logických částí obsahuje část “Správa servisních nástrojů” na stránce 58.

  Poznámka: Chcete-li produkt iSeries Navigator používat pro přístup k funkcím LPAR, musíte nejprve inicializovat server servisních nástrojů, neboli STS (Service Tools Server). Související informace najdete v rámci aplikace iSeries Information Center—>Zabezpečení—>Servisní nástroje. Informace o tom, jak spustit aplikaci iSeries Information Center najdete v části “Nezbytné předchozí a související informace” na stránce xii.
- Sekundární logické části si nemohou prohlížet ani používat hlavní paměť a diskové jednotky ostatních logických částí.
- Sekundární logické části ″vidí″ pouze své vlastní hardwarové prostředky.
- Primární logická část si může prohlížet všechny systémové hardwarové prostředky na obrazovkách DST a SST Work with System Partitions.
- Operační systém primární logické části nadále ″vidí″ pouze vlastní dostupné prostředky.
- Ovládací panel systému řídí primární logickou část. Když režim panelu nastavíte na hodnotu Secure, nelze z SST provádět žádné činnosti na obrazovce Work with Partition Status. Chcete-li prosadit DST z ovládacího panelu systému, musíte změnit režim na hodnotu Manual.
- Když nastavíte provozní režim sekundární logické části na hodnotu Secure, omezíte použití obrazovky Work with Partition Status těmito způsoby:
  - V sekundární logické části můžete ke změně stavu logické části používat pouze DST. Ke změně stavu logické části nelze použít SST.
  - V sekundární logické části můžete prosadit pouze DST, a to z obrazovky Work with Partition Status primární logické části buď pomocí DST, nebo SST.
  - V primární logické části můžete použít pouze DST ke změně režimu sekundární logické části z hodnoty Secure na jinou libovolnou hodnotu.

Jakmile už není režim sekundární logické části Secure, můžete v sekundární logické části použít ke změně stavu logické části jak DST, tak SST.

Další informace o zabezpečení vašeho serveru iSeries najdete v publikaci Security Reference a v tématu Základní zabezpečení systému a plánování v rámci aplikace iSeries Information Center.

Kapitola 8. Produkt iSeries Operations Console

Produkt Operations Console vám umožňuje používat PC k přístupu k serveru iSeries a k jeho řízení. Operations Console zahrnuje podporu pro vzdálené připojení k serverům iSeries přes komutovanou linku bez zařízení konzole, přičemž se konzolemi stávají vzdálené PC. Při práci s produktem Operations Console si uvědomte tyto skutečnosti:

- Z produktu Operations Console můžete provádět všechny úlohy jako z tradiční konzole. Například uživatelské profily, které mají zvláštní oprávnění *SERVICE nebo *ALLOBJ, jsou schopné přihlásit se k relaci Operations Console, i kdyby byly deaktivovány.
- Produkt Operations Console používá k navázání spojení se serverem iSeries uživatelské profily a hesla servisních nástrojů. Z toho důvodu je velmi důležitá změna uživatelských profilů a hesel servisních nástrojů. Hackeři pravděpodobně znají předvolená ID a hesla uživatelských profilů servisních nástrojů a mohou je používat při pokusech o vytvoření vzdálené relace s vaším serverem iSeries. Rady týkající se hesel najdete v částech “Změna známých hesel” na stránce 20 a “Jak zabránit používání předvolených hesel” na stránce 25.
- Chcete-li chránit své informace, když používáte vzdálenou konzoli, používejte volbu zpětného volání Telefonické připojení sítě operačního systému Windows.
- Při nastavování sekundární logické části je třeba zavést další opatření pro umístění karet. Pokud I/O procesor (IOP), který jste zvolili pro konzoli, má také kartu LAN a tato karta LAN není určena pro použití s produktem Operations Console, aktivuje se pro použití konzolí a vy ji možná nebudete schopni použít pro zamýšlené účely.

Ve verzi V5R1 byl produkt Operations Console zdokonalen tak, že umožňuje provádět z konzole činnosti v rámci sítě LAN. Zdokonalená autentizace a šifrování dat zajišťují zabezpečení sítě pro procedury konzole. Chcete-li používat produkt Operations Console s připojitelností přes LAN, rozhodně vám doporučujeme instalovat následující produkty:

- Produkt Cryptographic Access Provider, 5722–AC2 nebo 5722–AC3 na váš server iSeries.
- Produkt Client Encryption, 5722–CE2 nebo 5722–CE3 na váš PC s produktem Operations Console.

Aby mohla být data konzole šifrována, musí mít server iSeries nainstalován jeden z produktů Cryptographic Access Provider **a** na PC musí být nainstalován jeden z produktů Client Encryption.

Poznámka: Pokud nebude nainstalován žádný šifrovací produkt, nebude probíhat žádné šifrování dat.

Níže uvedená tabulka shrnuje výsledky šifrování pro jednotlivé dostupné produkty:

Tabulka 13. Výsledky šifrování

Cryptographic Access Provider na vašem serveru iSeries	**Client Encryption na vašem PC s produktem Operations Console**	**Výsledné šifrování dat**
Žádný	Žádný	Žádné
5722–AC2	5722–CE2	56bitové
5722–AC2	5722–CE3	56bitové
5722–AC3	5722–CE2	56bitové
5722–AC3	5722–CE3	128bitové

Další informace o nastavení a správě produktu iSeries Operations Console naleznete v rámci aplikace iSeries Information Center.

Přehled zabezpečení produktu Operations Console

Zabezpečení produktu Operations Console tvoří:

- autentizace zařízení konzole
- autentizace uživatele
- utajení dat
- integrita dat

Produkt Operations Console s přímou připojitelností má implicitní autentizaci zařízení, utajení dat a integritu dat díky svému dvoubodovému připojení. Pro přihlášení k obrazovce konzole je požadováno zabezpečení autentizace uživatele.

Autentizace zařízení konzole

Autentizace zařízení konzole poskytuje ujištění o tom, které fyzické zařízení je konzole. Produkt Operations Console s přímou připojitelností používá fyzické připojení podobné twinaxiální konzoli. Produkt Operations Console používající přímé připojení lze fyzicky zabezpečit podobně jako twinaxiální připojení za účelem řízení přístupu k fyzickému zařízení konzole.

Produkt Operations Console s připojitelností přes LAN používá verzi SSL (Secure Socket Layer), která podporuje autentizaci zařízení a uživatele, ale bez použití certifikátů. U této formy připojení je autentizace zařízení založena na profilu zařízení servisních nástrojů. Další informace najdete na stránce 65.

Autentizace uživatele

Autentizace uživatele poskytuje ujištění o tom, kdo používá zařízení konzole. Všechny otázky související s autentizací uživatele se shodují bez ohledu na typ konzole.

Utajení dat

Utajení dat poskytuje jistotu, že data konzole může číst pouze určený příjemce. Produkt Operations Console s přímou připojitelností používá k ochraně dat konzole fyzické připojení podobné twinaxiální konzoli nebo zabezpečenému připojení do sítě pro připojitelnost přes LAN. Produkt Operations Console používající přímé připojení má stejné utajení dat jako twinaxiální připojení. Pokud je fyzické připojení zabezpečené, zůstávají data konzole chráněná.

Produkt Operations Console s připojitelností přes LAN používá zabezpečené připojení do sítě, jsou-li instalovány příslušné šifrovací produkty (ACx a CEx). Relace konzole používá nejúčinnější možné šifrování v závislosti na tom, jaké šifrovací produkty jsou nainstalovány na serveru iSeries a na PC, na němž je spuštěn produkt Operations Console.

Poznámka: Pokud není nainstalován žádný šifrovací produkt, nebude probíhat žádné šifrování dat.

Integrita dat

Integrita dat poskytuje jistotu, že se data konzole v průběhu přenosové cesty k příjemci nezmění. Produkt Operations Console s přímou připojitelností používá k ochraně dat konzole fyzické připojení podobné twinaxiální konzoli nebo zabezpečenému připojení do sítě

pro připojitelnost přes LAN. Produkt Operations Console používající přímé připojení má stejnou integritu dat jako twinaxiální připojení. Pokud je fyzické připojení zabezpečené, zůstávají data konzole chráněná.

Produkt Operations Console s připojitelností přes LAN používá zabezpečené připojení do sítě, jsou-li instalovány příslušné šifrovací produkty (ACx a CEx). Relace konzole používá nejúčinnější možné šifrování v závislosti na tom, jaké šifrovací produkty jsou nainstalovány na serveru iSeries a na PC, na němž je spuštěn produkt Operations Console.

Poznámka: Pokud není nainstalován žádný šifrovací produkt, nebude probíhat žádné šifrování dat.

Použití produktu Operations Console s připojitelností přes LAN

Poznámka: Libovolné zařízení Operations Console může být konzolí, ale pouze konfigurace na bázi LAN používají uživatelský profil servisních nástrojů.

Server iSeries je dodáván s předvoleným profilem zařízení servisních nástrojů QCONSOLE, který má předvolené heslo QCONSOLE. Produkt Operations Console s připojitelností přes LAN změní heslo během každého úspěšného připojení. Další informace najdete v části "Použití průvodce nastavením produktu Operations Console".

Podrobné informace o produktu iSeries Operations Console s připojitelností přes LAN uvádí téma Konfigurování produktu Operations Console připojitelného k síti LAN v rámci aplikace Information Center.

Ochrana produktu Operations Console s připojitelností přes LAN

Pokud používáte produkt Operations Console s připojitelností přes LAN, jsou doporučována dále uvedená opatření:

- Vytvoření jiného profilu zařízení servisních nástrojů s atributy konzole a uložení informací profilu na bezpečném místě.
- Instalace produktu Cryptographic Access Provider, 5722–AC2 nebo 5722–AC3 na vašem serveru iSeries a produktu Client Encryption, 5722–CE2 nebo 5722–CE3 na PC s produktem Operations Console.
- Zvolení složitějšího hesla pro ochranu informací servisního zařízení.
- Ochrana PC s produktem Operations Console stejným způsobem, jako byste chránili twinaxiální konzoli nebo produkt Operations Console s přímou připojitelností.

Použití průvodce nastavením produktu Operations Console

Průvodce nastavením doplní nezbytné informace na váš PC, když používáte produkt Operations Console s připojitelností přes LAN. Průvodce nastavením požádá o profil zařízení servisních nástrojů, o heslo profilu zařízení servisních nástrojů a o heslo pro ochranu informací profilu zařízení servisních nástrojů.

Poznámka: Heslo pro ochranu informací profilu zařízení servisních nástrojů slouží k zamykání a odemykání informací profilu zařízení servisních nástrojů (profil a heslo zařízení servisních nástrojů) na PC.

Když budete vytvářet připojení do sítě, vyzve vás průvodce nastavením produktu Operations Console k zadání hesla pro informace servisního zařízení, aby se získal přístup k profilu a heslu zařízení servisních nástrojů. Také budete požádáni o zadání platné identifikace a hesla uživatele servisních nástrojů.

Kapitola 9. Detekce podezřelých programů

Nejnovější trendy ve využití počítačů zvýšily pravděpodobnost výskytu programů z nedůvěryhodných zdrojů nebo programů, které provádějí neznámé funkce, ve vašem systému. Dále uvádíme několik příkladů:

- Uživatel osobního počítače občas dostane programy od ostatních uživatelů PC. Je-li tento PC připojen k vašemu serveru iSeries, může mít takový program vliv na server iSeries.
- Uživatelé, kteří jsou připojeni k síti, mohou také získávat programy, např. z vývěsek.
- Hackeři jsou stále aktivnější a renomovanější. Často publikují své metody a jejich výsledky. To vede k tomu, že se je někdy snaží napodobovat i programátoři dodržující zákony.

Tyto trendy s sebou přinášejí problém v zabezpečení počítačů zvaný **počítačový vir**. Vir je program, který může měnit jiné programy tak, aby obsahovaly své vlastní kopie. O těchto jiných programech se pak říká, že jsou napadeny virem. Kromě toho může vir provádět další operace, které mohou přebrat systémové prostředky nebo zničit data.

Architektura serveru iSeries zajišťuje určitou ochranu před infekčními charakteristikami počítačových virů. Další informace najdete v části "Ochrana proti počítačovým virům". Administrátor serveru iSeries musí věnovat větší pozornost programům, které provádějí neautorizované funkce. Ostatní témata v této kapitole popisují způsoby, kterými by mohl někdo s nekalými úmysly instalovat škodlivé programy do vašeho systému. V těchto tématech naleznete rady, jak zabránit programům, aby prováděly neautorizované funkce.

Tip na zabezpečení

Oprávnění k objektu představuje vaši první zbraň při obraně. Pokud nemáte dobrý plán pro ochranu vašich objektů, je váš systém neochránitelný. V dále uvedených informacích jsou rozebrány způsoby, kterými by se autorizovaný uživatel mohl pokusit využít skulin ve vašem schématu oprávnění k objektům.

Ochrana proti počítačovým virům

Počítač, který je napaden počítačovým virem, obsahuje program, jenž může měnit ostatní programy. V objektově orientované architektuře serveru iSeries je vytváření a šíření tohoto typu viru daleko složitější než v jiných počítačových architekturách. Na serveru iSeries používáte k práci s jednotlivými typy objektů specifické příkazy a instrukce. Souborové instrukce nelze použít ke změně operovatelného objektu typu program (což provádí většina původců virů). Také nemůžete snadno vytvořit program, který mění jiné objekty typu program. Abyste toho dosáhli, museli byste vynaložit velké úsilí, museli byste mít k dispozici hodně času a zkušeností, a navíc byste potřebovali přístup k nástrojům a dokumentaci, které nejsou běžně dostupné.

Jelikož jsou však nyní k dispozici nové funkce serveru iSeries, které umožňují účast v prostředí otevřených systémů, neplatí již nadále některé z objektově orientovaných funkcí ochrany serverů iSeries. Například prostřednictvím IFS (integrovaný systém souborů) mohou uživatelé přímo pracovat s některými objekty v adresářích, např. s proudovými soubory.

Přestože architektura serveru iSeries komplikuje šíření viru mezi programy serveru iSeries, nedokáže zabránit tomu, aby byl server iSeries nositelem viru. Jako souborový server může server iSeries uchovávat programy, které mohou sdílet uživatelé PC. Kterýkoliv z těchto

programů může obsahovat vir, který server iSeries neodhalí. Pokud chcete předejít tomu, aby tento typ viru napadl PC, připojené k vašemu serveru iSeries, musíte na PC používat antivirový software.

Na serveru iSeries existuje několik funkcí, které znemožňují, aby někdo použil nižší programovací jazyk se schopností ukazatele k úpravě operovatelného objektu typu program:

- Pokud je váš systém provozován na úrovni zabezpečení 40 nebo vyšší, zahrnuje ochrana integrity ochranu proti změně objektů typu program. Například nemůžete úspěšně spustit program, který obsahuje zablokované (chráněné) strojové instrukce.
- Také hodnota ověření platnosti programu je určena pro ochranu, když obnovujete program, který byl uložen (a potenciálně změněn) v jiném systému. Funkce ochrany integrity při úrovni zabezpečení 40 či vyšší, včetně hodnot ověření platnosti programu, popisuje 2. kapitola v publikaci *Zabezpečení iSeries - referenční informace Reference*.

  Poznámka: Hodnota ověření platnosti programu není spolehlivá a nemůže nahradit opatrnost při ověřování programů, které obnovujete ve vašem systému.

Kromě toho máte k dispozici několik nástrojů, které vám pomohou zaznamenat zavedení upraveného programu do vašeho systému:

- Můžete použít příkaz CHKOBJITG (Kontrola integrity objektu) k vyhledání objektů (operovatelných), které splňují vaše hodnoty pro vyhledávání, abyste se mohli přesvědčit, že tyto objekty nebyly změněny. Je to obdoba antivirové funkce.
- Můžete použít funkci monitorování zabezpečení za účelem monitorování programů, které byly změněny nebo obnoveny. Hodnoty *PGMFAIL, *SAVRST a *SECURITY systémové hodnoty úrovně oprávnění poskytují monitorovací záznamy, které vám pomohou detekovat pokusy o zavedení programu typu vir do vašeho systému. Další informace o monitorovacích záznamech a záznamech monitorovacího žurnálu obsahuje 9. kapitola a dodatek F publikace *Zabezpečení iSeries - referenční informace Reference*.
- Můžete použít parametr FRCCRT příkazu CHGPGM (Změna programu) k opětnému vytvoření libovolného programu, který byl obnoven ve vašem systému. K opětnému vytvoření programu systém používá programovou šablonu. Pokud byl program změněn poté, co byl zkompilován, vytvoří systém znovu změněný objekt a nahradí jej. Jestliže programová šablona obsahuje zablokované (chráněné) instrukce, neprovede se opětné vytvoření úspěšně.
- Můžete použít systémovou hodnotu QFRCCVNRST (vynucení konverze při obnově) k opětnému vytvoření libovolného programu, když je obnoven ve vašem systému. K opětnému vytvoření programu systém používá programovou šablonu. Tato systémová hodnota poskytuje několik možností, jak programy opětně vytvořit.
- Máte možnost použít systémovou hodnotu QVFYOBJRST (ověření objektů při obnově), chcete-li zabránit obnově programů, které nemají digitální podpis nebo nemají platný digitální podpis. Pokud není digitální podpis platný, znamená to, že se program od doby, kdy jej podepsal jeho tvůrce, změnil. Existují rozhraní API, která vám umožňují podepsat vlastní programy, soubory typu save a proudové soubory.

Další informace o podpisech a způsobu jejich použití při ochraně systému před útoky uvádí část “Podepisování objektů” na stránce 78.

Monitorování použití adoptovaného oprávnění

Na serveru iSeries můžete vytvořit program, který přebírá (adoptuje) oprávnění vlastníka programu. To znamená, že libovolný uživatel, který spustí program, má stejná oprávnění (soukromá a zvláštní oprávnění) jako uživatelský profil, který vlastní daný program.

Pokud se správně používá, je adoptované oprávnění hodnotným nástrojem zabezpečení. Část "Zdokonalení řízení přístupu prostřednictvím menu pomocí zabezpečení na úrovni objektů" na stránce 42 například popisuje, jak je možné zkombinovat adoptované oprávnění a menu za účelem rozšíření řízení přístupu na úrovni menu. Adoptované oprávnění můžete používat k ochraně vašich důležitých souborů proti změnám prováděným mimo vaše schválené aplikační programy, přičemž je nadále dovoleno zadávat vůči těmto souborům dotazy.

Jako administrátor systému byste se měli ujistit, že je adoptované oprávnění používáno správným způsobem:

- Programy by měly přebírat oprávnění od uživatelského profilu, který má pouze takové oprávnění, které potřebuje k provádění nezbytných funkcí, a nikoliv vyšší. Měli byste být mimořádně obezřetní, pokud jde o programy, které přebírají oprávnění od uživatelského profilu, jenž má zvláštní oprávnění *ALLOBJ nebo vlastní důležité objekty.
- Programy, které přebírají oprávnění, by měly mít specifickou, omezenou funkci a neměly by umožňovat zadávání příkazů.
- Programy, které přebírají oprávnění, by měly být řádně zabezpečeny.
- Přehnané použití adoptovaného oprávnění může mít negativní dopad na výkon vašeho systému. Pokud chcete zabránit problémům s výkonností, řiďte se vývojovými diagramy a návrhy pro použití adoptovaného oprávnění v 5. kapitole publikace *Zabezpečení iSeries - referenční informace Reference*.

Volby menu SECBATCH:
1 *pro okamžité spuštění,* **40 pro použití plánovače úloh**

Chcete-li monitorovat použití adoptovaného oprávnění ve vašem systému, můžete použít příkaz PRTADPOBJ (Tisk adoptovaných objektů) (volba 21 v menu SECTOOLS).

Sestava uvádí zvláštní oprávnění určitého uživatelského profilu, programy, které přebírají oprávnění tohoto uživatelského profilu, a rovněž zařízení ASP, která používají oprávnění profilu. Když si již vytvoříte svou informační základnu, můžete si pravidelně tisknout změněnou verzi sestavy adoptovaných objektů. Obsahuje přehled nových programů, které přebírají oprávnění, a programů, které byly od posledního spuštění sestavy změněny tak, aby přebíraly oprávnění.

Pokud máte podezření, že se adoptované oprávnění ve vašem systému zneužívá, můžete nastavit systémovou hodnotu QAUDLVL na hodnotu *PGMADP. Když je tato hodnota aktivní, vytvoří systém záznam monitorovacího žurnálu vždy, když někdo spustí nebo ukončí program, který přebírá oprávnění. Záznam zahrnuje jméno uživatele, který program spustil, a jméno programu.

Omezení použití adoptovaného oprávnění

Když se spustí program serveru iSeries, může program za účelem získání přístupu k objektům použít adoptované oprávnění, a to dvěma různými způsoby:

- Samotný program může převzít oprávnění od svého vlastníka. To je určeno parametrem USRPRF (uživatelský profil) daného programu nebo servisního programu.
- Program může použít (zdědit) adoptované oprávnění od předešlého programu, který se ještě nachází v zásobníku volání dané úlohy. Program může zdědit adoptované oprávnění od předešlých programů, i když sám oprávnění nepřebírá. Parametr USEADPAUT (použití adoptovaného oprávnění) programu nebo servisního programu řídí to, zda program dědí adoptované oprávnění od předešlých programů v zásobníku programů.

Dále vám předkládáme příklad toho, jak funguje použití adoptovaného oprávnění od předešlých programů.

Předpokládejme, že uživatelský profil ICOWNER má k souboru ITEM oprávnění *CHANGE a že veřejné oprávnění k tomuto souboru je *USE. Žádné ostatní uživatelské profily nemají explicitně definované oprávnění k souboru ITEM. Tabulka 14 ukazuje atributy pro tři programy, které používají soubor ITEM:

Tabulka 14. Příklad použití adoptovaného oprávnění (USEADPAUT)

Jméno programu	Vlastník programu	Hodnota USRPRF	Hodnota USEADPAUT
PGMA	ICOWNER	*OWNER	*YES
PGMB	ICOWNER	*USER	*YES
PGMC	ICOWNER	*USER	*NO

1. příklad – adoptování oprávnění:
1. USERA spustí program PGMA.
2. Program PGMA se pokusí otevřít soubor ITEM s možností aktualizace.

Výsledek: Pokus je úspěšný. USERA má k souboru ITEM přístup *CHANGE, neboť program PGMA přebírá oprávnění od ICOWNER.

2. příklad – použití adoptovaného oprávnění:
1. USERA spustí program PGMA.
2. Program PGMA volá program PGMB.
3. Program PGMB se pokusí otevřít soubor ITEM s možností aktualizace.

Výsledek: Pokus je úspěšný. Ačkoliv program PGMB přebírá oprávnění (*USRPRF je *USER), umožňuje použít předešlé adoptované oprávnění (*USEADPAUT je *YES). Program PGMA je stále ještě v zásobníku programů. USERA tedy získá k souboru ITEM oprávnění *CHANGE, neboť program PGMA přebírá oprávnění od ICOWNER.

3. příklad – bez použití adoptovaného oprávnění:
1. USERA spustí program PGMA.
2. Program PGMA volá program PGMC.
3. Program PGMC se pokusí otevřít soubor ITEM s možností aktualizace.

Výsledek: Oprávnění selže. Program nepřebírá oprávnění. Program PGMC také neumožňuje použít adoptované oprávnění od předešlých programů. Ačkoliv je program PGMA stále ještě v zásobníku volání, jeho adoptované oprávnění se nepoužije.

Jak předejít tomu, aby nové programy používaly adoptované oprávnění

Předání adoptovaného oprávnění programům, které následují v zásobníku, poskytuje zkušeným programátorům příležitost vytvořit program typu trojský kůň. Program typu trojský kůň spoléhá na předešlé programy v zásobníku, že od nich získá oprávnění potřebné pro páchání škody. Chcete-li tomu zabránit, můžete omezit to, kterým uživatelům je dovoleno vytvářet programy používající adoptované oprávnění od předešlých programů.

Když vytváříte nový program, nastaví systém automaticky parametr USEADPAUT na hodnotu *YES. Jestliže si nepřejete, aby program přebíral adoptované oprávnění, musíte pomocí příkazu CHGPGM (Změna programu) nebo CHGSRVPGM (Změna servisního programu) nastavit parametr USEADPAUT na hodnotu *NO.

Chcete-li řídit, kdo může vytvářet programy, které přebírají adoptované oprávnění, můžete použít seznam oprávnění a systémovou hodnotu QUSEADPAUT (použití adoptovaného oprávnění). Když v systémové hodnotě QUSEADPAUT uvedete jméno seznamu oprávnění, systém tento seznam oprávnění použije k určení, jak vytvářet nové programy.

Když uživatel vytváří nějaký program nebo servisní program, zkontroluje systém oprávnění tohoto uživatele k seznamu oprávnění. Jestliže má uživatel oprávnění *USE, nastaví se parametr USEADPAUT pro nový program na hodnotu *YES. Pokud uživatel nemá oprávnění *USE, nastaví se parametr USEADPAUT na hodnotu *NO. Oprávnění uživatele k seznamu oprávnění pak není možné převzít z adoptovaného oprávnění.

Seznam oprávnění, který uvedete v systémové hodnotě QUSEADPAUT, rovněž řídí, zda uživatel může k nastavení hodnoty USEADPAUT pro program nebo servisní program použít příkaz CHGxxx.

Poznámky:

1. Není třeba volat váš seznam oprávnění QUESADPAUT. Můžete vytvořit seznam oprávnění s odlišným jménem. Potom tento seznam oprávnění zadejte do systémové hodnoty QUSEADPAUT. V příkazech následujícího příkladu dosaďte jméno vašeho seznamu oprávnění.
2. Systémová hodnota QUSEADPAUT neovlivňuje stávající programy ve vašem systému. Chcete-li nastavit parametr USEADPAUT pro stávající programy, použijte příkaz CGHPGM nebo CHGSRVPGM.

Prostředí s většími omezeními: Jestliže chcete, aby většina uživatelů vytvářela nové programy s parametrem USEADPAUT nastaveným na hodnotu *NO, postupujte takto:

1. Nastavte veřejné oprávnění pro seznam oprávnění na hodnotu *EXCLUDE tak, že napíšete tento příkaz:

   ```
   CHGAUTLE AUTL(QUSEADPAUT) USER(*PUBLIC)
      AUT(*EXCLUDE)
   ```

2. Pokud chcete některé uživatele nastavit tak, aby vytvářeli programy, které používají adoptované oprávnění od předešlých programů, napište tento příkaz:

   ```
   ADDAUTLE AUTL(QUSEADPAUT) USER(jméno-uživatele)
      AUT(*USE)
   ```

Prostředí s menšími omezeními: Jestliže chcete, aby většina uživatelů vytvářela nové programy s parametrem USEADPAUT nastaveným na hodnotu *YES, postupujte takto:

1. Veřejné oprávnění pro seznam oprávnění ponechejte nastavené na hodnotu *USE.
2. Pokud chcete některým uživatelům zabránit, aby vytvářeli programy, které používají adoptované oprávnění od předešlých programů, napište tento příkaz:

   ```
   ADDAUTLE AUTL(QUSEADPAUT)
      USER(jméno-uživatele) AUT(*EXCLUDE)
   ```

Monitorování použití triggerů

Produkt DB2 UDB poskytuje schopnost asociovat triggery s databázovými soubory. Tato schopnost je v rámci odvětví běžná u vysoce funkčních správců databází.

Když asociujete trigger s databázovým souborem, uvedete, kdy se má trigger spustit. Například můžete nastavit, aby soubor zákaznických objednávek spustil trigger, kdykoliv se do souboru přidá nový záznam. Když pohledávky za zákazníkem překročí kreditní limit, může trigger vytisknout pro zákazníka dopis s varováním a zaslat dopis správci pohledávek.

Triggery představují účinný způsob, jak zajišťovat funkce aplikací i správu informací. Nicméně triggery rovněž umožňují někomu s nekalými úmysly vytvořit ve vašem systému

program typu “trojský kůň”. Tento destruktivní program může být připraven a čekat na spuštění, až nastane určitá událost v databázovém souboru ve vašem systému.

Poznámka: V historii byl trojský kůň velkým dutým dřevěným koněm, který byl plný řeckých vojáků. Poté, co se kůň dostal za hradby Tróji, vylezli vojáci z koně a porazili Trójany. V počítačovém světě se proto program, který skrývá destruktivní funkce, často nazývá trojský kůň.

Volby menu SECBATCH:
27 *pro okamžité spuštění,* **66** *pro použití plánovače úloh*

Váš systém byl dodán s omezenou schopností přidávat triggery do databázového souboru. Pokud spravujete oprávnění k objektům obezřetně, nebude mít typický uživatel dostatečné oprávnění k přidávání triggerů do databázového souboru. (Požadovaná oprávnění a všechny příkazy, včetně příkazu ADDPFTRG (Přidání triggeru fyzického souboru), popisuje dodatek D publikace *Zabezpečení iSeries - referenční informace Reference*.)

K vytištění seznamu všech triggerů v určité knihovně nebo ve všech knihovnách můžete použít příkaz PRTTRGPGM (Tisk triggerů).

Výchozí sestavu můžete použít jako základ pro ohodnocení triggerů, které již existují ve vašem systému. Potom si můžete pravidelně tisknout sestavu změn, abyste měli přehled, zda byly do systému přidány nové triggery.

Při hodnocení triggerů zvažte tyto skutečnosti:

- Kdo vytvořil trigger? Ke zjištění této informace můžete použít příkaz DSPOBJD (Zobrazení popisu objektu).
- Co program dělá? Za účelem zjištění této informace se budete muset podívat do zdrojového programu nebo se zeptat tvůrce programu. Například, kontroluje trigger, o jakého uživatele se jedná? Možná trigger čeká na konkrétního uživatele QSECOFR, aby získal přístup k systémovým prostředkům.

Když si již vytvoříte svou informační základnu, můžete si pravidelně tisknout sestavu změn, abyste mohli monitorovat triggery, které byly přidány do systému.

Kontrola skrytých programů

Triggery nejsou jediným způsobem, jak do vašeho systému zavést trojského koně. Triggery jsou příkladem **ukončovacího programu**. Když nastane určitá situace, např. aktualizace souboru v případě triggeru, spustí systém ukončovací program, který je asociován s danou situací.

Tabulka 15 na stránce 73 popisuje další příklady ukončovacích programů, které mohou být ve vašem systému. Pro ohodnocení použití a obsahu těchto ukončovacích programů byste měli používat stejné metody jako pro triggery.

Poznámka: Tabulka 15 na stránce 73 není vyčerpávajícím seznamem možných ukončovacích programů.

.

Tabulka 15. Systémem dodávané ukončovací programy

Jméno programu	Kdy se program spouští
Uživatelem specifikované jméno v atributu sítě DDMACC.	Když se uživatel pokusí ve vašem systému otevřít soubor DDM nebo navázat spojení DRDA.
Uživatelem specifikované jméno v atributu sítě PCSACC.	Když se uživatel pokusí použít funkce produktu Client Access, přičemž za účelem přístupu k objektům ve vašem systému použije produkt Original Clients.
Uživatelem specifikované jméno v systémové hodnotě QPWDVLDPGM.	Když uživatel spustí funkci Změna hesla.
Uživatelem specifikované jméno v systémové hodnotě QRMTSIGN.	Když se uživatel pokusí interaktivně přihlásit ze vzdáleného systému.
QSYS/QEZUSRCLNP.	Když je spuštěna funkce automatického vyčištění.
Uživatelem specifikované jméno v parametru EXITPGM příkazu CHGBCKUP.	Když použijete funkci zálohování produktu Operation Assistant.
Uživatelem specifikované jméno v příkazu CRTPRDLOD.	Před nebo po uložení, obnovení nebo vymazání produktu, který byl vytvořen pomocí tohoto příkazu.
Uživatelem specifikované jméno v parametru DFTPGM příkazu CHGMSGD.	Je-li pro zprávu zadán předvolený program, spustí systém tento program, když je zpráva vydána. Jelikož se v běžném systému vyskytuje velké množství popisů zpráv, je velmi komplikované monitorovat použití předvolených programů. Chcete-li zabránit tomu, aby obecní uživatelé přidávali předvolené programy pro zprávy, zvažte nastavení veřejného oprávnění pro soubory zpráv (objekty *MSGF) na hodnotu *USE.
Uživatelem specifikované jméno v parametru FKEYPGM příkazu STREML3270.	Když uživatel stiskne funkční klávesy v průběhu relace emulace zařízení 3270. Po dokončení ukončovacího programu systém vrátí řízení zpět emulaci zařízení 3270.
Uživatelem specifikované jméno v parametru EXITPGM příkazů pro monitorování výkonu.	Pro zpracování dat shromažďovaných následujícími příkazy: STRPFRMON, ENDPFRMON, ADDPFRCOL a CHGPFRCOL. Program se spustí po dokončení sběru dat.
Uživatelem specifikované jméno v parametru EXITPGM příkazu RCVJRNE.	Pro každý záznam žurnálu nebo skupinu záznamů žurnálu, kterou čte ze zadaného žurnálu nebo příjemců žurnálu.
Uživatelem specifikované jméno v API QTNADDCR.	Během operace COMMIT (potvrzení) nebo ROLLBACK (vrácení do původního stavu).
Uživatelem specifikovaná jména v API QHFRGFS.	K provádění funkcí systému souborů.
Uživatelem specifikované jméno v parametru SEPPGM popisu zařízení tiskárny.	K určení, co se má vytisknout na oddělovací stránku před nebo za souborem pro souběžný tisk nebo tiskovou úlohou.
QGPL/QUSCLSXT.	Když se zavře databázový soubor, aby bylo možné sejmout informace o využití souboru.
Uživatelem specifikované jméno v parametru FMTSLR logického souboru.	Když je do databázového souboru zapsán záznam a jméno formátu záznamu není zahrnuto v programu ve vyšším programovacím jazyku. Program selektoru přijme záznam jako vstup, určí použitý formát záznamu a vrátí jej do databáze.
Uživatelem specifikované jméno, které je uvedeno v systémové hodnotě QATNPGM, parametru ATNPGM v uživatelském profilu nebo v parametru PGM příkazu SETATNPGM.	Když uživatel stiskne klávesu Attention.
Uživatelem specifikované jméno v parametru EXITPGM příkazu TRCJOB.	Před spuštěním procedury trasování úlohy.

U příkazů, které vám umožňují zadat ukončovací program, byste se měli ujistit, že se předvolená hodnota příkazu nezměnila a neuvádí nějaký ukončovací program. Také byste se měli přesvědčit, že veřejné oprávnění k těmto příkazům není postačující ke změně

předvolené hodnoty příkazu. Příkaz CHGCMDDFT vyžaduje oprávnění *OBJMGT k příkazu. Ke spuštění tohoto příkazu nemusíte mít oprávnění *OBJMGT.

Ohodnocení registrovaných ukončovacích programů

K registraci ukončovacích programů, které se mají spustit, když nastane určitá událost, můžete použít funkci registrace systému. Chcete-li vypsat informace o registraci ve vašem systému, napište příkaz WRKREGINF OUTPUT(*PRINT). Obrázek 8 je příkladem takové sestavy:

```
              Work with Registration Information
Exit point . . . . . . . . . . . . . . . :   QIBM_QGW_NJEOUTBOUND
Exit point format  . . . . . . . . . . . :   NJEO0100
Exit point registered  . . . . . . . . . :   *YES
Allow deregister . . . . . . . . . . . . :   *YES
Maximum number of exit programs  . . . . :   *NOMAX
Current number of exit programs  . . . . :   0
Preprocessing for add  . . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . . . . :
  Format . . . . . . . . . . . . . . . . :
Preprocessing for remove . . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . . . . :
  Format . . . . . . . . . . . . . . . . :
Preprocessing for retrieve . . . . . . . :   *NONE
  Library  . . . . . . . . . . . . . . . :
```

Obrázek 8. Příklad sestavy Work with Registration Information

Pro každý výstupní bod ve vašem systému sestava uvádí, zda jsou v danou chvíli registrovány nějaké ukončovací programy. Když má výstupní bod v současné době registrovány programy, můžete pomocí volby 8 (Zobrazení programů) obrazovkové verze WRKREGINF zobrazit informace o těchto programech:

```
                     Work with Registration Information

Type options, press Enter.
5=Display exit point   8=Work with exit programs

                           Exit
     Exit                  Point
Opt  Point                 Format    Registered  Text
     QIBM_QGW_NJEOUTBOUND  NJEO0100     *YES     Network Job Entry outbound ex
8    QIBM_QHQ_DTAQ         DTAQ0100     *YES     Original Data Queue Server
     QIBM_QLZP_LICENSE     LICM0100     *YES     Original License Mgmt Server
     QIBM_QMF_MESSAGE      MESS0100     *YES     Original Message Server
     QIBM_QNPS_ENTRY       ENTR0100     *YES     Network Print Server - entry
     QIBM_QNPS_SPLF        SPLF0100     *YES     Network Print Server - spool
     QIBM_QNS_CRADDACT     ADDA0100     *YES     Add CRQ description activity
     QIBM_QNS_CRCHGACT     CHGA0100     *YES     Change CRQ description activi
```

Pro ohodnocení těchto ukončovacích programů použijte stejné metody jako pro ostatní ukončovací programy a triggery.

Kontrola naplánovaných programů

Server iSeries poskytuje několik metod pro plánování úloh, které se mají spustit později, včetně plánovače úloh. Tyto metody obvykle nepředstavují žádné bezpečnostní riziko, neboť uživatel, který plánuje úlohu, musí mít stejné oprávnění, jako je požadováno k odeslání úlohy do dávky.

Přesto byste měli do budoucna pravidelně provádět kontrolu naplánovaných úloh. Nespokojený uživatel, který už nepracuje ve vaší organizaci, může tuto metodu využít k poškození vašeho systému.

Omezení schopnosti provádět uložení a obnovu

Většina uživatelů nepotřebuje ukládat a obnovovat objekty ve vašem systému. Příkazy pro uložení dávají možnost zkopírovat důležité informační zdroje vaší organizace na média nebo do jiného systému. Většina příkazů pro uložení podporuje soubory typu save, které lze poslat do jiného systému (pomocí příkazu SNDNETF), aniž by byl nutný přístup k médiím nebo zařízení pro ukládání či obnovu.

Příkazy pro obnovu poskytují příležitost obnovit ve vašem systému neautorizované objekty, např. programy, příkazy a soubory. Rovněž můžete prostřednictvím využití souborů typu save obnovit informace, aniž byste potřebovali přístup k médiím nebo zařízení pro ukládání či obnovu. Soubory typu save mohou být odeslány z jiného systému pomocí příkazu SNDNETF nebo funkce FTP.

Dále uvádíme některé návrhy pro omezení operací ukládání a obnovy ve vašem systému:

- Dohlížejte na to, kteří uživatelé mají zvláštní oprávnění *SAVSYS. Zvláštní oprávnění *SAVSYS umožňuje uživateli ukládat nebo obnovovat objekty, i když by uživatel neměl k objektům nezbytné oprávnění.
- Řiďte fyzický přístup k zařízením pro ukládání a obnovu.
- Omezte přístup k příkazům pro ukládání a obnovu. Když instalujete licencované programy OS/400, má veřejné oprávnění pro příkazy RSTxxx hodnotu *EXCLUDE. Veřejné oprávnění pro příkazy SAVxxx je *USE. Zvažte, zda byste neměli změnit veřejné oprávnění pro příkazy SAVxxx na hodnotu *EXCLUDE. Pečlivě vybírejte uživatele, kterým poskytnete oprávnění k příkazům RSTxxx.
- Pomocí systémové hodnoty QALWOBJRST omezte obnovu systémových stavových programů, programů, které přebírání oprávnění, a objektů, které vykazují chyby při ověření platnosti.
- Pomocí systémové hodnoty QVFYOBJRST můžete řídit obnovu podepsaných objektů ve vašem systému.
- Pomocí systémové hodnoty QFRCCVNRST můžete řídit opětné vytváření určitých objektů obnovovaných ve vašem systému.
- Používejte monitorování zabezpečení k monitorování operací obnovy. Zahrňte hodnotu *SAVRST do systémové hodnoty QAUDLVL a pravidelně si tiskněte monitorovací záznamy, které vznikly na základě operací obnovy. (Další informace o operacích monitorovacích záznamů uvádí 9. kapitola a dodatek F publikace *Zabezpečení iSeries - referenční informace Reference*.)

Kontrola uživatelských objektů v chráněných knihovnách

Každá úloha serveru iSeries má seznam knihoven. Seznam knihoven určuje pořadí, ve kterém systém hledá objekt, pokud v jeho jméně není uvedeno jméno knihovny. Například, když zavoláte nějaký program, aniž byste uvedli, kde se tento program nachází, prohledá systém postupně seznam knihoven a spustí první kopii programu, kterou nalezne.

Informace o bezpečnostních rizikách seznamů knihoven a volání programů bez jména knihovny (tzv. **nekvalifikované volání**) najdete v publikaci *Zabezpečení iSeries - referenční informace Reference*. Rovněž zde najdete návrhy pro řízení obsahu seznamů knihoven a schopnost změnit systémové seznamy knihoven.

Aby váš systém správně fungoval, musí být určité systémové knihovny, např. QSYS a QGPL, v seznamu knihoven pro každou úlohu. Za účelem řízení, kdo může přidávat programy do těchto knihoven, byste měli používat oprávnění k objektu. Tak zabráníte tomu, aby někdo do některé z těchto knihoven umístil podvodný program se stejným jménem, jako má program uložený v knihovně, která se nachází dále v seznamu knihoven.

Měli byste také ohodnotit, kdo má oprávnění k příkazu CHGSYSLIBL a monitorování záznamů SV v monitorovacím žurnálu zabezpečení. Nečestný uživatel by mohl do seznamu knihoven umístit nějakou knihovnu před knihovnu QSYS, což by mohlo vést k tomu, že by ostatní uživatelé spouštěli neautorizované příkazy se stejnými jmény, jako mají příkazy dodávané IBM.

Volby menu SECBATCH:
28 *pro okamžité spuštění,* **67** *pro použití plánovače úloh*

Příkaz PRTUSROBJ (Tisk uživatelských objektů) můžete použít k vytištění seznamu uživatelských objektů (objektů, které nebyly vytvořeny společností IBM), které jsou v určité knihovně. Potom můžete programy v seznamu ohodnotit z hlediska toho, kdo je vytvořil a jakou funkci plní.

Uživatelské objekty jiné než programy mohou rovněž představovat bezpečnostní riziko, pokud jsou uloženy v systémových knihovnách. Pokud například program zapisuje důvěrná data do souboru, jehož jméno není kvalifikované, může být tento program oklamán, aby otevřel podvodnou verzi takového souboru v systémové knihovně.

Kapitola 10. Prevence a detekce pirátských pokusů

V této kapitole naleznete nejrůznější rady, které vám pomohou odhalit potenciální bezpečnostní rizika a případné počítačové piráty.

Fyzické zabezpečení

Vaše systémová jednotka představuje významné obchodní jmění a potenciální dveře k vašemu systému. Některé systémové komponenty uvnitř systému jsou malé, ale za to cenné. Systémovou jednotku byste měli umístit na nějaké hlídané místo, abyste zabránili odcizení cenných systémových komponent.

Systémová jednotka má ovládací panel, který poskytuje možnost provádět základní funkce bez pracovní stanice. Ovládací panel můžete například využít k těmto činnostem:

- Zastavení systému.
- Spuštění systému.
- Zavedení operačního systému.
- Spuštění servisních funkcí.

Všechny tyto činnosti mohou narušit činnost uživatelů systému. Navíc pro váš systém představují potenciální bezpečnostní riziko. K řízení toho, kdy jsou tyto činnosti umožněny, slouží blokovací zámek, který byl dodán s vaším systémem. Chcete-li zabránit používání ovládacího panelu, uveďte blokovací zámek do polohy Secure, odstraňte klíč a uschovejte ho na bezpečném místě.

Poznámky:

1. Jestliže potřebujete provést vzdálený IPL nebo vzdálenou diagnostiku vašeho systému, budete možná muset nastavit blokovací zámek do jiné polohy. Informace o nastaveních blokovacího zámku uvádí téma Začínáme v rámci aplikace iSeries Information Center (viz část “Nezbytné předchozí a související informace” na stránce xii).
2. Pro některé modely systému není blokovací zámek zahrnut ve standardní dodávce.

Monitorování aktivity uživatelského profilu

Uživatelské profily umožňují vstup do systému. Parametry v uživatelském profilu určují prostředí a charakteristiky zabezpečení pro daného uživatele. Jako administrátor systému musíte řídit a monitorovat změny, které nastanou u uživatelských profilů ve vašem systému.

Monitorování zabezpečení můžete nastavit tak, aby systém zapsal záznam o každé změně v uživatelských profilech. Chcete-li si vytisknout sestavu s těmito změnami, použijte příkaz DSPAUDJRNE.

Za účelem vyhodnocení požadovaných akcí s uživatelskými profily si můžete vytvořit ukončovací programy. Tabulka 16 uvádí výstupní body, které jsou k dispozici pro příkazy pro práci s uživatelskými profily.

Tabulka 16. Výstupní body pro aktivitu uživatelského profilu

Příkaz pro práci s uživatelským profilem	Jméno výstupního bodu
CRTUSRPRF (Vytvoření uživatelského profilu)	QIBM_QSY_CRT_PROFILE
CHGUSRPRF (Změna uživatelského profilu)	QIBM_QSY_CHG_PROFILE
DLTUSRPRF (Výmaz uživatelského profilu)	QIBM_QSY_DLT_PROFILE

Tabulka 16. Výstupní body pro aktivitu uživatelského profilu (pokračování)

Příkaz pro práci s uživatelským profilem	Jméno výstupního bodu
RSTUSRPRF (Obnova uživatelského profilu)	QIBM_QSY_RST_PROFILE

Váš ukončovací program může například hledat změny, které by mohly vést k tomu, že uživatel spustí neautorizovanou verzi programu. Tyto změny mohou přiřazovat buď jiný popis úlohy, nebo novou aktuální knihovnu. Na základě informací, které ukončovací program obdrží, může buď upozornit frontu zpráv, nebo provést nějakou akci (např. změnit nebo deaktivovat uživatelský profil).

Další informace o ukončovacích programech pro činnosti s uživatelskými profily obsahuje publikace *Zabezpečení iSeries - referenční informace Reference*.

Podepisování objektů

Všechna vaše bezpečnostní opatření ztrácejí smysl, pokud je může někdo obejít tím, že do vašeho systému zavede nežádoucí data. Server iSeries obsahuje řadu vestavěných funkcí, které můžete použít jako prevenci před zavedením nežádoucího softwaru do vašeho systému a kterými můžete případně takový software odhalit, pokud již v systému existuje. Jednou z metod, které byly doplněny ve verzi V5R1, je podepisování objektů.

Podepisování objektů je implementace šifrovací koncepce zajišťovaná serverem iSeries, která je známá pod názvem ″digitální podpisy.″ Myšlenka je relativně jasná: když je tvůrce softwaru připraven dodat software zákazníkům, ″podepíše″ jej. Tento podpis není zárukou, že software provádí nějakou konkrétní funkci. Poskytuje však způsob, jak prokázat, že software pochází od tvůrce, který ho podepsal, a od chvíle dokončení a podepsání se tento software nezměnil. To je zvláště důležité, pokud byl software přenášen přes Internet nebo byl uložen na médiu, u kterého máte pocit, že mohlo být změněno.

Použití digitálních podpisů vám dává větší kontrolu nad tím, jaký software může být zaveden do vašeho systému, a umožňuje s větší jistotou odhalit změny poté, co byl zaveden. Nová systémová hodnota QVFYOBJRST (ověření obnovy objektu) nabízí mechanismus pro nastavení restriktivní strategie, který vyžaduje, aby byl veškerý software zavedený do systému podepsán známými softwarovými zdroji. Můžete se také rozhodnout pro otevřenější metodu a jednoduše ověřovat podpisy, pokud jsou přítomné.

Každý software operačního systému OS/400, stejně tak jako software pro volby a licencované programy serveru iSeries, byl podepsán zdrojem důvěryhodným pro systém. Tyto podpisy pomáhají systému chránit integritu. Podpisy se kontrolují, když se v systému aplikují opravy, aby se ověřilo, že opravy pocházejí ze zdroje, kterému systém důvěřuje, a že se během přenosu nezměnily. Tyto podpisy lze také kontrolovat, když už je software v systému. Příkaz CHKOBJITG (Kontrola integrity objektu) byl rozšířen tak, aby kromě ostatních funkcí integrity objektů v systému kontroloval také podpisy. Mimo to má funkce DCM (Digital Certificate Manager) panely, které můžete použít ke kontrole podpisů na objektech, včetně objektů v operačním systému.

Právě tak, jako byl podepsán operační systém, můžete digitální podpisy použít pro ochranu integrity softwaru, který je kritický z hlediska vaší činnosti. Možná jste nakoupili software, který byl podepsán jeho poskytovatelem, nebo si můžete podepsat software, který jste si koupili nebo napsali. Součástí vaší strategie zabezpečení ochrany dat by pak mělo být pravidelné použití příkazu CHKOBJITG nebo DCM za účelem ověření, že podpisy na daném softwaru jsou stále platné, tzn. že se objekty od jejich podepsání nezměnily. Dále byste mohli požadovat, aby veškerý obnovovaný software ve vašem systému byl podepsán buď vámi, nebo známým zdrojem. Jelikož je však většina softwaru serveru iSeries, který není vytvořen

společností IBM, v současné době bez podpisu, bylo by toto opatření ve vašem systému pravděpodobně příliš restriktivní. Nová podpora digitálních podpisů vám umožňuje pružně rozhodovat, jakou nejlepší cestu zvolit pro ochranu integrity vašeho softwaru.

Digitální podpisy, které chrání software, představují pouze jeden způsob použití digitálních certifikátů. Další informace o správě digitálních certifikátů naleznete v tématu DCM (Digital certificate management) v rámci aplikace Information Center (podrobnosti viz část "Nezbytné předchozí a související informace" na stránce xii).

Monitorování popisů podsystémů

Když spustíte podsystém na serveru iSeries, vytvoří systém prostředí pro práci, kterým je možné vstupovat do systému a spouštět systém. Popis podsystému definuje, jak toto prostředí vypadá. Popisy podsystémů tedy představují příležitost pro uživatele s nekalými úmysly. Počítačový piráti mohou použít popis podsystému k automatickému spuštění programu nebo k umožnění přihlášení bez uživatelského profilu.

Když spustíte příkaz RVKPUBAUT (Vyvolání obecného oprávnění), nastaví systém veřejné oprávnění k příkazům pro práci s popisy podsystémů na hodnotu *EXCLUDE. Tak se zabrání uživatelům, kteří nejsou specificky autorizováni (a nemají zvláštní oprávnění *ALLOBJ), měnit nebo vytvářet popisy podsystémů.

V následujících tématech najdete návrhy pro revidování popisů podsystémů, které aktuálně existují ve vašem systému. Pokud chcete vytvořit seznam všech popisů podsystémů, můžete použít příkaz WRKSBSD (Práce s popisem podsystému). Když v seznamu zadáte volbu 5 (Zobrazit), zobrazí se pro zvolený popis systému menu. Toto menu obsahuje seznam částí prostředí podsystému.

Chcete-li zobrazit podrobnosti o jednotlivých částech, zvolte příslušnou volbu. První dvě položky v menu změníte pomocí příkazu CHGSBSD (Změna popisu podsystému). Pokud chcete změnit další položky, použijte pro daný typ položky odpovídající příkaz pro přidání, odstranění nebo změnu. Jestliže například chcete změnit záznam pracovní stanice, použijte příkaz CHGWSE (Změna záznamu pracovní stanice).

Další informace o práci s popisy podsystémů obsahuje publikace *Work Management*. Najdete zde také seznam hodnot pro popisy podsystémů dodávané společností IBM.

Záznamy automaticky spuštěných úloh

Záznam automaticky spuštěné úlohy obsahuje jméno popisu úlohy. Popis úlohy může obsahovat data požadavku (RQSDTA), která mohou vést ke spuštění programu nebo příkazu. RQSDTA by mohla být například CALL LIB1/PROGRAM1. Kdykoliv se spustí podsystém, systém spustí program PROGRAM1 v knihovně LIB1.

Podívejte se na vaše záznamy automaticky spuštěných úloh a asociované popisy úloh. Ujistěte se, že rozumíte funkci všech programů, které se automaticky spouští, když se spustí podsystém.

Jména a typy pracovních stanic

Po spuštění podsystém přidělí všechny nepřidělené pracovní stanice, které jsou uvedeny (konkrétně nebo generický) v jeho záznamech pro jména pracovních stanic a typy pracovních stanic. Když se uživatel přihlašuje, přihlašuje se k podsystému, který má alokovánu pracovní stanici.

Záznam pracovní stanice uvádí, jaký popis úlohy se použije, když se na dané pracovní stanici spustí nějaká úloha. Popis úlohy může obsahovat data požadavku, která mohou vést ke spuštění programu nebo příkazu. Parametr RQSDTA by mohl mít například hodnotu CALL LIB1/PROGRAM1. Kdykoliv se uživatel přihlásí k pracovní stanici v daném podsystému, spustí systém program PROGRAM1 v knihovně LIB1.

Podívejte se na vaše záznamy pracovních stanic a asociované popisy úloh. Ujistěte se, že nikdo nepřidal nebo neaktualizoval žádné záznamy tak, aby spouštěly programy, o nichž nic nevíte.

Záznam pracovní stanice může rovněž specifikovat předvolený uživatelský profil. U určitých konfigurací podsystému tato skutečnost umožňuje, aby se někdo přihlásil pouhým stisknutím klávesy Enter. Je-li úroveň zabezpečení (systémová hodnota QSECURITY) ve vašem systému nižší než 40, měli byste zkontrolovat záznamy pracovní stanice, zda neobsahují předvolené uživatele.

Záznamy front úloh

Po spuštění podsystém přidělí všechny nepřidělené fronty úloh, které jsou uvedeny v popisu podsystému. Záznamy front úloh nepředstavují žádné přímé bezpečnostní riziko. Někomu však mohou poskytnout příležitost, aby si pohrával s výkonem systému tím způsobem, že by zapříčinil spouštění úloh v nezamýšlených prostředích.

Záznamy front úlohy byste měli pravidelně prohlížet, abyste měli jistotu, že jsou dávkové úlohy spouštěny tam, kde to předpokládáte.

Záznamy směrování

Záznam směrování definuje, co úloha dělá, když vstoupí do podsystému. Podsystém používá záznamy směrování pro všechny typy úloh: dávkové, interaktivní i komunikační. Záznam směrování specifikuje toto:

- Třídu úlohy. Stejně jako záznamy front úloh může třída, která je asociována s úlohou, ovlivnit její výkon, ale nepředstavuje žádné bezpečnostní riziko.
- Program, který se spustí, když se spustí úloha. Prohlédněte si záznamy směrování a ujistěte se, že nikdo nepřidal nebo neaktualizoval žádné záznamy tak, aby spouštěly programy, o nichž nic nevíte.

Záznamy komunikací a jména vzdálených systémů

Když do vašeho systému vstoupí komunikační úloha, určí systém na základě záznamů komunikací a záznamů jmen vzdálených systémů, jak bude tato úloha spuštěna. U těchto záznamů si všimněte následujícího:

- Všechny podsystémy jsou schopné spouštět komunikační úlohy. Není-li aktivní podsystém, který je určen pro danou komunikaci, může úloha, která se snaží dostat do vašeho systému, nalézt záznam v jiném popisu podsystému, který splňuje její potřeby. Je třeba si prohlédnout záznamy ve všech popisech podsystémů.
- Záznam komunikací obsahuje popis úlohy. Popis úlohy může obsahovat data požadavku, která spouští nějaký program nebo příkaz. Podívejte se na záznamy komunikací a s nimi asociované popisy úloh a ujistěte se, že je vám jasné, jak se úlohy spustí.
- Záznam komunikací také specifikuje předvolený uživatelský profil, který v některých situacích využívá systém. Ověřte si, že rozumíte úloze předvolených profilů. Jestliže váš systém obsahuje předvolené profily, měli byste zajistit, aby to byly profily s minimálním oprávněním. Další informace o předvolených uživatelských profilech uvádí Kapitola 12, “Zabezpečení komunikace APPC”.

Chcete-li zjistit záznamy komunikací, které uvádějí jméno uživatelského profilu, použijte příkaz PRTSBSDAUT (Tisk popisu podsystému).

Záznamy předspuštěných úloh

Záznamy předspuštěných úloh můžete použít za účelem připravení podsystému pro určité druhy úloh tak, aby se tyto úlohy spouštěly rychleji. Předspuštěné úlohy se mohou spustit, když se spustí podsystém nebo když jsou potřeba. Záznam předspuštěné úlohy specifikuje toto:

- Program, který se má spustit.

  Předvolený uživatelský profil.

  Popis úlohy.

Všechny tyto položky představují potenciální bezpečnostní riziko. Měli byste se ujistit, že záznamy předspuštěných úloh provádějí pouze autorizované a očekávané funkce.

Úlohy a popisy úloh

Popisy úloh obsahují data požadavku a údaje o směrování, které mohou vést k tomu, že se při použití daného popisu úlohy spustí určitý program. Když popis úlohy specifikuje nějaký program v parametru dat požadavku, systém tento program spustí. Pokud popis úlohy uvádí údaje o směrování, systém spustí program, který je specifikován v záznamu směrování, jenž odpovídá údajům o směrování.

Systém používá popisy úloh pro interaktivní i dávkové úlohy. U interaktivních úloh je popis úlohy uveden v záznamu pracovní stanice. Obvykle má záznam pracovní stanice hodnotu *USRPRF, takže systém používá popis úlohy, který je uveden v uživatelském profilu. U dávkových úloh zadáváte popis úlohy v okamžiku, kdy spouštíte úlohu.

Popisy úloh byste měli pravidelně prohlížet, abyste měli jistotu, že nespouštějí nežádoucí programy. Rovněž byste měli používat oprávnění k objektu, abyste zabránili změnám popisů úloh. Oprávnění *USE je dostačující pro spuštění úlohy v popisem úlohy. Běžný uživatel nepotřebuje oprávnění *CHANGE k popisům úloh.

Volby menu SECBATCH:
15 *pro okamžité spuštění,* **54** *pro použití plánovače úloh*

Popisy úloh mohou také specifikovat, pod kterým uživatelským profilem by měla být úloha spuštěna. Při úrovni zabezpečení 40 a vyšší musíte mít oprávnění *USE k popisu úlohy i k uživatelskému profilu, který je uveden v popisu úlohy. Při úrovni zabezpečení nižší než 40 potřebujete oprávnění *USE pouze k popisu úlohy.

Příkaz PRTJOBDAUT (Tisk oprávnění k popisu úlohy) můžete použít k vytištění seznamu popisů úloh, které specifikují uživatelský profil a mají veřejné oprávnění *USE.

Sestava ukazuje zvláštní oprávnění pro uživatelský profil, který je uveden v popisu úlohy. V sestavě jsou zahrnuta zvláštní oprávnění všech skupinových profilů, která má uživatelský profil. K zobrazení soukromých oprávnění uživatelského profilu můžete použít následující příkaz:

```
DSPUSRPRF USRPRF(jméno-profilu) TYPE(*OBJAUT)
```

Popis úlohy uvádí seznam knihoven, které úloha používá, když je spuštěná. Pokud může někdo změnit seznam knihoven uživatele, mohl by takový uživatel spustit nežádoucí verzi programu v jiné knihovně. Seznamy knihoven uvedené v popisech úloh ve vašem systému byste měli pravidelně prohlížet.

Nakonec byste se měli přesvědčit, že předvolené hodnoty pro příkaz SBMJOB (Zadání úlohy) a CRTUSRPRF (Vytvoření uživatelského profilu) nebyly změněny tak, aby ukazovaly na nežádoucí popisy úloh.

Jména TPN architektury

Některé komunikace vyžadují, aby byl do vašeho systému odeslán specifický typ signálu. Tento požadavek se nazývá **jméno TPN architektury** (architecture transaction program name), neboť jméno transakčního programu je součástí architektury APPC systému. Jménem TPN architektury je například požadavek na přímý průchod na obrazovkovou stanici. Jména TPN architektury přestavují normální způsob komunikace funkcí a nemusí nutně znamenat bezpečnostní riziko. Mohou však poskytovat neočekávaný vstup do vašeho systému.

Některá TPN nepředávají v požadavku žádný profil. Pokud se požadavek sdruží se záznamem komunikací, jehož předvolený uživatel je *SYS, může být požadavek ve vašem systému spuštěn. Profil *SYS však může spouštět pouze systémové funkce, nikoliv uživatelské aplikace.

Jestliže nechcete, aby se jména TPN spouštěla s předvoleným profilem, můžete změnit předvoleného uživatele v záznamech komunikací ze *SYS na *NONE. Část “Požadavky na jména TPN architektury” uvádí přehled jmen TPN a asociovaných uživatelských profilů.

Pokud chcete, aby se určité TPN ve vašem systému vůbec nespouštělo, postupujte takto:

1. Vytvořte program v jazyku CL, který přijímá několik parametrů. Program by neměl provádět žádnou funkci. Měl by být tvořen pouze příkazy DCL (Declare) pro parametry a pak by měl být ukončen.
2. Do každého podsystému, který má záznamy komunikací nebo záznamy jmen vzdálených systémů, přidejte záznam směrování pro TPN. V záznamu směrování by mělo být uvedeno toto:
   - Hodnota *CMPVAL* (porovnávací hodnota) rovná jménu programu pro TPN (viz část Požadavky na jména TPN architektury) s počáteční pozicí 37.
   - Hodnota *PGM* (program, který se má volat) rovná jménu programu, který jste vytvořili v kroku 1. Tím zabráníte tomu, aby TPN vyhledalo jiný záznam směrování, jako např. *ANY.

Několik TPN má již svůj vlastní záznam směrování v podsystému QCMN. Ty byly přidány z důvodu výkonu.

Požadavky na jména TPN architektury

Tabulka 17. Programy a uživatelé pro požadavky TPN

Požadavek TPN	Program	Uživatelský profil	Popis
X'30F0F8F1'	AMQCRC6A	*NONE	Zařazení do fronty zpráv.
X'06F3F0F1'	QACSOTP	QUSER	Transakční program pro přihlášení APPC.
X'30F0F2D1'	QANRTP	QADSM	Konfigurace APPC ADSM/400.
X'30F0F1F9'	QCNPCSUP	*NONE	Sdílené pořadače.
X'07F0F0F1'	QCNTEDDM	QUSER	DDM.

Tabulka 17. Programy a uživatelé pro požadavky TPN (pokračování)

Požadavek TPN	Program	Uživatelský profil	Popis
X'07F6C4C2'	QCNTEDDM	QUSER	Vzdálený SQL – DRDA1.
X'30F0F7F7'	QCQNRBAS	QSVCCS	SNA CC_Server.
X'30F0F1F4'	QDXPRCV	QUSER	Příjemce DSNX–PC.
X'30F0F1F3'	QDXPSEND	QUSER	Odesílatel DSNX–PC.
X'30F0F2C4'	QEVYMAIN	QUSER	ENVY**/400 Server.
X'30F0F6F0'	QHQTRGT	*NONE	PC datová fronta.
X'30F0F8F0'	QLZPSERV	*NONE	Správce licencí Client Access.
X'30F0F1F7'	QMFRCVR	*NONE	Příjemce PC zprávy.
X'30F0F1F8'	QMFSNDR	*NONE	Odesílatel PC zprávy.
X'30F0F6F6'	QND5MAIN	QUSER	Řadič pracovní stanice 5394 APPN.
DB2DRDA	QCNTEDDDM	QUSER	DB2DRDA.
APINGD	QNMAPINGD	QUSER	APINGD.
X'30F0F5F4'	QNMEVK	QUSER	Obslužné programy pro správu systému.
X'30F0F2C1'	QNPSERVR	*NONE	Síťový tiskový server PWS-I.
X'30F0F7F9'	QOCEVOKE	*NONE	Mezisystémový kalendář.
X'30F0F6F1'	QOKCSUP	QDOC	Stínování adresáře.
X'20F0F0F7'	QOQSESRV	QUSER	DIA verze 2.
X'20F0F0F8'	QOQSESRV	QUSER	DIA verze 2.
X'30F0F5F1'	QOQSESRV	QUSER	DIA verze 2.
X'20F0F0F0'	QOSAPPC	QUSER	DIA verze 1.
X'30F0F0F5'	QPAPAST2	QUSER	Přímý průchod S/36—S/38.
X'30F0F0F9'	QPAPAST2	QUSER	Přímý průchod na tiskárnu.
X'30F0F4F6'	QPWFSTP0	*NONE	Sdílené pořadače typu 2.
X'30F0F2C8'	QPWFSTP1	*NONE	Souborový server Client Access.
X'30F0F2C9'	QPWFSTP2	*NONE	Souborový server Windows** Client Access.
X'30F0F6F9'	QRQSRVX	*NONE	Vzdálený SQL – konvertovaný server.
X'30F0F6F5'	QRQSRV0	*NONE	Vzdálený SQL bez potvrzení.
X'30F0F6F4'	QRQSRV1	*NONE	Vzdálený SQL bez potvrzení.
X'30F0F2D2'	QSVRCI	QUSER	SOC/CT.
X'21F0F0F8'	QS2RCVR	QGATE	Příjemce SNADS FS2.
X'21F0F0F7'	QS2STSND	QGATE	Odesílatel SNADS FS2.
X'30F0F1F6'	QTFDWNLD	*NONE	Přenosová funkce PC.
X'30F0F2F4'	QTIHNPCS	QUSER	Funkce TIE.
X'30F0F1F5'	QVPPRINT	*NONE	Virtuální tisk PC.
X'30F0F2D3'	QWGMTP	QWGM	Ultimedia Mail/400 Server.
X'30F0F8F3'	QZDAINIT	QUSER	Datový přístupový server PWS-I.
X'21F0F0F2'	QZDRCVR	QSNADS	Příjemce SNADS.
X'21F0F0F1'	QZDSTSND	QSNADS	Odesílatel SNADS.
X'30F0F2C5'	QZHQTRG	*NONE	Server datových front PWS-I.
X'30F0F2C6'	QZRCSRVR	*NONE	Server vzdálených příkazů PWS-I.

Tabulka 17. Programy a uživatelé pro požadavky TPN (pokračování)

Požadavek TPN	Program	Uživatelský profil	Popis
X'30F0F2C7'	QZSCSRVR	*NONE	Centrální server PWS-I.

Metody monitorování událostí týkajících se zabezpečení

Nastavení zabezpečení ochrany dat není jednorázovou akcí. Je třeba průběžně hodnotit jak změny ve vašem systému, tak selhání zabezpečení. Na základě zjištěných skutečností pak musíte přizpůsobit vaše prostředí zabezpečení.

Změny týkající se zabezpečení, ke kterým došlo ve vašem systému, můžete sledovat pomocí sestav pro zabezpečení. Dále jsou uvedeny další systémové funkce, které můžete použít k odhalení bezpečnostních rizik a případných selhání zabezpečení.

- Monitorování zabezpečení je účinným nástrojem, jenž můžete použít ke sledování různých typů událostí souvisejících se zabezpečením, které se vyskytnou ve vašem systému. Například můžete systém nastavit tak, aby se zapsal monitorovací záznam vždy, když uživatel otevře určitý databázový soubor za účelem aktualizace. Můžete monitorovat všechny změny v systémových hodnotách. Lze monitorovat akce, ke kterým dojde, když uživatelé obnovují objekty.

  Vyčerpávající informace o funkci monitorování zabezpečení najdete v 9. kapitole publikace *Zabezpečení iSeries - referenční informace Reference*. Chcete-li nastavit monitorování zabezpečení ve vašem systému, použijte příkaz CHGSECAUD (Změna monitorování zabezpečení). Můžete také použít příkaz DSPAUDJRNE (Zobrazení záznamů monitorovacího žurnálu) k vytištění vybraných informací z monitorovacího žurnálu.
- Můžete vytvořit frontu zpráv QSYSMSG, do které se budou posílat kritické zprávy systémového operátora. V průběhu běžného pracovního dne přijímá fronta zpráv QSYSOPR velké množství zpráv rozdílné důležitosti. Kvůli tomu se může stát, že se kritické zprávy související se zabezpečením přehlédnou.

  Pokud ve vašem systému vytvoříte frontu zpráv QSYSMSG v knihovně QSYS, nasměruje systém automaticky určité kritické zprávy do fronty zpráv QSYSMSG namísto QSYSOPR.

  Buď můžete vytvořit program pro monitorování fronty zpráv QSYSMSG, nebo jí můžete přiřadit režim přerušení pro vás nebo pro nějakého jiného důvěryhodného uživatele.

Část 3. Aplikace a síťové komunikace

Kapitola 11. Použití integrovaného systému souborů k zabezpečení souborů

Integrovaný systém souborů vám nabízí několik způsobů, jak ukládat a prohlížet informace na serveru iSeries. Integrovaný systém souborů je součástí operačního systému OS/400, která podporuje proudové I/O operace. Poskytuje metody správy paměti, které jsou podobné (a kompatibilní) operačním systémům PC a UNIX.

S integrovaným systémem souborů můžete všechny objekty na serveru nahlížet z perspektivy hierarchické struktury adresářů. Ve většině případů však uživatelé nahlížejí na objekty způsobem, který je nejběžnější pro konkrétní systém souborů. Například ″tradiční″ objekty serveru iSeries jsou uloženy v systému souborů QSYS.LIB. Uživatelé na tyto objekty obvykle nahlížejí z hlediska knihoven. Na objekty v systému souborů QDLS uživatelé obvykle nahlížejí z perspektivy dokumentů v pořadačích. Systémy souborů root (/), QOpenSys a uživatelem definované systémy souborů představují strukturu hierarchických (vnořených) adresářů.

Jako administrátor systému musíte vědět toto:

- Které systémy souborů se používají ve vašem systému.
- Jedinečné charakteristiky jednotlivých systémů souborů.

V následujících částech najdete některá obecná doporučení pro zabezpečení integrovaného systému souborů.

Přístup k zabezpečení z hlediska integrovaného systému souborů

Systém souborů root vystupuje jako deštník (nebo jako základna) pro všechny ostatní systémy souborů na serverech iSeries. Na vyšší úrovni zajišťuje integrovaný pohled na všechny objekty v systému. Ostatní systémy souborů, které mohou existovat na serverech iSeries, poskytují nejrůznější přístupy ke správě a integritě objektů, v závislosti na hlavním účelu systému souborů. Systém souborů QOPT (optický) například umožňuje aplikacím a serverům iSeries (včetně souborového serveru iSeries Access for Windows) přístup k jednotce CD-ROM na serveru iSeries. Podobně systém souborů QFileSvr.400 umožňuje aplikacím přístup k datům integrovaného systému souborů na vzdálených serverech iSeries. Systém souborů QLANSrv umožňuje přístup k souborům uloženým na integrovaném serveru Integrated xSeries Server for iSeries nebo na jiných připojených serverech v síti.

Přístup k zabezpečení pro jednotlivé systémy souborů závisí na datech, která daný systém souborů zpřístupňuje. Například systém souborů QOPT nezajišťuje zabezpečení na úrovni objektu, neboť neexistuje žádná technologie, kterou by bylo možné zapsat informace o oprávněních na CD-ROM. U systému souborů QFileSvr.400 se řízení přístupu odehrává ve vzdáleném systému (kde jsou soubory fyzicky uloženy a spravovány). Pro soubory systémů, jako je QLANSrv, zajišťuje řízení přístupu server Integrated xSeries Server for iSeries. Přes rozdílné modely zabezpečení podporuje řada systémů souborů konzistentní správu řízení přístupu prostřednictvím příkazů integrovaného systému souborů, jako např. CHGAUT (Změna oprávnění) a CHGOWN (Změna vlastníka).

Zde je několik rad týkajících se zákoutí a skulin zabezpečení integrovaného systému souborů. Integrovaný systém souborů je navržen v co největším souladu se standardy POSIX. To vede k určitému zvláštnímu chování tam, kde dochází ke kombinaci oprávnění serveru iSeries a oprávnění POSIX:

1. Neodstraňujte pro uživatele soukromé oprávnění k adresáři, jehož je vlastníkem, i kdyby byl tento uživatel oprávněn prostřednictvím veřejného oprávnění, skupiny nebo seznamu oprávnění. Při práci s knihovnami a pořadači ve standardním modelu zabezpečení serveru iSeries by zrušení soukromého oprávnění vlastníka vedlo k redukci množství informací o oprávněních uložených pro uživatelský profil a neovlivnilo by jiné operace. Ale kvůli způsobu, kterým standard POSIX definuje přebírání oprávnění pro adresáře, bude mít vlastník nově vytvořeného adresáře stejná oprávnění k tomuto adresáři, jako má vlastník rodičovského objektu k rodičovskému objektu, i kdyby vlastník nově vytvořeného adresáře měl jiná soukromá oprávnění k rodičovskému objektu. Možná je to těžké na pochopení, proto zde uvádíme příklad: uživatel USERA vlastní adresář /DIRA, ale soukromá oprávnění USERA byla odstraněna. Uživatel USERB má soukromé oprávnění k adresáři /DIRA. USERB vytvoří adresář /DIRA/DIRB. Jelikož USERA nemá žádné oprávnění k objektu k adresáři /DIRA, nebude mít USERB žádné oprávnění k objektu k adresáři /DIRA/DIRB. USERB bude schopný přejmenovat nebo vymazat adresář /DIRA/DIRB, aniž by musel změnit oprávnění k objektu USERB. To také vstupuje do hry, když se vytváří soubory pomocí rozhraní open() API s využitím příznaku O_INHERITMODE. Pokud USERB vytvořil soubor /DIRA/FILEB, neměl by USERB žádné oprávnění k objektu a žádná oprávnění k datům. USERB by nemohl zapisovat do nového souboru.
2. Adoptované oprávnění není většinou systémů fyzických souborů uznáváno. Týká se to i systémů souborů root (/), QOpenSys, QDLS a uživatelem definovaných systémů souborů.
3. Objekty jsou vlastněny uživatelským profilem, který je vytvořil, i když je pole OWNER uživatelského profilu nastaveno na hodnotu *GRPPRF.
4. Mnoho operací systému souborů vyžaduje oprávnění k datům *RX ke každé části cesty, včetně kořenového adresáře (/). Když narazíte na problémy s oprávněními, nezapomeňte zkontrolovat oprávnění uživatele k samotnému kořenovému adresáři.
5. Zobrazení nebo načtení aktuálního pracovního adresáře (DSPCURDIR, getcwd(), atd.) vyžaduje oprávnění k datům *RX ke každé části cesty. Avšak změna aktuálního pracovního adresáře (CD, chdir(), atd.) vyžaduje ke každé části pouze oprávnění k datům *X. Proto může uživatel změnit aktuální pracovní adresář na určitou cestu a pak nemusí být schopen tuto cestu zobrazit.
6. Úkolem příkazu COPY je vytvořit kopii objektu. Nastavení oprávnění k novému souboru bude shodné s původním kromě vlastníka. Cílem příkazu CPYTOSTMF je však jenom zkopírování dat. Nastavení oprávnění pro nový soubor nemůže řídit uživatel. Tvůrce/vlastník bude mít oprávnění k datům *RWX, ale skupinová a veřejná oprávnění budou mít hodnotu *EXCLUDE. Uživatel musí použít jiné prostředky (CHGAUT, chmod(), atd.) k přiřazení požadovaných oprávnění.
7. Uživatel musí být vlastníkem nebo musí mít oprávnění k objektu *OBJMGT, aby mohl načíst informace o oprávněních pro daný objekt. To se může projevit na neočekávaných místech, např. u příkazu COPY, který musí načíst informace o oprávněních pro zdrojový objekt, aby mohl nastavit odpovídající oprávnění u cílového objektu.
8. Při změně vlastníka nebo skupiny objektu nestačí uživateli pouze odpovídající oprávnění k objektu, ale musí mít také oprávnění k datům *ADD k novému uživatelskému profilu vlastníka/skupiny a oprávnění k datům *DELETE k původnímu profilu vlastníka/skupiny. Tato oprávnění k datům se nevztahují k oprávněním k datům systému souborů. Tato oprávnění k datům lze zobrazit pomocí příkazu DSPOBJAUT a změnit pomocí příkazu EDTOBJAUT. Toto se může neočekávaně projevit také u příkazu COPY, když se pro nový objekt pokusí nastavit ID skupiny.
9. U příkazu MOV se mohou vyskytnout nejasné chyby oprávnění, a to zvláště při přenosu z jednoho systému souborů do jiného nebo při provádění konverze dat. V těchto případech se přesun ve skutečnosti stává operací kopírovat-a-vymazat. Proto může být příkaz MOV kromě dalších specifických pokynů ovlivněn stejnými pravidly týkajícími se oprávnění jako příkaz COPY (viz výše uvedený bod 7 a 8) a příkaz RMVLNK.

Následující části obsahují pokyny pro několik reprezentativních systémů souborů. Pokud potřebujete další informace o určitém systému souborů na vašem serveru iSeries, budete muset projít dokumentaci k licenčnímu programu, který používá daný systém souborů.

Systémy souborů root (/), QOpenSys a uživatelem definované systémy souborů

Dále uvádíme bezpečnostní pokyny k systémům souborů root, QOpenSys a uživatelem definovaným systémům souborů.

Jak funguje oprávnění

Systémy souborů root, QOpenSys a uživatelem definované systémy souborů poskytují kombinaci schopností serveru iSeries, PC a UNIX** jak pro správu objektů, tak pro zabezpečení. Když používáte příkazy integrovaného systému souborů z relace serveru iSeries (WRKAUT a CHGAUT), můžete nastavit všechna běžná oprávnění k objektu serveru iSeries. To zahrnuje oprávnění *R, *W a *X, která jsou kompatibilní se Spec 1170 (operační systémy typu UNIX).

Poznámka: Systémy souborů root, QOpenSys a uživatelem definované systémy souborů jsou funkčně ekvivalentní. Systém souborů QOpenSys rozlišuje malá a velká písmena. Systém souborů root velikost písmen nerozlišuje. Systémy souborů definované uživatelem lze definovat tak, aby rozlišovaly velká a malá písmena. Jelikož mají tyto systémy souborů stejné charakteristiky zabezpečení, můžete v následujících částech předpokládat, že je jejich jména možné zaměňovat.

Když k systému souborů root přistupujete jako administrátor z relace PC, můžete nastavit atributy objektů, které PC používá, za účelem omezení určitých typů přístupu:
- System (systém).
- Hidden (skrytý).
- Archive (archiv).
- Read-only (pouze pro čtení).

Tyto PC atributy jsou doplňkem, nikoliv nahrazením, hodnot oprávnění k objektu serveru iSeries.

Když se uživatel pokusí získat přístup k objektu v systému souborů root, vynutí operační systém OS/400 všechny hodnoty oprávnění k objektu a atributy pro daný objekt bez ohledu na to, zda jsou tato oprávnění ″viditelná″ z uživatelského rozhraní. Například předpokládejme, že je pro objekt aktivován atribut pouze pro čtení. Uživatel PC nemůže vymazat objekt prostřednictvím rozhraní produktu iSeries Access. Uživatel serveru iSeries s pevnou funkční pracovní stanicí nemůže vymazat objekt, ani kdyby měl zvláštní oprávnění *ALLOBJ. Aby bylo možné objekt vymazat, musí autorizovaný uživatel použít PC funkci k nastavení hodnoty read-only (pouze pro čtení) na off (vypnuto). Podobně uživatel PC nemusí mít dostatečné oprávnění operačního systému OS/400 ke změně atributů zabezpečení vztahujících se k PC pro nějaký objekt.

Aplikace typu UNIX, které běží na serverech iSeries, používají pro přístup k datům v systému souborů root rozhraní API podobná UNIX. Díky těmto rozhraním mohou aplikace rozpoznávat a udržovat následující informace o zabezpečení:
- Vlastník objektu.
- Skupinový vlastník (primární skupinové oprávnění serveru iSeries).
- Čtení (souborů).
- Zápis (změna obsahu).
- Provádění (spouštění programů nebo prohledávání adresářů).

Systém mapuje tato oprávnění k datům na existující oprávnění k objektům a datům serveru iSeries:

- Čtení (*R) = *OBJOPR a *READ
- Zápis (*W) = *OBJOPR, *ADD, *UPD, *DLT
- Provádění (*X) = *OBJOPR a *EXECUTE

Koncepce pro ostatní oprávnění k objektu (*OBJMGT, *OBJEXIST, *OBJALTER a *OBJREF) v prostředí typu UNIX neexistují.

Tato oprávnění k objektu však existují pro všechny objekty v systému souborů root. Když vytvoříte nějaký objekt pomocí rozhraní API podobného UNIX, zdědí daný objekt tato oprávnění od nadřízeného adresáře, což bude mít za výsledek toto:

- Vlastník nového objektu má stejné oprávnění k objektu jako vlastník nadřízeného adresáře.
- Primární skupina nového objektu má stejné oprávnění k objektu jako primární skupina nadřízeného adresáře.
- Obecní uživatelé nového objektu mají stejné oprávnění k objektu jako obecní uživatelé nadřízeného adresáře.

Oprávnění k datům nového objektu pro vlastníka, primární skupinu a obecné uživatele jsou určena v rozhraní API parametrem režimu. Když jsou všechna oprávnění k objektu nastavena na hodnotu 'on' (zapnuto), dočkáte se takového fungování oprávnění, jaké byste očekávali v prostředí typu UNIX. Nejlepší je ponechat všechna oprávnění nastavena na 'on', pokud ovšem nechcete simulovat prostředí POSIX.

Když spouštíte aplikace, které používají rozhraní API podobné UNIX, vynutí systém všechna oprávnění k objektům, bez ohledu na to, zda jsou v aplikacích typu UNIX ″viditelné″, či nikoliv. Systém například vynutí oprávnění seznamů oprávnění, přestože koncepce seznamů oprávnění v operačních systémech typu UNIX neexistuje.

Jestliže používáte smíšené aplikační prostředí, musíte zajistit, abyste neprováděli změny oprávnění v jednom prostředí, které naruší vaše aplikace v jiném prostředí.

Práce se zabezpečením pro systémy souborů root (/), QOpenSys a uživatelem definované systémy souborů

Se zavedením integrovaného systému souborů začaly servery iSeries také poskytovat novou příkazovou sadu pro práci s objekty ve více systémech souborů. Tato příkazová sada zahrnuje příkazy pro práci se zabezpečením:

- CHGAUD (Změna monitorování).
- CHGAUT (Změna oprávnění).
- CHGOWN (Změna vlastníka).
- CHGPGP (Změna primární skupiny).
- DSPAUT (Zobrazení oprávnění).
- WRKAUT (Práce s oprávněním).

Tyto příkazy seskupují hlavní oprávnění k datům a objektům do podmnožin oprávnění podobných UNIX:

***RWX** čtení/zápis/provádění
***RW** čtení/zápis
***R** čtení
***WX** zápis/provádění
***W** zápis
***X** provádění

Kromě toho lze rozhraní API podobná UNIX využívat pro práci se zabezpečením.

Veřejné oprávnění ke kořenovému adresáři

Když obdržíte váš systém, je veřejné oprávnění ke kořenovému adresáři nastaveno na hodnotu *ALL (oprávnění ke všem objektům a oprávnění ke všem datům). Toto nastavení zajišťuje flexibilitu a kompatibilitu jak s tím, co očekávají aplikace typu UNIX, tak s tím, co očekávají běžní uživatelé serveru iSeries. Uživatel serveru iSeries s možností využívat příkazovou řádku může vytvořit novou knihovnu v systému souborů QSYS.LIB tak, že jednoduše zadá příkaz CRTLIB. Obvykle to oprávnění na typickém serveru iSeries umožňuje. Podobně, dodané nastavení pro systém souborů root umožňuje typickému uživateli vytvořit nový adresář v systému souborů root (stejně, jako můžete vytvořit nový adresář na vašem PC).

Jako administrátor systému musíte vést vaše uživatele k tomu, aby adekvátním způsobem chránili objekty, které vytvoří. Když uživatel vytvoří knihovnu, nemělo by mít pravděpodobně veřejné oprávnění k této knihovně hodnotu *CHANGE (předvolba). Uživatel by měl nastavit veřejné oprávnění buď na hodnotu *USE, nebo *EXCLUDE, v závislosti na obsahu knihovny.

Pokud vaši uživatelé potřebují vytvářet nové adresáře v systémech souborů root (/), QOpenSys nebo uživatelem definovaných systémech souborů, máte několik možností zabezpečení:

- Můžete vaše uživatele naučit, jak se přepíše předvolené oprávnění, když vytvoří nové adresáře. Předvolenou hodnotou je převzít oprávnění od nejbližšího nadřazeného adresáře. V případě nově vytvořeného adresáře v kořenovém adresáři bude předvolenou hodnotou veřejného oprávnění hodnota *ALL.
- Pod kořenovým adresářem můžete vytvořit ″hlavní″ podadresář. Pro tento hlavní adresář nastavte veřejné oprávnění tak, aby odpovídalo požadavkům vaší organizace. Pak sdělte uživatelům, aby jakékoliv nové osobní adresáře vytvářeli v tomto hlavním podadresáři. Jejich nové adresáře převezmou jeho oprávnění.
- Můžete zvážit, zda byste neměli změnit veřejné oprávnění pro kořenový adresář, abyste v něm uživatelům zabránili vytvářet objekty. (Odstraňte oprávnění *W, *OBJEXIST, *OBJALTER, *OBJREF a *OBJMGT.) Musíte však zhodnotit, zda tato změna nepřinese problémy pro některé z vašich aplikací. Například můžete mít aplikace typu UNIX, které předpokládají, že budou schopny mazat objekty z kořenového adresáře.

Příkaz PRTPVTAUT (Tisk soukromých oprávnění k objektům)

Příkaz PRTPVTAUT (Tisk soukromých oprávnění) vám umožňuje vytisknout sestavu všech soukromých oprávnění pro objekty určitého typu v určité knihovně, pořadači nebo adresáři. Sestava uvádí seznam všech objektů zadaného typu a uživatele, kteří k nim mají oprávnění. Nabízí se vám tak způsob, jak kontrolovat různé zdroje oprávnění k objektům.

Tímto příkazem se pro zvolené objekty vytisknou tři sestavy. První sestava (úplná) obsahuje všechna soukromá oprávnění pro jednotlivé vybrané objekty. Druhá sestava (sestava změn) obsahuje doplnění a změny v soukromých oprávněních ke zvoleným objektům, pokud byl příkaz PRTPVTAUT dříve spuštěn pro určité objekty v určité knihovně, pořadači nebo adresáři. V sestavě změn jsou uvedeny veškeré nové objekty vybraného typu, nová oprávnění ke stávajícím objektům nebo změny ve stávajících oprávněních k existujícím objektům. Jestliže příkaz PRTPVTAUT ještě nebyl dříve spuštěn pro určité objekty v určité knihovně, pořadači nebo adresáři, nevytiskne se žádná sestava změn. Pokud byl příkaz již dříve spuštěn, ale nedošlo k žádným změnám v oprávněních k objektům, sestava změn se vytiskne, ale nebudou v ní uvedeny žádné objekty.

Třetí sestava (sestava výmazů) obsahuje veškeré výmazy uživatelů se soukromým oprávněním ze zadaných objektů od posledního spuštění příkazu PRTPVTAUT. V sestavě výmazů jsou uvedeny veškeré objekty, které byly vymazány, nebo uživatelé, kteří byly

odstraněni jako uživatelé se soukromým oprávněním. Jestliže příkaz PRTPVTAUT ještě nebyl dříve spuštěn, nevytiskne se žádná sestava výmazů. Pokud byl příkaz již dříve spuštěn, ale nedošlo k žádným operacím výmazu u objektů, sestava výmazů se vytiskne, ale nebudou v ní uvedeny žádné objekty.

Omezení: K použití tohoto příkazu musíte mít zvláštní oprávnění *ALLOBJ.

Příklady:

Tento příkaz vytvoří úplnou sestavu, sestavu změn a sestavu výmazů pro objekty typu soubor v PAYROLLLIB:

```
PRTPVTAUT OBJTYPE(*FILE) LIB(PAYROLLLIB)
```

Tento příkaz vytvoří úplnou sestavu, sestavu změn a sestavu výmazů pro všechny objekty typu proudový soubor v adresáři garry:

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*NO)
```

Tento příkaz vytvoří úplnou sestavu, sestavu změn a sestavu výmazů pro všechny objekty typu proudový soubor ve struktuře podadresářů, která začíná adresářem garry:

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*YES)
```

Příkaz PRTPUBAUT (Tisk veřejně oprávněných objektů)

Příkaz PRTPUBAUT (Tisk veřejně oprávněných objektů) vám umožňuje vytisknout sestavu zadaných objektů, které nemají veřejné oprávnění *EXCLUDE. U objektů *PGM budou do sestavy zahrnuty pouze ty programy, které nemají veřejné oprávnění *EXCLUDE, jež může volat uživatel (program je buď uživatelskou doménou, nebo má systémová hodnota QSECURITY (úroveň zabezpečení systému) hodnotu 30 či nižší). Nabízí se vám tak způsob, jak kontrolovat objekty, k nimž má autorizovaný přístup každý uživatel v systému.

Tento program vytiskne dvě sestavy. První sestava (úplná) bude obsahovat všechny uvedené objekty, které nemají veřejné oprávnění *EXCLUDE. Druhá sestava (sestava změn) bude obsahovat objekty, které nyní nemají veřejné oprávnění *EXCLUDE, které měly veřejné oprávnění *EXCLUDE nebo při posledním spuštění příkazu PRTPUBAUT neexistovaly. Jestliže příkaz PRTPUBAUT ještě nebyl dříve spuštěn pro určité objekty a knihovnu, pořadač nebo adresář, nevytiskne se žádná sestava změn. Pokud byl příkaz již dříve spuštěn, ale žádné další objekty nemají veřejné oprávnění *EXCLUDE, sestava změn se vytiskne, ale nebudou v ní uvedeny žádné objekty.

Omezení: K použití tohoto příkazu musíte mít zvláštní oprávnění *ALLOBJ.

Příklady:

Tento příkaz vytvoří úplnou sestavu a sestavu změn pro všechny objekty typu soubor v knihovně GARRY, které nemají veřejné oprávnění *EXCLUDE:

```
PRTPUBAUT OBJTYPE(*FILE) LIB(GARRY)
```

Tento příkaz vytvoří úplnou sestavu, sestavu změn a sestavu výmazů pro všechny objekty typu proudový soubor ve struktuře podadresářů počínaje adresářem garry, které nemají veřejné oprávnění *EXCLUDE:

```
PRTPUBAUT OBJTYPE(*STMF) DIR(GARRY) SCHSUBDIR(*YES)
```

Omezení přístupu k systému souborů QSYS.LIB

Jelikož je systém souborů root zaštiťujícím systémem souborů, jeví se systém souborů QSYS.LIB jako podadresář v rámci kořenového adresáře. Proto libovolný uživatel PC s přístupem k vašem serveru iSeries může manipulovat s objekty uloženými v knihovnách serveru iSeries (systém souborů QSYS.LIB) pomocí běžných příkazů a akcí PC. Uživatel PC by například mohl přetáhnout objekt QSYS.LIB (jako např. knihovnu s vašimi kritickými datovými soubory) do skartovače.

Jak jste se dověděli v části "Systémy souborů root (/), QOpenSys a uživatelem definované systémy souborů" na stránce 89, vynucuje systém oprávnění ke všem objektům bez ohledu na to, zda jsou viditelná v rozhraní, či nikoliv. Proto uživatel nemůže skartovat (vymazat) objekt, pokud ovšem k objektu nemá oprávnění *OBJEXIST. Jestliže však váš server iSeries spoléhá na řízení přístupu prostřednictvím menu místo na zabezpečení na úrovni objektů, mohl by uživatel PC velmi dobře objevit objekty v systému souborů QSYS.LIB, které jsou dostupné pro skartování.

S rozšiřováním využití vašeho systému a používáním různých metod přístupu brzy odhalíte, že zabezpečení přístupu na úrovni menu není dostačující. Kapitola 5, "Ochrana informačních hodnot prostřednictvím oprávnění k objektům", na stránce 41 rozebírá strategie pro rozšíření řízení přístupu prostřednictvím menu o zabezpečení na úrovni objektů. Servery iSeries však také poskytují snadný způsob, jak zabránit přístupu k systému souborů QSYS.LIB prostřednictvím adresářové struktury systému souborů root. Chcete-li řídit, kteří uživatelé mají mít přístup k systému souborů QSYS.LIB prostřednictvím kořenového adresáře, můžete použít seznam oprávnění QPWFSERVER.

Když má oprávnění uživatele k seznamu oprávnění QPWFSERVER hodnotu *EXCLUDE, nemůže uživatel vstupovat do adresáře QSYS.LIB z kořenového adresáře. Když má oprávnění uživatele hodnotu *USE, může uživatel do adresáře vstupovat. Jakmile má uživatel oprávnění ke vstupu do adresáře, vztahuje se normální oprávnění k objektu na libovolnou akci, kterou se uživatel pokusí provést s objektem v rámci systému souborů QSYS.LIB. Jinými slovy, oprávnění k seznamu oprávnění QPWFSERVER funguje jako brána k celému systému souborů QSYS.LIB. Pro uživatele s oprávněním *EXCLUDE je brána zamčena. Pro uživatele s oprávněním *USE (či vyšším) je brána otevřená.

Ve většině situací uživatelé nepotřebují za účelem přístupu k objektům v systému souborů QSYS.LIB používat adresářové rozhraní. Pravděpodobně budete chtít nastavit veřejné oprávnění k seznamu oprávnění QPWFSERVER na hodnotu *EXCLUDE. Uvědomte si, že oprávnění k seznamu oprávnění otevírá a zavírá dveře ke všem knihovnám v rámci systému souborů QSYS.LIB, včetně uživatelských knihoven. Pokud narazíte na uživatele, kteří mají námitky proti tomuto vyloučení, můžete individuálně zhodnotit jejich požadavky. Je-li to vhodné, můžete poskytnout oprávnění k seznamu oprávnění explicitně jednotlivým uživatelům. Musíte se však přesvědčit, že má uživatel odpovídající oprávnění k objektům v systému souborů QSYS.LIB. Jinak by mohl uživatel neúmyslně vymazat objekty nebo i celé knihovny.

Poznámky:

1. Když obdržíte váš systém, je veřejné oprávnění k seznamu oprávnění QPWFSERVER nastaveno na hodnotu *USE.
2. Pokud explicitně poskytnete oprávnění určitému uživateli, řídí seznam oprávnění přístup pouze pomocí souborových služeb iSeries, souborových služeb NetServer a souborových služeb mezi servery iSeries. To nezabrání přístupu k některým adresářům přes FTP, ODBC a jiné sítě.

Zabezpečení adresářů

Za účelem přístupu k objektu v rámci systému souborů root je třeba přečíst postupně celou cestu k danému objektu. Chcete-li adresář prohledat, musíte k němu mít oprávnění *X (*OBJOPR a *EXECUTE). Předpokládejme například, že chcete získat přístup k následujícímu objektu:

```
/companya/customers/custfile.dat
```

Musíte mít oprávnění *X k adresáři companya a adresáři customers.

Pomocí systému souborů root můžete vytvořit symbolický odkaz na objekt. Z hlediska pojmů znamená symbolický odkaz alias pro jméno cesty. Obvykle je kratší a snáze zapamatovatelný než plné jméno cesty. Symbolický odkaz však nevytváří jinou fyzickou cestu k objektu. Uživatel nadále potřebuje oprávnění *X ke každému adresáři a podadresáři ve fyzické cestě k objektu.

Pro objekty v systému souborů root můžete použít zabezpečení adresářů tak, jako byste použili zabezpečení knihoven v systému souborů QSYS.LIB. Například můžete nastavit veřejné oprávnění k adresáři na hodnotu *EXCLUDE, abyste znemožnili obecným uživatelům přístup ke všem objektům v daném stromu.

Zabezpečení pro nové objekty

Když v systému souborů root vytvoříte nový objekt, rozhraní, které použijete k jeho vytvoření, určí jeho oprávnění. Pokud například použijete příkaz CRTDIR a jeho předvolené hodnoty, převezme nový adresář všechny charakteristiky oprávnění nadřízeného adresáře, včetně soukromých oprávnění, oprávnění primární skupiny a přiřazení seznamu oprávnění. Následující části popisují, jak se v jednotlivých typech rozhraní určují oprávnění.

Oprávnění pocházejí od nejbližšího nadřízeného adresáře, nikoliv od adresářů, které jsou ve stromu ještě výše. Jako administrátor systému proto musíte nahlížet na oprávnění, které přiřadíte adresářům v hierarchii, ze dvou hledisek:

- Jak oprávnění ovlivňuje přístup k objektům ve stromu (jako např. oprávnění ke knihovně).
- Jak oprávnění ovlivňuje nově vytvořené objekty (např. hodnota CRTAUT pro knihovny).

Doporučení: Možná budete chtít uživatelům, kteří pracují v integrovaném systému souborů, přidělit domovský adresář (např. /home/usrxxx), a pak nastavit odpovídající oprávnění (např. PUBLIC *EXCLUDE). Jakékoliv adresáře, které uživatel vytvoří pod svým domovským adresářem, pak převezmou tato oprávnění.

Dále uvádíme popisy způsobu přebírání oprávnění pro různá rozhraní:

Použití příkazu Vytvoření adresáře

Když vytváříte nový podadresář pomocí příkazu CRTDIR, máte dvě možnosti, jak určit oprávnění:

- Můžete zadat veřejné oprávnění (oprávnění k datům, oprávnění k objektu nebo obojí).
- Můžete zadat hodnotu *INDIR pro oprávnění k datům, oprávnění k objektu nebo pro obojí. Když zadáte hodnotu *INDIR jak pro oprávnění k datům, tak pro oprávnění k objektu, vytvoří systém přesnou kopii všech informací o oprávněních z nadřízeného adresáře na nový objekt, včetně seznamu oprávnění, oprávnění primární skupiny, veřejného oprávnění i soukromých oprávnění. (Systém nezkopíruje soukromé oprávnění, které má k objektu profil QSYS nebo QSECOFR.)

Vytvoření adresáře pomocí rozhraní API

Když vytváříte adresář pomocí rozhraní mkdir() API, zadáváte oprávnění k datům pro vlastníka, primární skupinu a obecné uživatele (s využitím mapy oprávnění *R, *W a *X). K nastavení oprávnění k objektům pro vlastníka, primární skupinu a obecné uživatele systém používá informace z nadřízeného adresáře.

Jelikož operační systémy typu UNIX nepoužívají koncepci oprávnění k objektům, nepodporuje rozhraní mkdir() API zadávání oprávnění k objektu. Jestliže chcete odlišná oprávnění k objektům, můžete použít příkaz serveru iSeries (CHGAUT). Když však nějaká oprávnění k objektům odstraníte, nemusí aplikace typu UNIX fungovat tak, jak byste očekávali.

Vytvoření proudového souboru pomocí rozhraní open() nebo creat() API

Když k vytvoření proudového souboru používáte rozhraní creat() API, můžete zadat oprávnění k datům pro vlastníka, primární skupinu a obecné uživatele (s využitím oprávnění typu UNIX *R, *W a *X). K nastavení oprávnění k objektům pro vlastníka, primární skupinu a obecné uživatele systém používá informace z nadřízeného adresáře.

Tato oprávnění můžete také uvést, když používáte rozhraní open() API k vytvoření proudového souboru. Při použití open() API můžete zadat, že má objekt všechna oprávnění převzít od nadřízeného adresáře. To se nazývá režim dědění. Když zadáte režim dědění, vytvoří systém úplnou shodu s oprávněními nadřízeného objektu, včetně seznamu oprávnění, oprávnění primární skupiny, veřejného oprávnění a soukromých oprávnění. Tato volba funguje stejně, jako když zadáte hodnotu *INDIR v příkazu CRTDIR.

Vytvoření objektu pomocí rozhraní PC

Když k vytvoření objektu v systému souborů root použijete PC aplikaci, převezme systém automaticky veškerá oprávnění od nadřízeného adresáře. To zahrnuje seznam oprávnění, oprávnění primární skupiny, veřejné oprávnění a soukromá oprávnění. PC aplikace nemají žádný ekvivalent pro zadávání oprávnění při vytváření objektu.

Systém souborů QFileSvr.400

S využitím systému souborů QFileSvr.400 může uživatel (USERX) v jednom systému iSeries (SYSTEMA) mít přístup k datům v jiném připojeném systému iSeries (SYSTEMB). USERX má rozhraní, které je stejné jako rozhraní Client Access. Vzdálený server iSeries (SYSTEMB) se jeví jako adresář se všemi svými systémy souborů jako podadresáři.

Když se uživatel USERX pokusí pomocí tohoto rozhraní o přístup do systému SYSTEMB, odešle systém SYSTEMA jméno uživatelského profilu USERX a zašifrované heslo do systému SYSTEMB. V systému SYSTEMB musí existovat stejný uživatelský profil a heslo, jinak systém SYSTEMB požadavek zamítne.

Pokud systém SYSTEMB požadavek akceptuje, jeví se uživatel USERX vůči systému SYSTEMB jako kterýkoliv jiný uživatel Client Access. Na všechny akce, o které se USERX pokusí, se vztahují stejná pravidla kontroly oprávnění.

Jako administrátor systému si musíte být vědomi toho, že systém souborů QFileSvr.400 představuje další možná dvířka do vašeho systému. Nesmíte předpokládat, že jste omezili vzdálené uživatele na interaktivní přihlášení pomocí přímého průchodu (passthrough) na obrazovkovou stanici. Pokud máte spuštěn podsystém QSERVER a váš systém je připojen k jinému systému iSeries, mohou vzdálení uživatelé přistupovat k vašemu systému, jako by byli na svém lokálním PC s produktem Client Access. Je více než pravděpodobné, že váš

systém bude navazovat spojení, která budou vyžadovat spuštění podsystému QSERVER. To je jen další důvod, proč je pro vás stěžejní mít dobré schéma oprávnění k objektům.

Síťový systém souborů

Síťový systém souborů, neboli NFS (Network File System), umožňuje přístup k systémům, které mají implementace NFS. NFS je odvětvový standard pro sdílení informací mezi uživateli v systémech propojených sítí. Většina základních operačních systémů (včetně operačních systémů PC) poskytuje NFS. U systémů UNIX představuje NFS primární metodu přístupu k datům. Servery iSeries mohou vystupovat jako klient NFS i jako server NFS.

Pokud jste administrátor systému iSeries, který vystupuje jako server NFS, měli byste rozumět bezpečnostním aspektům NFS a umět je řídit. Níže jsou uvedeny určité návrhy a pokyny:

- Funkci serveru NFS musíte explicitně spustit pomocí příkazu STRNFSSVR. Sledujte, kdo má oprávnění k tomuto příkazu.
- Adresář nebo objekt zpřístupníte klientům NFS tím, že jej vyexportujete. Díky tomu máte velmi specifickou kontrolu nad tím, které části vašeho systému zpřístupníte klientům NFS v síti.
- Při exportu můžete zadat, kteří klienti mají přístup k objektům. Klienta určíte jménem systému nebo IP adresou. Klientem může být jednotlivý PC nebo celý server iSeries nebo systém UNIX. V terminologii NFS se klient (IP adresa) nazývá počítač.
- Při exportu můžete pro každý počítač, který má přístup k exportovanému adresáři nebo objektu, zadat přístup pouze pro čtení nebo čtení/zápis. Ve většině případů budete pravděpodobně chtít poskytnout přístup pouze pro čtení.
- NFS neposkytuje ochranu hesla. Je navržen a určen pro sdílení dat v rámci důvěryhodné komunity systémů. Když uživatel požádá o přístup, obdrží server jeho uid. Níže jsou uvedeny některé pokyny týkající se uid:
  - Server iSeries se snaží najít uživatelský profil se stejným uid. Pokud najde odpovídající uid, použije pověření daného uživatelského profilu. Pověření je termín NFS, který popisuje použití oprávnění uživatele. Je to obdoba výměny profilu v jiných aplikacích serveru iSeries.
  - Při exportu adresáře nebo objektu můžete uvést, zda umožníte přístup pro profil s kořenovým oprávněním. Server NFS na serverech iSeries považuje kořenové oprávnění za totožné se zvláštním oprávnění *ALLOBJ. Pokud zadáte, že nepovolíte kořenové oprávnění, nebude uživatel NFS s uid, který se mapuje na uživatelský profil se zvláštním oprávněním *ALLOBJ, mít přístup k objektu pod daným profilem. Jestliže místo toho bude povolen anonymní přístup, bude žadatel mapován na anonymní profil.
  - Při exportu adresáře nebo objektu můžete uvést, zda umožníte anonymní požadavky. Anonymní požadavek je požadavek s uid, který se neshoduje s žádným uid ve vašem systému. Pokud anonymní požadavky umožníte, bude systém mapovat anonymního uživatele na uživatelský profil QNFSANON dodávaný IBM. Tento uživatelský profil nemá žádná zvláštní ani explicitní oprávnění. (Chcete-li, můžete při exportu uvést pro anonymní požadavky jiný uživatelský profil.)
- Když je váš server iSeries zapojen v síti NFS (nebo nějaké jiné síti se systémy UNIX, které závisejí na uid), budete pravděpodobně muset sami spravovat vlastní uid a nebudete využívat toho, že je systém automaticky přiřadí. Budete muset zkoordinovat uid s ostatními systémy v síti.

  Možná zjistíte, že musíte uid změnit (i pro uživatelské profily dodávané IBM) tak, aby byly kompatibilní s ostatními systémy ve vaší síti. Pro snazší změnu uid uživatelského profilu je k dispozici program. (Když měníte uid pro uživatelský profil, musíte změnit také uid pro všechny objekty, které profil vlastní, jak v kořenovém adresáři, tak v adresáři

QOpenSrv.) Program QSYCHGID automaticky mění uid pro uživatelský profil i pro všechny vlastněné objekty. Informace o použití tohoto programu najdete v publikaci *iSeries System API Reference*.

Kapitola 12. Zabezpečení komunikace APPC

Je-li váš systém zapojen do sítě s jinými systémy, vzniká tak nová množina dveří do vašeho systému. Jako administrátor systému byste si měli být vědomi možností, které můžete použít k řízení vstupu do vašeho systému v prostředí APPC.

Protokol APPC (Advanced program-to-program communications) přestavuje způsob, kterým počítače (včetně osobních počítačů) mezi sebou komunikují. Komunikaci APPC může využívat přímý průchod (passthrough) na obrazovkovou stanici, distribuovaný systém řízení dat (DDM) i produkt iSeries Access for Windows.

V následujících částech najdete základní informace o tom, jak komunikace APPC funguje a jak můžete nastavit odpovídající zabezpečení. Tato témata jsou zaměřena především na prvky konfigurace APPC, které souvisejí se zabezpečením. Pokud budete chtít uvedený příklad přizpůsobit pro vaši situaci, budete muset spolupracovat s lidmi, kteří mají na starosti vaši komunikační síť, a možná i s dodavateli aplikací. Tyto informace použijte jako podklad, který vám pomůže pochopit problematiku zabezpečení a možnosti, které se nabízejí pro APPC.

Zabezpečení není nikdy “zadarmo”. Některé návrhy, které mají usnadnit zabezpečení sítě, mohou vést ke složitější administraci sítě. V těchto informacích například nezdůrazňujeme protokol APPN (Advanced Peer-to-Peer Networking), neboť zabezpečení je snazší pochopit i spravovat bez protokolu APPN. Bez protokolu APPN však musí správce sítě ručně vytvořit informace o konfiguraci, které by APPN vytvořil automaticky.

PC také používají komunikace

Řada metod pro připojení PC k vašim serverům iSeries závisí na komunikacích, jako např. APPC nebo TCP/IP. Když budete pročítat následující části, berte v úvahu otázky zabezpečení připojení jak k jiným systémům, tak k PC. Při plánování ochrany sítě musíte mít jistotu, že nebudou negativně ovlivněny PC připojené k vašemu systému.

Terminologie APPC

APPC umožňuje uživateli v jednom systému provádět práci v jiném systému. Systém, ze kterého vzešel požadavek, se označuje jedním z následujících výrazů:

- **zdrojový systém**
- **lokální systém**
- **klient**

Systém, který požadavek přijímá, se označuje jedním z následujících výrazů:

- **cílový systém**
- **vzdálený systém**
- **server**

Základní prvky komunikace APPC

Z hlediska administrátora systému je třeba zajistit následující podmínky, aby mohl uživatel v jednom systému (SYSTEMA) smysluplně pracovat v jiném systému (SYSTEMB):

- Zdrojový systém (SYSTEMA) musí poskytovat cestu k cílovému systému (SYSTEMB). Tato cesta se nazývá **relace APPC**.

- Cílový systém musí identifikovat uživatele a přiřadit mu uživatelský profil. Cílový systém musí podporovat šifrovací algoritmus zdrojového systému (další informace viz část “Úrovně hesla” na stránce 16).
- Cílový systém musí pro uživatele spustit úlohu s odpovídajícím prostředím (hodnoty funkce Work management).

V následujících částech jsou rozebrány tyto prvky a jejich vztah k zabezpečení. Administrátor cílového systému má hlavní odpovědnost za to, že uživatelé APPC nenaruší zabezpečení. Pokud však administrátoři obou systémů spolupracují, je správa zabezpečení APPC daleko snazší.

Příklad: základní relace APPC

Když v prostředí APPC nějaký uživatel nebo aplikace v jednom systému zadá požadavek na přístup do jiného systému, navážou tyto dva systémy relaci. K navázání relace musí systémy spojit dva odpovídající popisy zařízení APPC. Parametr RMTLOCNAME (jméno vzdáleného systému) v popisu zařízení SYSTEMA musí odpovídat parametru LCLLOCNAME (jméno lokálního systému) v popisu zařízení SYSTEMB, a naopak.

Aby dva systémy navázaly relaci APPC, musí být hesla systémů v popisech zařízení APPC v systému SYSTEMA i SYSTEMB totožné. Oba musí uvádět hodnotu *NONE nebo musí oba obsahovat stejnou hodnotu.

Pokud mají hesla jinou hodnotu než *NONE, jsou uložena a přenášena v zašifrovaném formátu. Jestliže si hesla odpovídají, systémy navážou relaci. Nejsou-li hesla stejná, je požadavek uživatele zamítnut. Když systémy za účelem navázání relace specifikují hesla, nazývá se to **zabezpečené spojení**.

Poznámka: Funkce zabezpečeného spojení není podporována všemi počítačovými systémy.

Omezení relací APPC

Jako administrátor zdrojového systému můžete pomocí oprávnění k objektu řídit, kdo se může pokoušet o přístup k jiným systémům. Veřejné oprávnění pro popis zařízení APPC nastavte na hodnotu *EXCLUDE a určitým uživatelům poskytněte oprávnění *CHANGE. Chcete-li zabránit uživatelům se zvláštním oprávněním *ALLOBJ, aby používali komunikaci APPC, použijte systémovou hodnotu QLMTSECOFR.

Jako administrátor cílového systému můžete rovněž pomocí oprávnění k zařízení APPC zabránit uživatelům, aby spouštěli relaci APPC ve vašem systému. Je však nutné, abyste věděli, které uživatelské ID se bude pokoušet o přístup k popisu zařízení APPC. Část “Přístup uživatelů APPC k cílovému systému” na stránce 101 popisuje, jak servery iSeries asociují uživatelské ID s požadavkem na relaci APPC.

Poznámka: Můžete použít příkaz PRTPUBAUT (Tisk veřejně oprávněných objektů) a příkaz PRTPVTAUT *DEVD (Tisk soukromých oprávnění) ke zjištění, kdo má oprávnění k popisům zařízení ve vašem systému.

Když váš systém používá APPN, automaticky vytvoří nové zařízení APPC, pokud není pro přenosovou cestu, kterou systém zvolil, k dispozici žádné existující zařízení. Jednou metodou omezení přístupu k zařízením APPC v systému, který používá APPN, je vytvořit seznam oprávnění. Seznam oprávnění obsahuje seznam uživatelů, kteří by měli být oprávněni k zařízení APPC. Chcete-li změnit příkaz CRTDEVAPPC, použijte příkaz CHGCMDDFT (Změna předvolby příkazu). Pro parametr AUT (oprávnění) v příkazu CRTDEVAPPC nastavte předvolenou hodnotu k seznamu oprávnění, který jste vytvořili.

Poznámka: Pokud má váš systém jiný jazyk než angličtinu, musíte změnit předvolbu příkazu v knihovně QSYSxxxx pro každý národní jazyk v systému.

Parametr LOCPWD (heslo umístění) v popisu zařízení slouží k ověření identity jiného systému, který žádá o relaci ve vašem systému (jménem uživatele nebo aplikace). Heslo umístění vám může pomoci odhalit pirátský systém.

Když používáte hesla umístění, musíte se zkoordinovat s administrátory ostatních systémů v síti. Také musíte řídit, kdo může vytvářet nebo měnit popisy zařízení APPC a konfigurační seznamy. Systém vyžaduje zvláštní oprávnění *IOSYSCFG k použití příkazů, které pracují se zařízeními a konfiguračními seznamy APPC.

Poznámka: Když používáte APPN, jsou hesla umístění uložena v konfiguračním seznamu QAPPNRMT namísto v popisech zařízení.

Přístup uživatelů APPC k cílovému systému

Když systémy navazují relaci APPC, vytvářejí cestu pro žádajícího uživatele, aby se dostal k bráně cílového systému. Ještě několik dalších prvků určuje, co musí uživatel provést, aby získal přístup do jiného systému.

Následující části popisují prvky, které určují, jak uživatel APPC získá přístup k cílovému systému.

Systémové metody pro posílání informací o uživateli

Architektura APPC poskytuje tři metody pro posílání zabezpečovacích informací o uživateli ze zdrojového systému do cílového systému. Tyto metody jsou označovány jako **hodnoty zabezpečení architektury**. Tabulka 18 uvádí uvedené metody:

Poznámka: Další informace o hodnotách zabezpečení architektury obsahuje publikace *APPC Programming*.

Tabulka 18. Hodnoty zabezpečení v architektuře

Hodnoty zabezpečení architektury	Uživatelské ID posíláno do cílového systému	Heslo posíláno do cílového systému
None	Ne	Ne
Same	Ano[1]	Viz pozn. 2.
Program	Ano	Ano[3]

Poznámky:

1. Zdrojový systém posílá uživatelské ID, pokud cílový systém specifikuje SECURELOC(*YES) nebo SECURELOC(*VFYENCPWD).
2. Uživatel nezadává heslo při požadavku, neboť heslo je už ověřeno zdrojovým systémem. Při hodnotách SECURELOC(*YES) a SECURELOC(*NO) zdrojový systém heslo neposílá. Při hodnotě SECURELOC(*VFYENCPWD) zdrojový systém načte uložené zašifrované heslo a pošle ho (v zašifrované formě).
3. Systém posílá heslo v zašifrované formě, pokud zdrojový i cílový systém podporuje šifrování hesla. Jinak není heslo zašifrováno.

Aplikace, kterou uživatel požaduje, určuje hodnotu zabezpečení architektury. Například SNADS vždy používá hodnotu SECURITY(NONE). DDM používá hodnotu SECURITY(SAME). Při přímém průchodu na obrazovkovou stanici uživatel specifikuje hodnotu zabezpečení pomocí parametrů v příkazu STRPASTHR.

Ve všech případech se cílový systém rozhoduje, zda akceptuje požadavek s hodnotou zabezpečení, která byla zadána ve zdrojovém systému. V některých situacích může cílový systém požadavek zcela zamítnout. V jiných situacích cílový systém může vynutit jinou hodnotu zabezpečení. Když například uživatel specifikuje v příkazu STRPASTHR jak uživatelské ID, tak heslo, požadavek použije hodnotu SECURITY(PGM). Pokud má však systémová hodnota QRMTSIGN v cílovém systému hodnotu *FRCSIGNON, bude se uživateli nadále zobrazovat přihlašovací obrazovka. Při nastavení hodnoty *FRCSIGNON systémy vždy používají hodnotu SECURITY(NONE), což je ekvivalent uživatele, který v příkazu STRPASTHR nezadává žádné uživatelské ID ani heslo.

Poznámky:

1. Zdrojový i cílový systém vyjednávají o hodnotě zabezpečení, než jsou data odeslána. V situaci, kdy cílový systém specifikuje hodnotu SECURELOC(*NO) a požadavek je SECURITY(SAME), sdělí cílový systém zdrojovému systému, aby použil SECURITY(NONE). Zdrojový systém neposílá uživatelské ID.
2. Cílový systém zamítne požadavek na relaci, když skončila platnost hesla uživatele v cílovém systému. To platí pouze pro požadavky na spojení, které posílají heslo, včetně těchto:
   - Požadavky na relaci typu SECURITY(PROGRAM).
   - Požadavky na relaci typu SECURITY(SAME), když má SECURELOC hodnotu *VFYENCPWD.

Možnosti rozdělení odpovědnosti za zabezpečení sítě

Když je váš systém zapojen v síti, musíte se rozhodnout, zda budete důvěřovat jiným systémům, že ověří identitu uživatele, který se pokouší vstoupit do vašeho systému. Budete důvěřovat systému SYSTEMA, že se ujistí, že uživatel USERA je skutečně USERA (nebo QSECOFR je skutečně QSECOFR)? Nebo budete požadovat, aby uživatel znovu poskytl uživatelské ID i heslo?

Parametr SECURELOC (zabezpečení umístění) v popisu zařízení APPC v cílovém systému určuje, zda je zdrojový systém zabezpečeným (důvěryhodným) umístěním.

Pokud oba systémy provozují vydání, které podporuje hodnotu *VFYENCPWD, poskytuje hodnota SECURELOC(*VFYENCPWD) další ochranu, když aplikace používají SECURITY(SAME). Ačkoliv žadatel nezadá heslo v požadavku, načte zdrojový systém heslo uživatele a odešle ho s požadavkem. Aby byl požadavek úspěšný, musí mít uživatel v obou systémech stejné uživatelské ID i heslo.

Když cílový systém specifikuje hodnotu SECURELOC(*VFYENCPWD) a zdrojový systém tuto hodnotu nepodporuje, zpracuje cílový systém požadavek jako SECURITY(NONE).

Tabulka 19 ukazuje, jak spolu fungují hodnota zabezpečení architektury a hodnota SECURELOC:

Tabulka 19. Jak spolu fungují hodnota zabezpečení architektury a hodnota SECURELOC

Zdrojový systém	**Cílový systém**	
Hodnoty zabezpečení architektury	**Hodnota SECURELOC**	**Uživatelský profil pro úlohu**
None	Libovolná	Předvolený uživatel[1].

Tabulka 19. Jak spolu fungují hodnota zabezpečení architektury a hodnota SECURELOC (pokračování)

Zdrojový systém	Cílový systém	
Hodnoty zabezpečení architektury	**Hodnota SECURELOC**	**Uživatelský profil pro úlohu**
Same	*NO	Předvolený uživatel[1].
	*YES	Stejné jméno uživatelského profilu jako žadatel ze zdrojového systému.
	*VFYENCPWD	Stejné jméno uživatelského profilu jako žadatel ze zdrojového systému. Uživatel musí mít v obou systémech stejné heslo.
Program	Libovolná	Uživatelský profil uvedený v požadavku ze zdrojového systému.

Poznámky:

1. Předvolený uživatel je určen záznamem komunikací v popisu podsystému. Viz část "Přiřazení uživatelských profilů pro úlohy prováděné cílovým systémem".

Přiřazení uživatelských profilů pro úlohy prováděné cílovým systémem

Když uživatel požaduje úlohu APPC v jiném systému, je požadavku přiřazeno jméno režimu. Jméno režimu může pocházet z požadavku uživatele nebo to může být předvolená hodnota z atributů sítí zdrojového systému.

Cílový systém používá jméno režimu a jméno zařízení APPC k určení toho, jak se má spustit daná úloha. Cílový systém prohledá aktivní podsystémy, zda neobsahují záznam komunikací, který nejlépe odpovídá jménu zařízení APPC a jménu režimu.

Záznam komunikací uvádí, jaký uživatelský profil systém používá pro požadavky SECURITY(NONE). Dále je uveden příklad záznamu komunikací v popisu podsystému:

```
                      Display Communications Entries

Subsystem description:   QCMN           Status:   ACTIVE

                          Job                            Default         Max
Device       Mode        Description    Library         User          Active
*ALL         *ANY        *USRPRF                        *SYS          *NOMAX
*ALL         QPCSUPP     *USRPRF                        *NONE         *NOMAX
```

Tabulka 20 uvádí možné hodnoty pro parametr předvoleného uživatele v záznamu komunikací:

Tabulka 20. Možné hodnoty pro parametr předvoleného uživatele

Hodnota	Výsledek
***NONE**	Není k dispozici žádný předvolený uživatel. Pokud zdrojový systém nedodá v požadavku uživatelské ID, úloha se nespustí.
***SYS**	Spustí se pouze programy dodané IBM (systémové úlohy). Nespustí se žádná uživatelská aplikace.
jméno-uživatele	Pokud zdrojový systém neodešle uživatelské ID, spustí se úloha po tímto uživatelským profilem.

Příkaz PRTSBSDAUT (Tisk popisu podsystému) můžete použít k vytištění seznamu všech podsystémů, které mají záznamy komunikací s předvoleným uživatelským profilem.

Volby přímého průchodu na obrazovkovou stanici

Přímý průchod (passthrough) na obrazovkovou stanici je příkladem aplikace, která používá komunikaci APPC. Přímý průchod na obrazovkovou stanici můžete použít k přihlášení do jiného systému, který je k vašemu systému připojen prostřednictvím sítě.

Tabulka 21 obsahuje příklady požadavků na přímý průchod (příkaz STRPASTHR) a způsob jejich zpracování cílovým systémem. Pro přímý průchod na obrazovkovou stanici systém používá základní prvky komunikace APPC a systémovou hodnotu QRMTSIGN (vzdálené přihlášení).

Poznámka: Požadavky na přímý průchod na obrazovkovou stanici již nejsou nadále směrovány prostřednictvím podsystémů QCMN či QBASE. Počínaje verzí V4R1 jsou požadavky směrovány prostřednictvím podsystému QSYSWRK. Před verzí V4R1 jste mohli předpokládat, že když nebudete mít spuštěny podsystémy QCMD nebo QBASE, nebude přímý průchod na obrazovkovou stanici fungovat. To už neplatí. Můžete prosadit, aby přímý průchod na obrazovkovou stanici šel přes podsystém QCMN (nebo QBASE, je-li aktivní) tak, že změníte systémovou hodnotu QPASTHRSVR na hodnotu 0.

Tabulka 21. Ukázky požadavků na přihlášení přímým průchodem

Hodnoty v příkazu STRPASTHR		**Cílový systém**		
ID uživatele	**Heslo**	**Hodnota SECURELOC**	**Hodnota QRMTSIGN**	**Výsledek**
*NONE	*NONE	Libovolná	Libovolná	Uživatel se musí přihlásit do cílového systému.
Jméno uživatelského profilu	Nezadáno	Libovolná	Libovolná	Požadavek selže.
*CURRENT	Nezadáno	*NO	Libovolná	Požadavek selže.
		*YES	*SAMEPRF	Interaktivní úloha se spouští se stejným jménem uživatelského profilu, jako má uživatelský profil ve zdrojovém systému. Do vzdáleného systému se nepředává žádné heslo. Jméno uživatelského profilu musí existovat v cílovém systému.
			*VERIFY	
			*FRCSIGNON	Uživatel se musí přihlásit do cílového systému.
		*VFYENCPWD	*SAMEPRF	Interaktivní úloha se spouští se stejným jménem uživatelského profilu, jako má uživatelský profil ve zdrojovém systému. Zdrojový systém načte heslo uživatele a odešle ho do cílového systému. Jméno uživatelského profilu musí existovat v cílovém systému.
			*VERIFY	
			*FRCSIGNON	Uživatel se musí přihlásit do cílového systému.

Tabulka 21. Ukázky požadavků na přihlášení přímým průchodem (pokračování)

Hodnoty v příkazu STRPASTHR		**Cílový systém**		
ID uživatele	**Heslo**	**Hodnota SECURELOC**	**Hodnota QRMTSIGN**	**Výsledek**
*CURRENT (nebo jméno aktuálního uživatelského profilu pro úlohu)	Zadáno	Libovolná	*SAMEPRF	Interaktivní úloha se spouští se stejným jménem uživatelského profilu, jako má uživatelský profil ve zdrojovém systému. Heslo *je* odesláno do vzdáleného systému. Jméno uživatelského profilu musí existovat v cílovém systému.
			*VERIFY	
			*FRCSIGNON	Uživatel se musí přihlásit do cílového systému.
Jméno uživatelského profilu (jméno odlišné od aktuálního uživatelského profilu pro úlohu)	Zadáno	Libovolná	*SAMEPRF	Požadavek selže.
			*VERIFY	Interaktivní úloha se spouští se stejným jménem uživatelského profilu, jako má uživatelský profil ve zdrojovém systému. Heslo *je* odesláno do vzdáleného systému. Jméno uživatelského profilu musí existovat v cílovém systému.
			*FRCSIGNON	Interaktivní úloha se spustí se zadaným jménem uživatelského profilu. Heslo se pošle do cílového systému. Jméno uživatelského profilu musí existovat v cílovém systému.

Jak se vyvarovat neočekávaných přiřazení zařízení

Když na aktivním zařízení dojde k selhání, systém se pokusí provést nápravu. V některých případech, když je přerušeno spojení, může jiný uživatel nechtěně znovu navázat relaci, která selhala. Například předpokládejme, že uživatel USERA vypnul pracovní stanici, aniž by se odhlásil. Uživatel USERB by mohl zapnout pracovní stanici a znovu bez přihlášení spustit relaci uživatele USERA.

Abyste tomuto zabránili, nastavte systémovou hodnotu QDEVRCYACN (akce při I/O chybě zařízení) na hodnotu *DSCMSG. Když zařízení selže, systém ukončí úlohu uživatele.

Řízení vzdálených příkazů a dávkových úloh

Existuje několik voleb, které vám pomohou řídit, jaké vzdálené příkazy a úlohy je možné provádět ve vašem systému:

- Pokud váš systém používá DDM, můžete omezit přístup k souborům DDM, abyste uživatelům zabránili používat příkaz SBMRMTCMD (Spuštění vzdáleného příkazu) z jiného systému. Aby mohl uživatel příkaz SBMRMTCMD použít, musí být schopen otevřít soubor DDM. Také musíte omezit schopnost vytvářet soubory DDM.
- Můžete zadat ukončovací program pro systémovou hodnotu DDMACC (přístup k požadavku DDM). V daném ukončovacím programu můžete zhodnotit všechny požadavky DDM dříve, než je povolíte.

- Můžete použít atribut sítě JOBACN (akce úlohy sítě), abyste zabránili spouštění síťových úloh nebo jejich automatickému spouštění.
- Můžete explicitně zadat, které programové požadavky mohou být zadávány ve vašem komunikačním prostředí, a to tak, že odstraníte záznam směrování PGMEVOKE z popisů podsystémů. Záznam směrování PGMEVOKE umožňuje žadateli specifikovat program, který je spuštěný. Když tento záznam směrování odstraníte z popisů podsystémů, např. z popisu podsystému QCMN, musíte přidat záznamy směrování pro požadavky na komunikaci, které musí proběhnout úspěšně.

  Část "Požadavky na jména TPN architektury" na stránce 82 obsahuje seznam jmen programů pro požadavky na komunikaci zadané aplikacemi dodanými IBM. Pro každý požadavek, který chcete povolit, můžete přidat záznam směrování obsahující porovnávací hodnotu i jméno programu, které se shodují se jménem programu.

  Když budete používat tuto metodu, musíte znát prostředí řízení práce (Work management) ve vašem systému a typy požadavků na komunikaci, které se ve vašem systému vyskytují. Je-li to možné, měli byste po změně záznamů směrování otestovat všechny typy požadavků na komunikaci, abyste měli jistotu, že fungují správně. Když požadavek na komunikaci nenalezne dostupný záznam směrování, dostanete zprávu CPF1269. Jinou alternativou (odolnější vůči chybám, ale možná trochu méně efektivní) je nastavit veřejné oprávnění pro transakční programy, které nechcete spouštět ve vašem systému, na hodnotu *EXCLUDE.

  Poznámka: Další informace o záznamech směrování a o způsobu zpracování požadavků na spuštění programu systémem uvádí publikace *Work Management*.

Ohodnocení vaší konfigurace APPC

Chcete-li vytisknout hodnoty konfigurace APPC týkající se zabezpečení, můžete použít příkaz PRTCMNSEC (Tisk zabezpečení komunikací) nebo volby menu. Následující části popisují informace uvedené v sestavách.

Důležité parametry pro zařízení APPC

Obrázek 9 je příkladem sestavy informací o komunikacích pro popisy zařízení. Obrázek 10 na stránce 107 je příkladem sestavy pro konfigurační seznamy. Po sestavách následující vysvětlení polí uvedených v sestavách.

```
                        Communications Information (Full Report)
                                                                                SYSTEM4
Object type  . . . . . . . . . :   *DEVD

                                                                                    Pre           SNUF
Object        Object        Device         Secure     Location     APPN      Single     Establish     Program
Name          Type          Category       Location   Password     Capable   Session     Session       Start

CDMDEV1       *DEVD         *APPC           *NO         *NO         *NO       *YES        *NO
CDMDEV2       *DEVD         *APPC           *NO         *NO         *NO       *YES        *NO
```

Obrázek 9. Popis zařízení APPC - ukázková sestava

```
                  Display Configuration List                      Page     1
                              SYSTEM4  12/17/95  07:24:36
Configuration list . . . . . . . . . :   QAPPNRMT
Configuration list type  . . . . . :   *APPNRMT
Text . . . . . . . . . . . . . . . . :
-----------------APPN Remote Locations------------------
          Remote              Remote    Control
Remote    Network   Local     Control   Point     Secure
Location  ID        Location  Point     Net ID     Loc
SYSTEM36  APPN      SYSTEM4   SYSTEM36  APPN       *NO
SYSTEM32  APPN      SYSTEM4   SYSTEM32  APPN       *NO
SYSTEMU   APPN      SYSTEM4   SYSTEM33  APPN       *YES
SYSTEMJ   APPN      SYSTEM4   SYSTEMJ   APPN       *NO
SYSTEMR2  APPN      SYSTEM4   SYSTEM1   APPN       *NO
--------------------------APPN Remote Locations---------------------------
          Remote                                          Local      Pre-
Remote    Network   Local     Single     Number of      Control  established
Location  ID        Location  Session  Conversations     Point     Session
SYSTEM36  APPN      SYSTEM4    *NO             10        *NO        *NO
SYSTEM32  APPN      SYSTEM4    *NO             10        *NO        *NO
```

Obrázek 10. Sestava konfiguračního seznamu - příklad

Pole Secure location

Pole Secure location (SECURELOC) určuje, zda lokální systém věří vzdálenému systému v tom směru, že za něj vzdálený systém provede ověření platnosti hesla. Pole SECURELOC se vztahuje pouze na aplikace, které používají hodnotu SECURITY(SAME), jako např. DDM, a aplikace, které používají rozhraní CPI-Communications API.

Hodnota SECURELOC(*YES) činí lokální systém zranitelným vůči případným slabostem ve vzdáleném systému. Jakýkoliv uživatel, který existuje v obou systémech, může volat programy v lokálním systému. To je zvláště nebezpečné, neboť uživatelský profil QSECOFR (správce systému) existuje v obou systémech iSeries a má zvláštní oprávnění *ALLOBJ. Pokud systém v síti nechrání dobře heslo QSECOFR, jsou ostatní systémy, které s daným systémem jednají jako se zabezpečeným místem, v nebezpečí.

Když používáte hodnotu SECURELOC(*VFYENCPWD), je váš systém odolnější vůči jiným systémům, které nechrání hesla odpovídajícím způsobem. Uživatel, který požaduje aplikaci, která používá hodnotu SECURITY(SAME), musí mít v obou systémech stejné uživatelské ID i heslo. Hodnota SECURELOC(*VFYENCPWD) vyžaduje jednotnou strategii správy hesel v rámci sítě, aby uživatelé měli stejné heslo ve všech systémech.

Poznámka: Hodnota SECURELOC(*VFYENCPWD) je podporována pouze mezi systémy s verzí V3R2, V3R7 nebo V4R1. Pokud cílový systém uvádí hodnotu SECURELOC(*VFYENCPWD) a zdrojový systém nepodporuje tuto funkci, je požadavek zpracován jako SECURITY(NONE).

Jestliže systém uvádí hodnotu SECURELOC(*NO), budou aplikace, které používají hodnotu SECURITY(SAME), vyžadovat, aby programy spouštěl předvolený uživatel. Předvolený uživatel závisí jak na popisu zařízení, tak na režimu, které jsou asociovány s daným požadavkem. (Viz část “Přiřazení uživatelských profilů pro úlohy prováděné cílovým systémem” na stránce 103.)

Pole Location password

Pole Location password určuje, zda si dva systémy budou vyměňovat hesla, aby si ověřili, že žádající systém není pirátský. V části “Příklad: základní relace APPC” na stránce 100 najdete další informace o heslech umístění.

Pole APPN Capable

Pole APPN-capable (APPN) určuje, zda vzdálený systém může podporovat rozšířené funkce vytváření sítí nebo je omezen na spojení s jedním přechodem. Hodnota APPN(*YES) znamená toto:

- Pokud je vzdálený systém síťovým uzlem, může být schopný připojit lokální systém k jiným systémům. To se nazývá **směrování prostředního uzlu**. Znamená to, že uživatelé ve vašem systému mohou být schopni používat vzdálený systém jako přenosovou cestu do větší sítě.
- Pokud je lokální systém síťovým uzlem, může vzdálený systém používat lokální systém k připojení k jiným systémům. Uživatelé ve vzdáleném systému mohou být schopni používat váš systém jako přenosovou cestu do větší sítě.

Poznámka: Chcete-li zjistit, zda je systém síťovým uzlem či koncovým uzlem, použijte příkaz DSPNETA.

Pole Single session

Pole Single session (SNGSSN) určuje, zda vzdálený systém může v daný okamžik spouštět více než jednu relaci s využitím stejného popisu zařízení APPC. Běžně se používá hodnota SNGSSN(*NO), neboť eliminuje potřebu vytvářet více popisů zařízení pro vzdálený systém. Například uživatel PC často požaduje více než jednu relaci emulace 5250 a relace pro funkce souborového a tiskového serveru. Při hodnotě SNGSSN(*NO) můžete tuto funkci zajistit s jedním popisem zařízení pro daný PC v systému iSeries.

Hodnota SNGSSN(*NO) znamená, že musíte spoléhat na záměrné zabezpečovací procedury uživatelů PC a ostatních uživatelů APPC. Váš systém je zranitelný vůči někomu ve vzdáleném systému, kdo spustí neautorizovanou relaci, která používá stejný popis zařízení jako stávající relace. (Tato praktika se někdy označuje jako **útok typu ″piggy-backing″**.)

Pole Pre-establish session

Pole Pre-establish session (PREESTSSN) pro zařízení s jednou relací řídí, zda lokální systém spustí relaci se vzdáleným systémem, když vzdálený systém jako první kontaktuje lokální systém. Hodnota PREESTSSN(*NO) znamená, že lokální systém počká se spuštěním relace, dokud nějaká aplikace nezadá požadavek na relaci se systémem. Hodnota PREESTSSN(*YES) je užitečná z hlediska zkrácení doby, po kterou trvá aplikačnímu programu navázání spojení.

Hodnota PREESTSSN(*YES) brání systému odpojit komutovanou linku, která se už nepoužívá. Linku musí explicitně logicky vypnout aplikace nebo uživatel. Hodnota PREESTSSN(*YES) může vést k prodloužení doby, po kterou je lokální systém náchylný k útokům typu ″piggy-backing″ při relaci.

Pole SNUF Program start

Pole SNUF program start určuje, zda vzdálený systém může spouštět programy v lokálním systému. Hodnota *YES znamená, že schéma oprávnění k objektům v lokálním systému musí odpovídajícím způsobem chránit objekty, když uživatelé ve vzdáleném systému spustí úlohy a programy v lokálním systému.

Parametry pro řadiče APPC

Obrázek 11 na stránce 109 je příkladem sestavy informací o komunikacích pro popisy řadiče. Po sestavě následují vysvětlení polí uvedených v sestavě.

```
                          Communications Information (Full Report)
                                                                        SYSTEM4
Object type  . . . . . . . . . . :   *CTLD

Object    Object    Controller    Auto     Switched      Call       APPN       CP      Disconnect   Delete    Device
Name      Type      Category      Create   Controller    Direction  Capable    Sessions    Timer      Seconds   Name
CTL01     *CTLD     *APPC         *YES       *YES        *DIAL      *YES       *YES          0        1440    AARON
CTL02     *CTLD     *APPC         *YES       *YES        *DIAL      *YES       *YES          0        1440    BASIC
CTL03     *CTLD     *APPC         *YES       *YES        *DIAL      *YES       *YES          0        1440    *NONE
```

Obrázek 11. Popisy řadiče APPC - ukázková sestava

Pole Auto-create

V popisu linky specifikuje pole Auto-create (AUTOCRTCTL), zda lokální systém automaticky vytvoří popis řadiče, když příchozí požadavek nemůže nalézt odpovídající popis řadiče. V popisu řadiče uvádí pole Auto-create (AUTOCRTDEV), zda lokální systém automaticky vytvoří popis zařízení, když příchozí požadavek nemůže nalézt odpovídající popis zařízení.

Na řadiče podporující APPN nemá pole Auto-create žádný vliv. Systém automaticky vytvoří popisy zařízení vždy, když je to nutné, bez ohledu na nastavení pole Auto-create.

Když pro popis linky zadáte hodnotu *YES, může se kdokoliv s přístupem k lince připojit k vašemu systému. To zahrnuje počítače připojené přes komunikační můstky a směrovače.

Pole Control point sessions

U řadičů podporujících APPN pole Control point sessions (CPSSN) řídí, zda systém automaticky navazuje spojení APPC se vzdáleným systémem. Systém používá relaci CP k výměně síťových informací a stavu sítě se vzdáleným systémem. Výměna aktuálních informací mezi síťovými uzly APPN je mimořádně důležitá pro hladké fungování vaší sítě.

Když zadáte hodnotu *YES, nečinná komutovaná linka se automaticky neodpojí. Kvůli tomu je váš systém náchylnější k relacím typu ″piggy-back″.

Pole Disconnect timer

U řadiče APPC specifikuje pole Disconnect timer, jak dlouho nesmí být řadič používán (žádné aktivní relace), aby systém zrušil spojení se vzdáleným systémem. Toto pole má dvě hodnoty. První hodnota určuje, jak dlouho řadič zůstane aktivní od chvíle, kdy byl původně spojen. Druhá hodnota určuje, jak dlouho po ukončení poslední relace na řadiči systém počká, než pustí linku.

Systém používá časovač odpojení pouze tehdy, když má pole SWTDSC (Switched disconnect) hodnotu *YES.

Pokud tyto hodnoty zvýšíte, bude váš systém náchylnější k relacím typu ″piggy-back″.

Parametry pro popisy linky

Obrázek 12 na stránce 110 je příkladem sestavy informací o komunikacích pro popisy linky. Po sestavě následují vysvětlení polí uvedených v sestavě.

```
                          Communications Information (Full Report)

Object type  . . . . . :   *LIND
Auto
Object         Object         Line           Auto      Delete       Auto      Auto
Name           Type           Category       Create    Seconds      Answer    Dial
LINE01          *LIND          *SDLC           *NO            0       *NO       *NO
LINE02          *LIND          *SDLC           *NO            0       *YES      *NO
LINE03          *LIND          *SDLC           *NO            0       *NO       *NO
LINE04          *LIND          *SDLC           *NO            0       *YES      *NO
```

Obrázek 12. Popisy linky APPC - ukázková sestava

Pole Auto answer

Pole Auto answer (AUTOANS) určuje, zda bude komutovaná linka akceptovat příchozí volání bez zásahu operátora.

Když zadáte hodnotu *YES, bude váš systém méně zabezpečený, neboť k němu bude umožněn snadnější přístup. Aby bylo při zadání hodnoty *YES bezpečnostní riziko minimální, měli byste linku logicky vypnout vždy, když ji nepotřebujete.

Pole Auto dial

Pole Auto dial (AUTODIAL) určuje, zda může komutovaná linka provádět odchozí volání bez zásahu operátora. Když zadáte hodnotu *YES, umožníte lokálním uživatelům, kteří nemají fyzický přístup ke komunikačním linkám a modemům, aby se připojovali k jiným systémům.

Kapitola 13. Zabezpečení komunikace TCP/IP

Řídicí protokol přenosu, neboli TCP/IP (Transmission Control Protocol/Internet Protocol), představuje běžný způsob, kterým mezi sebou vzájemně komunikují počítače všech typů. Aplikace TCP/IP jsou známé a všeobecně používané v rámci "výměny informací".

Tato kapitola obsahuje rady pro to:

- Jak zabránit tomu, aby byly aplikace TCP/IP spouštěny ve vašem systému.
- Jak chránit systémové prostředky, když umožníte, aby byly aplikace TCP/IP spouštěny ve vašem systému.

Podrobný zdroj informací o všech aplikacích TCP/IP najdete v rámci aplikace iSeries Information Center—>Síťové technologie—>TCP/IP. Publikace *SecureWay: iSeries a the Internet* (v rámci aplikace iSeries Information Center—>Zabezpečení—>SecureWay) popisuje pokyny k zabezpečení, když svůj server iSeries připojujete buď k Internetu (velmi rozsáhlá síť TCP/IP), nebo k intranetu. Informace o tom, jak spustit aplikaci iSeries Information Center najdete v části "Nezbytné předchozí a související informace" na stránce xii.

Nezapomeňte, že servery iSeries podporují řadu možných aplikací TCP/IP. Když se ve vašem systému rozhodnete povolit jednu aplikaci TCP/IP, můžete zároveň zablokovat ostatní aplikace TCP/IP. Jako administrátor systému si musíte být vědomi rozsahu aplikací TCP/IP a dopadu těchto aplikací na zabezpečení.

Jak zabránit zpracování TCP/IP

Úlohy serveru TCP/IP se zpracovávají v podsystému QSYSWRK. Ke spuštění TCP/IP v systému slouží příkaz STRTCP (Spuštění TCP/IP). Pokud nechcete, aby se spustilo nějaké zpracování či aplikace TCP/IP, nepoužívejte příkaz STRTCP. Váš systém je dodáván s veřejným oprávněním pro příkaz STRTCP nastaveným na hodnotu *EXCLUDE.

Jestliže máte podezření, že někdo s přístupem k tomuto příkazu, spouští TCP/IP (např. v době průměrného provozu), můžete v příkazu STRTCP nastavit monitorování objektů. Systém zapíše záznam do monitorovacího žurnálu, kdykoliv nějaký uživatel použije daný příkaz.

Komponenty zabezpečení TCP/IP

Máte možnost využít výhod několika komponent pro zabezpečení TCP/IP, které zlepšují zabezpečení sítě a zvyšují flexibilitu. Ačkoliv se některé z těchto technologií vyskytují rovněž v produktech ochranné bariéry (firewall), není zamýšleno, že by byly tyto komponenty pro zabezpečení TCP/IP pro operační systém OS/400 používány jako ochranná bariéra. Přesto můžete některé z těchto funkcí v určitých případech využít k eliminaci potřeby samostatného produktu ochranné bariéry. Tyto funkce TCP/IP budete možná také moci využít pro zajištění dodatečného zabezpečení v prostředích, v nichž už ochrannou bariéru používáte.

Za účelem zlepšení zabezpečení TCP/IP lze použít následující komponenty:

- Pravidla paketu.
- HTTP proxy server.
- VPN (vytváření virtuálních soukromých sítí).
- SSL (Secure Socket Layer).

Použití pravidel paketu pro zabezpečení provozu TCP/IP

Pravidla paketu, která představují kombinaci filtrování IP a převodu síťových adres (NAT), fungují jako ochranná bariéra, která chrání interní síť před vetřelci. Filtrování IP vám umožňuje řídit, jaký provoz IP může vstupovat do vaší sítě a vystupovat z vaší sítě. V podstatě chrání vaši síť prostřednictvím filtrování paketů v souladu s vámi definovanými pravidly. Na druhou stranu NAT vám umožňuje skrýt své neregistrované soukromé IP adresy za sadu registrovaných IP adres. Tím ochráníte svou interní síť před externími sítěmi. NAT také pomáhá zmírnit problém s vyčerpáním IP adres, neboť velké množství soukromých adres lze vyjádřit malou množinou registrovaných adres. Další informace najdete v rámci aplikace iSeries Information Center.

HTTP proxy server

HTTP proxy server se dodává se serverem IBM HTTP Server for iSeries. HTTP server je součástí licencovaného programu OS/400. Proxy server přijímá HTTP požadavky od webových prohlížečů a posílá je na webové servery. Webové servery, které obdrží požadavky, znají pouze IP adresu proxy serveru a nemohou zjistit jména nebo adresy osobních počítačů, které vydaly původní požadavky. Proxy server umí zpracovávat požadavky na URL pro HTTP, FTP, Gopher a WAIS.

Proxy server ukládá do rychlé vyrovnávací paměti (cache) vrácené webové stránky z požadavků, které provedli všichni uživatelé proxy serveru. Když uživatel požaduje nějakou stránku, proxy server zkontroluje, zda je daná stránka v rychlé vyrovnávací paměti. Pokud ano, proxy server vrátí tuto stránku z rychlé vyrovnávací paměti. Prostřednictvím používání stránek uložených v rychlé vyrovnávací paměti je proxy server schopen vrátit webovému serveru stránky rychleji, což eliminuje potenciální časově náročné požadavky na webový server.

Proxy server může rovněž zapisovat všechny požadavky na URL za účelem jejich monitorování. Díky prohlížení protokolů můžete monitorovat využívání a zneužívání síťových prostředků.

Podporu proxy, kterou poskytuje IBM HTTP server, můžete použít ke konsolidaci přístupu k WWW. Adresy PC klientů jsou před webovými servery, ke kterým daní klienti přistupují, skryty. Známa je pouze adresa proxy serveru. Ukládání webových stránek do rychlé vyrovnávací paměti navíc snižuje požadavky na šířku komunikačního pásma a snižuje zatížení ochranné bariéry. Další informace najdete na domovské stránce serveru IBM HTTP Server for iSeries na adrese http://www-1.ibm.com/servers/eserver/iseries/software/http/index.html

Vytváření virtuálních soukromých sítí (VPN)

Virtuální soukromá síť, neboli VPN (virtual private network), umožňuje vaší společnosti bezpečným způsobem rozšířit soukromý intranet v rámci stávajícího frameworku veřejné sítě, jako je např. Internet. S VPN může vaše společnost řídit provoz sítě a zároveň zajišťovat významné funkce zabezpečení, jako je např. autentizace a důvěrnost dat.

VPN OS/400 je volitelně instalovatelná komponenta produktu iSeries Navigator, grafického uživatelského rozhraní (GUI) operačního systému OS/400. Umožňuje vám vytvářet bezpečnou cestu mezi libovolnou kombinací hostitele a brány (gateway). Komponenta VPN OS/400 používá metody autentizace, šifrovací algoritmy a jiná opatření k zajištění bezpečnosti dat posílaných mezi dvěma koncovými body spojení.

VPN běží na síťové vrstvě modelu zásobníku TCP/IP Layered Communications Stack. VPN konkrétně používá otevřený framework IPSec (IP Security Architecture). IPSec poskytuje

základní funkce zabezpečení pro Internet a rovněž nabízí pružné stavební bloky, z nichž můžete vytvářet robustní, zabezpečené virtuální soukromé sítě.

VPN také podporuje řešení VPN protokolu L2TP (Layer 2 Tunnel Protocol). Spojení L2TP, která jsou označována také jako virtuální linky, obstarávají z hlediska nákladů efektivní přístup pro vzdálené uživatele tím, že podnikovému síťovému serveru umožňují řídit IP adresy přiřazované jeho vzdáleným uživatelům. Spojení L2TP dále poskytují zabezpečený přístup k vašemu systému nebo síti, když je chráníte pomocí IPSec.

Je důležité, abyste pochopili, jaký dopad bude mít VPN na vaši celou síť. Základní podmínkou úspěchu je řádné plánování a implementace. Abyste měli jistotu, že chápete fungování VPN a možnosti jejich využití, měli byste si přečíst témata věnovaná VPN v rámci aplikace iSeries Information Center. Další informace najdete v rámci aplikace iSeries Information Center—>Zabezpečení—>VPN (Virtual Private Networking). Informace o tom, jak spustit aplikaci iSeries Information Center najdete v části “Nezbytné předchozí a související informace” na stránce xii.

SSL

SSL (Secure Socket Layer) se stalo odvětvovým standardem, který umožňuje aplikacím navazovat zabezpečené komunikační relace v nechráněné síti, jako je Internet. Protokol SSL vytváří zabezpečená spojení mezi klientskými a serverovými aplikacemi, která zajišťují autentizaci jednoho nebo obou koncových bodů komunikační relace. SSL také obstarává důvěrnost a integritu dat, která si mezi sebou vyměňují klientské a serverové aplikace. Další informace uvádí aplikace iSeries Information Center–>Zabezpečení—>SSL (Secure Sockets Layer). Informace o tom, jak spustit aplikaci iSeries Information Center najdete v části “Nezbytné předchozí a související informace” na stránce xii.

Zabezpečení vašeho prostředí TCP/IP

Tato část obsahuje obecné návrhy, jak postupovat, chcete-li snížit bezpečnostní rizika v prostředí TCP/IP ve vašem systému. Tyto rady se nevztahují pouze na určité aplikace, které jsou probírány v následujících částech, ale na celé vaše prostředí TCP/IP.

- Když píšete aplikaci pro port TCP/IP, ujistěte se, že je tato aplikace řádně zabezpečená. Měli byste předpokládat, že by se nějaký neznámý člověk mohl pokusit o přístup k aplikaci prostřednictvím daného portu. Uživatel zvenčí s určitou úrovní znalostí se může pokusit o telnetové připojení k dané aplikaci.
- Monitorujte používání portů TCP/IP ve vašem systému. Uživatelská aplikace, která je asociována s portem TCP/IP, může umožňovat vstup do vašeho systému “zadními dveřmi” bez uživatelského ID nebo hesla. Asociovat aplikaci s portem TCP nebo UDP může někdo, kdo má pro to ve vašem systému dostatečné oprávnění.
- Jako administrátor systému byste si měli být vědomi technik zvaných *″IP spoofing″* používaných hackery. Každý systém v síti TCP/IP má nějakou IP adresu. Někdo, kdo používá útoky typu ″IP spoofing″, nastaví systém (obvykle PC) tak, aby předstíral, že je existující nebo důvěryhodná IP adresa. Tak může počítačový pirát navázat spojení s vaším systémem tím, že bude předstírat, že se jedná o systém, ke kterému se běžně připojujete.

  Pokud ve vašem systému používáte TCP/IP a váš systém je zapojen v síti, která není fyzicky chráněná (samé nekomutované linky a předdefinované linky), jste náchylní k útokům typu ″IP spoofing″. Chcete-li váš systém ochránit před poškozením od počítačového piráta, který využívá útoky typu “spoofing”, začněte uskutečňovat návrhy v této kapitole, jako jsou např. ochrana přihlášení a zabezpečení na úrovni objektů. Měli byste také zajistit, aby měl váš systém nastavena rozumná omezení pro vnější paměť. Tím počítačovým pirátům zabráníte v zaplavení systému poštou nebo soubory pro souběžný tisk v takové míře, že by se systém stal neovladatelným.

Kromě toho byste měli pravidelně monitorovat aktivitu TCP/IP v systému. Pokud detekujete útok typu ″IP spoofing″, můžete se pokusit odhalit slabá místa v nastavení TCP/IP a provést případné úpravy.

- Pro intranet (síť systémů, které se nepotřebují přímo připojovat ven) používejte IP adresy, které jsou znovu použitelné. Znovu použitelné adresy jsou určeny pro použití v rámci soukromých sítí. Páteřní síť Internet neurčuje přenosovou cestu pro pakety, které mají znovu použitelnou IP adresu. Znovu použitelné adresy tak představují další ochrannou vrstvu uvnitř vaší ochranné bariéry.

  V rámci aplikace iSeries Information Center—>Síťové technologie—>TCP/IP najdete další informace o přiřazování a rozsahu IP adres a také informace o TCP/IP.
- Pokud uvažujete o připojení vašeho systému k Internetu nebo intranetu, přečtěte si informace v publikaci *SecureWay: iSeries a Internet* (aplikace iSeries Information Center—>Zabezpečení—>SecureWay). Informace o tom, jak spustit aplikaci iSeries Information Center najdete v části “Nezbytné předchozí a související informace” na stránce xii.

Jak určit, které servery TCP/IP se mají spouštět automaticky

Jako administrátor systému musíte stanovit, které aplikace TCP/IP se automaticky spustí, když spustíte TCP/IP. Ke spuštění TCP/IP slouží dva příkazy. Pro každý příkaz systém používá různou metodu určení, které aplikace (servery) se spustí.

Tabulka 22 ukazuje uvedené dva příkazy a pro každý z nich uvádí doporučení týkající se zabezpečení. Tabulka 23 na stránce 115 uvádí předvolené hodnoty automatického spuštění pro servery. Pokud chcete změnit hodnotu automatického spuštění pro server, použijte příkaz CHGxxxA (Změna atributů xxx). Například příkaz pro TELNET je CHGTELNA.

Tabulka 22. Jak příkazy TCP/IP určují, které servery se spustí

Příkaz	Které servery se spustí	Doporučení týkající se zabezpečení
STRTCP (Spuštění TCP/IP)	Systém spustí každý server, který specifikuje hodnotu AUTOSTART(*YES). Tabulka 23 na stránce 115 obsahuje dodávané hodnoty pro jednotlivé servery TCP/IP.	• Obezřetně přidělujte zvláštní oprávnění *IOSYSCFG pro řízení, kdo může měnit nastavení automatického spuštění. • Pečlivě sledujte, kdo má oprávnění používat příkaz STRTCP. Předvolené veřejné oprávnění pro tento příkaz je *EXCLUDE. • Nastavte monitorování objektů pro příkazy Změna atributů *jméno-serveru* (např. CHGTELNA) tak, aby se monitorovali uživatelé, kteří se pro server pokusí změnit hodnotu AUTOSTART.
STRTCPSVR (Spuštění serveru TCP/IP)	K zadání, které servery se spustí, se používá parametr. Dodanou předvolbou pro tento příkaz je spuštění všech serverů.	• Použijte příkaz CHGCMDDFT (Změna předvolby příkazu) k nastavení příkazu STRTCPSVR tak, aby se spouštěl pouze určitý server. Tím nezabráníte uživatelům, aby spouštěli jiné servery. Když však změníte předvolbu příkazu, zvýšíte pravděpodobnost, že uživatelé spustí všechny servery jen nešťastnou náhodou. Například pomocí následujícího příkazu můžete nastavit předvolbu tak, aby se spouštěl pouze server TELNET: `CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*TELNET)')` **Poznámka:** Když změníte předvolenou hodnotu, můžete zadat jen jeden server. Zvolte buď server, který používáte pravidelně, nebo server, u něhož je nejnižší pravděpodobnost vzniku bezpečnostních rizik (např. TFTP). • Pečlivě sledujte, kdo má oprávnění používat příkaz STRTCPSVR. Předvolené veřejné oprávnění pro tento příkaz je *EXCLUDE.

Následující tabulka obsahuje hodnoty automatického spuštění pro servery TCP/IP. Podrobné informace o jednotlivých serverech najdete v rámci aplikace iSeries Information Center

(**Síťové technologie—>TCP/IP**). Informace o přístupu k aplikaci iSeries Information Center najdete v části "Nezbytné předchozí a související informace" na stránce xii.

Tabulka 23. Hodnota automatického spuštění pro servery TCP/IP

Server	Předvolená hodnota	Vaše hodnota
TELNET	AUTOSTART(*YES)	
FTP (File Transfer Protocol)	AUTOSTART(*YES)	
BOOTP (Bootstrap Protocol)	AUTOSTART(*NO)	
TFTP (Trivial File Transfer Protocol)	AUTOSTART(*NO)	
REXEC (Remote EXECution server)	AUTOSTART(*NO)	
RouteD (Route Daemon)	AUTOSTART(*NO)	
SMTP (Simple Mail Transfer Protocol)	AUTOSTART(*YES)	
POP (Post Office Protocol)	AUTOSTART(*NO)	
HTTP (Hypertext Transfer Protocol) [1]	AUTOSTART(*NO)	
ICS (Internet Connection Server)[1]	AUTOSTART(*NO)	
LPD (Line Printer Daemon)	AUTOSTART(*YES)	
SNMP (Simple Network Management Protocol (SNMP))	AUTOSTART(*YES)	
DNS (DNS)	AUTOSTART(*NO)	
DDM	AUTOSTART(*NO)	
DHCP (DHCP)	AUTOSTART(*NO)	
NSMI	AUTOSTART(*NO)	
INETD	AUTOSTART(*NO)	

Poznámky:

1. U serveru IBM HTTP Server pro server iSeries se příkaz CHGHTTPA používá k nastavení hodnoty AUTOSTART.

Pokyny k zabezpečení při používání SLIP

Podpora TCP/IP serveru iSeries zahrnuje protokol SLIP (Serial Interface Line Protocol). SLIP zajišťuje úspornou dvoubodovou připojitelnost. Uživatel SLIP se může připojit k síti LAN nebo WAN tím, že vytvoří dvoubodové připojení se systémem, který je součástí LAN nebo WAN.

Protokol SLIP se spouští v asynchronních spojeních. Protokol SLIP můžete použít pro připojení po komutované lince do nebo ze serverů iSeries. SLIP lze například použít k připojení po komutované lince z vašeho PC do systému iSeries. Po navázání spojení můžete na vašem PC použít aplikaci TELNET k připojení k serveru TELNET iSeries. Nebo můžete použít aplikaci FTP k přenosu souborů mezi dvěma systémy.

Když je systém dodán, neexistuje v něm žádná konfigurace SLIP. Pokud si tedy ve vašem systému nepřejete provozovat SLIP (a připojení TCP/IP po komutované lince), nekonfigurujte žádné konfigurační profily pro SLIP. K vytvoření konfigurací SLIP se používá příkaz WRKTCPPTP (Práce s dvoubodovým připojením TCP/IP). Chcete-li použít příkaz WRKTCPPTP, musíte mít zvláštní oprávnění *IOSYSCFG.

Jestliže chcete ve svém systému provozovat protokol SLIP, vytvořte si jeden či více konfiguračních profilů SLIP (dvoubodových). Konfigurační profily můžete vytvořit s následujícími provozními režimy:

- *ANS (příchozí připojení)
- *DIAL (odchozí připojení)

V následujících částech je popsáno, jak můžete nastavit zabezpečení pro konfigurační profily SLIP.

Poznámka: **Uživatelský profil** je objekt serveru iSeries, který umožňuje přihlásit se do systému. Každá úloha serveru iSeries musí mít nějaký uživatelský profil, aby mohla být spuštěna. **Konfigurační profil** uchovává informace, které se používají k navázání spojení SLIP se systémem iSeries. Na začátku spojení SLIP se servery iSeries jednoduše vytvoříte propojení. Ještě jste se nepřihlásili a nespustili žádnou úlohu serveru iSeries. Proto není nezbytně nutné, abyste pro zahájení spojení SLIP se servery iSeries měli nějaký uživatelský profil. Jak však uvidíte v následující diskusi, může konfigurační profil SLIP vyžadovat uživatelský profil k určení, zda má spojení povolit.

Řízení spojení příchozích hovorů po komutované lince s využitím SLIP

Aby bylo možné vytvořit spojení příchozích hovorů po komutované lince s vaším systémem s využitím protokolu SLIP, musíte spustit konfigurační profil SLIP *ANS. Ke změně konfiguračního profilu SLIP se používá příkaz WRKTCPPTP (Práce s dvoubodovým připojením TCP/IP). Ke spuštění konfiguračního profilu lze použít buď příkaz STRTCPPTP (Spuštění dvoubodového připojení TCP/IP), nebo volbu z obrazovky WRKTCPPTP. Když obdržíte váš systém, je veřejné oprávnění pro příkazy STRTCPPTP a ENDTCPPTP nastaveno na hodnotu *EXCLUDE. Volby pro přidání, změnu a výmaz konfiguračních profilů SLIP jsou k dispozici pouze tehdy, máte-li zvláštní oprávnění *IOSYSCFG. Jako administrátor systému můžete používat oprávnění k příkazu i zvláštní oprávnění za účelem určení, kdo může nastavovat váš systém, aby umožňoval spojení příchozích hovorů po komutované lince.

Zabezpečení spojení příchozích hovorů po komutované lince s využitím SLIP

Pokud chcete ověřit systémy, které se chtějí k vašemu systému připojit po komutované lince, pak od žádajícího systému požadujete, aby poslal uživatelské ID a heslo. Váš systém pak může toto uživatelské ID a heslo ověřit. Pokud uživatelské ID nebo heslo není platné, může váš systém požadavek na relaci zamítnout.

Chcete-li nastavit ověření platnosti příchozího spojení po komutované lince, postupujte takto:

__ Krok 1. Vytvořte uživatelský profil, který bude moci žádající systém používat k navázání spojení. Uživatelské ID a heslo, které žadatel pošle, musí odpovídat tomuto uživatelského profilu a heslu.

Poznámka: Má-li systém provádět ověření platnosti hesla, musí být systémová hodnota QSECURITY nastavena na hodnotu 20 či vyšší.

V rámci rozšíření ochrany budete pravděpodobně chtít vytvořit uživatelské profily výslovně pro navazování spojení SLIP. Tyto uživatelské profily by měly mít omezené oprávnění v systému. Pokud nemáte v úmyslu používat uvedené profily pro jiné funkce než navázání spojení SLIP, můžete v uživatelských profilech nastavit tyto hodnoty:
- Počáteční menu (INLMNU): hodnota *SIGNOFF.
- Počáteční program (INLPGM): hodnota *NONE.
- Omezení schopností (LMTCPB): hodnota *YES.

Tyto hodnoty zabrání tomu, aby se kdokoliv mohl interaktivně přihlásit pomocí tohoto uživatelského profilu.

__ Krok 2. Pro systém vytvořte seznam oprávnění, který se zkontroluje vždy, když žadatel bude zkoušet navázat spojení SLIP.

Poznámka: Tento seznam oprávnění se zadává do pole *System access authorization list*, když vytváříte nebo měníte profil SLIP. (Viz krok 4.)

__ Krok 3. Pomocí příkazu ADDAUTLE (Přidání záznamu oprávnění) přidejte do seznamu oprávnění uživatelský profil, který jste vytvořili v kroku 1. Pro každý konfigurační profil PPP můžete vytvořit jedinečný seznam oprávnění nebo můžete vytvořit seznam oprávnění, který bude sdílen několika konfiguračními profily.

__ Krok 4. Pomocí příkazu WRKTCPPTP nastavte profil *ANS dvoubodového spojení TCP/IP, který má následující vlastnosti:

- Konfigurační profil musí používat skript pro spojovací dialog, který zahrnuje funkci ověření uživatele. Ověření uživatele spočívá v přijetí uživatelského ID a hesla od žadatele a ověření jejich platnosti. Systém je dodáván s několika vzorovými skripty pro dialogy, které zajišťují tuto funkci.
- Konfigurační profil musí uvádět jméno seznamu oprávnění, který jste vytvořili v kroku 2. Uživatelské ID, které obdrží skript pro spojovací dialog, musí být uvedeno v daném seznamu oprávnění.

Zapamatujte si, že hodnota nastavení zabezpečení příchozích připojení je ovlivněna způsoby a schopnostmi zabezpečení systémů, které se pokoušejí o příchozí připojení. Pokud požadujete uživatelské ID a heslo, musí skript pro spojovací dialog v žádajícím systému odeslat uživatelské ID a heslo. Některé systémy, jako např. servery iSeries, poskytují nějakou metodu zabezpečení pro ukládání uživatelských ID a hesel. (Tato metoda je popsána v části “Zabezpečení odchozích relací” na stránce 118.) Jiné systémy ukládají uživatelské ID i heslo do skriptu, který může být přístupný komukoliv, kdo ví, kde tento skript v systému hledat.

Vzhledem k rozdílným způsobům a schopnostem zabezpečení vašich partnerů v komunikaci možná budete chtít vytvořit různé konfigurační profily pro různá žádající prostředí. Pomocí příkazu STRTCPPTP nastavte systém tak, aby akceptoval relaci pro určitý konfigurační profil. Například relace pro některé konfigurační profily můžete spouštět pouze v určitou dobu během dne. Chcete-li sledovat aktivitu pro přidružené uživatelské profily, můžete použít monitorování zabezpečení.

Jak zabránit původcům příchozích připojení v přístupu k jiným systémům

V závislosti na konfiguraci vašeho systému a sítě, může být uživateli, který navazuje spojení SLIP, umožněn přístup k jinému systému ve vaší síti, aniž by se přihlásil do vašeho systému. Uživatel by mohl například navázat spojení SLIP s vaším systémem. Pak by mohl navázat spojení FTP s jiným systémem ve vaší síti, který neumožňuje příchozí připojení.

Uživatelům SLIP můžete znemožnit přístup k jiným systémům ve vaší síti tak, že do pole *Allow IP datagram forwarding* v konfiguračním profilu zadáte hodnotu N (ne). Tím uživateli zabráníte, aby měl přístup k vaší síti dříve, než se přihlásí do vašeho systému. Jakmile se však uživatel úspěšně přihlásí do vašeho systému, nemá již výše uvedená hodnota žádný vliv. Neomezuje schopnost uživatele použít ve vašem systému iSeries aplikaci TCP/IP (např. FTP nebo TELNET) k navázání spojení s jiným systémem v síti.

Řízení odchozích relací

Aby mohl někdo vytvořit spojení odchozích hovorů po komutované lince z vašeho systému s využitím SLIP, musíte spustit konfigurační profil SLIP *DIAL. Ke změně konfiguračního profilu SLIP se používá příkaz WRKTCPPTP. Ke spuštění konfiguračního profilu lze použít buď příkaz STRTCPPTP (Spuštění dvoubodového připojení TCP/IP), nebo volbu

z obrazovky WRKTCPPTP. Když obdržíte váš systém, je veřejné oprávnění pro příkazy STRTCPPTP a ENDTCPPTP nastaveno na hodnotu *EXCLUDE. Volby pro přidání, změnu a výmaz konfiguračních profilů SLIP jsou k dispozici pouze tehdy, máte-li zvláštní oprávnění *IOSYSCFG. Jako administrátor systému můžete používat oprávnění k příkazu i zvláštní oprávnění za účelem určení, kdo může nastavovat váš systém, aby umožňoval spojení odchozích hovorů po komutované lince.

Zabezpečení odchozích relací

Uživatelé ve vašem systému iSeries mohou chtít navazovat spojení odchozích hovorů po komutované lince se systémy, které vyžadují ověření uživatele. Skript pro spojovací dialog na vašem serveru iSeries musí odeslat uživatelské ID a heslo do vzdáleného systému. Servery iSeries poskytují bezpečnou metodu pro uložení daného hesla. Heslo není nutné ukládat do skriptu pro spojovací dialog.

Poznámky:

1. I když váš systém ukládá heslo pro spojení v zašifrované formě, systém heslo před odesláním dešifruje. Hesla SLIP, stejně jako hesla FTP a TELNET, se posílají nezašifrovaná. Na rozdíl od hesel FTP a TELNET je heslo SLIP odesláno dříve, než systém vytvoří režim TCP/IP.

   Jelikož SLIP používá dvoubodové spojení v asynchronním režimu, je bezpečnostní riziko při posílání nezašifrovaných hesel odlišné než u hesel FTP a TELNET. Nezašifrovaná hesla FTP a TELNET mohou být poslána v rámci IP provozu v síti a jsou proto náchylná k elektronickým útokům typu ″sniffing″. Přenos hesla SLIP je stejně zabezpečený jako telefonické spojení mezi dvěma systémy.
2. Předvolený soubor pro ukládání skriptů pro spojovací dialog SLIP je QUSRSYS/QATOCPPSCR. Veřejné oprávnění pro tento soubor je *USE, takže obecní uživatelé nemohou předvolené skripty pro spojovací dialog měnit.

Při vytváření profilu spojení pro vzdálenou relaci, která vyžaduje ověření platnosti, postupujte takto:

__ Krok 1. Zajistěte, aby systémová hodnota QRETSVRSEC (zachycení dat zabezpečení serveru) měla hodnotu 1 (ano). Tato systémová hodnota určuje, zda dovolíte, aby hesla, která je možné dešifrovat, byla uložena v chráněné oblasti ve vašem systému.

__ Krok 2. Pomocí příkazu WRKTCPPTP vytvořte konfigurační profil, který má následující vlastnosti:

- Pro režim konfiguračního profilu zadejte hodnotu *DIAL.
- Do pole *Remote service access name* zadejte uživatelské ID, které vzdálený systém očekává. Pokud se například připojujete k jinému serveru iSeries, zadejte jméno uživatelského profilu na daném serveru iSeries.
- Do pole *Remote service access password* zadejte heslo, které vzdálený systém očekává pro toto uživatelské ID. Na vašem serveru iSeries je toto heslo uloženo v chráněné oblasti ve formě, kterou lze dešifrovat. Jména a hesla, která přiřadíte konfiguračním profilům, jsou asociována s uživatelským profilem QTCP. Tato jména a hesla nejsou přístupná pomocí žádných uživatelských příkazů nebo rozhraní. K informacím o heslech mají přístup pouze registrované systémové programy.

  Poznámka: Zapamatujte si, že hesla pro vaše profily spojení se neuloží, když uložíte konfigurační soubory TCP/IP. Aby se hesla SLIP uložila, musíte k uložení uživatelského profilu QTCP použít příkaz SAVSECDTA (Uložení informací o zabezpečení).
- Jako skript pro spojovací dialog zadejte skript, který odesílá uživatelské ID a heslo. Systém je dodáván s několika vzorovými skripty pro dialogy, které

zajišťují tuto funkci. Když systém spustí daný skript, načte systém heslo, dešifruje ho a odešle ho do vzdáleného systému.

Pokyny k zabezpečení pro protokol PPP

Protokol pro dvoubodové připojení, neboli PPP (Point-to-point protocol), je součástí TCP/IP. PPP je odvětvovým standardem pro dvoubodová připojení, jenž poskytuje další funkce, které nepokrývá protokol SLIP.

S využitím protokolu PPP může váš server iSeries navázat přímá vysokorychlostní připojení k poskytovatelům služeb sítě Internet (ISP) nebo k jiným systémům v rámci intranetu nebo extranetu. Vzdálené sítě LAN mohou reálně vytvářet připojení po komutované lince k vašemu serveru iSeries.

Uvědomte si, že protokol PPP, stejně jako SLIP, umožňuje síťové připojení k vašemu serveru iSeries. Připojení PPP v podstatě přivádí žadatele k bráně do vašeho systému. Žadatel nicméně potřebuje uživatelské ID a heslo, aby se dostal do vašeho systému a mohl se připojit k serveru TCP/IP, jako je TELNET nebo FTP. Níže jsou uvedeny pokyny k zabezpečení zohledňující tuto novou schopnost připojení.

Poznámka: Konfigurace protokolu PPP se provádí pomocí produktu iSeries Navigator na pracovní stanici s produktem IBM iSeries Access for Windows.

- Protokol PPP poskytuje schopnost využívat jednouživatelská připojení (kdy má stejný uživatel vždy stejnou IP adresu). Při použití jednouživatelských adres vzniká riziko útoků typu ″IP spoofing″ (podvodný systém, který předstírá, že je důvěryhodný systém se známou IP adresou). Rozšířené schopnosti autentizace zajišťované protokolem PPP vám však pomohou chránit se před těmito útoky.
- U protokolu PPP, stejně jako u protokolu SLIP, vytváříte profily připojení, které mají jméno uživatele a přiřazené heslo. Na rozdíl od SLIP však uživatel nemusí mít platný uživatelský profil a heslo. Jméno ani heslo uživatele není asociováno s uživatelským profilem. Místo toho se pro účely autentizace PPP používají ověřovací seznamy. Protokol PPP navíc nevyžaduje skript pro spojení. Autentizace (výměna jména a hesla uživatele) je součástí architektury PPP a odehrává se na nižší úrovni než u protokolu SLIP.
- Díky PPP máte možnost používat protokol CHAP (Challenge Handshake Authentication Protocol). Už nebudete muset mít obavy z odhalení vašich hesel, neboť protokol CHAP šifruje jména i hesla uživatele.

  Připojení PPP používá protokol CHAP pouze tehdy, když obě strany podporují CHAP. Během výměny signálů za účelem nastavení komunikace mezi dvěma modemy spolu dva systémy vyjednávají. Pokud například systém SYSTEMA podporuje CHAP a systém SYSTEMB nikoliv, může systém SYSTEMA buď odmítnout relaci, nebo souhlasit s použitím nezašifrovaného jména a hesla uživatele. Odsouhlasení použití nezašifrovaného jména a hesla uživatele se označuje jako ″negotiating down″. ″Negotiate down″ je volba konfigurace. Například ve svém intranetu, kde víte, že všechny systémy mají podporu CHAP, byste měli nakonfigurovat profil připojení tak, aby nebyla nastavena volba ″Negotiate down″. U veřejného připojení, kde váš systém provádí vytáčení, si asi budete přát nastavit volbu ″Negotiate down″.

  Profil připojení pro PPP umožňuje specifikovat platné IP adresy. Například můžete označit, že pro určitého uživatele očekáváte určitou adresu nebo rozsah adres. Tato schopnost společně se schopností šifrovaní hesel rozšiřuje možnosti ochrany proti útokům typu ″spoofing″.

  Jako další ochranu proti tomuto typu útoků nebo proti napadení typu ″piggy-backing″ při aktivní relaci můžete protokol PPP nakonfigurovat tak, aby opakoval výzvu v označených intervalech. Například, když je aktivní relace PPP, může váš server iSeries vyzvat jiný systém, aby zadal uživatele a heslo. To provádí každých 15 minut, aby se ujistil, že se

jedná stále o tentýž profil připojení. (Koncový uživatel si nebude vědom těchto opakovaných výzev. Systémy si vyměňují jména a hesla pod úrovní, kterou vidí koncový uživatel.)

Při použití protokolu PPP je reálné očekávat, že vzdálené sítě LAN mohou vytvořit připojení po komutované lince k vašemu serveru iSeries a k rozšířené síti. V tomto prostředí se bude pravděpodobně požadovat, abyste měli zapnuto směrování pomocí IP. Směrování pomocí IP v sobě obsahuje latentní možnost, že by mohl nějaký vetřelec procházet vaší sítí. Protokol PPP je však vybaven silnější ochranou (jako např. šifrování hesel a ověření platnosti IP adres). Díky tomu se výrazně snižuje pravděpodobnost, že by vetřelec mohl vytvořit připojení do sítě.

Další informace o protokolu PPP najdete v rámci aplikace iSeries Information Center.

Pokyny k zabezpečení při používání serveru Bootstrap Protocol

Protokol BOOTP (Bootstrap Protocol) poskytuje dynamickou metodu pro asociaci pracovních stanic se servery a přiřazení IP adres a zdrojů IPL.

BOOTP je protokol TCP/IP, pomocí něhož se povoluje pracovní stanici bez datových médií (klient), aby od serveru v síti požadovala soubor obsahující zaváděcí kód. Server BOOTP naslouchá na známém portu 67 serveru BOOTP. Když obdrží požadavek klienta, podívá se server na IP adresu definovanou pro klienta a vrátí odpověď s IP adresou klienta a jménem zaváděcího souboru. Klient pak iniciuje požadavek TFTP na zaváděcí soubor vůči serveru. Mapování mezi hardwarovou adresou klienta a IP adresou je uchováváno v tabulce BOOTP na serveru iSeries.

Jak zabránit v přístupu BOOTP

Pokud nemáte v síti připojené žádné tenké klienty, nemusíte ve svém systému spouštět server BOOTP. Lze ho použít pro jiná zařízení, ale doporučeným řešením pro tato zařízení je použít DHCP. Pokud nechcete, aby se server BOOTP spouštěl, postupujte takto:

__ Krok 1. Chcete-li zabránit automatickému spuštění úloh serveru BOOTP při spuštění TCP/IP, napište tento příkaz:

```
CHGBPA AUTOSTART(*NO)
```

Poznámky:

1. AUTOSTART(*NO) je předvolená hodnota.
2. Další informace o tom, jak řídit, které servery TCP/IP se spouštějí automaticky, uvádí část “Jak určit, které servery TCP/IP se mají spouštět automaticky” na stránce 114.

__ Krok 2. Pokud nechcete nikomu dovolit přiřadit uživatelskou aplikaci, jako například aplikaci typu soket, k portu, který systém obvykle používá pro BOOTP, postupujte takto:

Poznámka: Jelikož DHCP i BOOTP používají stejné číslo portu, potlačí se tím také port, který používá DHCP. Port tedy neomezujte, jestliže chcete používat DHCP.

__ Krok a. Napište příkaz GO CFGTCP. Zobrazí se menu Konfigurace TCP/IP.

__ Krok b. Vyberte volbu 4 (Práce s omezením portu TCP/IP).

__ Krok c. Na obrazovce Práce s omezením portu TCP/IP zadejte volbu 1 (Přidat).

__ Krok d. Pro spodní rozsah portu zadejte hodnotu 67.

__ Krok e. Pro horní rozsah portu zadejte hodnotu *ONLY.

Poznámky:

1. Omezení portu nabudou platnosti při příštím spuštění TCP/IP. Jestliže je během nastavování omezení portu protokol TCP/IP aktivní, měli byste TCP/IP ukončit a opět ho spustit.
2. RFC1700 obsahuje informace o obecných přiřazeních čísel portů.

__ Krok f. Pro protokol zadejte hodnotu *UDP.

__ Krok g. Do pole uživatelského profilu zadejte jméno uživatelského profilu, který je chráněn ve vašem systému. (Chráněný uživatelský profil, který nevlastní programy přebírající oprávnění a který nemá heslo, jež je známo ostatním uživatelům.) Tím, že omezíte port na určitého uživatele, automaticky vyřadíte všechny ostatní uživatele.

Zabezpečení serveru BOOTP

Server BOOTP neposkytuje přímý přístup k vašemu systému iSeries a tak představuje jen omezené bezpečnostní riziko. Jako administrátor systému máte za cíl především zajištění, aby správné informace byly asociovány se správným tenkým klientem. Jinými slovy, nějaký počítačový pirát by mohl změnit tabulku BOOTP a způsobit, že by tencí klienti pracovali chybně nebo vůbec ne.

Pro administraci serveru BOOTP a tabulky BOOTP musíte mít zvláštní oprávnění *IOSYSCFG. Musíte pečlivě řídit, které uživatelské profily ve vašem systému mají toto zvláštní oprávnění.

Pokyny k zabezpečení při používání serveru DHCP

Protokol DHCP (DHCP) poskytuje framework pro předávání informací o konfiguraci hostitelským systémů v síti TCP/IP. Pro vaše klientské pracovní stanice může protokol DHCP zajišťovat funkce podobné automatické konfiguraci. Program podporující DHCP na klientské pracovní stanici vyšle požadavek na informace o konfiguraci. Pokud je na vašem serveru iSeries spuštěn server DHCP, server odpoví na požadavek odesláním informací, které klientská pracovní stanice potřebuje ke správnému nakonfigurování TCP/IP.

Protokol DHCP můžete použít k usnadnění prvního připojení uživatelů k vašemu serveru iSeries. Připojení je snazší, neboť uživatel nemusí zadávat informace o konfiguraci TCP/IP. Protokol DHCP lze také využít ke snížení počtu interních adres TCP/IP, které potřebujete v podsíti. Server DHCP může dočasně alokovat IP adresy pro aktivní uživatele (ze své společné oblasti IP adres).

Pro tyto klienty můžete použít protokol DHCP místo protokolu BOOTP. DHCP poskytuje více funkcí než BOOTP a může podporovat dynamickou konfiguraci jak tenkých klientů, tak PC.

Jak zabránit v přístupu DHCP

Pokud chcete, aby *nikdo* ve vašem systému nemohl používat server DHCP, postupujte takto:

1. Chcete-li zabránit automatickému spuštění úloh serveru DHCP při spuštění TCP/IP, napište tento příkaz:

   ```
   CHGDHCPA AUTOSTART(*NO)
   ```

   Poznámky:

   1. AUTOSTART(*NO) je předvolená hodnota.
   2. Další informace o tom, jak řídit, které servery TCP/IP se spouštějí automaticky, uvádí část “Jak určit, které servery TCP/IP se mají spouštět automaticky” na stránce 114.

2. Pokud nechcete nikomu dovolit přiřadit uživatelskou aplikaci, jako například aplikaci typu soket, k portu, který systém obvykle používá pro DHCP, postupujte takto:
   a. Napište příkaz GO CFGTCP. Zobrazí se menu Konfigurace TCP/IP.
   b. Vyberte volbu 4 (Práce s omezením portu TCP/IP).
   c. Na obrazovce Práce s omezením portu TCP/IP zadejte volbu 1 (Přidat).
   d. Pro spodní rozsah portu zadejte hodnotu 67.
   e. Pro horní rozsah portu zadejte hodnotu 68.

      Poznámky:

      1. Omezení portu nabudou platnosti při příštím spuštění TCP/IP. Jestliže je během nastavování omezení portu protokol TCP/IP aktivní, měli byste TCP/IP ukončit a opět ho spustit.
      2. RFC1700 obsahuje informace o obecných přiřazeních čísel portů.

   f. Pro protokol zadejte hodnotu *UDP.
   g. Do pole uživatelského profilu zadejte jméno uživatelského profilu, který je chráněn ve vašem systému. (Chráněný uživatelský profil, který nevlastní programy přebírající oprávnění a který nemá heslo, jež je známo ostatním uživatelům.) Tím, že omezíte port na určitého uživatele, automaticky vyřadíte všechny ostatní uživatele.

Zabezpečení serveru DHCP

Dále jsou uvedeny pokyny k zabezpečení, když se rozhodnete spouštět DHCP ve svém systému iSeries:

- Omezte počet uživatelů, kteří mají oprávnění k administraci DHCP. Administrace DHCP vyžaduje následující oprávnění:
  - zvláštní oprávnění *IOSYSCFG
  - oprávnění *RW k následujícím souborům:

    ```
    /QIBM/UserData/OS400/DHCP/dhcpsd.cfg
    /QIBM/UserData/OS400/DHCP/dhcprd.cfg
    ```
- Ohodnoťte, jak je vaše síť LAN fyzicky přístupná. Může nějaká cizí osoba snadno procházet vaším pracovištěm s laptopem a fyzicky se připojit k vaší LAN? Pokud existuje jisté riziko, DHCP poskytuje schopnost vytvořit seznam klientů (hardwarové adresy), které server DHCP nakonfiguruje. Když použijete tuto funkci, ztratíte některé výhody v oblasti produktivity, které DHCP poskytuje vašim správcům sítě. Zabráníte však systému, aby konfiguroval neznámé pracovní stanice.
- Je-li to možné, použijte společnou oblast IP adres, která je opětovně použitelná (není komponovaná pro Internet). To vám pomůže zabránit tomu, aby pracovní stanice mimo vaši síť získala ze serveru užitečné informace o konfiguraci.
- Pokud potřebujete dodatečné zabezpečení ochrany dat, použijte výstupní body DHCP. Níže najdete přehled výstupních bodů a jejich schopností. Způsob použití těchto výstupních bodů je popsán v publikaci *iSeries System API Reference*.

  Položka portu
  Systém volá váš ukončovací program, kdykoliv přečte datový paket z portu 67 (port DHCP). Váš ukončovací program obdrží celý datový paket. Může rozhodnout, zda má systém paket zpracovat či vyřadit. Tento výstupní bod můžete použít, když stávající kontrolní funkce DHCP nejsou dostatečné pro vaše potřeby.

  Přiřazení adresy
  Systém volá váš ukončovací program, kdykoliv DHCP formálně přiřadí adresu nějakému klientovi.

  Uvolnění adresy
  Systém volá váš ukončovací program, kdykoliv DHCP formálně uvolní adresu a umístí ji zpět do společné oblasti adres.

Pokyny k zabezpečení při používání serveru TFTP

Protokol TFTP (Trivial file transfer protocol) zajišťuje základní přenos souborů bez provádění autentizace uživatelů. Server TFTP používá buď protokoly BOOTP (Bootstrap Protocol), nebo protokoly DHCP (Dynamic Host Configuration Protocol).

Klient se nejprve připojí buď k serveru BOOTP, nebo k serveru DHCP. Server BOOTP nebo DHCP odpoví IP adresou klienta a jménem zaváděcího souboru. Klient pak iniciuje požadavek TFTP na zaváděcí soubor vůči serveru. Když klient dokončí zavádění zaváděcího souboru, ukončí relaci TFTP.

Jak zabránit v přístupu TFTP

Pokud nemáte v síti připojené žádné tenké klienty, nemusíte pravděpodobně ve svém systému spouštět server TFTP. Pokud nechcete, aby se server TFTP spouštěl, postupujte takto:

__ Krok 1. Chcete-li zabránit automatickému spuštění úloh serveru TFTP při spuštění TCP/IP, napište tento příkaz:

```
CHGTFTPA AUTOSTART(*NO)
```

Poznámky:

1. AUTOSTART(*NO) je předvolená hodnota.
2. Další informace o tom, jak řídit, které servery TCP/IP se spouštějí automaticky, uvádí část “Jak určit, které servery TCP/IP se mají spouštět automaticky” na stránce 114.

__ Krok 2. Pokud nechcete nikomu dovolit přiřadit uživatelskou aplikaci, jako například aplikaci typu soket, k portu, který systém obvykle používá pro TFTP, postupujte takto:

__ Krok a. Napište příkaz GO CFGTCP. Zobrazí se menu Konfigurace TCP/IP.

__ Krok b. Vyberte volbu 4 (Práce s omezením portu TCP/IP).

__ Krok c. Na obrazovce Práce s omezením portu TCP/IP zadejte volbu 1 (Přidat).

__ Krok d. Pro spodní rozsah portu zadejte hodnotu 69.

__ Krok e. Pro horní rozsah portu zadejte hodnotu *ONLY.

Poznámky:

1. Omezení portu nabudou platnosti při příštím spuštění TCP/IP. Jestliže je během nastavování omezení portu protokol TCP/IP aktivní, měli byste TCP/IP ukončit a opět ho spustit.
2. RFC1700 obsahuje informace o obecných přiřazeních čísel portů.

__ Krok f. Pro protokol zadejte hodnotu *UDP.

__ Krok g. Do pole uživatelského profilu zadejte jméno uživatelského profilu, který je chráněn ve vašem systému. (Chráněný uživatelský profil, který nevlastní programy přebírající oprávnění a který nemá heslo, jež je známo ostatním uživatelům.) Tím, že omezíte port na určitého uživatele, automaticky vyřadíte všechny ostatní uživatele.

Zabezpečení serveru TFTP

Standardně server TFTP poskytuje velmi omezený přístup k vašemu systému iSeries. Je specificky nakonfigurován tak, aby poskytoval zaváděcí kód pro tenké klienty. Jako administrátor systému byste si měli uvědomit následující vlastnosti serveru TFTP:

- Server TFTP nevyžaduje autentizaci (uživatelské ID a heslo). Všechny úlohy TFTP běží pod uživatelským profilem QTFTP. Uživatelský profil QTFTP nemá žádné heslo. Proto není k dispozici pro interaktivní přihlášení. Uživatelský profil QTFTP nemá žádná zvláštní oprávnění a nemá ani explicitní oprávnění k systémovým prostředkům. Za účelem přístupu k prostředkům, které potřebuje pro tenké klienty, používá veřejné oprávnění.
- Když obdržíte server TFTP, je nakonfigurován pro přístup k adresáři, který obsahuje informace o tenkých klientech. Abyste mohli v rámci tohoto adresáře provádět zápis nebo čtení, musíte mít oprávnění *PUBLIC nebo QTFTP. Pro zápis do daného adresáře musíte mít v parametru ″Povolit zápis do souboru″ příkazu CHGTFTPA zadánu hodnotu *CREATE. Chcete-li zapisovat do existujícího souboru, musíte mít v parametru ″Povolit zápis do souboru″ příkazu CHGTFTPA zadánu hodnotu *REPLACE. Hodnota *CREATE umožňuje nahrazovat stávající soubory a vytvářet nové soubory. Hodnota *REPLACE umožňuje pouze nahrazovat stávající soubory.

  Klient TFTP nemá přístup k žádným jiným adresářům, ledaže byste explicitně nějaký adresář definovali pomocí příkazu CHGTFTPA (Změna atributů TFTP). Proto, pokud se vzdálený uživatel pokusí ve vašem systému zahájit relaci TFTP, je jeho schopnost přistupovat k informacím nebo způsobit nějaké škody mimořádně omezená.
- Pokud se rozhodnete nakonfigurovat server TFTP tak, aby kromě práce s tenkými klienty poskytoval i jiné služby, můžete definovat ukončovací program, který by hodnotil a autorizoval každý požadavek TFTP. Server TFTP poskytuje výstupní bod pro ověření platnosti požadavku podobný výstupnímu bodu, který je k dispozici pro server FTP. Další informace najdete v rámci aplikace iSeries Information Center—>Síťové technologie—>TCP/IP—>TFTP. Informace o tom, jak spustit aplikaci iSeries Information Center najdete v části “Nezbytné předchozí a související informace” na stránce xii.

Pokyny k zabezpečení při používání serveru REXEC

Server REXEC (Remote EXECution server) přijímá a spouští příkazy z klienta REXEC. Klientem REXEC je obvykle PC nebo UNIX aplikace, která podporuje odesílání příkazů pro REXEC. Podpora, kterou tento server poskytuje, je podobná schopnosti dostupné, když použijete podpříkaz RCMD (Vzdálený příkaz) pro server FTP.

Jak zabránit v přístupu REXEC

Pokud si nepřejete, aby váš server iSeries přijímal příkazy z klienta REXEC, proveďte následující kroky, kterými zamezíte spouštění serveru REXEC.

__ Krok 1. Chcete-li zabránit automatickému spuštění úloh serveru REXEC při spuštění TCP/IP, napište tento příkaz:

```
CHGRXCA AUTOSTART(*NO)
```

Poznámky:

1. AUTOSTART(*NO) je předvolená hodnota.
2. Další informace o tom, jak řídit, které servery TCP/IP se spouštějí automaticky, uvádí část “Jak určit, které servery TCP/IP se mají spouštět automaticky” na stránce 114.

__ Krok 2. Pokud nechcete nikomu dovolit přiřadit uživatelskou aplikaci, jako například aplikaci typu soket, k portu, který systém obvykle používá pro REXEC, postupujte takto:

__ Krok a. Napište příkaz GO CFGTCP. Zobrazí se menu Konfigurace TCP/IP.

__ Krok b. Vyberte volbu 4 (Práce s omezením portu TCP/IP).

__ Krok c. Na obrazovce Práce s omezením portu TCP/IP zadejte volbu 1 (Přidat).

__ Krok d. Pro spodní rozsah portu zadejte hodnotu 512.

__ Krok e. Pro horní rozsah portu zadejte hodnotu *ONLY.

__ Krok f. Pro protokol zadejte hodnotu *TCP.

__ Krok g. Do pole uživatelského profilu zadejte jméno uživatelského profilu, který je chráněn ve vašem systému. (Chráněný uživatelský profil, který nevlastní programy přebírající oprávnění a který nemá heslo, jež je známo ostatním uživatelům.) Tím, že omezíte port na určitého uživatele, automaticky vyřadíte všechny ostatní uživatele.

Poznámky:

1. Omezení portu nabudou platnosti při příštím spuštění TCP/IP. Jestliže je během nastavování omezení portu protokol TCP/IP aktivní, měli byste TCP/IP ukončit a opět ho spustit.
2. RFC1700 obsahuje informace o obecných přiřazeních čísel portů.

Zabezpečení serveru REXEC

Dále jsou uvedeny pokyny k zabezpečení, když se rozhodnete spouštět server REXEC ve svém systému:

- Požadavek REXEC zahrnuje uživatelské ID, heslo a příkaz, který se má spustit. Normální autentizace serveru iSeries a kontrola oprávnění vyžaduje splnění těchto podmínek:
  - Kombinace uživatelského profilu a hesla musí být platná.
  - Systém vynucuje pro uživatelský profil hodnotu LMTCPB (*Omezení schopností*).
  - Uživatel musí mít oprávnění k danému příkazu a ke všem prostředkům, které příkaz používá.
- Server REXEC poskytuje výstupní body podobné výstupním bodům, které jsou k dispozici pro server FTP. Můžete používat výstupní bod pro ověření platnosti, který ohodnotí příkaz a rozhodne, zda ho povolit. Další informace najdete v rámci aplikace iSeries Information Center—>Síťové technologie—>TCP/IP—>REXEC. Informace o tom, jak spustit aplikaci iSeries Information Center najdete v části “Nezbytné předchozí a související informace” na stránce xii.
- Když se rozhodnete používat server REXEC, pohybujete se mimo veškeré řízení přístupu na úrovni menu, které máte ve svém systému. Musíte se ujistit, že vaše schéma oprávnění k objektům zajišťuje adekvátní ochranu vašich prostředků.

Pokyny k zabezpečení při používání serveru RouteD

Server RouteD (Route Daemon) poskytuje podporu pro protokol RIP (Routing Information Protocol) na serverech iSeries. Protokol RIP je nejčastěji používaným přenosovým protokolem. Je to protokol Interior Gateway Protocol, který pomáhá TCP/IP při směrování IP paketů v rámci autonomního systému.

Server RouteD je určen pro zvýšení efektivnosti síťového provozu. Dosahuje toho tím, že umožňuje systémům v rámci důvěryhodné sítě vzájemně se aktualizovat s využitím aktuálních informací o přenosových cestách. Když spustíte RouteD, může váš systém přijímat aktualizace z jiných účastnických systémů týkající se způsobu, jakým mají být směrovány přenosy (pakety). A proto, je-li váš server RouteD přístupný hackerům, může ho některý z nich využít k přesměrování vašich paketů do systému, který je může detekovat a modifikovat. Níže jsou uvedeny určité návrhy pro zabezpečení serveru RouteD:

- Servery iSeries používají RIPv1, který neposkytuje žádnou metodu pro autentizaci směrovačů. Je určen pro použití v rámci důvěryhodné sítě. Je-li váš systém v síti s jiným systémy, kterým ″nedůvěřujete″, neměli byste server RouteD spouštět. Abyste zajistili, že se server RouteD nebude spouštět automaticky, napište tento příkaz:

  ```
  CHGRTDA AUTOSTART(*NO)
  ```

Poznámky:

1. AUTOSTART(*NO) je předvolená hodnota.
2. Další informace o tom, jak řídit, které servery TCP/IP se spouštějí automaticky, uvádí část “Jak určit, které servery TCP/IP se mají spouštět automaticky” na stránce 114.

- Ujistěte se, že máte přehled, kdo může měnit konfiguraci RouteD, což vyžaduje zvláštní oprávnění *IOSYSCFG.
- Pokud je váš systém zapojen ve více sítích (např. intranetu a Internetu), můžete server RouteD nakonfigurovat tak, aby odesílal a přijímal aktualizace pouze v rámci zabezpečené sítě.

Pokyny k zabezpečení při používání serveru DNS

Server DNS (Domain Name System) zajišťuje převod hostitelského jména na IP adresy a naopak. U serverů iSeries je server DNS určen pro překlad adres v rámci interní zabezpečené sítě (intranetu).

Jak zabránit v přístupu DNS

Pokud chcete, aby *nikdo* ve vašem systému nemohl používat server DNS, postupujte takto:

1. Chcete-li zabránit automatickému spuštění úloh serveru DNS při spuštění TCP/IP, napište tento příkaz:

   ```
   CHGDNSA AUTOSTART(*NO)
   ```

   Poznámky:

   1. AUTOSTART(*NO) je předvolená hodnota.
   2. Další informace o tom, jak řídit, které servery TCP/IP se spouštějí automaticky, uvádí část “Jak určit, které servery TCP/IP se mají spouštět automaticky” na stránce 114.
2. Pokud nechcete nikomu dovolit přiřadit uživatelskou aplikaci, jako například aplikaci typu soket, k portu, který systém obvykle používá pro DNS, postupujte takto:
   a. Napište příkaz GO CFGTCP. Zobrazí se menu Konfigurace TCP/IP.
   b. Vyberte volbu 4 (Práce s omezením portu TCP/IP).
   c. Na obrazovce Práce s omezením portu TCP/IP zadejte volbu 1 (Přidat).
   d. Pro spodní rozsah portu zadejte hodnotu 53.
   e. Pro horní rozsah portu zadejte hodnotu *ONLY.

      Poznámky:

      1. Omezení portu nabudou platnosti při příštím spuštění TCP/IP. Jestliže je během nastavování omezení portu protokol TCP/IP aktivní, měli byste TCP/IP ukončit a opět ho spustit.
      2. RFC1700 obsahuje informace o obecných přiřazeních čísel portů.

   f. Pro protokol zadejte hodnotu *TCP.
   g. Do pole uživatelského profilu zadejte jméno uživatelského profilu, který je chráněn ve vašem systému. (Chráněný uživatelský profil, který nevlastní programy přebírající oprávnění a který nemá heslo, jež je známo ostatním uživatelům.) Tím, že omezíte port na určitého uživatele, automaticky vyřadíte všechny ostatní uživatele.
   h. Kroky 2c až 2g zopakujte pro protokol *UDP (uživatelský datagram).

Zabezpečení serveru DNS

Dále jsou uvedeny pokyny k zabezpečení, když se rozhodnete spouštět DNS ve svém systému iSeries:

- Server DNS poskytuje funkci překladu IP adres a překladu jmen. Nezajišťuje žádný přístup k objektům v systému iSeries. Riziko, když by nějaká cizí osoba získala přístup k vašemu

serveru DNS, spočívá v tom, že server umožňuje snadné prohlížení topologie vaší sítě. Server DNS by mohl ušetřit hackerovi jisté úsilí, které by musel vyvinout při zjišťování adres potenciálních cílů. DNS však neposkytuje informace, které by pomohly proniknout do takových cílových systémů.

- Server iSeries DNS se obvykle používá pro intranet. Proto pravděpodobně nebudete muset omezovat schopnost pokládat DNS dotazy. Například však můžete mít v rámci intranetu několik podsítí. Možná nebudete chtít, aby uživatelé z jiné podsítě byli schopni pokládat dotazy DNS na vašem serveru iSeries. Volba zabezpečení DNS umožňuje omezit přístup k primární doméně. Pomocí produktu iSeries Navigator určete IP adresy, kterým by měl server DNS odpovídat.

  Další volba zabezpečení umožňuje zadat, které sekundární servery mohou kopírovat informace z vašeho primárního serveru DNS. Když použijete tuto volbu, bude váš server akceptovat požadavky na zónové přenosy (požadavek na kopírování informací) pouze ze sekundárních serverů, které výslovně uvedete.
- Ujistěte se, že jste pozorně omezili schopnost měnit konfigurační soubor pro server DNS. Někdo s nekalými úmysly by mohl například změnit váš soubor DNS tak, aby ukazoval na IP adresu mimo vaši síť. Mohl by simulovat server ve vaší síti a případně získat přístup k důvěrným informacím od uživatelů, kteří server navštěvují.

Pokyny k zabezpečení při používání serveru HTTP Server for iSeries

Server HTTP poskytuje klientům webových prohlížečů přístup k multimediálním objektům serveru iSeries, jako jsou např. dokumenty HTML. Rovněž podporuje specifikaci CGI (*Common Gateway Interface*). Aplikační programátoři mohou vytvářet CGI programy, které rozšiřují funkční vybavení serveru.

Administrátor může používat server Internet Connection Server nebo server IBM HTTP Server for iSeries za účelem souběžného spuštění několika serverů na jednom serveru iSeries. Každý server, který je spuštěný, se nazývá **instance serveru**. Každá instance serveru má své jedinečné jméno. Administrátor řídí, které instance jsou spuštěny a co každá z instancí může provádět.

Poznámka: Chcete-li provádět konfiguraci nebo administraci následujících položek pomocí webového prohlížeče, musíte provozovat instanci *ADMIN serveru HTTP:

- Firewall for iSeries.
- Internet Connection Server
- Internet Connection Secure Server
- IBM HTTP Server for iSeries

Uživateli (návštěvníku webových stránek) se nikdy nezobrazí přihlašovací obrazovka serveru iSeries. Administrátor serveru iSeries však musí explicitně oprávnit všechny dokumenty HTML a CGI programy tím, že je definuje v direktivách HTTP. Kromě toho může administrátor pro některé nebo pro všechny požadavky nastavit zabezpečení na úrovni prostředků a autentizaci uživatele (uživatelské ID a heslo).

Útok hackera by mohl způsobit zamítnutí služby vašemu webovému serveru. Váš server může napadení typu zamítnutí služby zjistit na základě měření prodlev u určitých klientských požadavků. Pokud server neobdrží požadavek z klienta, určí, že právě probíhá napadení typu zamítnutí služby. To se stává po navázání výchozího připojení klienta k vašemu serveru. Předvolbou serveru je provádět detekci napadení a potrestání.

Jak zabránit v přístupu HTTP

Pokud chcete, aby *nikdo* ve vašem systému nemohl používat program pro přístup k vašemu systému, měli byste zabránit spuštění serveru HTTP. Postupujte takto:

__ Krok 1. Chcete-li zabránit automatickému spuštění úloh serveru HTTP při spuštění TCP/IP, napište tento příkaz:

```
CHGHTTPA AUTOSTART(*NO)
```

Poznámky:

1. AUTOSTART(*NO) je předvolená hodnota.
2. Další informace o tom, jak řídit, které servery TCP/IP se spouštějí automaticky, uvádí část “Jak určit, které servery TCP/IP se mají spouštět automaticky” na stránce 114.

__ Krok 2. Standardně server HTTP používá uživatelský profil QTMHHTTP. Chcete-li zajistit, aby se server HTTP nespustil, nastavte stav uživatelského profilu QTMHHTTP na hodnotu *DISABLED.

Řízení přístupu k serveru HTTP

Hlavním účelem spouštění serveru HTTP je zajištění přístupu k vašemu systému iSeries pro návštěvníky webových stránek. O někom, kdo navštívil vaše webové stránky, byste mohli uvažovat jako o někom, kdo si prohlíží inzerát v obchodním časopise. Návštěvník si neuvědomuje, na jakém hardwaru a softwaru jsou vaše webové stránky provozovány, tj. neví, jaký typ serveru používáte nebo kde je server fyzicky umístěn. Obvykle nechcete klást nějaké překážky (např. přihlašovací obrazovku) mezi potenciálního návštěvníka a vaše webové stránky. Můžete však chtít omezit přístup k některým dokumentům nebo CGI programům, které vaše webové stránky poskytují.

Rovněž byste mohli chtít, aby jeden systém iSeries poskytoval několik logických webových stanic. Váš systém iSeries by mohl například podporovat různá odvětví podnikání, která oslovují odlišné skupiny zákazníků. Pro každé toto odvětví chcete jedinečné webové stránky, které se budou návštěvníkovi jevit jako zcela nezávislé. Navíc byste mohli chtít poskytovat interní webové stránky (intranet) s důvěrnými informace o vašem podnikání.

Jako administrátor systému musíte chránit obsah webových stránek a zároveň musíte zajistit, aby vaše techniky zabezpečení neměly negativní dopad na hodnotu webových stránek. Kromě toho musíte zajistit, aby činnost HTTP neohrožovala integritu vašeho systému nebo sítě. V následujících částech najdete návrhy pro zabezpečení, když používáte daný program.

Pokyny k administraci

Dále uvádíme některé pokyny k zabezpečení týkající se administrace vašeho internetového serveru.

- Instalační a konfigurační funkce se provádějí pomocí webového prohlížeče a instance *ADMIN. Pro některé funkce, jako je vytvoření dalších instancí na serveru, *musíte* použít server *ADMIN.
- Předvolená adresa URL pro domovskou stránku administrace (domovská stránka serveru *ADMIN) je uveřejněna v dokumentaci k produktům, které poskytují administrační funkce prohlížeče. Proto bude předvolená adresa URL pravděpodobně známa hackerům a zveřejněna v hackerských fórech, stejně tak jako jsou známa a zveřejněna předvolená hesla pro uživatelské profily dodané IBM. Před tímto rizikem se můžete chránit několika způsoby:
  - Instanci *ADMIN serveru HTTP spouštějte pouze tehdy, když budete potřebovat provádět administrativní funkce. Nemějte instanci *ADMIN nepřetržitě spuštěnou.
  - Aktivní podpora SSL pro instanci *ADMIN (s využitím produktu Digital Certificate Manager). Instance *ADMIN používá direktivy ochrany HTTP k vyžádání uživatelského ID a hesla. Když používáte SSL, je vaše uživatelské ID i heslo zašifrováno (společně se všemi ostatními informacemi o vaší konfiguraci, které se vyskytují v administračních formulářích).

– Používejte ochrannou bariéru (firewall) jak za účelem zabránění v přístupu k serveru *ADMIN z Internetu, tak ke skrytí vašich jmen systému a domén, které jsou součástí adresy URL.

- Když provádíte administrační funkce, musíte se přihlásit uživatelským profilem, který má zvláštní oprávnění *IOSYSCFG. Můžete také potřebovat oprávnění k určitým objektům v systému, jako jsou např.:
  – Knihovny nebo adresáře, které obsahují vaše dokumenty HTML a CGI programy.
  – Libovolné uživatelské profily, které máte v plánu vyměnit v rámci direktiv pro daný server.
  – Přístupové seznamy (ACL) pro libovolné adresáře, které vaše direktivy používají.
  – Objekt typu ověřovací seznam pro vytvoření a údržbu uživatelských ID a hesel.

  Díky serveru *ADMIN a TELNET máte schopnost provádět administrační funkce vzdáleně, třeba přes internetové připojení. Uvědomte si, že pokud provádíte administraci přes veřejné spojení (Internet), můžete vystavit mocné uživatelské ID a heslo odhalení. Počítačový pirát používající útoky typu ″sniffing″ se pak může pomocí tohoto uživatelského ID a hesla pokusit získat přístup do vašeho systému, např. s využitím TELNET nebo FTP.

  Poznámky:

  1. U TELNET se s přihlašovací obrazovkou pracuje jako s každou jinou obrazovkou. Ačkoliv se heslo nezobrazuje, když je píšete, systém je přenáší, aniž by provedl nějaké šifrování nebo kódování.
  2. U serveru *ADMIN je heslo zakódováno, ale není zašifrováno. Kódovací schéma je odvětvovým standardem a je tedy v komunitě hackerů všeobecně známé. Ačkoliv kódování není pro náhodného počítačového piráta na první pohled srozumitelné, má zkušený pirát pravděpodobně k dispozici nástroje, kterými se může pokusit heslo dekódovat.

  Tip na zabezpečení

  Pokud máte v plánu provádět vzdálenou administraci přes Internet, měli byste instanci *ADMIN použít s SSL, aby byl přenos zašifrován. Nepoužívejte nezabezpečenou aplikaci, jako je např. verze TELNET nižší než V4R4 (TELNET podporuje SSL počínaje verzí V4R4). Pokud používáte server *ADMIN v rámci intranetu tvořeného *důvěryhodnými* uživateli, můžete jej pravděpodobně bezpečně používat pro administraci.

- Direktivy HTTP tvoří základnu pro všechny aktivity na vašem serveru. Dodaná konfigurace umožňuje obsluhovat předvolenou uvítací (Welcome) stránku. Klient si nemůže prohlížet žádné dokumenty kromě uvítací stránky, dokud administrátor serveru nedefinuje direktivy pro daný server. K definici direktiv použijte webový prohlížeč a server *ADMIN nebo příkaz WRKHTTPCFG (Práce s konfigurací HTTP). Obě metody vyžadují zvláštní oprávnění *IOSYSCFG. Když připojíte váš server iSeries k Internetu, nabyde pro vás na významu sledování a řízení počtu uživatelů ve vaší organizaci, kteří mají zvláštní oprávnění *IOSYSCFG.

Ochrana prostředků

Server IBM HTTP Server for iSeries zahrnuje direktivy HTTP, které mohou zajišťovat detailní řízení informačních hodnot, které server používá. Direktivy můžete použít k určení toho, ze kterých adresářů má webový server obsluhovat adresy URL jak pro soubory HTML, tak pro CGI programy, za účelem výměny za jiné uživatelské profily a vyžádání autentizace pro některé prostředky.

Poznámka: Podrobné popisy dostupných direktiv HTTP a jejich použití najdete v dokumentaci pod tématem ″Webové služby″ v rámci aplikace Information Center. Dále jsou uvedeny některé návrhy a pokyny pro použití této podpory:

- Server HTTP se spouští na bázi ″explicitního oprávnění.″ Server neakceptuje požadavek, pokud tento požadavek není explicitně definován v direktivách. Jinými slovy, server okamžitě zamítne jakýkoliv požadavek na URL, pokud tato URL není definována v direktivách (buď jmenovitě, nebo generický).
- Můžete použít ochranné direktivy k vyžádání uživatelského ID a hesla dříve, než akceptujete požadavek na některé nebo všechny vaše prostředky.
  - Když uživatel (klient) požaduje chráněný prostředek, předá server prohlížeči výzvu k zadání uživatelského ID a hesla. Prohlížeč vyzve uživatele k zadání uživatelského ID a hesla a pak tyto informace odešle serveru. Některé prohlížeče ukládají uživatelské ID a heslo a posílají je automaticky s následujícími požadavky. To uživatele zbaví nutnosti opakovaně zadávat stejné uživatelské ID a heslo při každém požadavku.

    Jelikož některé prohlížeče ukládají uživatelské ID a heslo, stojí před vámi stejný úkol v oblasti vyškolení, jako když uživatelé vstupují do vašeho systému prostřednictvím přihlašovací obrazovky serveru iSeries nebo pomocí směrovače. Plně automatizovaná relace s prohlížečem představuje bezpečnostní riziko.
  - Existují tři možnosti, jak systém pracuje s uživatelskými ID a hesly (zadanými v ochranných direktivách).
    1. Můžete použít normální uživatelský profil a ověření platnosti hesla serveru iSeries. To se nejvíce využívá k ochraně prostředků v intranetu (zabezpečené síti).
    2. Můžete vytvořit ″internetové uživatele″: uživatele, kteří mohou být prověřováni, ale nemají uživatelský profil na serveru iSeries. Internetoví uživatelé se implementují prostřednictvím objektu serveru iSeries, který se nazývá ″ověřovací seznam″. Objekty typu ověřovací seznam obsahují seznamy uživatelů a hesel, které jsou specificky definovány pro použití s určitou aplikací.

       Vy rozhodujete o tom, jak budou ID a hesla internetových uživatelů dodávána (např. aplikací nebo administrátorem jako reakce na požadavek elektronické pošty), a také o tom, jak budou internetoví uživatelé řízeni. K tomuto nastavení použijte rozhraní na bázi prohlížečů serveru HTTP.

       U nezabezpečených sítí (Internet) poskytuje použití internetových uživatelů lepší celkovou ochranu než běžné uživatelské profily a hesla. Jedinečná množina uživatelských ID a hesel představuje vestavěné omezení pro to, co mohou tito uživatelé provádět. Uživatelská ID a hesla nejsou dostupná pro normální přihlášení (např. pomocí TELNET nebo FTP). Kromě toho nevystavujete běžná uživatelská ID a hesla případnému odhalení.
    3. Protokol LDAP (Lightweight Directory Access Protocol) je protokol adresářových služeb, který zajišťuje přístup k adresáři přes protokol TCP (Transmission Control Protocol). To vám umožňuje ukládat informace do dané adresářové služby a pokládat na ně dotazy. Protokol LDAP je nyní podporován jako volba pro autentizaci uživatele.

    Poznámky:

    1. Když prohlížeč odešle uživatelské ID a heslo (ať už pro uživatelský profil, nebo pro internetového uživatele), dojde k jejich zakódování, nikoliv k zašifrování. Kódovací schéma je odvětvovým standardem a je tedy v komunitě hackerů všeobecně známé. Ačkoliv kódování není pro náhodného počítačového piráta na první pohled srozumitelné, má zkušený pirát pravděpodobně k dispozici nástroje, kterými se může pokusit heslo dekódovat.
    2. Server iSeries ukládá ověřovací objekt do chráněné systémové oblasti. Přístup k ní je možný pouze pomocí definovaného systémového rozhraní API a patřičné autorizace.

- Chcete-li vytvořit svého vlastního vydavatele certifikátů pro intranet, můžete k tomu použít produkt DCM (Digital Certificate Manager). Digitální certifikát automaticky přiřadí certifikát uživatelskému profilu vlastníka. Certifikát má stejná oprávnění a povolení jako asociovaný profil.

- Když server přijme požadavek, převezme se běžné zabezpečení na úrovni prostředků serveru iSeries. Uživatelský profil, který požaduje daný prostředek, musí mít oprávnění k tomuto prostředku (např. pořadači nebo zdrojovému fyzickému souboru, který obsahuje dokument HTML). Standardně jsou úlohy spouštěny pod uživatelským profilem QTMHHTTP. Chcete-li uživatelský profil vyměnit za jiný, můžete použít direktivu. Systém pak pro přístup k objektům použije oprávnění nového uživatelského profilu. Níže jsou uvedeny některé pokyny pro tuto podporu:
  - Výměna uživatelských profilů může být užitečná především tehdy, když váš server poskytuje více logických webových stanic. Pomocí direktiv můžete s jednotlivými webovými stanicemi asociovat rozdílné uživatelské profily a díky tomu můžete k ochraně dokumentů pro jednotlivé webové stanice používat běžné zabezpečení na úrovni prostředků serveru iSeries.
  - Schopnost výměny uživatelských profilů lze využít v kombinaci s ověřovacím objektem. Server používá jedinečné uživatelské ID a heslo (oddělené od vašeho běžného uživatelského ID a hesla) k ohodnocení výchozího požadavku. Poté, co server provede autentizaci uživatele, prohodí systém uživatelské profily a tak využije výhod zabezpečení na úrovni prostředků. Uživatel si tedy není vědom skutečného jména uživatelského profilu a nemůže ho zkoušet používat jinými způsoby (např. FTP).
- Některé požadavky serveru HTTP vyžadují spuštění programu na serveru HTTP. Tento program může například přistupovat k datům ve vašem systému. Dříve, než je možné program spustit, musí administrátor serveru namapovat požadavek (URL) na specifický uživatelem definovaný program, který podléhá standardům pro uživatelská rozhraní CGI. Níže jsou uvedeny některé pokyny pro CGI programy:
  - Pro CGI programy můžete použít ochranné direktivy stejně tak, jako je používáte pro dokumenty HTML. Tak můžete požadovat uživatelské ID a heslo dříve, než se daný program spustí.
  - CGI programy se standardně spouští pod uživatelským profilem QTMHHTP1. Před spuštěním programu můžete vyměnit uživatelský profil za jiný. Proto můžete pro prostředky, ke kterým CGI programy přistupují, nastavit běžné zabezpečení na úrovni prostředků serveru iSeries.
  - Jako administrátor systému byste měli provést kontrolu zabezpečení dříve, než poskytnete oprávnění k použití libovolného CGI programu ve vašem systému. Měli byste vědět, odkud CGI program pochází a jaké funkce provádí. Rovněž byste měli monitorovat schopnosti uživatelských profilů, pod nimiž se CGI programy spouští. Kromě toho byste měli provádět testování CGI programů, na jehož základě byste například určili, zda můžete získat přístup k příkazové řádce. S CGI programy pracujte stejně obezřetně jako s programy, které přebírají (adoptují) oprávnění.
  - Navíc nezapomeňte vyhodnocovat, které citlivé objekty mají neodpovídající veřejné oprávnění. Špatně navržený CGI program by mohl ve výjimečných případech umožnit zkušenému, nečestnému uživateli zkoušet procházet vaším systémem.
  - K uložení všech vašich CGI programů používejte určitou uživatelskou knihovnu, např. CGILIB. Pomocí oprávnění k objektu řiďte, kdo může umísťovat nové objekty do této knihovny a kdo může spouštět programy v této knihovně. Prostřednictvím direktiv omezte server HTTP tak, aby spouštěl pouze CGI programy, které jsou uloženy v této knihovně.

    Poznámka: Pokud váš server poskytuje několik logických webových stanic, budete možná chtít pro každou ze stanic nastavit samostatnou knihovnu pro CGI programy.

Další pokyny k zabezpečení

Níže jsou uvedeny další pokyny k zabezpečení:

- HTTP poskytuje přístup k vašemu systému iSeries pouze za účelem čtení. Požadavky serveru HTTP nemohou přímo aktualizovat nebo mazat data ve vašem systému. Můžete však mít CGI programy, které data aktualizují. Kromě toho můžete aktivovat CGI programy v jazyce Net.Data, které zajišťují přístup k databázi serveru iSeries. K ohodnocení požadavků na program v jazyce Net.Data používá systém skript (podobný ukončovacímu programu). Díky tomu může administrátor systému řídit, jaké akce může program v jazyce Net.Data provádět.
- Server HTTP poskytuje protokol přístupů, který můžete použít k monitorování přístupů i pokusů o přístupy prostřednictvím serveru.

Pokyny k zabezpečení při používání SSL se serverem IBM HTTP Server for iSeries

Server IBM HTTP Server for iSeries může poskytovat zabezpečená webová připojení k vašem serveru iSeries. **Zabezpečené webové stránky** znamenají, že přenosy mezi klientem a serverem (v obou směrech) jsou zašifrovány. Tyto zašifrované přenosy jsou chráněné před zkoumáním počítačových pirátů a před těmi, kdo se pokouší přenosy sejmout nebo pozměnit.

Poznámka: Uvědomte si, že zabezpečené webové stránky se vztahují výhradně na zabezpečení informací, které jsou předávány mezi klientem a serverem. Jejich cílem není snížit zranitelnost serveru vůči hackerům. Přesto však rozhodně omezují informace, které by případní hackeři mohli snadno získat prostřednictvím útoků typu ″sniffing″.

Podrobné informace o instalaci, konfiguraci a řízení procesu šifrování uvádí témata o SSL a obsluhování webu (HTTP) v rámci aplikace Information Center. Tato témata poskytují přehled funkcí serveru a pokyny pro používání serveru.

Server pro připojení k Internetu (Internet Connection Server) poskytuje podporu HTTP a HTTPS, pokud je instalován některý z následujících licencovaných programů:

- 5722–NC1
- 5722–NCE

Když jsou instalovány tyto volby, je daný produkt označován jako server pro zabezpečení připojení k Internetu.

Server IBM HTTP Server for iSeries (5722–DG1) zajišťuje jak podporu HTTP, tak podporu HTTPS. Chcete-li aktivovat SSL, musíte nainstalovat jeden z následujících šifrovacích produktů:

- 5722–AC2
- 5722–AC3

Zabezpečení, které závisí na šifrování, má několik požadavků:

- Odesílatel i příjemce (server a klient) musí ″rozumět″ šifrovacímu mechanismu a musí být schopni provádět šifrování a dešifrování. Server HTTP požaduje klienta podporujícího SSL. (Většina oblíbených webových prohlížečů podporuje SSL.) Šifrovací licencované programy serveru iSeries podporují několik metod, které jsou odvětvovým standardem. Když se klient pokusí navázat zabezpečenou relaci, začne server a klient vyjednávat, aby nalezli co nejbezpečnější metodu šifrování, kterou oba podporují.
- Přenos nesmí být možné dešifrovat na základě odposlouchávání. Proto metody šifrování vyžadují, aby obě strany měly **soukromý klíč** pro šifrování/dešifrování, který znají jen ony. Chcete-li mít zabezpečenou *externí* webovou stanici, měli byste k vytváření a vydávání

digitálních certifikátů pro uživatele a servery používat nezávislého vydavatele certifikátů (CA). Vydavatel certifikátu je znám jako důvěryhodná strana.

Šifrování chrání důvěrnost přenášených informací. U citlivých informací, jako jsou např. finanční údaje, však vyžadujete kromě důvěrnosti také integritu a pravost. Jinými slovy, klient a (volitelně) server musí důvěřovat straně na druhém konci (na základě nezávislého doporučení) a musí si být jisti, že přenos nebyl pozměněn. Digitální podpis, který poskytuje vydavatel certifikátů (CA), zajišťuje tato zabezpečení pravosti a integrity. Protokol SSL umožňuje autentizaci tím, že ověřuje digitální podpis certifikátu serveru (a volitelně certifikátu klienta).

Šifrování a dešifrování vyžaduje čas na zpracování a ovlivní výkon vašich přenosů. Proto servery iSeries nabízejí možnost spouštět oba programy pro zabezpečené i nezabezpečené služby ve stejnou dobu. Nezabezpečený server HTTP můžete použít k obsluze dokumentů, které nevyžadují zabezpečení, jako jsou např. katalogy produktů. Tyto dokumenty budou mít adresu URL, která začíná http://. Zabezpečený server HTTP lze použít pro citlivé informace, jako jsou např. formuláře, kde zákazník zadává informace o své kreditní kartě. Tento program může pracovat s dokumenty, jejichž adresa URL začíná buď http://, nebo https://.

Připomínka

Dobrým, byť nepsaným pravidlem na Internetu je informovat klienty, kdy jsou přenosy zabezpečené a kdy zabezpečené nejsou, především tehdy, když vaše webové stránky používají zabezpečený server pouze pro některé dokumenty.

Nezapomeňte, že šifrování vyžaduje, aby byl zabezpečený klient i server. Zabezpečené prohlížeče (klienti HTTP) jsou již nyní poměrně běžnými.

Pokyny k zabezpečení pro LDAP

Funkce zabezpečení LDAP (Lightweight Directory Access Protocol) zahrnují SSL (Secure Sockets Layer), přístupové seznamy (ACL) a šifrování hesel CRAM-MD5. Ve verzi V5R1 bylo zabezpečení LDAP rozšířeno o podporu spojení Kerberos a monitorování zabezpečení.

Další informace o těchto oblastech najdete v rámci aplikace iSeries Information Center—>Síťové technologie–>TCP/IP–>LDAP (Directory Services). Informace o tom, jak spustit aplikaci iSeries Information Center najdete v části “Nezbytné předchozí a související informace” na stránce xii.

Pokyny k zabezpečení pro LPD

Démon řádkové tiskárny, neboli LPD (line printer daemon), umožňuje distribuovat tiskový výstup do vašeho systému. Systém neprovádí žádné zpracování přihlášení pro LPD.

Jak zabránit v přístupu LPD

Pokud chcete, aby *nikdo* ve vašem systému nemohl používat LPD pro přístup k vašemu systému, měli byste zabránit spuštění serveru LPD. Postupujte takto:

__ Krok 1. Chcete-li zabránit automatickému spuštění úloh serveru LPD při spuštění TCP/IP, napište tento příkaz:

```
CHGLPDA AUTOSTART(*NO)
```

Poznámky:

1. AUTOSTART(*YES) je předvolená hodnota.

2. Další informace o tom, jak řídit, které servery TCP/IP se spouštějí automaticky, uvádí část "Jak určit, které servery TCP/IP se mají spouštět automaticky" na stránce 114.

__ Krok 2. Pokud nechcete nikomu dovolit přiřadit uživatelskou aplikaci, jako například aplikaci typu soket, k portu, který systém obvykle používá pro LPD, postupujte takto:

__ Krok a. Napište příkaz GO CFGTCP. Zobrazí se menu Konfigurace TCP/IP.

__ Krok b. Vyberte volbu 4 (Práce s omezením portu TCP/IP).

__ Krok c. Na obrazovce Práce s omezením portu TCP/IP zadejte volbu 1 (Přidat).

__ Krok d. Pro spodní rozsah portu zadejte hodnotu 515.

__ Krok e. Pro horní rozsah portu zadejte hodnotu *ONLY.

Poznámky:

1. Omezení portu nabudou platnosti při příštím spuštění TCP/IP. Jestliže je během nastavování omezení portu protokol TCP/IP aktivní, měli byste TCP/IP ukončit a opět ho spustit.
2. RFC1700 obsahuje informace o obecných přiřazeních čísel portů.

__ Krok f. Pro protokol zadejte hodnotu *TCP.

__ Krok g. Do pole uživatelského profilu zadejte jméno uživatelského profilu, který je chráněn ve vašem systému. (Chráněný uživatelský profil, který nevlastní programy přebírající oprávnění a který nemá heslo, jež je známo ostatním uživatelům.) Tím, že omezíte port na určitého uživatele, automaticky vyřadíte všechny ostatní uživatele.

__ Krok h. Kroky 2c až 2g zopakujte pro protokol *UDP.

Řízení přístupu LPD

Pokud chcete, aby vaši klienti LPD měli přístup k systému, měli byste zvážit tyto otázky týkající se zabezpečení:

- Abyste zabránili svévolnému zahlcení vašeho systému nežádoucími objekty, ujistěte se, že jste pro ASP nastavili odpovídající prahové hodnoty. Prahové hodnoty pro ASP můžete zobrazit nebo nastavit buď pomocí SST (system service tools), nebo pomocí DST (dedicated service tools). Další informace o prahových hodnotách ASP obsahuje publikace *Zálohování a obnova*.
- Pokud chcete omezit, kdo může posílat soubory pro souběžný tisk do vašeho systému, použijte oprávnění k výstupním frontám. Uživatelé LPD bez uživatelského ID používají uživatelský profil QTMPLPD. Tomuto uživatelskému profilu můžete poskytnout přístup pouze k malému počtu výstupních front.

Pokyny k zabezpečení pro SNMP

Server iSeries může vystupovat jako agent SNMP (Simple Network Management Protocol) v síti. Protokol SNMP poskytuje prostředky pro správu bran (gateway), směrovačů a hostitelských systémů v síťovém prostředí. Agent SNMP shromažďuje informace o systému a provádí funkce, které vyžadují správci vzdálených sítí SNMP.

Jak zabránit v přístupu SNMP

Pokud chcete, aby *nikdo* ve vašem systému nemohl používat SNMP pro přístup k vašemu systému, měli byste zabránit spuštění serveru SNMP. Postupujte takto:

__ Krok 1. Chcete-li zabránit automatickému spuštění úloh serveru SNMP při spuštění TCP/IP, napište tento příkaz:

```
CHGSNMPA AUTOSTART(*NO)
```

Poznámky:

1. AUTOSTART(*YES) je předvolená hodnota.
2. Další informace o tom, jak řídit, které servery TCP/IP se spouštějí automaticky, uvádí část “Jak určit, které servery TCP/IP se mají spouštět automaticky” na stránce 114.

__ Krok 2. Pokud nechcete nikomu dovolit přiřadit uživatelskou aplikaci, jako například aplikaci typu soket, k portu, který systém obvykle používá pro SNMP, postupujte takto:

__ Krok a. Napište příkaz GO CFGTCP. Zobrazí se menu Konfigurace TCP/IP.

__ Krok b. Vyberte volbu 4 (Práce s omezením portu TCP/IP).

__ Krok c. Na obrazovce Práce s omezením portu TCP/IP zadejte volbu 1 (Přidat).

__ Krok d. Pro spodní rozsah portu zadejte hodnotu 161.

__ Krok e. Pro horní rozsah portu zadejte hodnotu *ONLY.

Poznámky:

1. Omezení portu nabudou platnosti při příštím spuštění TCP/IP. Jestliže je během nastavování omezení portu protokol TCP/IP aktivní, měli byste TCP/IP ukončit a opět ho spustit.
2. RFC1700 obsahuje informace o obecných přiřazeních čísel portů.

__ Krok f. Pro protokol zadejte hodnotu *TCP.

__ Krok g. Do pole uživatelského profilu zadejte jméno uživatelského profilu, který je chráněn ve vašem systému. (Chráněný uživatelský profil, který nevlastní programy přebírající oprávnění a který nemá heslo, jež je známo ostatním uživatelům.) Tím, že omezíte port na určitého uživatele, automaticky vyřadíte všechny ostatní uživatele.

__ Krok h. Kroky 2c až 2g zopakujte pro protokol *UDP.

Řízení přístupu SNMP

Pokud chcete, aby správci SNMP měli přístup k systému, měli byste zvážit tyto otázky týkající se zabezpečení:

- Někdo, kdo má přístup do vaší sítě pomocí protokolu SNMP, může shromáždit informace o vaší síti. Informace, které jste skryli pomocí aliasů a serveru jmen domény, se stávají dostupnými pro případného vetřelce využívajícího protokol SNMP. Kromě toho by mohl vetřelec použít protokol SNMP k upravení vaší konfigurace sítě a narušit tak vaši komunikaci.
- Protokol SNMP spoléhá v přístupu na jméno komunity. Jméno komunity je v podstatě podobné heslu. Jméno komunity není zašifrováno. Proto je náchylné k útokům typu ″sniffing″. Můžete použít příkaz ADDCOMSNMP (Přidání komunity pro SNMP) k nastavení parametru INTNETADR (internetová adresa správce) na jednu nebo více specifických IP adres místo hodnoty *ANY. Chcete-li správcům v komunitě znemožnit přístup k objektům MIB, můžete také nastavit parametr OBJACC příkazu ADDCOMSNMP nebo CHGCOMSNMP na hodnotu *NONE. Toto opatření je určeno pouze pro dočasné použití, kterým se zamítne přístup pro správce v komunitě, aniž by byla tato komunita odstraněna.

Pokyny k zabezpečení pro server INETD

Na rozdíl od většiny serverů TCP/IP server INETD nezajišťuje pro klienty pouze jednu jedinou službu. Místo toho poskytuje celou škálu nejrůznějších služeb, které mohou administrátoři přizpůsobovat. Z toho důvodu bývá server INETD někdy označován jako ″super server″. Server INETD obsahuje následující vestavěné služby:

- time
- daytime
- echo
- discard
- changed

Tyto služby jsou podporovány jak pro protokol TCP, tak pro protokol UDP. V případě protokolu UDP obdrží služby echo, time, daytime a changed pakety UDP a pak tyto pakety odešlou zpět původci. Server echo zopakuje (jako ozvěna) pakety, které obdrží, servery time a daytime vygenerují čas v určitém formátu a pošlou ho zpět a server changed vygeneruje paket tisknutelných znaků ve formátu ASCII a odešle ho zpět.

Podstata těchto služeb UDP činí systém náchylným k napadení typu zamítnutí služby. Například předpokládejme, že máte dva servery iSeries: SYSTEMA a SYSTEMB. Zlomyslný programátor by mohl vymyslet záhlaví IP a záhlaví UDP se zdrojovou adresou systému SYSTEMA a číslem portu UDP serveru time. Potom může odeslat tento paket na server time v systému SYSTEMB, který odešle čas do systému SYSTEMA, jenž odpoví zpět systému SYSTEMB, a tak dále, čímž se vygeneruje nekonečná smyčka, která bude spotřebovávat prostředky CPU v obou systémech, stejně tak jako šířku pásma sítě.

Proto byste měli zvážit riziko takového napadení vašeho systému iSeries a tyto služby byste měli spouštět pouze v zabezpečené síti. Server INETD je dodáván tak, že se automaticky nespustí při spuštění TCP/IP. Můžete nakonfigurovat, zda se mají služby spouštět, když se spustí INETD, či nikoliv. Standardně se servery time a daytime pro TCP i pro UDP spouští, když spustíte server INETD.

Pro server INETD existují dva konfigurační soubory:

```
/QIBM/UserData/OS400/inetd/inetd.conf
/QIBM/ProdData/OS400/inetd/inetd.conf
```

Tyto soubory určují, které programy se spustí, když se spustí server INETD. Také určují, pod kterým uživatelským profilem tyto programy poběží, kdy je server INETD spustí.

Poznámka: Konfigurační soubor v adresáři proddata byste nikdy neměli upravovat. Nahrazuje se pokaždé, když se znovu zavádí systém. Zákaznické změny konfigurace by se měly provádět pouze v souboru v adresářovém stromu userdata, jelikož tento soubor **není** aktualizován během přechodů na vyšší vydání.

Pokud zlomyslný programátor získal přístup k těmto souborům, mohl by je nakonfigurovat tak, aby spouštěly nějaký program, když se spustí server INETD. Proto je velmi důležité chránit tyto soubory. Standardně je k provádění jejich změn požadováno oprávnění QSECOFR. Oprávnění požadované pro přístup k nim byste neměli snižovat.

Poznámka: Konfigurační soubor v adresáři ProdData byste neměli upravovat. Tento soubor se nahrazuje pokaždé, když se znovu zavádí systém. Zákaznické změny konfigurace by se měly provádět pouze v souboru v adresářovém stromu UserData, jelikož tento soubor není aktualizován během přechodů na vyšší vydání.

Pokyny k zabezpečení pro omezení průchodů TCP/IP

Pokud je váš systém zapojen v síti, budete možná chtít omezit schopnost uživatelů procházet sítí pomocí aplikací TCP/IP. Jedním způsobem, jak to provést, je omezit přístup k následujícím klientským příkazům TCP/IP:

Poznámka: Tyto příkazy mohou existovat v několika knihovnách ve vašem systému. Minimálně jsou uloženy v knihovnách QSYS a QTCP. Ujistěte se, že jste našli a zabezpečili všechny jejich výskyty.

- STRTCPFTP
- FTP
- STRTCPTELN
- TELNET
- LPR
- SNDTCPSPLF
- RUNRMTCMD (klient REXEC)

Možná místa určení vašich uživatelů jsou dána těmito položkami:

- Položky ve vaší hostitelské tabulce TCP/IP.
- Položka *DFTROUTE ve směrovací tabulce TCP/IP. To umožňuje uživatelům zadat IP adresu dalšího uzlu, je-li jejich místem určení neznámá síť. Uživatel může dosáhnout nebo kontaktovat vzdálenou síť s využitím předvolené přenosové cesty.
- Konfigurace vzdáleného serveru jmen. Tato podpora umožňuje jinému serveru v síti nalézt hostitelská jména pro vaše uživatele.
- Tabulka vzdáleného systému.

Je třeba, abyste řídili, kdo může přidávat položky do těchto tabulek a měnit vaši konfiguraci. Také byste měli znát dopady položek v tabulkách a vaší konfigurace.

Uvědomte si, že zkušený uživatel s přístupem ke kompilátoru ILE C může vytvořit program typu soket, který se může připojit k portu TCP nebo UDP. Provedení této akce můžete ztížit tím, že omezíte přístup k následujícím souborům soketových rozhraní v knihovně QSYSINC:

- SYS
- NETINET
- H
- ARPA
- sokety a SSL

U servisních programů můžete omezit použití aplikací typu soket a aplikací SSL, které jsou již zkompilovány, na základě omezení použití těchto servisních programů:

- QSOSRV1
- QSOSRV2
- QSOSKIT(SSL)
- QSOSSLSR(SSL)

Servisní programy jsou dodávány s veřejným oprávněním *USE. Toto oprávnění však lze změnit na hodnotu *EXCLUDE (nebo jinou požadovanou hodnotu).

Kapitola 14. Zabezpečení přístupu prostřednictvím pracovní stanice

Mnoho vašich systémových uživatelů používá osobní počítače (PC) jako pracovní stanice. Používají nástroje, které se zpracovávají na PC, a PC používají k připojení k serveru iSeries.

Většina metod připojení PC k serverům iSeries poskytuje více funkcí než emulace pracovní stanice. PC se může vůči serveru iSeries jevit jako obrazovka a může pro uživatele zajišťovat interaktivní přihlašovací relace. Kromě toho se PC může jevit serveru iSeries jako jiný počítač a poskytovat funkce typu přenos souborů a vzdálené volání procedur.

Jako administrátor serveru iSeries musíte znát toto:

- Funkce, které jsou k dispozici uživatelům PC, jež jsou připojeni k vašemu systému.
- Prostředky serveru iSeries, k nimž mají přístup uživatelé PC.

Možná budete chtít potlačit pokročilé funkce PC (např. přenos souborů nebo vzdálené volání procedur), pokud vaše schéma zabezpečení serveru iSeries ještě není na tyto funkce připraveno. Vaším pravděpodobným dlouhodobým cílem je umožnit pokročilé funkce PC, ale zároveň chránit informace ve vašem systému. V následujících částech jsou rozebrány některé otázky zabezpečení, které se vztahují k přístupu PC.

Prevence virů z pracovních stanic

Zde najdete návrhy, jakými způsoby se mohou administrátoři systému bránit proti PC virům.

Zabezpečení přístupu k datům pracovní stanice

Některý software klientů PC používá sdílené pořadače k ukládání informací na server. Pro účely přístupu k databázovým souborům serveru iSeries má uživatel PC omezenou, dobře definovanou sadu rozhraní. Díky schopnosti přenosu souborů, která je součástí většiny softwarového vybavení klienta/serveru, může uživatel PC kopírovat soubory mezi serverem a PC. Prostřednictvím schopnosti databázového přístupu, jako je např. soubor DDM, vzdálený SQL nebo ovladač ODBC, má uživatel zajištěn přístup k datům na serveru.

V tomto prostředí můžete vytvářet programy, které podchytí a ohodnotí požadavky uživatelů PC na přístup k prostředkům serveru. Když požadavky používají soubor DDM, zadejte ukončovací program do atributu sítě DDMACC (přístup k požadavku DDM). Pro některé metody přenosu souborů PC se ukončovací program zadává do atributu sítě PCSACC (přístup k požadavku klienta). Nebo můžete zadat PCSACC (*REGFAC), aby se použila funkce registrace. Jestliže požadavky používají pro přístup k datům jiné funkce serveru, můžete pomocí příkazu WRKREGINF registrovat ukončovací programy pro tyto funkce serveru.

Ukončovací programy však není snadné navrhnout a jen výjimečně bývají zcela spolehlivé. Ukončovací programy nenahrazují oprávnění k objektu, které je navrženo tak, aby chránilo vaše objekty před neautorizovaným přístupem z libovolného zdroje.

Některý klientský software, jako např. produkt IBM iSeries Access for Windows, používá integrovaný systém souborů za účelem ukládání dat a přístupu k datům na serverech iSeries. Díky integrovanému systému souborů se celý server stává snáze dostupným pro uživatele PC. Oprávnění k objektu je stále nepostradatelnější. Prostřednictvím integrovaného systému souborů si může uživatel s dostatečným oprávněním prohlížet knihovnu serveru stejně, jako

by to byl adresář na PC. Jednoduché příkazy pro přesun a kopírování mohou ihned přesunout data z knihovny serveru iSeries do adresáře PC a naopak. Systém automaticky provádí odpovídající změny ve formátu dat.

Poznámky:

1. K řízení použití objektů v systému souborů QSYS.LIB můžete využít seznam oprávnění. Další informace najdete v části “Omezení přístupu k systému souborů QSYS.LIB” na stránce 93.
2. Kapitola 11, “Použití integrovaného systému souborů k zabezpečení souborů”, na stránce 87 uvádí podrobnější informace o otázkách zabezpečení v souvislosti s integrovaným systémem souborů.

Předností integrovaného systému souborů je jeho jednoduchost pro uživatele i vývojáře. S využitím jednoduchého rozhraní může uživatel pracovat s objekty v několika prostředích. Uživatel PC nepotřebuje pro přístup k objektům zvláštní software nebo rozhraní API. Místo toho může využívat jemu dobře známé příkazy PC nebo metodu “ukázat a klepnout” pro přímou práci s objekty.

Pro všechny systémy, které mají připojené PC, ale především pro systémy s klientským softwarem, který používá integrovaný systém souborů , je nezbytností dobré schéma oprávnění k objektům. Jelikož je zabezpečení integrováno do produktu OS/400, musí veškeré požadavky na přístup k datům procházet procesem kontroly oprávnění. Kontrola oprávnění se vztahuje na požadavky z libovolného zdroje a na přístup k datům, který používá libovolné metody.

Oprávnění k objektu a přístup prostřednictvím pracovní stanice

Když nastavujete oprávnění pro objekty, musíte vyhodnotit, co toto oprávnění umožňuje uživateli PC. Když má uživatel k souboru například oprávnění *USE, může si prohlížet nebo tisknout data v daném souboru. Uživatel nemůže změnit informace v souboru nebo vymazat soubor. Pro uživatele PC je prohlížení ekvivalentem “čtení”, které mu poskytuje dostatečné oprávnění ke zkopírování souboru na PC. To možná není to, co byste měli v úmyslu.

Pro některé kritické soubory možná budete muset nastavit veřejné oprávnění na hodnotu *EXCLUDE, abyste zabránili načtení. Potom můžete poskytnout jinou metodu pro “prohlížení” souboru na serveru, jako je např. použití menu a programů, které přebírají oprávnění.

Další možností prevence načtení je použít ukončovací program, který se spustí vždy, když uživatel PC spustí nějakou funkci serveru (jinou než interaktivní přihlášení). Ukončovací program můžete zadat do atributu sítě PCSACC pomocí příkazu CHGNETA (Změna atributu sítě). Nebo můžete ukončovací programy registrovat pomocí příkazu WRKREGINF (Práce s informacemi o registraci). Metoda, kterou použijete závisí na tom, jakým způsobem PC přistupují k datům ve vašem systému a jaký klientský program PC používají. Ukončovací program (QIBM_QPWFS_FILE_SERV) se používá pro produkt iSeries Access a pro přístup serveru Net Server k IFS. Nebrání přístupu z PC s využitím jiných mechanismů, např. FTP nebo ODBC.

Software PC obvykle zajišťuje také schopnost odeslání, takže uživatel může kopírovat data z PC do databázového souboru serveru. Pokud nemáte správně nastaveno schéma oprávnění, mohl by uživatel PC překrýt všechna data v souboru daty z PC. Oprávnění *CHANGE je třeba přiřazovat velmi obezřetně. Přehled oprávnění, která jsou potřebná pro jednotlivé operace se soubory, obsahuje dodatek D publikace *Zabezpečení iSeries - referenční informace Reference*.

Další informace o oprávnění pro funkce PC a o použití ukončovacích programů najdete v rámci aplikace iSeries Information Center. Další podrobnosti uvádí část “Nezbytné předchozí a související informace” na stránce xii.

Administrativa aplikací

Administrativa aplikací je volitelně instalovatelnou komponentou produktu iSeries Navigator, grafického uživatelského rozhraní (GUI) pro server iSeries. Administrativa aplikací umožňuje administrátorům systému řídit funkce nebo aplikace dostupné uživatelům nebo skupinám na určitém serveru. To zahrnuje řízení funkcí dostupných uživatelům, kteří k serveru přistupují prostřednictvím klientů. Zde je důležité si povšimnout, že pokud k serveru přistupujete z klienta Windows, určuje uživatel serveru iSeries, a nikoliv uživatel Windows, které funkce budou k dispozici pro administraci.

Podrobnou dokumentaci k Administrativě aplikací produktu iSeries Navigator najdete v tématu iSeries Information Center–>Připojení k iSeries—>K čemu se připojit—>iSeries Navigator (../html/as400/v5r2/ic2924/info/rzaj3/rzaj3overview.htm).

Administrace metod

Metody jsou nástrojem administrátorů, který slouží ke konfiguraci softwaru na klientských PC. Metody mohou vymezit, ke kterým funkcím a aplikacím má uživatel přístup na PC. Metody mohou také navrhovat nebo přikazovat, jaké konfigurace mají použít určití uživatelé nebo určité PC.

Poznámka: Metody nezajišťují kontrolu nad prostředky serveru. Nejsou proto náhradou za zabezpečení serveru. Metody lze použít k ovlivnění způsobu, jakým je produkt iSeries Access schopný přistupovat k serveru z konkrétního PC a konkrétního uživatele. Nemění však způsob, jakým lze k prostředkům serveru přistupovat prostřednictvím jiných mechanismů.

Metody jsou uloženy na souborovém serveru. Pokaždé, když se uživatel přihlásí k pracovní stanici Windows, načtou se ze souborového serveru metody, které se vztahují na daného uživatele Windows. Metody se aplikují na registr dříve, než uživatel na pracovní stanici cokoliv provede.

Metody Microsoft versus Administrativa aplikací

Produkt iSeries Access Express podporuje dvě různé strategie pro implementaci administrativního řízení v rámci vaší sítě: metody Microsoft a Administrativu aplikací, která je komponentou produktu iSeries Navigator. Když se budete rozhodovat, která strategie je pro vaše potřeby vhodnější, zvažte následující skutečnosti.

Metody systému Microsoft

Metody jsou řízené PC, nezávislé na určitém vydání operačního systému OS/400. Metody se mohou aplikovat na PC, stejně tak jako na uživatele Windows. To znamená, že se uživatelé odkazují na uživatelský profil Windows, nikoliv na uživatelský profil serveru. Metody lze použít ke ″konfiguraci″ i k omezení. Ve srovnání s Administrativou aplikací vykazují metody obvykle větší nespojitost a mohou nabízet širší škálu funkcí. Je to způsobeno tím, že k určení, zda uživatel může funkci použít, či nikoliv, není potřeba připojení k serveru. Implementace metod je poněkud složitější než implementace Administrativy aplikací, neboť je k tomu nutné použít editor metod systému Microsoft a navíc musí být PC přímo nakonfigurován pro načtení metod.

Administrativa aplikací produktu iSeries Navigator

Administrativa aplikací sdružuje data s uživatelským profilem místo s profilem Windows, s nímž se asociují metody systému Microsoft. Zatímco k používání Administrativy aplikací jsou požadovány servery iSeries s verzí operačního systému OS/400 V4R3 nebo vyšší, jsou některé funkce dostupné pouze ve verzi V4R4 nebo vyšší. Administrativa aplikací používá k administraci grafické uživatelské rozhraní produktu iSeries Navigator, jehož použití je výrazně jednodušší než použití editoru metod. Informace Administrativy aplikací se vztahují na uživatele bez ohledu na to, z kterého PC se přihlásil. Určité funkce v rámci produktu iSeries Navigator mohou být vyhrazené. Administrativa aplikací je preferovanou variantou, pokud všechny funkce, které vyžadujete k omezení, podporují Administrativu aplikací a pokud použitá verze operačního systému OS/400 podporuje Administrativu aplikací.

Použití SSL s produktem iSeries Access for Windows

Informace o použití produktu iSeries Access Express s SSL najdete v rámci aplikace iSeries Information Center pod hesly *Administrace SSL (Secure Sockets Layer), Zabezpečení iSeries Access Express a iSeries Navigator, iSeries Developer Kit for Java a iSeries Java Toolbox* v hlavním tématu Java. Tyto informace si rovněž můžete prohlédnout na CD, který jste obdrželi s vaším systémem.

Zabezpečení produktu iSeries Navigator

Produkt iSeries Navigator poskytuje snadno použitelné rozhraní k vašemu serveru těm uživatelům, kteří mají produkt iSeries Access. S každým novým vydáním operačního systému OS/400 přibývá funkcí serveru, které jsou dostupné prostřednictvím produktu iSeries Navigator. Snadno použitelné rozhraní přináší řadu výhod, včetně nižších nákladů na technickou podporu a lepšího vzhledu vašeho systému. Kromě toho představuje výzvy v oblasti zabezpečení.

Jako administrátor systému nemůžete již při ochraně zdrojů nadále spoléhat na neznalost vašich uživatelů. Produkt iSeries Navigator vašim uživatelům ulehčuje a zviditelňuje řadu funkcí. Je třeba navrhnout a implementovat metody zabezpečení pro uživatelské profily a objekty tak, aby byly splněny vaše potřeby v oblasti zabezpečení.

Produkt IBM e(logo)server iSeries Access for Windows verze V4R4 nebo vyšší verze nabízí následující metody řízení funkcí, které mohou uživatelé provádět prostřednictvím produktu iSeries Navigator:

- Výběrová instalace.
- Administrativa aplikací.
- Podpora metod systému Windows NT.

Produkt iSeries Navigator je sbalen do několika komponent, které můžete nainstalovat samostatně. Díky tomu můžete nainstalovat pouze ty funkce, které potřebujete. Administrativa aplikací umožňuje administrátorovi řídit funkce, k nimž má uživatel nebo skupina přístup prostřednictvím produktu iSeries Navigator. Administrativa aplikací sdružuje aplikace do následujících kategorií:

iSeries Navigator
Zahrnuje produkt iSeries Navigator a libovolné programy typu plug-in.

Aplikace typu klient
Zahrnuje všechny aplikace typu klient, včetně produktu iSeries Access, jenž na klientech poskytuje funkce, které jsou spravovány prostřednictvím Administrativy aplikací.

Hostitelské aplikace
Zahrnuje všechny aplikace, které jsou uloženy na vašem serveru a poskytují funkce, jež jsou spravovány prostřednictvím Administrativy aplikací.

Výběrovou instalaci, administrativu aplikací i metody můžete použít k omezení funkcí produktu iSeries Navigator, k nimž má uživatel přístup. Žádná z těchto metod by se však neměla používat pro zabezpečení na úrovni prostředků.

Počínaje verzí V4R4, produkt IBM e(logo)server iSeries Access for Windows podporuje také použití editoru metod systému Windows NT k řízení toho, jaké funkce lze provádět z určitého klienta PC bez ohledu na to, kdo tento PC používá.

Další informace o výběrové instalaci, administrativě aplikací a administraci metod najdete v rámci aplikace iSeries Information Center. Administrativě aplikací se věnuje také část “Omezený přístup k funkci programů” na stránce 5 této publikace.

Jak zabránit v přístupu ODBC

ODBC (Open DataBase Connectivity) je nástroj, který mohou využívat PC aplikace k přístupu k datům serveru iSeries, jako by to byla data PC. Programátor ODBC může uživateli PC aplikace zprůhlednit fyzické umístění dat. Další informace týkající se pokynů k zabezpečení ODBC najdete pod tématem ″Zabezpečení iSeries Access for Windows ODBC″ (/rzaii/rzaiiodbc09.HTM) v rámci aplikace iSeries Information Center.

Pokyny k zabezpečení pro hesla pracovních stanic

Obvykle, když uživatel PC spustí software pro připojení, jako je např. iSeries Access, napíše uživatel jednou uživatelské ID a heslo pro daný server. Heslo se zašifruje a uloží do paměti PC. Kdykoliv uživatel naváže novou relaci se stejným serverem, PC automaticky odešle uživatelské ID a heslo.

Některý software klienta/serveru rovněž umožňuje přeskočit přihlašovací obrazovku pro interaktivní relace. Software odešle uživatelské ID a zašifrované heslo, když uživatel zahájí interaktivní relaci (emulaci 5250). Aby byla tato volba podporovaná, musí být systémová hodnota QRMTSIGN na serveru nastavena na hodnotu *VERIFY.

Když se rozhodnete umožnit vynechání přihlašovací obrazovky, měli byste zvážit spojitost se zabezpečením.

Bezpečnostní riziko: Pro emulaci 5250 nebo libovolný jiný typ interaktivní relace je přihlašovací obrazovka stejná jako všechny ostatní obrazovky. Ačkoliv se heslo na obrazovce při zadávání nezobrazuje, je odesláno přes linku v nezašifrované formě jako všechna ostatní datová pole. U některých typů spojení to může případnému vetřelci poskytnout příležitost monitorovat spojení a odhalit uživatelské ID a heslo. Monitorování spojení s využitím elektronických přístrojů se často nazývá jako **útok typu ″sniffing″**. Počínaje verzí V4R4 můžete k šifrování komunikace mezi iSeries Access a servery iSeries používat SSL (Secure Socket Layer). To chrání vaše data, včetně hesel, před útoky typu ″sniffing″.

Když se rozhodnete pro vynechání přihlašovací obrazovky, zašifruje PC heslo dříve, než jej odešle. Díky šifrování se vyvarujete možnosti ukradení hesla na základě útoku typu ″sniffing″. Musíte však zajistit, aby vaši uživatelé PC dodržovali provozní praktiky zabezpečení. Plně automatizovaný PC s aktivní relací se systémem iSeries může pro někoho představovat příležitost spustit jinou relaci bez znalosti uživatelského ID a hesla. PC by měly být nastaveny tak, aby se zablokovaly, když je systém po delší dobu neaktivní, a aby k obnovení relace vyžadovaly zadání hesla.

I když se pro vynechání přihlašovací obrazovky nerozhodnete, představuje plně automatizovaný PC s aktivní relací bezpečnostní riziko. S využitím softwaru PC může někdo

spustit relaci serveru a získat přístup k datům, aniž by musel znát uživatelské ID a heslo. Riziko při emulaci 5250 je o něco vyšší, neboť spuštění relace a získání přístupu k datům vyžaduje méně znalostí.

Také byste měli poučit vaše uživatele o důsledcích odpojení jejich relace iSeries Access. Mnoho uživatelů předpokládá (sice logicky, ale nesprávně), že volba odpojení zcela ukončí jejich spojení se serverem. Ve skutečnosti, když uživatel vybere volbu odpojení, dá server relaci (licenci) uživatele k dispozici pro jiného uživatele. Spojení klienta se serverem je však nadále otevřené. Jiný uživatel by mohl vstoupit do nechráněného PC a získat přístup k prostředkům serveru, aniž by kdy zadal uživatelské ID a heslo.

Vašim uživatelům, kteří potřebují odpojit své relace, můžete navrhnout tyto dvě možnosti:

- Zajistit, aby měl jejich PC funkci zablokování, která vyžaduje heslo. Tím se plně automatizovaný PC stává nedostupným pro kohokoliv, kdo nezná heslo.
- Zcela odpojit relaci, buď se odhlásit z Windows nebo znovu spustit PC (znovu zavést operační systém). Tím se ukončí relace se serverem iSeries.

Vaše uživatele byste měli rovněž poučit o možných bezpečnostních rizikách, když používají produkt iSeries Access for Windows. Když uživatel zadá UNC (univerzální konvence pojmenování) za účelem identifikace prostředku serveru iSeries, vytvoří klient Win95 nebo NT síťové spojení se serverem. Protože uživatel uvedl UNC, neuvidí ho jako mapovanou síťovou jednotku. Uživatel si často není vůbec vědom existence připojení do sítě. Toto připojení do sítě však představuje bezpečnostní riziko u plně automatizovaného PC, neboť server se v adresářovém stromu PC objevuje jako adresář. Pokud relace uživatele má účinný uživatelský profil, mohly by být prostředky serveru na plně automatizovaném PC nechráněny. Stejně jako v předchozím příkladu je řešením zajistit, aby uživatelé znali rizika a aby používali funkci zablokování PC.

Ochrana serveru před vzdálenými příkazy a procedurami

Zkušený uživatel PC se softwarem, jako je iSeries Access, může spouštět příkazy na serveru, aniž by prošel přihlašovací obrazovkou. Níže je uvedeno několik metod, které mohou uživatelé PC použít ke spuštění příkazů serveru. Metody, které mají uživatelé PC k dispozici, určuje váš software klienta/serveru.

- Uživatel může otevřít soubor DDM a použít funkci vzdáleného příkazu ke spuštění příkazu.
- Některý software, jako např. optimalizovaní klienti iSeries Access, poskytuje funkci vzdáleného příkazu prostřednictvím rozhraní API DPC (Volání distribuovaného programu) bez použití DDM.
- Některý software, jako např. vzdálený SQL a ODBC, poskytuje funkci vzdáleného příkazu bez DDM nebo DPC.

Pro software klienta/serveru, který k podpoře vzdálených příkazů používá DDM, můžete použít atribut sítě DDMACC, chcete-li zcela zabránit spouštění vzdálených příkazů. U softwaru klienta/serveru, který používá jinou podporu serveru, můžete pro server registrovat ukončovací program. Pokud chcete umožnit vzdálené příkazy, musíte se ujistit, že vaše schéma oprávnění k objektům odpovídajícím způsobem chrání vaše data. Schopnost vzdálených příkazů je obdobná, jako kdybyste uživateli zpřístupnili příkazovou řádku. Kromě toho, když server iSeries přijme vzdálený příkaz přes DDM, nevynutí systém nastavení hodnoty LMTCPB (omezení schopností) u uživatelských profilů.

Ochrana pracovních stanic před vzdálenými příkazy a procedurami

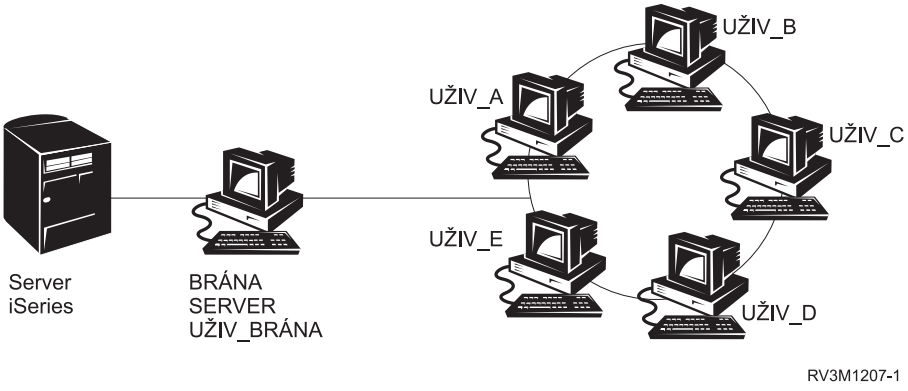
Produkt IBM iSeries Access for Windows umožňuje přijímání vzdálených příkazů na PC. Chcete-li ze serveru spustit proceduru na připojeném PC, můžete na serveru použít příkaz RUNRMTCMD (Spuštění vzdáleného příkazu). Schopnost RUNRMTCMD je cenným nástrojem pro administrátora systému a personál v rámci služby help-desk. Zároveň však nabízí příležitost pro zničení dat na PC, ať už záměrné či neúmyslné.

PC nemají stejné funkce oprávnění k objektům jako servery iSeries. Nejlepší ochranou před problémy s příkazem RUNRMTCMD je pečlivě omezit uživatele systému, kteří k tomuto příkazu mají přístup. Produkt IBM iSeries Access for Windows poskytuje schopnost registrovat, kteří uživatelé mohou spouštět vzdálené příkazy na určitém PC. Když je spojení navázáno přes TCP/IP, můžete k řízení přístupu ke vzdáleným příkazům použít ovládací panel vlastností na klientovi. Uživatelům můžete poskytnout oprávnění pomocí uživatelského ID nebo jména vzdáleného systému. Pokud je spojení navázáno přes SNA, poskytuje některý klientský software schopnost nastavit zabezpečení konverzace. U jiného klientského softwaru jednoduše zvolíte, zda se má či nemá nastavit schopnost příchozích příkazů.

Pro každou kombinaci klientského softwaru a typu spojení (např. TCP/IP nebo SNA) musíte přezkoumat potenciální možnost příchozích příkazů do připojených PC. V dokumentaci klienta vyhledejte informace k heslům "příchozí příkaz" nebo "RUNRMTCMD". Buďte připraveni poradit uživatelům PC a správcům sítě ohledně správného (bezpečného) nakonfigurování klientů, pokud chtějí tuto schopnost povolit nebo znemožnit.

Gateway servery

Váš systém může být zapojen v síti s pomocným serverem nebo gateway serverem mezi systémem iSeries a PC. Systém iSeries může být například připojen k síti LAN pomocí serveru PC, k němuž jsou připojeny PC. Otázky zabezpečení v této situaci závisí na schopnostech softwaru, který je spuštěn na gateway serveru. Obrázek 13 znázorňuje příklad konfigurace s gateway serverem:



Obrázek 13. Systém iSeries s gateway serverem

S některým softwarem váš systém iSeries nebude vědět o žádných uživatelích (jako je např. USERA nebo USERC), kteří jsou po směru od gateway serveru. Server se přihlásí do systému jako jediný uživatel (USERGTW). Ke zpracování všech požadavků od uživatelů po směru použije uživatelské ID USERGTW. Požadavek od uživatele USERA se bude serveru jevit jako požadavek od uživatele USERGTW.

V takovém případě musíte s prosazením zabezpečení spoléhat na gateway server. Je třeba pochopit a řídit schopnosti zabezpečení gateway serveru. Z hlediska serveru iSeries má každý uživatel stejné oprávnění jako uživatelské ID, které gateway server používá k zahájení

relace. Mohli byste si to představit jako ekvivalent spuštění programu, který přebírá (adoptuje) oprávnění a poskytuje přístup k příkazové řádce.

U jiného softwaru předává gateway server požadavky od jednotlivých uživatelů serverům iSeries. Server iSeries ví, že uživatel USERA žádá o přístup k určitému objektu. Brána je pro systém téměř průhledná.

Je-li váš systém v síti, jež obsahuje gateway servery, musíte vyhodnotit, kolik oprávnění je vhodné poskytnout uživatelským ID, která jsou používána gateway servery. Měli byste se také seznámit s následujícím:
- Mechanismy zabezpečení, které vynucují gateway servery.
- Jak se uživatelé po směru budou jevit vašemu systému iSeries.

Komunikace přes bezdrátovou síť LAN

Někteří klienty mohou používat bezdrátovou síť LAN serveru iSeries (iSeries Wireless LAN), která jim umožňuje komunikovat s vaším systémem bez drátového spojení. Bezdrátová síť LAN serveru iSeries používá komunikační technologii na bázi rádiové frekvence. Jako administrátor systému byste si měli uvědomit následující vlastnosti produktů bezdrátové sítě LAN serveru iSeries:

- Tyto produkty bezdrátové sítě LAN používají technologii širokého spektra. Stejnou technologii v minulosti používala vláda k zabezpečení rádiového přenosu. Někomu, kdo se pokouší elektronicky monitorovat přenos dat, se přenos jeví spíše jako šum než jako skutečný přenos.
- Bezdrátové spojení má tyto tři konfigurační parametry týkající se zabezpečení:
  - přenosová rychlost dat (dvě možné rychlosti)
  - frekvence (pět možných frekvencí)
  - identifikátor systému (8 milionů možných identifikátorů)

  Kombinací těchto konfiguračních prvků vzniká 80 milionů možných konfigurací, díky čemuž je pravděpodobnost uhodnutí správné konfigurace nějakým hackerem mimořádně malá.
- Stejně jako u jiných komunikačních metod je zabezpečení bezdrátového spojení ovlivněno zabezpečením klientského zařízení. Informace o ID systému a další konfigurační parametry jsou uloženy v souboru na klientském zařízení a měly by být chráněny.
- Pokud se bezdrátové zařízení ztratí nebo ho někdo odcizí, zajišťují běžná bezpečnostní opatření serveru, jako jsou přihlašovací hesla a zabezpečení objektů, ochranu pro případ, že by se nějaký neautorizovaný uživatel pokoušel využít ztracenou nebo odcizenou jednotku za účelem přístupu k vašem systému.
- Pokud dojde ke ztrátě nebo odcizení bezdrátové klientské jednotky, měli byste zvážit, zda neprovést změnu informací o ID systému pro všechny uživatele, přístupové body a systémy. Uvažujte o tom stejně, jako o výměně zámku u dveří, když by vám někdo ukradl klíče.
- Možná budete chtít rozdělit váš server na skupiny klientů, kteří mají jedinečné ID systému. Tím omezíte dopad případné ztráty nebo odcizení jednotky. Tuto metodu lze aplikovat pouze tehdy, když jste schopni vymezit skupinu uživatelů na určitou část vaší instalace.
- Na rozdíl od drátové technologie LAN je bezdrátová technologie LAN chráněná. Proto nejsou pro tyto bezdrátové produkty LAN veřejně dostupná žádná elektronická odposlouchávací zařízení. Odposlouchávací zařízení je elektronické zařízení, které provádí neoprávněné monitorování přenosu.

Kapitola 15. Bezpečnostní ukončovací programy

Některé funkce iSeries poskytují ukončení, takže váš systém může spustit uživatelem vytvořený program, který provede dodatečnou kontrolu a ověření. Například můžete svůj systém nastavit tak, že spustí ukončovací program pokaždé, když se někdo pokusí otevřít soubor DDM (distributed data management) ve vašem systému. Ke specifikování ukončovacích programů, které mají být spouštěny za určitých podmínek, můžete použít registrační funkci.

Některé publikace týkající se serverů iSeries obsahují příklady ukončovacích programů, které provádějí funkce zabezpečení. Tabulka 24 obsahuje seznam těchto ukončovacích programů a zdrojů pro vzorové programy.

Tabulka 24. Zdroje vzorových ukončovacích programů

Typ ukončovacího programu	**Účel**	**Kde najdete příklady**
Ověření platnosti hesla	Systémová hodnota QPWDVLDPGM může specifikovat jméno programu nebo indikuje, že mají být použity ověřovací programy registrované pro výstupní bod QIBM_QSY_VLD_PASSWRD za účelem kontroly nového hesla pro dodatečné požadavky, které nejsou zpracovávány systémovými hodnotami QPWDxxx. Použití tohoto programu by mělo být pečlivě monitorováno, protože přijímá nezašifrovaná hesla. Tento program **nesmí** ukládat hesla do souboru nebo je předávat jinému programu.	• Publikace *An Implementation Guide for iSeries Security and Auditing, GG24–4200*. • *Zabezpečení iSeries - referenční informace Reference*, SC09-3697-07
Přístup PC Support/400 nebo Client Access[1]	V parametru PCSACC (přístup k požadavku klienta) atributů sítě můžete specifikovat jméno tohoto programu za účelem řízení níže uvedených funkcí: • Funkce virtuální tiskárny. • Funkce přenosu souborů. • Funkce sdílení pořadačů typu 2. • Funkce zpráv produktu Client Access. • Datové fronty. • Funkce vzdáleného SQL.	Publikace *An Implementation Guide for iSeries Security and Auditing, GG24–4200*.
Přístup DDM (Distributed Data Management)	V parametru DDMACC (přístup k požadavku DDM) atributů sítě můžete specifikovat jméno tohoto programu za účelem řízení níže uvedených funkcí. • Funkce sdílení pořadačů typu 0 a 1. • Funkce spuštění vzdáleného příkazu (Submit Remote Command).	Publikace *An Implementation Guide for iSeries Security and Auditing, GG24–4200*.
Vzdálené přihlášení	V systémové hodnotě QRMTSIGN můžete specifikovat program za účelem řízení toho, kteří uživatelé budou automaticky přihlášeni nebo ze kterých míst (funkce přímého průchodu).	Publikace *An Implementation Guide for iSeries Security and Auditing, GG24–4200*.

Tabulka 24. Zdroje vzorových ukončovacích programů (pokračování)

Typ ukončovacího programu	**Účel**	**Kde najdete příklady**
ODBC (Open Database Connectivity) with iSeries Access[1]	Řízení níže uvedených funkcí ODBC: • Zda je vůbec ODBC povolena. • Které funkce jsou povoleny pro databázové soubory iSeries. • Které příkazy SQL jsou povoleny. • Které informace lze načíst o objektech databázového serveru. • Které funkce katalogu SQL jsou povoleny.	Nejsou k dispozici.
Program pro ošetření přerušení zpracování QSYSMSG	Můžete vytvořit program, který bude monitorovat frontu zpráv QSYSMSG a provede příslušnou akci (jako je oznámení administrátorovi zabezpečení) v závislosti na typu zprávy.	Publikace *An Implementation Guide for iSeries Security and Auditing, GG24–4200*.
TCP/IP	Některé servery TCP/IP (jako je FTP, TFTP, TELNET a REXEC) poskytují ukončovací programy. Tyto ukončovací programy máte možnost přidávat za účelem zpracování přihlášení a ověření uživatelských požadavků, jako jsou např. požadavky na získání nebo vložení specifického souboru. Dále můžete tyto ukončovací programy použít k zajištění anonymního FTP ve svém systému.	Téma "TCP/IP User Exits″ v publikaci *iSeries System API Reference*".
Změny uživatelských profilů	Máte možnost vytvářet ukončovací programy pro níže uvedené příkazy uživatelských profilů: CHGUSRPRF CRTUSRPRF DLTUSRPRF RSTUSRPRF	• *Zabezpečení iSeries - referenční informace Reference*, SC09-3697-07 • Téma "TCP/IP User Exits″ v publikaci *iSeries System API Reference*."

Poznámky:

1. Další informace o tomto tématu najdete v rámci aplikace iSeries Information Center. Další podrobnosti najdete v části "Nezbytné předchozí a související informace" na stránce xii.

Kapitola 16. Pokyny k zabezpečení pro webové prohlížeče

Mnoho uživatelů PC ve vaší organizaci má na své pracovní stanici webové prohlížeče. Mohou se připojit k Internetu. Mohou se rovněž připojit k vašemu serveru. Níže jsou uvedeny bezpečnostní pokyny jak pro PC, tak pro váš server.

Riziko: poškození pracovní stanice

Webová stránka, kterou váš uživatel navštíví, může mít asociovaný program, např. Java applet nebo ovladač Active-X nebo nějaký typ prostředku typu plug-in. I když se to vyskytuje vzácně, může takovýto typ programu po spuštění na PC způsobit poškození informací na PC. Jako administrátor systému byste měli vzít v úvahu níže uvedená opatření sloužící k ochraně osobních počítačů ve vaší organizaci.

- Pochopit volby v oblasti zabezpečení pro různé prohlížeče, které mají nainstalovány vaši uživatelé. Například u některých prohlížečů můžete řídit přístup, který mají Java applety mimo prohlížeč (omezené provozní prostředí Javy se nazývá *sandbox*). Tím můžete appletům zabránit v poškození dat na PC.

  Poznámka: Koncepce ″sandbox″ a související bezpečnostní omezení nejsou k dispozici pro ovladač Active-X a další prostředky typu plug-in.
- Poučit uživatele o vhodném nastavení prohlížeče. Pravděpodobně nemáte čas ani prostředky na to, abyste zajistili, že se vaši uživatelé budou řídit vašimi doporučeními. Proto je musíte informovat o možném riziku souvisejícím s nesprávným nastavením prohlížeče.
- Zvážit standardizaci webových prohlížečů a tím zajistit volby v oblasti zabezpečení, které potřebujete.
- Poučit uživatele, aby vás informovali o každém podezřelém chování nebo symptomech, které by mohly souviset s určitými webovými stránkami.

Riziko: přístup k adresářům serveru iSeries prostřednictvím mapovaných jednotek

Předpokládejme, že je PC připojen k vašemu serveru prostřednictvím relace produktu IBM iSeries Access for Windows. Relace nastaví mapované jednotky na spojení s integrovaným systémem souborů iSeries. Například jednotka **G** na PC se může namapovat na integrovaný systém souborů na serveru SYSTEM1 v síti.

Nyní předpokládejme, že tentýž uživatel PC má prohlížeč a má možnost přístupu na Internet. Uživatel požaduje webovou stránku, která provozuje potenciálně závadný ″program″, jako je Java applet nebo ovladač Active-X. Program se tudíž může pokusit vymazat cokoliv na jednotce G na PC.

Proti škodám na namapovaných jednotkách můžete bojovat několika prostředky:

- Vaší nejdůležitější ochranou je zabezpečení prostředků na serveru. Java applet nebo ovladač Active-X se pro server tváří jako uživatel, který vytvořil PC relaci. Musíte pečlivě řídit, kteří uživatelé PC jsou oprávněni tak činit na vašem serveru.
- Doporučte uživatelům PC, aby své prohlížeče nastavili tak, aby nebyl možný přístup na namapované jednotky. Tato ochrana funguje pro Java applety, není však účinná pro ovladače Active-X, které nepoužívají koncepci ″sandbox″.

- Poučte své uživatele o nebezpečí, které vyplývá ze současného připojení k serveru i k Internetu v rámci téže relace. Dále zajistěte, aby vaši uživatelé PC (například s klienty Windows 95) pochopili, že jednotky zůstanou namapované, i když relace iSeries Access vypadá, že skončila.

Riziko: důvěryhodné podepsané applety

Uživatelé mohou uposlechnout vaší rady a nastavit své prohlížeče tak, aby appletům zabránili v zapisování na jakékoliv zařízení na PC. Vaši uživatelé si však musí být vědomi toho, že *podepsaný applet* může nastavení jejich prohlížeče přepsat.

Podepsaný applet má připojen digitální podpis, který ověřuje jeho autenticitu. Když uživatel navštíví webovou stránku, která obsahuje podepsaný applet, zobrazí se mu zpráva. Tato zpráva indikuje podpis appletu (kým a kdy byl podepsán). Tím, že uživatel applet akceptuje, uděluje uživatel appletu právo přepsat bezpečnostní nastavení prohlížeče. Podepsaný applet může zapisovat na lokální jednotky PC, i když to předvolené nastavení prohlížeče zakazuje. Podepsaný applet může rovněž zapisovat na namapované jednotky vašeho serveru, protože se vůči PC jeví jako lokální jednotky.

Pro své vlastní Java applety, které pocházejí z vašeho serveru, možná budete muset použít podepsané applety. Avšak měli byste poučit své uživatele, aby všeobecně neakceptovali podepsané applety z neznámého zdroje.

Kapitola 17. Související informace

Manuály

- Publikace *APPC Programming*, SC41-5443-00 popisuje podporu APPC (advanced program-to-program communications) pro systém iSeries. Tato publikace vás provede vývojem aplikačních programů, které používají APPC, a definováním komunikačních prostředí pro komunikace APPC. Zahrnuje pokyny týkající se aplikačních programů, požadavky na konfiguraci, příkazy, správu problémů pro APPC a obecné pokyny týkající se sítí. Viz iSeries Information Center CD-ROM.
- Červená kniha *AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet*, SG24-4929, pojednává o otázkách zabezpečení a o riziku souvisejícím s připojením serveru iSeries k Internetu. Obsahuje příklady, doporučení, rady a metody pro aplikace TCP/IP.
- Publikace *Zálohování a obnova*, SC09-3599-07 popisuje strategii plánování zálohování a obnovy, metody ukládání informací z vašeho systému a postup obnovy systému. Viz aplikace iSeries Information Center. Další informace o těchto tématech najdete rovněž v rámci aplikace iSeries Information Center. Další podrobnosti najdete v části "Nezbytné předchozí a související informace" na stránce xii.
- Publikace *CL Programming*, SC41-5721-06 uvádí podrobný popis kódování DDS (specifikací popisu dat) pro soubory, které lze popsat externě. Jedná se o soubory fyzické, logické, obrazovkové, tiskové a ICF (intersystem communication function). Viz aplikace iSeries Information Center.
- Téma CL v rámci aplikace Information Center (další podrobnosti najdete v části "Nezbytné předchozí a související informace" na stránce xii) poskytuje popis jazyka iSeries CL (control language) a jeho příkazů OS/400. Příkazy OS/400 se používají k vyžádání funkcí licencovaného programu Operating System/400 (5722-SS1). Všechny příkazy, které nejsou příkazy CL OS/400, tj. příkazy, které jsou svázány s jinými licencovanými programy včetně všech různých jazyků a obslužných programů, jsou popsány v jiných publikacích, jež podporují příslušné licencované programy.
- *Implementing iSeries Security, 3rd Edition* by Wayne Madden and Carol Woodbury. Loveland, Colorado: 29th Street Press, a division of Duke Communications International, 1998. Tato publikace poskytuje návod a praktické návrhy týkající se plánování, nastavení a správy zabezpečení serveru iSeries.

  Objednací číslo ISBN:

  1-882419-78-2
- Další informace týkající se HTTP serveru najdete na adrese:

  `http://www.ibm.com/eserver/iseries/software/http/docs/doc.htm`
- Publikace *Zabezpečení iSeries - referenční informace Reference*, SC09-3697-07 poskytuje úplné informace o systémových hodnotách zabezpečení, o uživatelských profilech, zabezpečení prostředků a kontrole zabezpečení. Tato publikace nepopisuje zabezpečení specifických licencovaných programů, jazyků a obslužných programů. Viz aplikace iSeries Information Center.
- Téma ″Základní systémové operace″ v rámci aplikace Information Center popisuje některé z klíčových koncepcí a úloh, které jsou nutné pro základní operace serveru iSeries. Podrobnější informace naleznete v části "Nezbytné předchozí a související informace" na stránce xii.
- V aplikaci Information Center najdete informace o tom, jak používat a konfigurovat TCP/IP a několik aplikací TCP/IP, jako je FTP, SMTP a TELNET. Další podrobnosti najdete v části "Nezbytné předchozí a související informace" na stránce xii.

- Publikace *TCP/IP File Server Support for OS/400 Installation and User's Guide*, SC41-0125 poskytuje úvodní informace, pokyny pro instalaci a procedury nastavení licencovaného programu File Server Support. Vysvětluje funkce, které produkt poskytuje, a obsahuje příklady a pokyny, jak tento licencovaný program používat s jinými systémy.
- Publikace *Trusted Computer Systems Evaluation Criteria* DoD 5200.28.STD, popisuje kritéria pro úroveň důvěryhodnosti počítačových systémů. TCSEC je publikace, kterou vydává vláda Spojených států. Máte-li zájem o kopie, obraťte se na:

  Office of Standards and
  Products
  National Computer Security Center
  Fort Meade, Maryland 20755-6000 USA
  Attention: Chief, Computer Security Standards
- Aplikace Information Center obsahuje několik témat týkajících se správy systému a funkce Work Management na serveru iSeries. Některé z těchto témat zahrnují shromažďování dat o výkonu, správu systémových hodnot a správu paměti. Podrobné informace o tom, jak získat přístup k aplikaci Information Center, najdete v části "Nezbytné předchozí a související informace" na stránce xii. Publikace Work Management, SC41-5306-03, popisuje, jak vytvářet a měnit prostředí pro řízení práce. Viz aplikace iSeries Information Center.

Kromě témat v aplikaci Information Center a Doplňkových manuálů máte k dispozici tyto zdroje.

- **IBM SecureWay**
  Produkt IBM SecureWay poskytuje obecnou značku pro široké spektrum IBM nabídek v oblasti zabezpečení, hardware, software, konzultace a služby, které zákazníkům pomohou zabezpečit jejich informační technologii. Ať už se jedná o jednotlivou potřebu nebo o celopodnikové řešení, nabídka IBM SecureWay poskytuje zkušenosti nezbytné pro plánování, návrh, implementaci a provoz bezpečných řešení v oblasti e-businessu. Další informace o nabídce IBM SecureWay najdete na domovské stránce IBM SecureWay:

  `http://www.ibm.com/secureway`
- **Nabídky v oblasti servisních služeb**
  Instalace nového hardwaru nebo softwaru může výrazně zvýšit vaši efektivitu a zlepšit vaše podnikové operace. Avšak vzniká zde také nebezpečí přerušení obchodní činnosti a prostojů, které by mohly zatížit vaše cenné interní zdroje. IBM Global Services poskytuje služby, které se vztahují k zabezpečení serverů iSeries. Na níže uvedené webové stránce najdete úplný seznam služeb pro váš server iSeries:

  `http://www.as.ibm.com/asus`

Poznámky

Tyto informace byly vyvinuty pro produkty a služby nabízené v USA.

IBM nemusí produkty, služby nebo funkce, o nichž se pojednává v tomto dokumentu, nabízet 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 autorských práv IBM. Je však v odpovědnosti uživatele vyhodnotit a ověřit činnost libovolného produktu, programu nebo služby, které pocházejí z jiného zdroje než od IBM.

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 na licence můžete posílat na adresu:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
U.S.A.

Dotazy na licence týkající se informací DBCS směřujte na oddělení IBM Intellectual Property Department ve vaší zemi nebo je zašlete písemně na adresu

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, 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, MIMO JINÉ, ODVOZENÉ ZÁRUKY NEPORUŠENÍ PRÁV TŘETÍCH STRAN, ZÁRUKY PRODEJNOSTI NEBO VHODNOSTI PRO URČITÝ ÚČEL. Některé státy nepovolují odmítnutí vyjádřených nebo odvozených záruk při určitých transakcích, a proto se vás předchozí prohlášení nemusí týkat.

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 může produkt(y) anebo program(y) popsané v této publikaci kdykoli bez ohlášení zdokonalit nebo změnit.

Všechny odkazy v těchto informacích na webové stránky jiné než stránky IBM jsou poskytovány pouze pro pohodlí uživatele a žádným způsobem neslouží jako doporučení těchto webových stránek. Materiály obsažené na takovýchto webových stránkách nejsou součástí materiálů tohoto produktu IBM a mohou být používány pouze na vlastní riziko.

IBM může použít nebo distribuovat veškeré vámi zaslané informace jakýmkoliv způsobem, aniž by jí tím vznikl jakýkoliv závazek vůči vám.

Ten, kdo si přeje získat informace o licencích k tomuto programu za účelem umožnit: (i) výměnu informací mezi nezávisle vytvořenými programy a ostatními programy (včetně tohoto) a (ii) společné použití vyměněných informací, by měl kontaktovat koordinátora softwarové interoperability na adrese:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Informace tohoto typu mohou být za odpovídajících podmínek dostupné. V některých případech připadá v úvahu zaplacení poplatku.

Licencovaný program popsaný v těchto informacích a veškeré dostupné licencované materiály jsou společností IBM poskytovány na základě podmínek uvedených ve smlouvách IBM ICA (Customer Agreement), IBM IPLA (International Program License Agreement) 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 významně lišit. Některá měření mohla být prováděna v systémech na úrovni vývoje a nelze tedy zaručit, že tato měření budou ve všeobecně dostupných systémech stejná. Některá měření mohla být navíc odhadnuta pomocí extrapolace. Skutečné výsledky se mohou lišit. Uživatelé tohoto dokumentu by měli verifikovat použitelná data pro své specifické prostředí.

Informace týkající se produktů jiných společností byly získány od dodavatelů těchto produktů, z jejich tištěných materiálů nebo z jiných veřejně dostupných zdrojů. IBM tyto produkty netestovala a nemůže potvrdit přesnost údajů o výkonu, kompatibilitě nebo jiná tvrzení, která se k produktům od jiných společností vztahují. Otázky týkající se možností produktů jiných společností adresujte dodavatelům těchto produktů.

Všechna prohlášení týkající se budoucích směrů nebo úmyslů IBM mohou být bez upozornění změněna nebo odvolána a představují pouze záměry a cíle.

Tyto informace slouží pouze pro účely plánování. Informace uvedené v tomto dokumentu podléhají změně před zpřístupněním produktů uvedených v této publikaci.

Tyto informace obsahují příklady dat a sestav používaných v každodenních operacích. Za účelem co nejpřesnější ilustrace obsahují tyto příklady jména osob, společností, značek a produktů. Všechna tato jména jsou smyšlená a jakákoliv podobnost se jmény a adresami používanými ve skutečném podniku je čistě náhodná.

COPYRIGHT - LICENCE:

Tyto informace obsahují vzorové aplikační programy ve zdrojovém jazyku, které ilustrují programovací metody na různých operačních platformách. Vzorové programy smíte kopírovat, modifikovat a distribuovat v jakékoliv formě, aniž byste museli společnosti IBM platit jakýkoliv poplatek, pro účely vývoje, použití, marketingu nebo distribuce aplikačních programů, které vyhovují rozhraní API pro provozní platformu, pro kterou byly napsány vzorové programy. Tyto vzorové programy nebyly důkladně testovány za všech podmínek. IBM proto nezaručuje ani neodvozuje spolehlivost, obsluhovatelnost nebo funkčnost těchto programů. Tyto vzorové programy smíte kopírovat, modifikovat a distribuovat v jakékoliv formě, aniž byste museli společnosti IBM platit jakýkoliv poplatek, pro účely vývoje, použití, marketingu nebo distribuce aplikačních programů, které vyhovují IBM rozhraním API.

Pokud si tuto publikaci prohlížíte ve formě softcopy, nemusí se zobrazit fotografie a barevné ilustrace.

Ochranné známky

Níže uvedené termíny jsou ochrannými známkami společnosti IBM v USA nebo v jiných zemích:

Advanced Peer-to-Peer Networking
APPN
AS/400
DB2
DRDA
e (logo)
IBM
iSeries
Net.Data
Operating System/400
OS/400
PowerPC
SecureWay
System/36
System/38
400

ActionMedia, LANDesk, MMX, Pentium a ProShare jsou ochranné známky nebo registrované obchodní známky společnosti Intel Corporation ve Spojených státech anebo jiných zemích.

Microsoft, Windows, Windows NT a Windows logo jsou ochranné známky společnosti Microsoft Corporation ve Spojených státech anebo jiných zemích.

Java a všechny ochranné známky obsahující výraz Java jsou ochranné známky společnosti Sun Microsystems, Inc. ve Spojených státech anebo jiných ostatních zemích.

UNIX je registrovaná obchodní známka společnosti The Open Group ve Spojených státech anebo jiných zemích.

Ostatní jména společností, produktů a služeb mohou být ochrannými známkami nebo servisními značkami jiných firem.

Rejstřík

Speciální znaky

(SNMP), Simple Network Management Protocol 134

A

adoptované oprávnění
  monitorování použití 68
  omezení 69
  tisk seznamu objektů 31
adresáře iSeries 400, přístup prostřednictvím mapovaných jednotek 149
adresáře, zabezpečení 94
advanced program-to-program communications (APPC)
  Viz APPC
akce monitorování 49
akce, monitorování 49
aktivace
  uživatelský profil 23, 28
    automaticky 28
analýza
  chyba v programu 49
  oprávnění k objektu 48
  uživatelské profily 46
  uživatelský profil
    dle třídy uživatele 31
    dle zvláštních oprávnění 31
antivirový program 68
API QHFRGFS
  ukončovací program 72
API QTNADDCR
  ukončovací program 72
APPC (advanced program-to-program communications)
  hodnoty zabezpečení architektury
    popis 101
    příklady aplikací 101
    s parametrem SECURELOC (zabezpečení umístění) 102
  identifikace uživatele 101
  ohodnocení konfigurace 106, 110
  omezení relací 100
  popis linky 109
    parametry týkající se zabezpečení 109
    pole AUTOANS (Auto answer) 110
    pole AUTODIAL (Auto dial) 110
  popis řadiče
    parametr AUTOCRTDEV (automatické vytvoření zařízení) 109
    parametr CPSSN (relace řídicího bodu) 109
    parametr časovače odpojení 109
    parametry týkající se zabezpečení 108
  popis zařízení
    omezení pomocí oprávnění k objektu 100
APPC (advanced program-to-program communications) *(pokračování)*
  popis zařízení *(pokračování)*
    parametr APPN (podporující APPN) 108
    parametr LOCPWD (heslo umístění) 100
    parametr PREESTSSN (předvytvořená relace) 108
    parametr SECURELOC (zabezpečení umístění) 102, 107
    parametr SNGSSN (jedna relace) 108
    parametr SNUF program start 108
    parametry týkající se zabezpečení 106
    role v zabezpečení 100
    zabezpečení s APPN 100
  přiřazení uživatelského profilu 103
  rady týkající se zabezpečení 99
  relace 100
  rozdělení odpovědnosti za zabezpečení 102
  spuštění úlohy přímého průchodu 104
  terminologie 99
  vzdálený příkaz 106
    omezení pomocí záznamu PGMEVOKE 106
  základní prvky 99
atribut sítě
  DDMACC (přístup k požadavku DDM)
    omezení přístupu k datům z PC 139
    omezení vzdálených příkazů 144
    použití ukončovacího programu 72, 105
    zdroj vzorového ukončovacího programu 147
  JOBACN (akce úlohy sítě) 106
  PCSACC (přístup k požadavku klienta)
    omezení přístupu k datům z PC 139
    použití ukončovacího programu 72
    zdroj vzorového ukončovacího programu 147
  příkaz pro nastavení 35
  tisk souvisejících se zabezpečením 7, 31
atribut sítě akce úlohy sítě (JOBACN) 106
atribut sítě DDMACC (přístup k požadavku DDM)
  omezení přístupu k datům z PC 139
  omezení vzdálených příkazů 144
  použití ukončovacího programu 72, 105
  zdroj vzorového ukončovacího programu 147
atribut sítě JOBACN (akce úlohy sítě) 106
atribut sítě PCSACC (přístup k požadavku klienta)
  omezení přístupu k datům z PC 139
  použití ukončovacího programu 72
  zdroj vzorového ukončovacího programu 147
atribut sítě přístup k požadavku klienta (PCSACC)
  omezení přístupu k datům z PC 139
  použití ukončovacího programu 72
  zdroj vzorového ukončovacího programu 147
atributy zabezpečení
  tisk 7
automatické řízení, které servery TCP/IP se spouštějí 114
automatické vyčištění
  ukončovací program 72

B

bezdrátová komunikace 146
bezpečnostní ukončovací programy, použití 147
BOOTP (Bootstrap Protocol)
  omezení portu 120
  rady týkající se zabezpečení 120
Bootstrap Protocol (BOOTP)
  omezení portu 120
  rady týkající se zabezpečení 120

C

CFGSYSSEC (Konfigurace zabezpečení ochrany dat)
  navrhované použití 15
  popis 35
cílový systém
  definice 99
communications, APPC
  Viz APPC
communications, TCP/IP
  Viz komunikace TCP/IP

Č

části, logické 62

D

databázový soubor
  ochrana před přístupem z PC 139
  ukončovací program pro informace o využití 72
deaktivace
  uživatelský profil 23
    automaticky 24, 28
    důsledky 25
detekce podezřelých programů 67
DHCP
  omezení portu 122
  rady týkající se zabezpečení 121
digitální podpisy
  úvod 78

DNS
omezení portu 126
rady týkající se zabezpečení 126
doporučení
systémové hodnoty pro heslo 15
systémové hodnoty pro přihlášení 22
DST (Dedicated Service Tools)
hesla 22
důvěryhodné podepsané applety 150

E

emulace zařízení 3270
ukončovací program 72
eServer Security Planner 11
eServer Security Planner (poradce pro zabezpečení serveru) 13

F

File Transfer Protocol (FTP)
zdroj vzorového ukončovacího programu 147
fronta úloh
monitorování přístupu 55
tisk parametrů souvisejících se zabezpečením 33
fronta zpráv pro systémové zprávy (QSYSMSG)
navrhované použití 84
zdroj vzorového ukončovacího programu 147
fronta zpráv QSYSMSG (systémová zpráva)
navrhované použití 84
zdroj vzorového ukončovacího programu 147
FTP (File Transfer Protocol)
zdroj vzorového ukončovacího programu 147
funkce systému souborů
ukončovací program 72
funkce zabezpečení, monitorování 45
funkce, monitorování zabezpečení 45
fyzické zabezpečení 77

G

gateway server
otázky zabezpečení 145
globální nastavení 4

H

hesla
změna 20
heslo
jednosměrné kódování 25
kontrola předvolby 28
monitorování aktivit 26
předvolba 25
QSYSOPR (systémový operátor) 37
stanovení pravidel 15
systémová hodnota pro interval ukončení platnosti (QPWDEXPITV)
doporučené nastavení 15
heslo *(pokračování)*
systémová hodnota pro interval ukončení platnosti (QPWDEXPITV) *(pokračování)*
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota pro limit opakování znaků (QPWDLMTREP)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota pro maximální délku (QPWDMAXLEN)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota pro minimální délku (QPWDMINLEN)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota pro omezené sousední znaky v hesle (QPWDLMTAJC)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota pro omezené znaky v hesle (QPWDLMTCHR)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota pro požadovaný numerický znak (QPWDRQDDGT)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota pro požadovaný rozdíl (QPWDRQDDIF)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota pro požadovaný rozdíl mezi pozicemi (QPWDPOSDIF)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota pro program pro ověření (QPWDVLDPGM)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
šifrování
relace PC 143
uložení 26
uživatelský profil QPGMR (programátor) 37
uživatelský profil QSRV (servis) 37
uživatelský profil QSRVBAS (základní servis) 37
uživatelský profil QUSER (uživatel) 37
změna dodaných IBM 20
heslo umístění
APPN 101
hodnota *VFYENCPWD (ověření zašifrovaného hesla) 102, 107
hodnota ověření platnosti 68
hodnota ověření platnosti programu 68
hodnota zabezpečení
nastavení 35
hodnota zabezpečení, architektura
popis 101
příklady aplikací 101
s parametrem SECURELOC (zabezpečení umístění) 102
hodnoty zabezpečení architektury
popis 101
příklady aplikací 101
s parametrem SECURELOC (zabezpečení umístění) 102

CH

chráněná knihovna
kontrola uživatelských objektů 75
chránit licenčním klíčem
Viz řízení
chyba v programu
monitorování 49

I

ICS (Internet Connection Server)
popis 127
rady týkající se zabezpečení 127
zabránění automatickému spuštění serveru 128
ICSS (Internet Connection Secure Server)
popis 132
rady týkající se zabezpečení 132
identifikace
uživatel APPC 101
INETD 136
integrita
kontrola
popis 48
integrita objektu
monitorování 48
integrovaný systém souborů 87
důsledky zabezpečení 139
integrovaný systém souborů, zabezpečení 87
Internet Connection Secure Server (ICSS)
popis 132
rady týkající se zabezpečení 132
Internet Connection Server (ICS)
popis 127
rady týkající se zabezpečení 127
zabránění automatickému spuštění serveru 128
iSeries Access
důsledky integrovaného systému souborů 139
důsledky zabezpečení 139
gateway servery 145
metody přístupu k datům 139
ochrana před vzdálenými příkazy 145
omezení vzdálených příkazů 144
oprávnění k objektu 140
prevence PC virů 139
přenos souborů 139
řízení přístupu k datům 139
šifrování hesel 143
viry na PC 139
vynechání přihlášení 143

iSeries Access for Windows
použití SSL s 142
iSeries Security Wizard 11

J

jak zabránit původcům příchozích připojení v přístupu k jiným systémům 117
jednosměrné kódování 25
jména TPN architektury
rady týkající se zabezpečení 82
seznam dodaných IBM 82

K

klientský systém
definice 99
knihovna
výpis
obsah 48
všechny knihovny 48
knihovna QSYS38 (System/38)
omezení příkazů 45
knihovna System/38 (QSYS38)
omezení příkazů 45
kolekce údajů o výkonu
ukončovací program 72
komunikace APPC, základní prvky 99
komunikace TCP/IP
BOOTP (Bootstrap Protocol)
omezení portu 120
rady týkající se zabezpečení 120
DHCP
omezení portu 122
rady týkající se zabezpečení 121
DNS
omezení portu 126
rady týkající se zabezpečení 126
FTP (File Transfer Protocol)
zdroj vzorového ukončovacího programu 147
Internet Connection Secure Server (ICSS)
popis 132
rady týkající se zabezpečení 132
Internet Connection Server (ICS)
popis 127
rady týkající se zabezpečení 127
zabránění automatickému spuštění serveru 128
LPD (Line Printer Daemon)
omezení portu 134
popis 133
rady týkající se zabezpečení 133
zabránění automatickému spuštění serveru 133
ochrana aplikací pro port 113
omezení
existuje 137
konfigurační soubory 113
parametr INTNETADR (internetová adresa správce) 135
procházení 137
příkaz STRTCP 111
rady pro zabezpečení 111
REXECD (Remote EXECution server)
omezení portu 124
komunikace TCP/IP *(pokračování)*
REXECD (Remote EXECution server) *(pokračování)*
rady týkající se zabezpečení 124
RouteD (Route Daemon)
rady týkající se zabezpečení 125
SLIP (Serial Interface Line Protocol)
popis 115
řízení 115
zabezpečení odchozích hovorů 117
zabezpečení příchozích hovorů 116
SNMP (simple network management protocol)
omezení portu 135
rady týkající se zabezpečení 134, 136
zabránění automatickému spuštění serveru 135
TFTP (Trivial File Transfer Protocol)
omezení portu 123
rady týkající se zabezpečení 123
zabránění vstupu 111
komunikace, zabezpečení APPC 99
komunikace, základní prvky APPC 99
konfigurační soubory, TCP/IP
omezení přístupu 113
kontrola
integrita objektu 31, 68
popis 48
předvolená hesla 28
skryté programy 72
změněné objekty 48
kořenový adresář, veřejné oprávnění 91

L

Line Printer Daemon (LDP)
omezení portu 134
popis 133
rady týkající se zabezpečení 133
zabránění automatickému spuštění serveru 133
literatura 151
logické části, zabezpečení 62
logický soubor
ukončovací program pro výběr formátu záznamu 72
lokální systém
definice 99
LPD (Line Printer Daemon)
omezení portu 134
popis 133
rady týkající se zabezpečení 133
zabránění automatickému spuštění serveru 133

M

mapované jednotky, přístup k adresářů iSeries 400 jejich prostřednictvím 149
maximum
velikost
příjemce monitorovacího žurnálu (QAUDJRN) 50
menu
nástroje zabezpečení 28
menu řízení přístupu
omezení řízení přístupu prostřednictvím menu 42
parametry uživatelského profilu 42
popis 41
přechodné prostředí 43
rozšíření o oprávnění k objektu 42
menu SECBATCH (Submit Batch Reports)
zadání sestav 30
menu zabezpečení ochrany dat
omezení řízení přístupu prostřednictvím menu 42
parametry uživatelského profilu 42
popis 41
přechodné prostředí 43
rozšíření o oprávnění k objektu 42
metody, které systém používá k posílání informací o uživateli 101
monitorovací žurnál
tisk záznamů 31
monitorovací žurnál (QAUDJRN)
poškozený 50
prahová hodnota paměti příjemce 50
správa 49
systémové záznamy 50
monitorování
adoptované oprávnění 68, 69
aktivity související s hesly 26
aktivity související s přihlašováním 26
fronty úloh 55
chyba v programu 49
integrita objektu 48
naplánované programy 74
oprávnění 51
oprávnění k novým objektům 52
oprávnění k objektu 48
popis podsystému 79
seznamy oprávnění 52
schopnost obnovení 68, 75
schopnost uložení 68, 75
soukromé oprávnění 55
triggery 71
uživatelské prostředí 57
uživatelský profil
změny 77
veřejné oprávnění 51
výstupní fronty 55
zvláštní oprávnění 56
monitorování funkcí zabezpečení 45
monitorování zabezpečení
nastavení 29
operace obnovy 75
pokyny pro použití
hodnota *PGMFAIL 68
hodnota *SAVRST 68
hodnota *SECURITY 68
monitorování objektů 111
přehled 84
úroveň monitorování *PGMADP 69
záznam žurnálu CP (změna profilu) 23, 24
záznam žurnálu SV (systémová hodnota) 76
úvod 7, 45
zobrazení 29

monitorování, zabezpečení
pokyny pro použití
hodnota *PGMFAIL 68
hodnota *SAVRST 68
hodnota *SECURITY 68
monitorování objektů 111
přehled 84
úroveň monitorování *PGMADP 69
záznam žurnálu CP (změna profilu) 23, 24
záznam žurnálu SV (systémová hodnota) 76
možnost zadávat příkazy
výpis uživatelů 47

N

načtení
požadované oprávnění 140
nastavení
atributy sítí 35
hodnoty zabezpečení 35
monitorování zabezpečení 29
systémové hodnoty 35
nástroje zabezpečení
konflikty mezi soubory 27
menu 28
obsah 28
ochrana výstupu 27
oprávnění pro příkazy 27
příkazy 28
soubory 27
uložení 28
zabezpečení 27
neaktivní
uživatel
výpis 47
nekvalifikované volání 75
nové objekty, zabezpečení 94
nový objekt
správa oprávnění 52

O

obecný uživatel
definice 51
objekt
správa oprávnění k novým 52
tisk
adoptované oprávnění 31
jiný než IBM 31
zdroj oprávnění 31
zdroj oprávnění
tisk seznamu 52
změněný
kontrola 48
objektově orientovaný systém
důsledky zabezpečení 41
ochrana proti počítačovým virům 67
objekty, zabezpečení pro nové 94
obnova
poškozený monitorovací žurnál 50
Obrazovka Display Authorized Users (DSPAUTUSR) 46
obsah
nástroje zabezpečení 28
ODBC (Open DataBase Connectivity)
řízení přístupu 143
zdroj vzorového ukončovacího programu 147
oddělovací stránka
ukončovací program 72
odeslání
požadované oprávnění 140
záznam žurnálu 49
odstranění
neaktivní uživatelské profily 24
uživatelský profil
automaticky 24, 28
záznamy směrování PGMEVOKE 106
ochrana
aplikace pro port TCP/IP 113
proti počítačovým virům 67
ochrana integrity
úroveň zabezpečení 40 (QSECURITY) 3
omezení
Viz též řízení
adoptované 69
možnosti
výpis uživatelů 47
omezení přístupu k systému souborů QSYS.LIB 93
omezení relací APPC 100
operace potvrzení
ukončovací program 72
operace vrácení do původního stavu
ukončovací program 72
Operations Console s připojitelností přes LAN
použití 65
změna hesla 65
oprávnění
adoptované 68
monitorování 49, 68
omezení 69
fronty úloh 55
kdy je vynuceno 41
monitorování 51, 55
na úrovni zabezpečení 10 nebo 20 41
národní jazyky 45
nové objekty 52
přehled 41
přechodné prostředí 43
příkazy nástrojů zabezpečení 27
přístup k příkazům pro obnovu 75
přístup k příkazům pro uložení 75
přístup uživatelů PC k datům 140
rozšíření řízení přístupu prostřednictvím menu 42
správa 51
úvod 5
veřejné 51
výstupní fronty 55
zabezpečení na úrovni knihoven 44
začínáme 43
zvláštní 56
zvláštní oprávnění *SAVSYS (uložení systému) 75
řízení 75
oprávnění k objektu
adoptované 68
monitorování 68
omezení 69
analýza 48
oprávnění k objektu *(pokračování)*
fronty úloh 55
kdy je vynuceno 41
monitorování 51, 55
na úrovni zabezpečení 10 nebo 20 41
národní jazyky 45
nové objekty 52
přehled 41
přechodné prostředí 43
příkazy nástrojů zabezpečení 27
přístup k příkazům pro obnovu 75
přístup k příkazům pro uložení 75
přístup uživatelů PC k datům 140
rozšíření řízení přístupu prostřednictvím menu 42
správa 51
úvod 5
veřejné 51
výstupní fronty 55
zabezpečení na úrovni knihoven 44
začínáme 43
zobrazení 48
zvláštní 56
zvláštní oprávnění *SAVSYS (uložení systému) 75
řízení 75
oprávnění, objekt
Viz oprávnění k objektu
osobní počítač
Viz PC (osobní počítač)

P

paměť
prahová hodnota
příjemce monitorovacího žurnálu (QAUDJRN) 50
parametr ANN (podporující APPN) 108
parametr AUTOCRTCTL (automatické vytvoření řadiče) 109
parametr CPSSN (relace řídicího bodu) 109
parametr CURLIB (aktuální knihovna) 57
parametr časovače odpojení 109
parametr FMTSLR (program pro výběr formátu záznamu) 72
parametr FRCCRT (vynucené vytvoření) 68
parametr INLMNU (počáteční menu) 57
parametr INLPGM (počáteční program) 57
parametr INTNETADR (internetová adresa správce)
omezení 135
parametr LOCPWD (heslo umístění) 100
parametr MSGQ (fronta zpráv) 57
parametr PREESTSSN (předvytvořená relace) 108
parametr SECURELOC (zabezpečení umístění) 107
diagram 100
hodnota *VFYENCPWD (ověření zašifrovaného hesla) 102, 107
popis 102
parametr SNGSSN (jedna relace) 108
parametr SNUF program start 108
parametr USEADPAUT (použití adoptovaného oprávnění) 69

PC (osobní počítač)
  důsledky integrovaného systému souborů 139
  důsledky zabezpečení 139
  gateway servery 145
  metody přístupu k datům 139
  ochrana před vzdálenými příkazy 145
  omezení vzdálených příkazů 144
  oprávnění k objektu 140
  prevence PC virů 139
  přenos souborů 139
  řízení přístupu k datům 139
  šifrování hesel 143
  viry na PC 139
  vynechání přihlášení 143
plánovač úloh
  vyhodnocení programů 74
plánování
  uživatelský profil
    aktivace 23, 28
    deaktivace 23
    ukončení platnosti 24, 28
plánování změn úrovně hesla
  snížení úrovní hesla 19, 20
  změna úrovně hesla z 1 na 0 20
  změna úrovně hesla ze 2 na 0 20
  změna úrovně hesla ze 2 na 1 19
  změna úrovně hesla ze 3 na 0 19
  změna úrovně hesla ze 3 na 1 19
  změna úrovně hesla ze 3 na 2 19
  změna úrovní hesla
    plánování změn úrovně 16, 17
  změna úrovní hesla (0 na 1) 17
  změna úrovní hesla (0 na 2) 17
  změna úrovní hesla (1 na 2) 17
  změna úrovní hesla (2 na 3) 19
  změny QPWDLVL 16, 17
  zvýšení úrovně hesla 17
plný
  příjemce monitorovacího žurnálu (QAUDJRN) 50
počítačový vir
  definice 67
  ochrana proti 67
  ochranné mechanismy serveru iSeries 68
  prozkoumání 68
podepisování objektů 78
  úvod 78
podepsané applety, důvěryhodné 150
podezřelé programy, detekce 67
podpora národního prostředí
  oprávnění k objektu 45
podpora systémem řízené změny žurnálu 50
podvody, prevence a detekce 77
pokyny k zabezpečení pro webové prohlížeče 149
pole Auto answer (AUTOANS) 110
pole Auto dial (AUTODIAL) 110
pole AUTOANS (Auto answer) 110
pole AUTODIAL (Auto dial) 110
popis podsystému
  hodnoty související se zabezpečením 79
  monitorování hodnot souvisejících se zabezpečením 79
  rady týkající se zabezpečení
    záznam automaticky spuštěné úlohy 79
popis podsystému *(pokračování)*
  rady týkající se zabezpečení *(pokračování)*
    záznam fronty úloh 80
    záznam jména pracovní stanice 79
    záznam jména vzdáleného systému 80
    záznam komunikací 80
    záznam předspuštěné úlohy 81
    záznam směrování 80
    záznam typu pracovní stanice 79
  tisk parametrů souvisejících se zabezpečením 31
  záznam komunikací
    předvolený uživatel 103
    režim 103
  záznam směrování
    odstranění záznamu PGMEVOKE 106
popis řadiče
  tisk parametrů souvisejících se zabezpečením 31
popis tiskového zařízení
  ukončovací program pro oddělovací stránku 72
popis úlohy
  rady týkající se zabezpečení 81
  tisk parametrů souvisejících se zabezpečením 31
  tisk pro uživatelské profily 57
popis zařízení
  tisk parametrů souvisejících se zabezpečením 31
popis zařízení, APPC
  Viz popis zařízení APPC
poradce, zabezpečení 13
poškozený monitorovací žurnál 50
použití SSL s produktem iSeries Access Express 142
prevence a detekce podvodů 77
produkt iSeries Access Express, použití SSL 142
produkt iSeries Navigator, zabezpečení 142
produkt Operations Console
  autentizace uživatele 64
  autentizace zařízení 64
  integrita dat 64
  použití 63
  průvodce nastavením 65
  přímá připojitelnost 64
  připojitelnost přes LAN 64
  šifrování 63
  utajení dat 64
  uživatelské profily 63
  uživatelské profily servisních nástrojů 63
  vzdálená konzole 63
produkt Operations Console s připojitelností přes LAN
  použití 65
  průvodce nastavením
    heslo profilu zařízení servisních nástrojů 65
    profil zařízení servisních nástrojů 65
profil
  analýza pomocí dotazu 46
  uživatel 46
    velký, prozkoumání 47
    výpis neaktivních 47
profil *(pokračování)*
  uživatel *(pokračování)*
    výpis uživatelů s možností zadávat příkazy 47
    výpis uživatelů se zvláštním oprávněním 47
    výpis vybraných 47
profil dodaný IBM
  změna hesla 20
profil zařízení servisních nástrojů
  atributy
    konzole 65
  heslo 65
  ochrana 65
  předvolené heslo 65
  změna hesla 65
profil, skupinový
  Viz skupinový profil
profil, uživatelský
  Viz uživatelský profil
program
  Viz též trigger
  funkce přebírání oprávnění
    monitorování 49
  naplánovaný
    vyhodnocení 74
  skrytý
    kontrola 72
  vynucení vytvoření 68
program klávesy Attention
  tisk pro uživatelské profily 57
  ukončovací program 72
program QUSCLSXT 72
programy, které adoptují
  zobrazení 49
programy, které přebírají oprávnění
  monitorování použití 68
  omezení 69
programy, použití bezpečnostních ukončovacích 147
prohlížeče, pokyny k zabezpečení 149
procházení, TCP/IP
  omezení 137
prostředek
  bezpečnostní ukončovací programy 147
protokol (SNMP), jednoduchá správa sítě 134
protokol LDAP (Lightweight Directory Access Protocol)
  funkce zabezpečení 133
protokol pro dvoubodové připojení (PPP)
  pokyny k zabezpečení 119
protokol pro správu (SNMP), jednoduchá síť 134
protokol SNMP (Simple Network Management Protocol) 134
průvodce, zabezpečení 11
předejití
  konflikty mezi soubory nástrojů zabezpečení 27
předvolený uživatel
  pro jména TPN architektury 82
  záznam komunikací
    možné hodnoty 103
přenos souborů
  omezení 45
  PC (osobní počítač) 139

přenos souborů v systému System/36
omezení 45
přihlášení
monitorování pokusů 26
nastavení systémových hodnot 22
řízení 15
vynechání 143
přihlašovací obrazovka
změna chybových zpráv 22
příjemce žurnálu, monitorovací
prahová hodnota paměti 50
příkaz
vyvolání obecného oprávnění 35
příkaz (PRTPVTAUT), Tisk soukromých oprávnění k objektům 91
příkaz ADDPFRCOL (Přidání kolekce údajů o výkonu)
ukončovací program 72
příkaz Analýza aktivity profilu (ANZPRFACT)
navrhované použití 24
popis 28
vytvoření vyloučených uživatelů 28
příkaz Analýza předvolených hesel (ANZDFTPWD)
navrhované použití 25
popis 28
příkaz ANZDFTPWD (Analýza předvolených hesel)
navrhované použití 25
popis 28
příkaz ANZPRFACT (Analýza aktivity profilu)
navrhované použití 24
popis 28
vytvoření vyloučených uživatelů 28
příkaz CFGSYSSEC (Konfigurace zabezpečení systému)
navrhované použití 15
popis 35
příkaz CRTPRDLOD (Vytvoření loadu produktu)
ukončovací program 72
příkaz DSPACTPRFL (Zobrazení seznamu aktivních profilů)
popis 28
příkaz DSPACTSCD (Zobrazení plánu aktivace)
popis 28
příkaz DSPAUDJRNE (Zobrazení záznamů monitorovacího žurnálu)
navrhované použití 84
popis 31
příkaz DSPAUTUSR (Zobrazení oprávněných uživatelů)
monitorování 46
příkaz DSPEXPSCD (Zobrazení plánu expirace)
navrhované použití 25
popis 28
příkaz DSPLIB (Zobrazení knihovny)
použití 48
příkaz DSPOBJAUT (Zobrazení oprávnění k objektu)
použití 48
příkaz DSPOBJD (Zobrazení popisu objektu)
použití výstupního souboru 47
příkaz DSPPGMADP (Zobrazení programů, které adoptují oprávnění)
monitorování 49
příkaz DSPSECAUD (Zobrazení monitorování zabezpečení)
popis 29
příkaz DSPUSRPRF (Zobrazení uživatelského profilu)
použití výstupního souboru 47
příkaz ENDPFRMON (Ukončení monitoru výkonu)
ukončovací program 72
příkaz CHGACTPRFL (Změna seznamu aktivních profilů)
navrhované použití 24
popis 28
příkaz CHGACTSCDE (Změna záznamu plánu aktivace)
navrhované použití 23
popis 28
příkaz CHGBCKUP (Změna zálohy)
ukončovací program 72
příkaz CHGEXPSCDE (Změna záznamu o plánovaném ukončení platnosti)
navrhované použití 24
popis 28
příkaz CHGMSGD (Změna popisu zprávy)
ukončovací program 72
příkaz CHGPFRCOL (Změna kolekce údajů o výkonu)
ukončovací program 72
příkaz CHGSECAUD (Změna monitorování zabezpečení)
navrhované použití 84
popis 29
příkaz CHGSYSLIBL (Změna systémového seznamu knihoven)
omezení přístupu 76
příkaz CHKOBJITG (Kontrola integrity objektu)
navrhované použití 68
popis 31, 48
příkaz Kontrola integrity objektu (CHKOBJITG)
navrhované použití 68
popis 31, 48
příkaz Nastavení programu klávesy Attention (SETATNPGM)
ukončovací program 72
příkaz Odeslání záznamu žurnálu (SNDJRNE) 49
příkaz Práce s informacemi o registraci (WRKREGINF)
ukončovací program 74
příkaz Práce s popisem podsystému (WRKSBSD) 79
příkaz pro obnovu
omezení přístupu 75
příkaz pro uložení
omezení přístupu 75
příkaz PRTADPOBJ (Tisk adoptovaných objektů)
popis 31
příkaz PRTCMNSEC (Tisk zabezpečení komunikací)
popis 31
příklad 106, 110
příkaz PRTJOBDAUT (Tisk oprávnění k popisu úlohy)
navrhované použití 81
popis 31
příkaz PRTPUBAUT (Tisk veřejně oprávněných objektů)
navrhované použití 100
popis 31
příkaz PRTPUBAUT, Tisk veřejně oprávněných objektů 92
příkaz PRTPVTAUT (Tisk soukromých oprávnění k objektům) 91
příkaz PRTPVTAUT (Tisk soukromých oprávnění)
navrhované použití 100
popis 33
seznam oprávnění 31, 52
příkaz PRTQAUT (Tisk oprávnění k frontě)
popis 33
příkaz PRTSBSDAUT (Tisk popisu podsystému)
navrhované použití 103
popis 31
příkaz PRTSYSSECA (Tisk atributů zabezpečení systému)
navrhované použití 15
popis 31
vzorový výstup 7
příkaz PRTTRGPGM (Tisk triggerů)
popis 31
příkaz PRTUSROBJ (Tisk uživatelský objektů)
navrhované použití 76
popis 31
příkaz PRTUSRPRF (Tisk uživatelského profilu)
informace o hesle 23, 26
popis 31
příklad informací o prostředí 58
příklad nesrovnalostí 57
příklad zvláštních oprávnění 56
příkaz Přidání kolekce údajů o výkonu (ADDPFRCOL)
ukončovací program 72
příkaz RUNRMTCMD (Spuštění vzdáleného příkazu)
omezení 145
příkaz RVKPUBAUT (Vyvolání obecného oprávnění)
navrhované použití 79
podrobnosti 37
popis 35
příkaz SBMRMTCMD (Spuštění vzdáleného příkazu)
omezení 105
příkaz SETATNPGM (Nastavení programu klávesy Attention)
ukončovací program 72
příkaz SNDJRNE (Odeslání záznamu žurnálu) 49
příkaz Soukromá oprávnění k objektům (PRTPVTAUT), tisk 91
příkaz Spuštění emulace obrazovky 3270 (STREML3270)
ukončovací program 72

příkaz Spuštění monitoru výkonu (STRPFRMON)
ukončovací program 72
příkaz Spuštění TCP/IP (STRTCP)
omezení 111
příkaz Spuštění vzdáleného příkazu (RUNRMTCMD)
omezení 145
příkaz STRPFRMON (Spuštění monitoru výkonu)
ukončovací program 72
příkaz STRTCP (Spuštění TCP/IP)
omezení 111
příkaz Tisk adoptovaných objektů (PRTADPOBJ)
popis 31
příkaz Tisk atributů zabezpečení systému (PRTSYSSECA)
navrhované použití 15
popis 31
vzorový výstup 7
příkaz Tisk oprávnění k frontě (PRTQAUT)
popis 33
příkaz Tisk oprávnění k popisu úlohy (PRTJOBDAUT)
navrhované použití 81
popis 31
příkaz Tisk popisu podsystému (PRTSBSDAUT)
navrhované použití 103
popis 31
příkaz Tisk soukromých oprávnění (PRTPVTAUT)
navrhované použití 100
popis 33
seznam oprávnění 31, 52
příkaz Tisk triggerů (PRTTRGPGM)
popis 31
příkaz Tisk uživatelského profilu (PRTUSRPRF)
informace o hesle 23, 26
popis 31
příklad informací o prostředí 58
příklad nesrovnalostí 57
příklad zvláštních oprávnění 56
příkaz Tisk uživatelských objektů (PRTUSROBJ)
navrhované použití 76
popis 31
příkaz Tisk veřejně oprávněných objektů (PRTPUBAUT) 92
navrhované použití 100
popis 33
příkaz Tisk zabezpečení komunikací (PRTCMNSEC)
popis 31
příklad 106, 110
příkaz Trasování úlohy (TRCJOB)
ukončovací program 72
příkaz TRCJOB (Trasování úlohy)
ukončovací program 72
příkaz Ukončení monitoru výkonu (ENDPFRMON)
ukončovací program 72
příkaz Veřejně oprávněné objekty (PRTPUBAUT), tisk 92
příkaz Vytvoření adresáře 94
příkaz Vytvoření adresáře iSeries 400 94
příkaz Vytvoření loadu produktu (CRTPRDLOD)
ukončovací program 72
příkaz Vyvolání obecného oprávnění (RVKPUBAUT)
navrhované použití 79
podrobnosti 37
popis 35
příkaz WRKREGINF (Práce s informacemi o registraci)
ukončovací program 74
příkaz WRKSBSD (Práce s popisem podsystému) 79
příkaz Změna kolekce údajů o výkonu (CHGPFRCOL)
ukončovací program 72
příkaz Změna monitorování zabezpečení (CHGSECAUD)
navrhované použití 84
popis 29
příkaz Změna popisu zprávy (CHGMSGD)
ukončovací program 72
příkaz Změna seznamu aktivních profilů (CHGACTPRFL)
navrhované použití 24
popis 28
příkaz Změna systémového seznamu knihoven (CHGSYSLIBL)
omezení přístupu 76
příkaz Změna zálohy (CHGBCKUP)
ukončovací program 72
příkaz Změna záznamu o plánovaném ukončení platnosti (CHGEXPSCDE)
navrhované použití 24
popis 28
příkaz Změna záznamu plánu aktivace (CHGACTSCDE)
navrhované použití 23
popis 28
příkaz Zobrazení knihovny (DSPLIB) 48
příkaz Zobrazení monitorování zabezpečení (DSPSECAUD)
popis 29
příkaz Zobrazení oprávnění k objektu (DSPOBJAUT) 48
příkaz Zobrazení oprávněných uživatelů (DSPAUTUSR)
monitorování 46
příkaz Zobrazení plánu aktivace (DSPACTSCD)
popis 28
příkaz Zobrazení plánu expirace (DSPEXPSCD)
navrhované použití 25
popis 28
příkaz Zobrazení popisu objektu (DSPOBJD)
použití výstupního souboru 47
příkaz Zobrazení programů, které adoptují oprávnění (DSPPGMADP)
monitorování 49
příkaz Zobrazení uživatelského profilu (DSPUSRPRF)
použití výstupního souboru 47
příkaz Zobrazení záznamů monitorovacího žurnálu (DSPAUDJRNE)
navrhované použití 84
příkaz Zobrazení záznamů monitorovacího žurnálu (DSPAUDJRNE) *(pokračování)*
popis 31
příkaz, CL
ADDPFRCOL (Přidání kolekce údajů o výkonu)
ukončovací program 72
ANZDFTPWD (Analýza předvolených hesel)
navrhované použití 25
popis 28
ANZPRFACT (Analýza aktivity profilu)
navrhované použití 24
popis 28
vytvoření vyloučených uživatelů 28
CFGSYSSEC (Konfigurace zabezpečení ochrany dat)
navrhované použití 15
popis 35
CRTPRDLOD (Vytvoření loadu produktu)
ukončovací program 72
DSPACTPRFL (Zobrazení seznamu aktivních profilů)
popis 28
DSPACTSCD (Zobrazení plánu aktivace)
popis 28
DSPAUDJRNE (Zobrazení záznamů monitorovacího žurnálu)
navrhované použití 84
popis 31
DSPAUTUSR (Zobrazení oprávněných uživatelů)
monitorování 46
DSPEXPSCD (Zobrazení plánu expirace)
navrhované použití 25
popis 28
DSPLIB (Zobrazení knihovny) 48
DSPOBJAUT (Zobrazení oprávnění k objektu) 48
DSPOBJD (Zobrazení popisu objektu)
použití výstupního souboru 47
DSPPGMADP (Zobrazení programů, které adoptují oprávnění)
monitorování 49
DSPSECAUD (Zobrazení monitorování zabezpečení)
popis 29
DSPUSRPRF (Zobrazení uživatelského profilu)
použití výstupního souboru 47
ENDPFRMON (Ukončení monitoru výkonu)
ukončovací program 72
CHGACTPRFL (Změna seznamu aktivních profilů)
navrhované použití 24
popis 28
CHGACTSCDE (Změna záznamu plánu aktivace)
navrhované použití 23
popis 28
CHGBCKUP (Změna zálohy)
ukončovací program 72
CHGEXPSCDE (Změna záznamu o plánovaném ukončení platnosti)
navrhované použití 24
popis 28

příkaz, CL *(pokračování)*
CHGMSGD (Změna popisu zprávy)
ukončovací program 72
CHGPFRCOL (Změna kolekce údajů o výkonu)
ukončovací program 72
CHGSECAUD (Změna monitorování zabezpečení)
navrhované použití 84
popis 29
CHGSYSLIBL (Změna systémového seznamu knihoven)
omezení přístupu 76
CHKOBJITG (Kontrola integrity objektu)
navrhované použití 68
popis 31, 48
Kontrola integrity objektu (CHKOBJITG)
popis 48
nástroje zabezpečení 28
Odeslání záznamu žurnálu (SNDJRNE) 49
plán aktivace 28
PRTADPOBJ (Tisk adoptovaných objektů)
popis 31
PRTCMNSEC (Tisk zabezpečení komunikací)
popis 31
příklad 106, 110
PRTJOBDAUT (Tisk oprávnění k popisu úlohy)
navrhované použití 81
popis 31
PRTPUBAUT (Tisk veřejně oprávněných objektů)
navrhované použití 100
popis 31
PRTPVTAUT (Tisk soukromých oprávnění)
navrhované použití 100
popis 33
seznam oprávnění 31, 52
PRTQAUT (Tisk oprávnění k frontě)
popis 33
PRTSBSDAUT (Tisk popisu podsystému)
navrhované použití 103
popis 31
PRTSYSSECA (Tisk atributů zabezpečení systému)
navrhované použití 15
popis 31
vzorový výstup 7
PRTTRGPGM (Tisk triggerů)
popis 31
PRTUSROBJ (Tisk uživatelský objektů)
navrhované použití 76
popis 31
PRTUSRPRF (Tisk uživatelského profilu)
informace o hesle 23, 26
popis 31
příklad informací o prostředí 58
příklad nesrovnalostí 57
příklad zvláštních oprávnění 56
RCVJRNE (Získání záznamů žurnálu)
ukončovací program 72
RUNRMTCMD (Spuštění vzdáleného příkazu)
omezení 145
příkaz, CL *(pokračování)*
RVKPUBAUT (Vyvolání obecného oprávnění)
navrhované použití 79
podrobnosti 37
popis 35
SBMRMTCMD (Spuštění vzdáleného příkazu)
omezení 105
SETATNPGM (Nastavení programu klávesy Attention)
ukončovací program 72
SNDJRNE (Odeslání záznamu žurnálu) 49
STREML3270 (Spuštění emulace obrazovky 3270)
ukončovací program 72
STRPFRMON (Spuštění monitoru výkonu)
ukončovací program 72
STRTCP (Spuštění TCP/IP)
omezení 111
TRCJOB (Trasování úlohy)
ukončovací program 72
WRKREGINF (Práce s informacemi o registraci)
ukončovací program 74
WRKSBSD (Práce s popisem podsystému) 79
Zobrazení knihovny (DSPLIB) 48
Zobrazení oprávnění k objektu (DSPOBJAUT) 48
Zobrazení oprávněných uživatelů (DSPAUTUSR)
monitorování 46
Zobrazení programů, které adoptují oprávnění (DSPPGMADP)
monitorování 49
Zobrazení uživatelského profilu (DSPUSRPRF)
použití výstupního souboru 47
příkaz, Tisk soukromých oprávnění k objektům (PRTPVTAUT) 91
příkaz, Tisk veřejně oprávněných objektů (PRTPUBAUT) 92
příkaz, Vytvoření adresáře iSeries 400 94
přiřazení
uživatelský profil pro úlohu APPC 103
přístup
řízení 41
přístup k systému souborů QSYS.LIB, omezení 93
přístup k adresářům iSeries 400 prostřednictvím mapovaných jednotek 149
přístup původců příchozích připojení k jiným systémům, zabránění 117
přizpůsobení
hodnoty zabezpečení 35
publikace
související 151

Q

QCONSOLE
předvolené heslo 65
QMAXSIGN (maximální počet pokusů o přihlášení)
doporučené nastavení 22
QPWFSERVER 93
QSYSOPR (systémový operátor)
heslo nastavené příkazem CFGSYSSEC 37
QVFYOBJRST (ověření obnovy objektu)
systémová hodnota 78

R

RCVJRNE (Získání záznamů žurnálu)
ukončovací program 72
registrovaný ukončovací
vyhodnocení 74
relace APPC, omezení 100
relace, základy APPC 100
Remote EXECution server (REXECD)
omezení portu 124
rady týkající se zabezpečení 124
REXECD (Remote EXECution server)
omezení portu 124
rady týkající se zabezpečení 124
režim
záznam komunikací 103
Route Daemon (RouteD)
rady týkající se zabezpečení 125
RouteD (Route Daemon)
rady týkající se zabezpečení 125
rozhraní API Volání distribuovaného programu 144
rozhraní API, vytvoření adresáře 95
rozhraní API, vytvoření proudového souboru pomocí open() nebo creat() 95
rozhraní QSYSCHID (Change uid) API 97
rozšířená ochrana integrity
úroveň zabezpečení 50 (QSECURITY) 3

Ř

řízení
adoptované oprávnění 68, 69
hesla 15
jména TPN architektury 82
naplánované programy 74
ODBC (Open DataBase Connectivity) 143
parametr INTNETADR (internetová adresa správce) 135
PC (osobní počítač) 139
popis zařízení APPC 100
popisy podsystémů 79
přenos souborů v systému System/36 45
přihlášení 15
přístup
k informacím 41
k příkazům pro obnovu 75
k příkazům pro uložení 75
přístup k datům z PC 139
relace APPC 100
schopnost obnovení 75
schopnost uložení 75
TCP/IP
existuje 137
konfigurační soubory 113
vstup 111
triggery 71
ukončovací programy 72

řízení *(pokračování)*
vzdálené příkazy 105, 144
změny seznamu knihoven 76
zvláštní oprávnění *SAVSYS (uložení systému) 75
řízení spojení příchozích hovorů po komutované lince s využitím SLIP 116
řízení, které servery TCP/IP se spouštějí automaticky 114

S

SECURE(NONE)
popis 101
SECURE(PROGRAM)
popis 101
SECURE(SAME)
popis 101
Security Wizard (průvodce zabezpečením) 11
SECURITY(NONE)
s hodnotou *FRCSIGNON pro systémovou hodnotu QRMTSIGN 102
Serial Interface Line Protocol (SLIP)
popis 115
řízení 115
zabezpečení odchozích hovorů 117
zabezpečení příchozích hovorů 116
server
definice 99
server servisních nástrojů (STS)
logické části 62
servisní nástroje
uživatelské profily (servisní nástroje) 58
sestava zobrazení objektů seznamu oprávnění 53
seznam aktivních profilů
změna 28
seznam knihoven
důsledky zabezpečení 75
seznam oprávnění
monitorování 52
řízení použití adoptovaného oprávnění 71
tisk informací o oprávněních 52
tisk informací o oprávněních 31
seznam záloh
ukončovací program 72
schopnost obnovení
monitorování 68
řízení 75
schopnost uložení
monitorování 68
řízení 75
simple network management protocol (SNMP)
omezení portu 135
rady týkající se zabezpečení 134, 136
zabránění automatickému spuštění serveru 135
síťový systém souborů 96
skrytý program
kontrola 72
skupinový profil
úvod 5
SLIP (Serial Interface Line Protocol)
popis 115
řízení 115
zabezpečení odchozích hovorů 117
SLIP (Serial Interface Line Protocol) *(pokračování)*
zabezpečení příchozích hovorů 116
směrování prostředního uzlu 108
snímání
úpravy objektu 48
SNMP (simple network management protocol)
omezení portu 135
rady týkající se zabezpečení 134, 136
zabránění automatickému spuštění serveru 135
soubor
nástroje zabezpečení 27
soukromé oprávnění
monitorování 55
související publikace 151
spojení, řízení příchozích hovorů po komutované lince s využitím SLIP 116
správa
adoptované oprávnění 68, 69
fronty úloh 55
monitorovací žurnál 49
naplánované programy 74
oprávnění 51
oprávnění k novým objektům 52
popis podsystému 79
seznamy oprávnění 52
schopnost obnovení 68, 75
schopnost uložení 68, 75
soukromé oprávnění 55
triggery 71
uživatelské prostředí 57
veřejné oprávnění 51
výstupní fronty 55
zvláštní oprávnění 56
spuštění
úloha přímého průchodu 104
SSL
použití s produktem iSeries Access for Windows 142
SSL (Secure Socket Layer)
použití s produktem iSeries Access for Windows 142
STS (server servisních nástrojů)
logické části 62
systém souborů QFileSvr.400 95
systém souborů QSYS.LIB, omezení přístupu k 93
systém souborů, integrovaný 87
systém souborů, omezení přístupu ke QSYS.LIB 93
systém souborů, QFileSvr.400 95
systém souborů, síťový 96
systém, omezení přístupu k souboru QSYS.LIB 93
systém, síťový soubor 96
systém, soubor QFileSvr.400 95
systémová hodnota
přihlášení
doporučení 22
příkaz pro nastavení 35
QALWOBJRST (umožnění obnovy objektu)
hodnota nastavená příkazem CFGSYSSEC 35
navrhované použití 75
systémová hodnota *(pokračování)*
QAUDCTL (řízení monitorování)
změna 29
zobrazení 29
QAUDLVL (úroveň monitorování)
změna 29
zobrazení 29
QAUTOCFG (automatická konfigurace)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
QAUTOVRT (automatická konfigurace virtuálního zařízení)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
QDEVRCYACN (akce obnovy zařízení)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
vyvarování se bezpečnostního rizika 105
QDSCJOBITV (prodleva odpojené úlohy)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
QDSPSGNINF (zobrazení informací o přihlášení)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
QINACTITV (prodleva neaktivní úlohy)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
QINACTMSGQ (fronta zpráv neaktivní úlohy)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
QLMTSECOFR (omezení správce systému)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
QMAXSGNACN (akce, která se má provést, když se dosáhne maxima pokusů o zadání hesla)
hodnota nastavená příkazem CFGSYSSEC 35
QMAXSIGN (maximální počet pokusů o přihlášení)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
QPWDEXPITV (interval ukončení platnosti)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
QPWDLMTAJC (omezené sousední znaky v hesle)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35

systémová hodnota *(pokračování)*
QPWDLMTCHR (omezené znaky v hesle)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
QPWDLMTREP (limit opakování znaků v hesle)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
QPWDLMTREP (požadovaný rozdíl mezi pozicemi v hesle)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
QPWDLVL (úroveň hesla)
doporučené nastavení 15
QPWDMAXLEN (maximální délka hesla)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
QPWDMINLEN (minimální délka hesla)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
QPWDRQDDGT (požadovaný numerický znak v hesle)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
QPWDRQDDIF (požadovaný rozdíl mezi hesly)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
QPWDVLDPGM (program pro ověření platnosti hesla)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
použití ukončovacího programu 72
zdroj vzorového ukončovacího programu 147
QRETSVRSEC (zachycení dat zabezpečení serveru)
použití pro odchozí připojení SLIP 118
QRMTSIGN (umožnění vzdáleného přihlášení)
hodnota nastavená příkazem CFGSYSSEC 35
použití ukončovacího programu 72
vliv hodnoty *FRCSIGNON 102
zdroj vzorového ukončovacího programu 147
QSECURITY (úroveň zabezpečení)
hodnota nastavená příkazem CFGSYSSEC 35
popis 3
QSYSLIBL (systémový seznam knihoven)
ochrana 76
QUSEADPAUT (použití adoptovaného oprávnění) 71
tisk souvisejících se zabezpečením 7, 31
úvod 4
systémová hodnota *(pokračování)*
zabezpečení
nastavení 35
zachycení dat zabezpečení serveru (QRETSVRSEC)
popis 26
systémová hodnota akce obnovy zařízení (QDEVRCYACN)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
vyvarování se bezpečnostního rizika 105
systémová hodnota akce, která se má provést, když se dosáhne maxima pokusů o zadání hesla (QMAXSGNACN)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota automatická konfigurace (QAUTOCFG)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota automatická konfigurace virtuálního zařízení (QAUTOVRT)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota fronta zpráv neaktivní úlohy (QINACTMSGQ)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota maximální počet pokusů o přihlášení (QMAXSIGN)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota omezení správce systému (QLMTSECOFR)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota ověření objektů při obnově (QVFYOBJRST)
digitální podpis 68
systémové hodnoty pro obnovu
systémové hodnoty pro obnovu (QVFYOBJRST) 68
systémová hodnota ověření obnovy objektu (QVFYOBJRST)
navrhované použití 75
systémová hodnota použití adoptovaného oprávnění (QUSEADPAUT) 71
systémová hodnota pro požadovaný rozdíl mezi hesly (QPWDRQDDIF)
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota prodleva neaktivní úlohy (QINACTITV)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota prodleva odpojené úlohy (QDSCJOBITV)
doporučené nastavení 22
systémová hodnota prodleva odpojené úlohy (QDSCJOBITV) *(pokračování)*
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota programu pro ověření platnosti hesla (QPWDVLDPGM)
použití ukončovacího programu 72
zdroj vzorového ukončovacího programu 147
systémová hodnota QALWOBJRST (umožnění obnovy objektu)
hodnota nastavená příkazem CFGSYSSEC 35
navrhované použití 75
systémová hodnota QAUDCTL (řízení monitorování)
změna 29
zobrazení 29
systémová hodnota QAUDLVL (úroveň monitorování)
změna 29
zobrazení 29
systémová hodnota QAUTOCFG (automatická konfigurace)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota QAUTOVRT (automatická konfigurace virtuálního zařízení)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota QDEVRCYACN (akce obnovy zařízení)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
vyvarování se bezpečnostního rizika 105
systémová hodnota QDSCJOBITV (prodleva odpojené úlohy)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota QDSPSGNINF (zobrazení informací o přihlášení)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota QINACTITV (prodleva neaktivní úlohy)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota QINACTMSGQ (fronta zpráv neaktivní úlohy)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota QLMTSECOFR (omezení správce systému)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota QMAXSGNACN (akce, která se má provést, když se dosáhne maxima pokusů o zadání hesla)
doporučené nastavení 22

systémová hodnota QMAXSGNACN (akce, která se má provést, když se dosáhne maxima pokusů o zadání hesla) *(pokračování)*
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota QMAXSIGN (maximální počet pokusů o přihlášení)
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota QPWDEXPITV (interval ukončení platnosti hesla)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota QPWDLMTAJC (omezené sousední znaky v hesle)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota QPWDLMTCHR (omezené znaky v hesle)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota QPWDMAXLEN (maximální délka hesla)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota QPWDMINLEN (minimální délka hesla)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota QPWDPOSDIF (požadovaný rozdíl mezi pozicemi v hesle)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota QPWDRQDDGT (požadovaný numerický znak v hesle)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota QPWDRQDDIF (požadovaný rozdíl mezi hesly)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
systémová hodnota QPWDVLDPGM (program pro ověření platnosti hesla)
doporučené nastavení 15
hodnota nastavená příkazem CFGSYSSEC 35
použití ukončovacího programu 72
zdroj vzorového ukončovacího programu 147
systémová hodnota QRETSVRSEC (zachycení dat zabezpečení serveru)
popis 26
použití pro odchozí připojení SLIP 118
systémová hodnota QRMTSIGN (umožnění vzdáleného přihlášení)
hodnota nastavená příkazem CFGSYSSEC 35
použití ukončovacího programu 72
systémová hodnota QRMTSIGN (umožnění vzdáleného přihlášení) *(pokračování)*
vliv hodnoty *FRCSIGNON 102
zdroj vzorového ukončovacího programu 147
systémová hodnota QSECURITY (úroveň zabezpečení)
hodnota nastavená příkazem CFGSYSSEC 35
popis 3
systémová hodnota QSYSLIBL (systémový seznam knihoven)
ochrana 76
systémová hodnota QUSEADPAUT (použití adoptovaného oprávnění) 71
systémová hodnota QVFYOBJRST (ověření obnovy objektu)
navrhované použití 75
systémová hodnota řízení monitorování (QAUDCTL)
změna 29
zobrazení 29
systémová hodnota systémový seznam knihoven (QSYSLIBL)
ochrana 76
systémová hodnota umožnění obnovy objektu (QALWOBJRST)
hodnota nastavená příkazem CFGSYSSEC 35
navrhované použití 75
systémová hodnota umožnění vzdáleného přihlášení (QRMTSIGN)
hodnota nastavená příkazem CFGSYSSEC 35
použití ukončovacího programu 72
vliv hodnoty *FRCSIGNON 102
zdroj vzorového ukončovacího programu 147
systémová hodnota úroveň monitorování (QAUDLVL)
změna 29
zobrazení 29
systémová hodnota zachycení dat zabezpečení serveru (QRETSVRSEC)
popis 26
použití pro odchozí připojení SLIP 118
systémová hodnota zobrazení informací o přihlášení (QDSPSGNINF)
doporučené nastavení 22
hodnota nastavená příkazem CFGSYSSEC 35
systémy souborů root (/), QOpenSys a uživatelem definované systémy souborů 89
systémy souborů, root (/), QOpenSys a uživatelem definované 89
systémy souborů, zabezpečení pro root (/), QOpenSys a uživatelem definované 90
systémy, zabezpečení pro root (/), QOpenSys a uživatelem definované soubory 90

Š

šifrování
heslo
relace PC 143

T

TCP/IP
protokol pro dvoubodové připojení (PPP)
pokyny k zabezpečení 119
TFTP (Trivial File Transfer Protocol)
omezení portu 123
rady týkající se zabezpečení 123
tisk
atributy sítí 31
atributy zabezpečení systému 7
hodnoty popisu podsystému související se zabezpečením 31
informace o seznamu oprávnění 52
informace o adoptovaných objektech 31
informace o seznamu oprávnění 31
nastavení komunikací související se zabezpečením 31
parametry fronty úloh související se zabezpečením 33
parametry výstupní fronty související se zabezpečením 33
seznam objektů jiných než IBM 31
systémové hodnoty 31
triggery 31
veřejně oprávněné objekty 33
záznamy monitorovacího žurnálu 31
trigger
monitorování použití 71
ohodnocení použití 72
výpis všech 31
Trivial File Transfer Protocol (TFTP)
omezení portu 123
rady týkající se zabezpečení 123
trojský kůň
kontrola 72
popis 72
převzetí adoptovaného oprávnění 70
třída uživatele
analýza přiřazení 31
nesrovnalost se zvláštním oprávněním 57

U

uid
změna 97
ukončení platnosti
uživatelský profil
nastavení plánu 24, 28
zobrazení plánu 28
ukončovací program
API QHFRGFS 72
API QTNADDCR 72
atribut sítě přístup k požadavku DDM (DDMACC) 72, 147
atribut sítě přístup k požadavku klienta (PCSACC) 72, 147
automatické vyčištění (QEZUSRCLNP) 72
funkce registrace 74
funkce systému souborů 72
funkční klávesa emulace 3270 72
kolekce údajů o výkonu 72
ODBC (Open DataBase Connectivity) 147
oddělovací stránky 72
operace potvrzení 72

ukončovací program *(pokračování)*
operace vrácení do původního stavu 72
popis tiskového zařízení 72
popis zprávy 72
program klávesy Attention 72
program QUSCLSXT 72
prostředky 147
příkaz RCVJRNE 72
příkaz SETATNPGM (Nastavení programu klávesy Attention) 72
příkaz STREML3270 (Spuštění emulace obrazovky 3270) 72
příkaz TRCJOB (Trasování úlohy) 72
seznam záloh (příkaz CHGBCKUP) 72
systémová hodnota programu pro ověření platnosti hesla (QPWDVLDPGM) 72, 147
systémová hodnota QATNPGM (program klávesy Attention) 72
systémová hodnota umožnění vzdáleného přihlášení (QRMTSIGN) 72, 147
výběr formátu 72
výběr formátu logického souboru 72
vyhodnocení 72
vytvoření loadu produktu (příkaz CRTPRDLOD) 72
využití databázového souboru 72
získání záznamů žurnálu 72
změna popisu zprávy (příkaz CHGMSGD) 72
ukončovací program QEZUSRCLNP 72
úloha přímého průchodu
spuštění 104
úloha, APPC
přiřazení uživatelského profilu 103
uložení
hesla 26
nástroje zabezpečení 28
Upozornění 153
úroveň monitorování *PGMADP (adoptování programů) 69
úroveň monitorování adoptování programů (*PGMADP) 69
úroveň zabezpečení 10
migrace z 41
oprávnění k objektu 41
úroveň zabezpečení 20
migrace z 41
oprávnění k objektu 41
úrovně hesla
nastavení 16
plánování 16
úvod 16
změna 16, 17, 19, 20
útok typu ″piggy-backing″ 108
útok typu ″sniffing″ 143
uživatel
úloha APPC 101
uživatel APPC získává přístup k cílovému systému 101
uživatel, metody, které systém používá k posílání informací o 101
uživatelské profily servisních nástrojů
správa DST 58
uživatelské profily servisních nástrojů (DST) 58
uživatelské prostředí
monitorování 57
uživatelský objekt
v chráněných knihovnách 75
uživatelský profil
analýza
dle třídy uživatele 31
dle zvláštních oprávnění 31
analýza pomocí dotazu 46
automatické odstranění 24
deaktivace
automaticky 24
kontrola existence předvolených hesel 28
menu řízení přístupu 42
monitorování 77
oprávnění uživatelé 46
monitorování nastavení prostředí 57
monitorování třídy uživatele 57
monitorování zvláštních oprávnění 56
nesrovnalosti mezi zvláštními oprávněními a třídou uživatele 57
odstranění neaktivních 24
plánování aktivace 23
plánování deaktivace 23
plánování ukončení platnosti 24
předvolené heslo 25
přiřazení pro úlohu APPC 103
seznam trvale aktivních
změna 28
stav deaktivace (*DISABLED) 25
tisk
Viz též výpis
prostředí 58
zvláštní oprávnění 56
úvod 4
velký, prozkoumání 47
výpis
neaktivní 47
uživatelé s možností zadávat příkazy 47
uživatelé se zvláštním oprávněním 47
vybraný 47
zabránění deaktivaci 24
zobrazení plánu expirace 25
zpracování neaktivních 24
uživatelský profil QPGMR (programátor)
heslo nastavené příkazem CFGSYSSEC 37
uživatelský profil QSRV (servis)
heslo nastavené příkazem CFGSYSSEC 37
uživatelský profil QSRVBAS (základní servis)
heslo nastavené příkazem CFGSYSSEC 37
uživatelský profil QUSER (uživatel)
heslo nastavené příkazem CFGSYSSEC 37

V

velký uživatelský profil 47
veřejné oprávnění
monitorování 51
tisk 33
vyvolání 35
vyvolání pomocí příkazu RVKPUBAUT 37
veřejné oprávnění ke kořenovému adresáři 91
vir
definice 67
detekce 48
ochrana proti 67
ochranné mechanismy serveru iSeries 68
prozkoumání 68
snímání 48
vlastnictví objektů 45
vlastnictví, objekty 45
vyčištění, automatické
ukončovací program 72
vyhodnocení
naplánované programy 74
registrovaný ukončovací 74
vynechání přihlášení
důsledky zabezpečení 143
vynucení
vytvoření programu 68
výpis
obsah knihovny 48
všechny knihovny 48
vybrané uživatelské profily 47
výstupní fronta
monitorování přístupu 55
tisk parametrů souvisejících se zabezpečením 33
tisk pro uživatelské profily 57
vytvoření adresáře pomocí rozhraní API 95
vytvoření objektu pomocí rozhraní PC 95
vytvoření proudového souboru pomocí rozhraní open() nebo creat() 95
využití souboru
ukončovací program 72
vyvolání
veřejné oprávnění 35
vzdálená úloha
zabránění 105
vzdálený příkaz
omezení pomocí záznamu PGMEVOKE 106
zabránění 105, 144
vzdálený systém
definice 99

Z

zabezpečené spojení 100
zabezpečené webové stránky 132
zabezpečení
komunikace TCP/IP 111
nástroje zabezpečení 27
zabezpečení a produkt iSeries Navigator 142
zabezpečení adresářů 94
zabezpečení komunikace APPC 99
zabezpečení LP 61
zabezpečení na úrovni knihoven 44
zabezpečení na úrovni prostředků
definice 3
omezený přístup
úvod 5
úvod 5
zabezpečení na úrovni přihlášení
definice 3
zabezpečení pro nové objekty 94

zabezpečení pro systémy souborů root (/), QOpenSys a uživatelem definované systémy souborů 90
zabezpečení, fyzické 77
zabezpečení, integrovaný systém souborů 87
zabezpečení, LP 61
zabránění
  vstup TCP/IP 111
zadání
  sestavy o zabezpečení 30
základní prvky komunikace APPC 99
základní prvky zabezpečení 3
základy relace APPC 100
záznam fronty úloh
  rady týkající se zabezpečení 80
záznam jména pracovní stanice
  rady týkající se zabezpečení 79
záznam jména vzdáleného systému
  rady týkající se zabezpečení 80
záznam komunikací
  předvolený uživatel 103
  rady týkající se zabezpečení 80
  režim 103
záznam směrování
  odstranění záznamu PGMEVOKE 106
  rady týkající se zabezpečení 80
záznam typu pracovní stanice
  rady týkající se zabezpečení 79
záznam žurnálu
  CP (změna profilu)
    navrhované použití 23, 24
  odeslání 49
  získání
    ukončovací program 72
záznam žurnálu CP (změna profilu)
  navrhované použití 23, 24
záznam žurnálu SV (systémová hodnota)
  navrhované použití 76
zdrojový systém
  definice 99
získání záznamů žurnálu
  ukončovací program 72
Získání záznamů žurnálu (RCVJRNE)
  ukončovací program 72
změna
  hesla dodaná IBM 20
  chybové zprávy pro přihlášení 22
  monitorování zabezpečení 29
  seznam aktivních profilů 28
  uid 97
  známá hesla 20
známé heslo
  změna 20
zobrazení
  členy skupinového profilu 43
  monitorování zabezpečení 29
  oprávnění k objektu 48
  oprávnění uživatelé 46
  programy, které adoptují 49
  systémová hodnota QAUDCTL (řízení monitorování) 29
  systémová hodnota QAUDLVL (úroveň monitorování) 29
  uživatelský profil
    plán aktivace 28
    plán expirace 28
    seznam aktivních profilů 28
zobrazení *(pokračování)*
  uživatelský profil *(pokračování)*
    soukromá oprávnění 81
zpráva
  CPF1107 22
  CPF1120 22
  ukončovací program 72
zpráva CPF1107 22
zpráva CPF1120 22
zvláštní oprávnění
  *SAVSYS (uložení systému)
    řízení 75
  analýza přiřazení 31
  monitorování 56
  nesrovnalost s třídou uživatele 57
  výpis uživatelů 47
zvláštní oprávnění *IOSYSCFG (konfigurace systému)
  požadované pro příkazy pro konfiguraci APPC 101
zvláštní oprávnění *SAVSYS (uložení systému)
  řízení 75

Ž

žurnál monitorování zabezpečení
  tisk záznamů 31
žurnál QAUDJRN (monitorovací)
  poškozený 50
  prahová hodnota paměti příjemce 50
  správa 49
  systémové záznamy 50

Připomínky čtenářů

iSeries
Rady a nástroje pro zabezpečení serveru iSeries
Verze 5

Publikace č. SC09-3653-07

Uvítali bychom jakoukoli připomínku k této publikaci. Může se týkat chyb nebo vynechání, přesnosti, organizace, témat nebo úplnosti této knihy. Měla by se ale týkat pouze informací v tomto manuálu a způsobu jejich prezentace.

Technické dotazy zodpoví a informace o produktech a cenách podá zástupce IBM, obchodní partner IBM nebo autorizovaný prodejce IBM.

Se všeobecnými dotazy se obracejte na IBM DM/CRC (telefon 272131111).

Pokud odešlete připomínky IBM, udělujete tím společnosti IBM nevýhradní právo takovéto připomínky používat nebo distribuovat libovolným způsobem dle svého uvážení, aniž by tím vznikl IBM jakýkoli závazek vůči vám.

Připomínky:

Děkujeme vám za pomoc.

Své připomínky můžete zaslat následujícími způsoby:
- Zašlete formulář poštou na adresu uvedenou na druhé straně.
- Zašlete fax na následující číslo: Spojené státy a Kanada: 1-800-937-3430
- Své připomínky zašlete e-mailem na adresu: RCHCLERK@us.ibm.com

Pokud chcete odpověď od IBM, vyplňte, prosím, následující údaje:

Jméno | Adresa

Firma

Telefon | E-mail

IBM ČESKÁ REPUBLIKA
ODDĚLENÍ DM/CRC
V Parku 2294/4, The Park
148 00 Praha 4 - Chodov

Vytištěno v Dánsku společností IBM Danmark A/S.

SC09-3653-07