IBM

eserver

iSeries

# Tipy a nástroje pre zabezpečenie vášho iSeries

*Verzia 5*

SA12-6235-07

IBM

@server

iSeries

# Tipy a nástroje pre zabezpečenie vášho iSeries

*Verzia 5*

SA12-6235-07

**Poznámka**

Pred použitím týchto informácií a produktu, ktorý podporujú, si nezabudnite prečítať informácie v “Poznámky” na strane 149.

**Ôsme vydanie (Apríl 2004)**

Toto vydanie sa týka verzie 5, vydania 3, modifikácie 0 operačného systému IBM Operating System/400 (číslo produktu 5722-SS1) a všetkých následných vydaní a modifikácií pokiaľ nebude v nových vydaniach uvedené inak. Táto verzia nebeží na všetkých modeloch počítačov RISC (reduced instruction set computer) ani na modeloch CISC.

Toto vydanie nahrádza SC41-5300-06.

# Obsah

# Obrázky

# Tabuľky

# Tipy a nástroje pre zabezpečenie Vášho iSeries (SC41-5300-07)

Úloha počítačov v organizáciách sa rýchle mení. IT manažéri, poskytovatelia softvéru, správcovia bezpečnosti a audítori sa musia preto na veľa oblastí pozerať v inom svetle. Na tomto zozname by sa mala nachádzať bezpečnosť iSeries.

Systémy poskytujú mnoho nových funkcií, ktoré sú veľmi odlišné od tradičných účtovných aplikácií. Používatelia vstupujú do systémov novými spôsobmi: pomocou LAN, komunikačnými linkami (volajúcimi), bezdrôtovými spojeniami, sieťami všetkých typov. Často používatelia nikdy neuvidia prihlasovaciu obrazovku. Mnoho organizácií sa rozmáha, aby sa stali "rozšírenými podnikmi", buď pomocou vlastných sietí alebo pomocou internetu

Zrazu sa zdá, že systémy majú celú novú sadu dverí a okien. Manažéri a správcovia bezpečnosti systému sa oprávnene zaujímajú o to, ako ochrániť informačný majetok v tomto rapídne sa meniacom prostredí.

Tieto informácie poskytujú množinu praktických návrhov pre používanie bezpečnostných funkcií iSeries a pre vytvorenie prevádzkových postupov, ktoré sú bezpečné. Odporúčania v týchto informáciách platia pre inštaláciu s priemernými požiadavkami a odhaleniami bezpečnosti. Tieto informácie neposkytujú úplný opis dostupných bezpečnostných vlastností iSeries. Ak si chcete prečítať o ďalších voľbách alebo ak potrebujete úplnejšie základné informácie, pozrite si publikácie, ktoré sú popísané v Kapitola 17, "Súvisiace informácie", na strane 147.

Tieto informácie tiež opisujú, ako sa majú nastaviť a používať bezpečnostné nástroje, ktoré sú súčasťou OS/400. Kapitola 4, "Konfigurácia iSeries na používanie Security Tools", na strane 25 a "Príkazy a ponuky pre príkazy bezpečnosti" na strane 26 poskytujú referenčné informácie o bezpečnostných nástrojoch. Tieto informácie poskytujú príklady pre používanie týchto nástrojov.

## Kto by si mal prečítať túto knihu

Za bezpečnosť systému je zodpovedný **správca bezpečnosti** alebo **administrátor bezpečnosti**. Táto zodpovednosť zvyčajne zahŕňa nasledujúce úlohy:

- Nastavovanie a riadenie užívateľských profilov
- Nastavenie hodnôt v celom systéme, ktoré ovplyvnia bezpečnosť
- Správa oprávnení na objekty
- Presadzovanie a monitorovanie bezpečnostných politík

Ak ste zodpovedný za správu bezpečnosti pre jeden alebo viac systémov iSeries, tieto informácie sú určené vám. Pokyny v týchto informáciách predpokladajú nasledujúce:

- Poznáte základné iSeries operačné postupy, ako napríklad prihlásenie sa a používanie príkazov.
- Poznáte základné zložky iSeries bezpečnosti: bezpečnostné úrovne, bezpečnostné systémové hodnoty, užívateľské profily a bezpečnosť objektov.

**Poznámka:** Kapitola 1, "Základné komponenty bezpečnosti iSeries", na strane 3 poskytuje prehľad týchto zložiek. Ak sú tieto prvky pre vás nové, prečítajte si tému *Základná bezpečnosť a plánovanie* v Informačnom centre. Pozrite si časť "Nevyhnutné predpoklady a súvisiace informácie" na strane xii, kde nájdete viac informácií.

- Aktivovali ste bezpečnosť na vašom systéme nastavením systémovej hodnoty bezpečnostnej úrovne (QSECURITY) najmenej na 30.

IBM neustále vylepšuje bezpečnostné schopnosti iSeries. Ak chcete využívať tieto výhody, mali by ste pravidelne používať kumulatívny opravný balík, ktorý je dostupný pre vaše vydanie. Pozrite si, či obsahuje opravy, týkajúce sa bezpečnosti.

## Ako tieto informácie používať

Ak ste nenastavili váš systém na používanie bezpečnostných nástrojov, alebo ak ste nainštalovali Security ToolKit for OS/400 pre skoršie vydania, urobte nasledovné:

1. Začnite s časťou Kapitola 2, “Sprievodca bezpečnosťou iSeries a Plánovač bezpečnosti eServer”, na strane 9. Táto opisuje, ako používať tieto vlastnosti na výber, ktoré bezpečnostné nástroje sú odporúčané a ako s nimi začať.
2. Viac informácií o základnej bezpečnosti si môžete prezrieť v informáciách Prehľadu bezpečnosťou, ktoré sú umiestnené on-line v iSeries Information Center.

**Poznámka**

Tieto informácie obsahujú *mnoho* tipov pre zabezpečenie iSeries. Váš systém možno potrebuje ochranu len v niektorých oblastiach. Tieto informácie použite na to, aby ste sa naučili o možných odhaleniach bezpečnosti a ich náprave. Potom zamerajte vaše úsilie na oblasti, ktoré sú najkritickejšie vo vašom systéme.

## Nevyhnutné predpoklady a súvisiace informácie

Použite iSeries Information Center ako východiskový bod pre vyhľadanie technických informácií o iSeries.

Na Information Center sa môžete dostať dvomi spôsobmi:

- Na nasledovnej WWW lokalite:

  `http://www.ibm.com/eserver/iseries/infocenter`
- Z *Informačné centrum iSeries*, SK3T-4091-04 CD-ROM. Tento CD-ROM sa dodáva s vaším novým hardvérom iSeries alebo s objednávkou novej verzie softvéru IBM Operating System/400. CD-ROM si môžete objednať z IBM Publications Center:

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

iSeries Information Center obsahuje nové a aktualizované informácie o iSeries ako je inštalácia softvéru a hardvéru, Linux, WebSphere, Java, vysoká dostupnosť, databáza, logické oddiely, CL príkazy a systémové API (aplikačné programovacie rozhrania). Okrem toho poskytuje poradcov a vyhľadávače, ktoré vám pomôžu pri plánovaní, odstraňovaní problémov a konfigurácii vášho hardvéru a softvéru iSeries.

S každou novou objednávkou hardvéru dostanete *iSeries Setup and Operations CD-ROM*, SK3T-4098-02. Tento CD-ROM obsahuje IBM **@server** IBM e(logo)server iSeries Access for Windows a Sprievodcu EZ-Setup. iSeries Access Family ponúka výkonnú sadu klientskych a serverových schopností na pripojenie PC k serverom iSeries. Sprievodca EZ-Setup automatizuje mnohé úlohy nastavovania iSeries.

## Ako posielať vaše pripomienky

Spätná väzba z vašej strany je dôležitá, lebo pomáha poskytovať presnejšie a kvalitnejšie informácie. Ak máte k tejto publikácii alebo k ľubovoľnej dokumentácii k iSeries nejaké pripomienky, vyplňte formulár pripomienok čitateľa na konci tejto publikácie.

- Ak dávate prednosť zaslaniu pripomienok poštou, použite formulár na pripomienky čitateľov s adresou, ktorá je vytlačená na jeho zadnej strane. Ak posielate komentáre čitateľa poštou z inej krajiny ako USA, môžete dať tento formulár miestnej pobočke IBM alebo predstaviteľovi IBM, ktorý tento formulár doručí zadarmo namiesto vás.
- Ak chcete poslať pripomienky faxom, použite jedno z nasledujúcich čísel:
  - USA, Kanada a Portoriko: 1-800-937-3430
  - Ostatné krajiny: 1-507-253-5192
- Ak radšej posielate pripomienky elektronicky, použite tieto e-mailové adresy:
  - Pripomienky k príručkám:

    RCHCLERK@us.ibm.com
  - Pripomienky k informačnému centru iSeries:

    RCHINFOC@us.ibm.com

Uistite sa, že ste uviedli nasledujúce

- Názov publikácie alebo tému v informačnom centre iSeries.
- Číslo vydania knihy.
- Číslo strany alebo tému v publikácii, ktorej sa týkajú pripomienky.

# Časť 1. Základná bezpečnosť iSeries

# Kapitola 1. Základné komponenty bezpečnosti iSeries

Táto téma poskytuje stručný prehľad základných komponentov, ktoré fungujú spolu za účelom poskytovania bezpečnosti iSeries. V ostatných častiach tejto príručky ideme až mimo základov, aby sme poskytli tipy na používanie týchto komponentov bezpečnosti, ktoré by spĺňali potreby vašej organizácie.

## Úrovne bezpečnosti

Nastavením systémovej hodnoty úrovne bezpečnosti (QSECURITY) môžete vybrať, akou úrovňou bezpečnosti by mal váš systém operovať. Systém ponúka päť úrovní bezpečnosti:

**Úroveň 10:**

**Systém si nepresadzuje žiadnu bezpečnosť.** Nie je potrebné žiadne heslo. Ak daný užívateľský profil neexistuje v systéme, keď sa niekto prihlasuje, systém ho vytvorí.

**POZOR:**

Počnúc V4R3 a budúcimi vydaniami nebudete môcť nastaviť systémovú hodnotu QSECURITY na hodnotu 10. Ak je váš systém v súčasnosti nastavený na úroveň bezpečnosti 10, pri inštalácii verzie 4 vydanie 3 zostane na úrovni 10. Ak zmeníte úroveň bezpečnosti na inú hodnotu, nemôžete ju zmeniť späť na hodnotu 10. Pretože hodnota 10 neposkytuje žiadnu ochranu bezpečnosti, bezpečnostnú úroveň 10 IBM neodporúča. **IBM nebude poskytovať podporu pre žiadne problémy, ktoré sa vyskytnú na úrovni 10, ak sa tento problém netýka aj vyšších úrovní bezpečnosti.**

**Úroveň 20:**

Systém vyžaduje užívateľské ID a heslo pre prihlasovanie. Bezpečnostná úroveň 20 sa často spomína ako **prihlasovacia bezpečnosť**.Štandardne majú všetci používatelia prístup ku všetkým objektom, pretože všetci používatelia majú špeciálne oprávnenie *ALLOBJ.

**Úroveň 30:**

Systém vyžaduje užívateľské ID a heslo pre prihlasovanie. Používatelia musia mať oprávnenie na používanie objektov, pretože štandardne sa im neprideľujú žiadne oprávnenia. Nazýva sa to **zdrojová bezpečnosť**.

**Úroveň 40:**

Systém vyžaduje užívateľské ID a heslo pre prihlasovanie. Okrem zdrojovej bezpečnosti systém poskytuje **ochranu integrity** funkcie. Funkcie ochrany integrity, ako napríklad validácia parametrov pre rozhrania na operačný systém, sú určené na ochranu vášho systému i na ochranu objektov vo vašom systéme, aby ich nesfalšovali skúsení používatelia systému. Pre väčšinu inštalácií sa odporúča bezpečnostná úroveň 40. Keď dostanete nový systém iSeries s V4R5 alebo s novším vydaním, úroveň bezpečnosti bude nastavená na 40.

**Úroveň 50:**

Systém vyžaduje užívateľské ID a heslo pre prihlasovanie. Systém posilňuje bezpečnosť zdroja, ako aj ochranu integrity úrovne 40, ale pridáva **rozšírenú ochranu integrity**, ako je napríklad, obmedzenie spracovania správ medzi stavovými programami systému a stavovými programami užívateľa. Bezpečnostná úroveň 50 je určená pre systémy iSeries s vysokými bezpečnostnými požiadavkami.

**Poznámka:** Úroveň 50 je požadovaná úroveň pre certifikáciu C2 (a certifikáciu FIPS-140).

Kapitola 2 príručky *iSeries Security Reference* poskytuje viac informácií o bezpečnostných úrovniach a popisuje ako prechádzať z jednej bezpečnostnej úrovne na druhú.

## Globálne nastavenia

Váš systém má globálne nastavenia, ktoré majú vplyv na to, ako práca vstupuje do systému a na to, ako sa systém objaví ostatným užívateľom systému. Tieto nastavenia zahŕňajú nasledovné:

**Bezpečnostné systémové hodnoty:**
Bezpečnostné systémové hodnoty sa používajú na riadenie bezpečnosti vo vašom systéme. Tieto hodnoty sú rozdelené do štyroch skupín:
- Všeobecné bezpečnostné systémové hodnoty
- Ostatné systémové hodnoty, súvisiace s bezpečnosťou
- Systémové hodnoty, ktoré riadia heslá
- Systémové hodnoty, ktoré riadia auditovanie

Niektoré témy v tomto kniha pojednávajú o zmysle špecifických systémových hodnôt. Kapitola 3 v knihe *iSeries Security Reference* popisuje všetky systémové hodnoty vzťahujúce sa na bezpečnosť.

**Atribúty siete:**
Atribúty siete regulujú participáciu vášho systému v sieti s inými systémami (alebo zvolia možnosť neparticipovať). Viac informácií o atribútoch siete nájdete v knihe *Work Management*.

**Opisy podsystémov a ďalšie komponenty riadenia práce:**
Komponenty riadenia práce určujú, ako práca vstupuje do systému a v akom prostredí práca prebieha. Niekoľko tém o týchto informáciách pojednáva o bezpečnostných implikáciách niektorých hodnôt riadenia práce. Kniha *Work Management* poskytuje kompletné informácie.

**Konfigurácia komunikácií:**
Vaša konfigurácia komunikácií tiež ovplyvní vstup práce do vášho systému. Niekoľko tém o týchto informáciách poskytuje návrhy na ochranu vášho systému, keď sa nachádza v sieti.

## Užívateľské profily

Každý systémový užívateľ **musí** mať užívateľský profil. Najprv musíte vytvoriť užívateľský profil, a potom sa užívateľ môže prihlásiť. Užívateľské profily sa môžu použiť aj na riadenie prístupu na servisné nástroje, akými sú DASD a výpisy hlavnej pamäte. Pozrite si “Riadenie servisných nástrojov” na strane 57, kde nájdete viac informácií.

Užívateľský profil je výkonný a flexibilný nástroj. Reguluje činnosti, ktoré môže užívateľ vykonávať a upravuje spôsob, ako sa systém užívateľovi objaví. Príručka *iSeries Security Reference* popisuje všetky parametre v užívateľskom profile.

## Skupinové profily

Skupinový profil je špeciálnym typom užívateľského profilu. Skupinový profil môžete použiť na definovanie oprávnenia pre skupinu užívateľov, aby ste nemuseli zadávať oprávnenia pre každého užívateľa zvlášť. Skupinový profil môžete použiť aj ako vzor keď vytvárate jednotlivé užívateľské profily s použitím funkcie kopírovania profilu, alebo ak používate iSeries Navigator, môžete na úpravu užívateľských oprávnení použiť ponuku bezpečnostných politík.

Kapitoly 5 a 7 v knihe *iSeries Security Reference* poskytujú viac informácií o plánovaní a používaní skupinových profilov.

## Zdrojová bezpečnosť

Zdrojová bezpečnosť v systéme vám umožňuje definovať, kto môže používať objekty, a ako tieto objekty môžu byť používané. Schopnosť sprístupniť objekt sa nazýva **oprávnenie**. Keď nastavujete oprávnenie na objekt, musíte sa postarať o to, aby ste dali vašim užívateľom dostatok oprávnenia na ich prácu bez toho, aby ste im dali oprávnenie na prehliadanie a zmenu systému. Oprávnenie na objekt dáva užívateľovi povolenia pre špecifický objekt a môže zadať, čo má užívateľ dovolené s objektom robiť. Zdroj objektov môže byť obmedzený prostredníctvom určitých podrobných užívateľských oprávnení, ako je pridávanie záznamov alebo ich zmena. Systémové zdroje sa môžu používať na udelenie prístupu užívateľovi k určitých systémom definovaným podsadám oprávnení: *ALL, *CHANGE, *USE a *EXCLUDE.

Súbory, programy, knižnice a adresáre sú najbežnejšími systémovými objektmi, ktoré vyžadujú ochranu bezpečnosti zdroja, ale vy môžete uviesť oprávnenie pre ľubovoľný objekt v systéme.

Kapitola 5, “Ochrana informačného majetku s oprávnením k objektu” pojednáva o dôležitosti nastavovania oprávnenia objektu vo vašom systéme. Kapitola 5 v knihe *iSeries Security Reference* popisuje možnosti pre nastavenie zdrojovej bezpečnosti.

## Obmedzenie prístupu k funkciám programu

Obmedzenie prístupu k funkciám programu vám umožňuje poskytovať bezpečnosť pre program, keď nemáte objekt iSeries na zabezpečenie programu. Aj keď V4R3 ešte neobsahuje podporu obmedzovania prístupu k funkciám programu, je možné uplatňovať obmedzenia prístupu, ak vytvoríte autorizačný zoznam alebo iný objekt, a pomocou neho budete riadiť prístup k funkciám programu. Takto vám obmedzovanie prístupu k funkciám programu zabezpečí ľahkú kontrolu prístupu k aplikáciám, jednotlivým častiam aplikácií alebo funkciám v rámci programu.

Existujú dve metódy, ktoré môžete použiť na riadenie užívateľského prístupu na funkcie aplikácií prostredníctvom iSeries Navigator. Prvá metóda používa podporu Správy aplikácie:

1. Pravým tlačidlom kliknite na systém, ktorý obsahuje funkciu, ktorej chcete zmeniť nastavenie prístupu.
2. Vyberte **Správa aplikácií**.
3. Ak sa nachádzate na administračnom systéme, vyberte **Lokálne nastavenia**. Inak, pokračujte s ďalším krokom.
4. Vyberte spravovateľnú funkciu.
5. Ak je to použiteľné, vyberte **Štandardný prístup**. Výberom tejto voľby umožníte všetkým užívateľom štandardne získať prístup na funkciu.
6. Ak je to použiteľné, vyberte **Prístup na všetky objekty**. Výberom tejto voľby umožníte všetkým užívateľom so systémovým privilégiom na všetky objekty, aby mali prístup na túto funkciu.
7. Ak je to použiteľné, vyberte **Prispôsobiť**. V dialógu **Prispôsobiť prístup** použite tlačidlá **Pridať** a **Odstrániť**, aby ste v zoznamoch **Prístup povolený** a **Prístup zakázaný** pridali alebo odstránili užívateľov alebo skupiny.
8. Ak sa to dá použiť, vyberte **Odstrániť prispôsobenie**. Výberom tejto voľby vymažete všetky prispôsobené prístupy pre vybranú funkciu.
9. Kliknite na **OK**, aby sa dialóg **Správa aplikácií** zatvoril.

Druhá metóda riadenia užívateľského prístupu vyžaduje podporu Užívateľov a skupín aplikácie iSeries Navigator:

1. V iSeries Navigator rozviňte **Používatelia a Skupiny**.
2. Vyberte **Všetci používatelia**, **Skupiny**, alebo **Používatelia mimo skupiny**, aby sa zobrazil zoznam užívateľov a skupín.
3. Pravým tlačidlom kliknite na užívateľa alebo skupinu a vyberte **Vlastnosti**.
4. Kliknite na **Schopnosti**.
5. Kliknite na záložku **Aplikácie**.
6. Túto stránku použite na zmenu nastavenia prístupu pre užívateľa alebo skupinu.
7. Dvakrát kliknite na **OK**, aby sa dialóg **Vlastnosti** zatvoril.

V “Bezpečnosť iSeries Navigator” na strane 138 nájdete viac informácií o bezpečnostných problémoch iSeries Navigator.

Ak ste vy tvorcom aplikácie, obmedziť prístup k funkcii programu API je možné nasledovným spôsobom:

- Registráciou funkcie
- Obnovou informácií o funkcii
- Zadaním, kto môže, a kto nemôže používať funkciu
- Kontrolou, či má užívateľ povolenie používať túto funkciu

**Poznámka:** Táto podpora **nie** je náhradou zdrojovej bezpečnosti. Funkcia limitovania prístupu k programu neochráni užívateľa od sprístupnenia zdroja (ako napríklad súbor alebo program) z iného prostredia.

Aby sa táto podpora mohla používať v rámci aplikácie, poskytovateľ tejto aplikácie musí zaregistrovať funkcie pri inštalovaní aplikácie. Zaregistrované funkcie sa zhodujú s kódovým blokom pre špecifické funkcie v aplikácii. Keď je aplikácia spustená užívateľom, táto aplikácia zavolá API ešte predtým, ako vyvolá kódový blok. Tento API zavolá API na kontrolu používania, aby zistil, či má užívateľ povolenie používať funkciu. Ak má užívateľ povolené používať zaregistrovanú funkciu, spustí sa kódový blok. Ak užívateľ nemá povolené používať túto funkciu, nie je mu umožnené spustiť kódový blok.

**Poznámka:** API vyžaduje zaregistrovanie 30 znakového ID funkcie v registračnej databáze (WRKREGINF). Aj keď neexistujú koncové body, týkajúce sa funkčných ID, používaných obmedzeným prístupom k funkčným API, vyžaduje sa mať koncové body. Ak chcete čokoľvek do tohto registra zaregistrovať, **musíte** dodať názov formátu koncového bodu. Aby ste to mohli urobiť, Registračná funkcia API vytvorí fiktívny názov formátu a použije tento fiktívny názov formátu pre všetky funkcie, ktoré sú zaregistrované. Keďže ide o fiktívny názov formátu, žiadny program koncového bodu nebude nikdy vyvolaný.

Správca systému určí, kto má prístup k funkcii povolený alebo zakázaný. Správca môže na riadenie prístupu do programových funkcií použiť buď API alebo GUI správy aplikácií aplikácie iSeries Navigator. Príručka *iSeries server API Reference* poskytuje informácie o obmedzení prístupu na programovú funkciu API. Viac informácií o kontrolovaní prístupu k funkciám nájdete v “Bezpečnosť iSeries Navigator” na strane 138.

## Audity bezpečnosti

Ľudia auditujú bezpečnosť ich systému z niekoľkých dôvodov:

- Na vyhodnotenie, či je ich bezpečnostný plán úplný.

- Na overenie, že všetky naplánované bezpečnostné prvky sú na mieste a fungujú. Tento typ auditovania zvyčajne vykonáva správca bezpečnosti ako súčasť dennej správy bezpečnosti. Tiež sa vykonáva, niekedy oveľa podrobnejšie, ako súčasť pravidelného vyhodnocovania bezpečnosti internými alebo externými audítormi.
- Na overenie, že bezpečnosť systému drží krok so zmenami v systémovom prostredí. K príkladom zmien, ktoré ovplyvňujú bezpečnosť patria:
  - Vytvorenie nových objektov užívateľmi systému
  - Povolenie vstupu nových užívateľov do systému
  - Zmena vlastníctva objektu (nenastavená autorizácia)
  - Zmena zodpovedností (zmena skupiny užívateľov)
  - Dočasné oprávnenie (včasné neodobratie)
  - Inštalácia nových produktov
- Aby ste sa pripravili na budúcu udalosť, ako je inštalácia novej aplikácie, prechodom na vyššiu bezpečnostnú úroveň alebo nastavením komunikačnej siete.

Tu popísané techniky sú vhodné pre všetky tieto situácie. Čo máte auditovať a ako často závisí na veľkosti a bezpečnostných potrebách vašej organizácie.

Auditovanie bezpečnosti vyžaduje používanie príkazov na vašom systéme a sprístupnenie protokolu a informácií o žurnáli. Môžete vytvoriť osobitný profil, ktorý použije ten, kto vykonáva audit bezpečnosti vášho systému. Profil audítora potrebuje mimoriadne oprávnenie *AUDIT, aby mohol zmeniť charakteristiky auditu systému. Niektoré z odporučených úloh v tejto kapitole vyžadujú užívateľský profil so špeciálnym oprávnením *ALLOBJ a *SECADM. Heslo pre profil audítora nastavte na *NONE, keď sa obdobie auditu ukončí.

Viac informácií o auditovaní bezpečnosti nájdete v kapitole 9 príručky *Prehľad bezpečnosťou*.

## Príklad: Správa o atribútoch systémovej bezpečnosti

Obrázok 1 ukazuje príklad výstupu z príkazu Print System Security Attributes (PRTSYSSECA). Toto hlásenie ukazuje nastavenia pre systémové hodnoty, týkajúce sa bezpečnosti, a sieťové atribúty, ktoré sa odporúčajú pre systémy s normálnymi požiadavkami na bezpečnosť. Tiež ukazuje súčasné nastavenia na vašom systéme.

**Poznámka:** Stĺpec *Current Value* v hlásení zobrazuje súčasné nastavenie na vašom systéme. Porovnajte ho s odporúčanými hodnotami a nájdete tak možné bezpečnostné riziká.

```
System Security Attributes

System Value
Name            Current value          Recommended value
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
```

*Obrázok 1. Hlásenie atribútov systémovej bezpečnosti - Príklad (Diel 1 z 4)*

```
QAUTOCFG         0                    0
QAUTORMT         1                    0
QAUTOVRT         9999                 0
QCMNRCYLMT       0 0                  0 0
QCRTAUT          *CHANGE              Control at library level.
QCRTOBJAUD       *NONE                Control at library level.
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
```

*Obrázok 1. Hlásenie atribútov systémovej bezpečnosti - Príklad (Diel 2 z 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
```

*Obrázok 1. Hlásenie atribútov systémovej bezpečnosti - Príklad (Diel 3 z 4)*

```
System Security Attributes

Network Attribute
Name             Current value        Recommended value
DDMACC           *OBJAUT              *REJECT
JOBACN           *FILE                *REJECT
PCSACC           *OBJAUT              *REJECT
```

*Obrázok 1. Hlásenie atribútov systémovej bezpečnosti - Príklad (Diel 4 z 4)*

# Kapitola 2. Sprievodca bezpečnosťou iSeries a Plánovač bezpečnosti eServer

Nástroje Sprievodca bezpečnosťou servera iSeries a Plánovač bezpečnosti eServer vám môžu pomôcť rozhodnúť sa, ktoré bezpečnostné hodnoty realizovať na vašom serveri iSeries. Pomocou Sprievodcu bezpečnosti servera iSeries v iSeries Navigator môžete vytvoriť výpisy, ktoré odrážajú vaše bezpečnostné potreby na základe vašich vybratých odpovedí. Toto potom môžete použiť na nakonfigurovanie bezpečnosti vášho systému.

Sprievodcu bezpečnosťou iSeries alebo Plánovač bezpečnosti eServer použite na pomoc pri plánovaní a implementácii základnej bezpečnostnej politiky pre vaše servery iSeries. Cieľom oboch nástrojov je uľahčiť vám implementáciu a riadenie bezpečnosti na vašich systémoch. Sprievodca, ktorý je dostupný ako súčasť OS/400, vám položí niekoľko otázok vyššej úrovne o vašom serverovom prostredí a na základe vašich odpovedí vám poskytne sadu odporúčaní, ktoré sprievodca dokáže ihneď použiť vo vašom systéme.

Plánovač bezpečnosti eServer je on-line verzia Sprievodcu bezpečnosti. Umožňuje vám vybrať vaše voľby na základe vašich bezpečnostných požiadaviek a potom vám dá výpis s návrhom, čo je potrebné na zabezpečenie vášho systému.

Plánovač bezpečnosti eServer je webová verzia sprievodcu. Poskytuje odporúčania pre implementáciu bezpečnosti do vášho systému tak, ako to robí sprievodca. Poradca však nemôže aplikovať odporúčania. Namiesto toho vygeneruje zoznam hodnôt systémovej bezpečnosti a iné atribúty, ktoré by ste, na základe odpovedí na otázky poradcu, mali vo vašom systéme použiť.

## Sprievodca bezpečnosťou

Rozhodovanie o tom, ktoré bezpečnostné hodnoty systému iSeries by ste mali použiť pre vašu firmu, môže byť komplikované. Ak je implementácia bezpečnosti do serverov iSeries alebo keď sa prostredie, v ktorom máte spustený svoj server iSeries, nedávno zmenilo s rozhodnutím vám dokáže pomôcť Sprievodca bezpečnosťou.

**Čo je to sprievodca?**

- Sprievodca je nástroj, ktorý je vytvorený, aby ho mohol spúšťať používateľ, ktorý je nováčikom, keď chce v systéme niečo nakonfigurovať alebo nainštalovať.
- Sprievodca vyzve používateľa na zadanie informácií pomocou otázok. Odpoveď na každú otázku určuje, aká otázka bude nasledovať.
- Keď sa sprievodca spýta všetky otázky, používateľovi sa zobrazí záverečné dialógové okno. Používateľovi zostáva už len stlačiť tlačidlo **Dokončiť**, aby sa nainštalovali a nakonfigurovali položky.

**Ciele Sprievodcu bezpečnosťou**

Cieľom sprievodcu bezpečnosťou je na základe odpovedí užívateľa nakonfigurovať nasledujúce.

- Systémové hodnoty týkajúce sa bezpečnosti a sieťové atribúty.
- Vydávanie správ súvisiacich s bezpečnosťou pri monitorovaní systému.
- Generovanie Správy s informáciami pre správcu a Správy s informáciami pre užívateľa:
  - Správa s informáciami pre správcu obsahuje odporúčané bezpečnostné nastavenia a procedúry, ktoré je potrebné dodržiavať ešte pred uskutočnením týchto odporúčaní.

- Správa s informáciami pre používateľa obsahuje informácie, ktoré je možné použiť pre bezpečnostnú politiku vašej práce. Sú tu napríklad zahrnuté pravidlá na zostavenie hesla.

- Zabezpečovanie odporúčaných nastavení pre rôzne položky v systéme, ktoré súvisia s bezpečnosťou.

**Ciele Sprievodcu bezpečnosťou**

- Cieľom Sprievodcu bezpečnosťou je:
  - Určiť vhodné nastavenia systémovej bezpečnosti podľa odpovedí používateľov na otázky sprievodcu a potom podľa vhodnosti tieto nastavenia implementovať.
  - Sprievodca vytvára podrobné informačné správy vrátane nasledovného.
    - Správu, vysvetľujúcu odporúčania Sprievodcu.
    - Správu, podrobne vysvetľujúcu procedúry, ktoré by mali byť vykonané pred implementáciou.
    - Správu, uvádzajúcu príslušné informácie, ktoré majú byť distribuované používateľom systému.
- Tieto položky vytvoria základnú bezpečnostnú politiku vo vašom systéme.
- Sprievodca odporúča auditovať žurnálové správy, ktoré by ste mali naplánovať na periodické spustenie. Ak nastavíte tieto hlásenia, môžu vám pomôcť pri:
  - Kontrole, že sa dodržuje bezpečnostná politika.
  - Kontrole, že zmeny bezpečnostnej politiky sa vykonávajú iba s vaším schválením.
  - Navrhne hlásenie, pomocou ktorých sa budú monitorovať udalosti vo vašom systéme týkajúce sa bezpečnosti.
- Sprievodca vám umožní uložiť uvedené odporúčania alebo aplikovať niektoré, prípadne všetky tieto odporúčania vo vašom systéme.

**Poznámka:** Sprievodca bezpečnosťou môže byť v rovnakom systéme použitý viac než jedenkrát, aby tak umožnil používateľom, ktorí majú staršiu inštaláciu, zrevidovať svoju momentálnu bezpečnosť. Sprievodcu bezpečnosťou môžete používať od systému V3R7 a novšieho (keď bol zavedený iSeries Navigator).

Keď chcete používať iSeries Navigator, musíte mať IBM iSeries Access for Windows nainštalovaný na vašom Windows 95/NT PC a mať pripojený server iSeries server z tohto PC. Užívateľ sprievodcu musí byť pripojený k serveru iSeries. Tento používateľ musí mať užívateľské ID, ktoré má špeciálne oprávnenie *ALLOBJ, *SECADM, *AUDIT a *IOSYSCFG. Pomoc ohľadne pripájania vášho PC s Windows 95/NT k vášmu systému iSeries nájdete v téme IBM iSeries Access for Windows v Information Center (podrobnosti nájdete v “Nevyhnutné predpoklady a súvisiace informácie” na strane xii).

**Ak chcete mať prístup k Sprievodcovi bezpečnosťou**, vykonajte nasledovné:

1. V iSeries Navigator rozviňte váš server.
2. Kliknite pravým tlačidlom na **Bezpečnosť** a vyberte **Konfigurácia**.
   - Keď užívateľ spustí voľbu **Bezpečnosť** aplikácie iSeries Navigator, do servera iSeries sa odošle požiadavka na overenie mimoriadneho oprávnenia užívateľa.
   - Ak používateľ nemá všetky vyžadované špeciálne oprávnenia (*ALLOBJ, *AUDIT, *IOSYSCFG, *SECADM), neuvidí voľbu **Konfigurovať** a nie je schopný spustiť Sprievodcu bezpečnosťou.
3. Za predpokladu, že používateľ má potrebné oprávnenie:
   - budú načítané predošlé odpovede sprievodcu.
   - bude načítané aktuálne nastavenie bezpečnosti.

Sprievodca bezpečnosťou vám zobrazí jednu z nasledovných úvodných obrazoviek. Ktorú z týchto obrazoviek uvidíte záleží od týchto podmienok:

- Sprievodca nebol nikdy spustený pre cieľový server iSeries.
- Sprievodca už bol spustený predtým, ale vykonanie zmien bezpečnosti boli odložené.

- Sprievodca už bol spustený predtým a zmeny bezpečnosti boli implementované

Ak nepoužívate iSeries Navigator, stále môžete získať pomoc pri plánovaní svojich bezpečnostných potrieb. Plánovač bezpečnosti eServer je on-line verzia Sprievodcu bezpečnosťou s jedným rozdielom. Poradca nenakonfiguruje váš systém automaticky. Bude však na základe vašich odpovedí generovať správu odporúčaných volieb bezpečnosti. Keď sa chcete dostať k Plánovaču bezpečnosti eServer, choďte do Informačného centra eServer:

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

## Plánovač bezpečnosti eServer

Plánovač bezpečnosti eServer je on-line verzia Sprievodcu bezpečnosťou. Pýta sa tie isté otázky ako Sprievodca bezpečnosťou a na základe vašich odpovedí generuje rovnaké odporúčania. Najväčšie rozdiely medzi týmito dvomi nástrojmi spočívajú v tom, že:

- Plánovač bezpečnosti eServer **neprodukuje**—
  - výpisy.
  - Porovnajte aktuálne nastavenie s odporúčaným nastavením.
  - Nastavte ľubovoľnú systémovú hodnotu automaticky.
- Nemôžete aplikovať odporúčania z Plánovača bezpečnosti eServer.

Plánovač bezpečnosti eServer generuje CL program, ktorý môžete skopírovať a upraviť pre vlastné použitie na automatizáciu bezpečnostnej konfigurácie. Môžete sa tiež pripojiť priamo k dokumentácii servera iSeries z Plánovača bezpečnosti eServer. Táto poskytuje informácie o systémových hodnotách alebo oznámenie, ktoré vám pomôže zistiť, či toto nastavenie prislúcha vášmu prostrediu.

Na prístup k Plánovaču bezpečnosti eServer nasmerujte svoj internetový prehliadač na nasledujúce URL:

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

# Kapitola 3. Riadenie interaktívneho prihlasovania

Keď premýšľate o zadaní obmedzení do vášho systému, začnite hneď s prihlasovacou obrazovkou. Nasledujú voľby, ktoré môžete použiť na sťaženie prihlásenia sa do vášho systému s použitím prihlasovacej obrazovky.

## Pravidlá nastavenie hesla

Ak chcete zabezpečiť prihlasovanie vášho systému, urobte nasledovné:
- Nastavte politiku tak, aby povoľovala netriviálne heslá, ktoré sa nesmú zdieľať.
- Toto môžete dosiahnuť nastavením systémových hodnôt. Tabuľka 1 zobrazuje odporúčané nastavenia systémových hodnôt.

Kombinácia hodnôt v Tabuľka 1 je dôkladne obmedzujúca a jej cieľom je výrazne zmenšiť pravdepodobnosť triviálnych hesiel. Je však možné, že používatelia budú spôsob voľby hesla rešpektujúci takéto pravidlá považovať za náročný alebo obmedzujúci.

Možno zobrať do úvahy aj takýchto užívateľov, a to pomocou:
1. Zoznamu s uvedenými kritériami pre heslá.
2. Príkladov hesiel, ktoré nie sú platné.
3. Návrhov ako vytvoriť platné heslo.

Spustite príkaz CFGSYSSEC (Configure System Security) pre nastaviť tieto hodnoty. Použite príkaz PRTSYSSECA (System Security Attributes) na vytlačenie vašich súčasných nastavení pre tieto systémové hodnoty.

Kapitola 3 knihy *iSeries Security Reference*. “Hodnoty nastavené pomocou príkazu Configure System Security” na strane 33 poskytuje viac informácií o príkaze CFGSYSSEC.

*Tabuľka 1. Systémové hodnoty pre heslá*

| Názov systémovej hodnoty | Opis | Odporúčaná hodnota |
|---|---|---|
| QPWDEXPITV | Ako často musia používatelia meniť svoje heslá. V užívateľskom profile môžete špecifikovať rôzne hodnoty pre jednotlivých užívateľov. | 60 (dní) |
| QPWDLMTAJC | Či systém zabraňuje rovnakým susedným znakom. | 1 (áno) |
| QPWDLMTCHR | Ktoré znaky sa nemôžu použiť v heslách.[2] | AEIOU#$@ |
| QPWDLMTREP | Či systém zabraňuje výskytu znaku v hesle viac ako jedenkrát. | 2 (nedovolené následne za sebou) |
| QPWDLVL | Ktoré heslá užívateľských profilov sú obmedzená na 10 znakov alebo maximálne 128. | 0[3] |
| QPWDMAXLEN | Maximálny počet znakov v hesle. | 8 |
| QPWDMINLEN | Minimálny počet znakov v hesle. | 6 |
| QPWDPOSDIF | Či sa musí znak v hesle odlišovať od znaku na rovnakej pozícii v predchádzajúcom hesle. | 1 (áno) |
| QPWDRQDDGT | Či musí heslo obsahovať aspoň jeden číselný znak. | 1 (áno) |
| QPWDRQDDIF | Ako dlho musí užívateľ čakať pred opakovaným použitím hesla.[2] | 5 alebo menej (intervaly exspirácie)[1] |
| QPWDVLDPGM | Ktorý ukončovací program sa volá na overenie novo priradeného hesla. | *NONE |

*Tabuľka 1. Systémové hodnoty pre heslá (pokračovanie)*

| Názov systémovej hodnoty | Opis | Odporúčaná hodnota |
|---|---|---|

**Poznámky:**

1. Systémová hodnoty QPWDEXPITV určuje, ako často si musíte meniť svoje heslo, napríklad každých 60 dní. Toto je **interval exspirácie**. Systémová hodnota QPWDRQDDIF určuje, koľko intervalov exspirácie musí prejsť, aby ste mohli použiť opäť rovnaké heslo. Kapitola 3 v knihe *iSeries Security Reference* poskytuje viac informácií o tom, ako tieto systémové hodnoty spolupracujú.
2. QPWDLMTCHR nie je vnútené na úrovniach hesiel 2 alebo 3. Pozrite si "Úrovne hesla", kde nájdete detaily.
3. Pozrite si časť "Plánovanie zmien úrovne hesiel", pomocou ktorej určíte správu úroveň hesiel pre vaše potreby.

## Úrovne hesla

Od verzie operačného systému V5R1 ponúka systémová hodnota QPWDLVL zvýšenú bezpečnosť hesiel. V predchádzajúcich vydaniach boli používatelia obmedzení na heslá, ktoré neboli dlhšie ako 10 znakov a boli z obmedzeného rozsahu znakov. Teraz si môžu používatelia vybrať heslo (alebo heslovú frázu) s najviac 128 znakmi, v závislosti od nastavenej úrovne hesiel na ich systéme. Úrovne hesiel sú:

- **Úroveň 0:** Systémy sa dodávajú s touto úrovňou. Na úrovni 0 nemajú heslá viac ako 10 znakov, obsahujú len znaky A-Z, 0–9, #, @, $ a _. Heslá na úrovni 0 sú menej bezpečné ako heslá na vyšších úrovniach hesiel.
- **Úroveň 1:** Rovnaké pravidlá ako pre heslá úrovne 0, ale heslá pre Podporu iSeries pre Windows Network Neighborhood (ďalej nazývané ako iSeries NetServer) sa neuložia.
- **Úroveň 2:** Na tejto úrovni sú heslá bezpečné. Táto úroveň sa môže využívať na testovanie. Heslá sa uložia pre užívateľov na úrovni 0 alebo 1, ak majú 10 znakov alebo menej a používajú znakovú sadu pre heslá úrovne 0 alebo 1. Heslá (alebo heslové frázy) na tejto úrovni majú nasledujúce charakteristiky:
  - maximálne 128 znakové heslá.
  - zložené z ľubovoľných znakov, dostupných na klávesnici.
  - nemôžu obsahovať len medzery; medzery sa odstraňujú zo začiatku a konca hesla.
  - rozlišujú veľkosť písmen.
- **Úroveň 3:** Heslá na tejto úrovni sú najbezpečnejšie a využívajú najmodernejšie šifrovacie algoritmy, ktoré sú dostupné. Heslá na tejto úrovni majú rovnaké charakteristiky ako na úrovni 2. Heslá pre iSeries NetServer sa na tejto úrovni neukladajú.

Ak každý systém vo vašej sieti spĺňa nasledujúce kritéria, mali by ste používať iba heslá úrovne 2 a 3:

- Operačný systém má verziu V5R1 alebo novšiu
- Úroveň hesiel je nastavená na 2 alebo 3

Podobne, používatelia sa musia všetci prihlasovať pomocou rovnakej úrovne hesiel. Úrovne hesiel sú globálne; používatelia si nemôžu vybrať úroveň, na ktorej chcú svoje heslá zabezpečiť.

## Plánovanie zmien úrovne hesiel

Zmena úrovní hesiel by sa mala dôkladne naplánovať. Operácie s ostatnými systémami môžu zlyhať alebo používatelia sa nebudú môcť prihlásiť do systému, ak ste zmeny úrovne hesiel nenaplánovali v dostatočnej miere. Pred zmenou systémovej hodnoty QPWDLVL sa uistite, že ste uložili svoje bezpečnostné údaje pomocou príkazu SAVSECDTA alebo SAVSYS. Ak máte súčasnú zálohu, budete schopní opätovne nastaviť heslá pre profily všetkých užívateľov, ak budete potrebovať vrátiť sa späť na nižšiu úroveň hesiel.

Produkty, ktoré používate v systéme a na klientoch, s ktorými je systém spojený cez rozhrania, môžu mať problémy, keď je systémová hodnota (QPWDLVL) úrovne hesiel nastavená na 2 alebo 3. Každý produkt alebo klient, ktorý odosiela heslá do systému skôr v zašifrovanej podobe a nie v čisto textovom tvare, ktorý užívateľ zadá na prihlasovacej obrazovke, sa musí rozšíriť na prácu s novými pravidlami šifrovania hesiel pre QPWDLVL 2 alebo 3. Odosielanie zašifrovaného hesla je známe ako **náhrada hesla**.

Náhrada hesla sa používa na ochranu hesla pred odchytením počas prenosu cez sieť. Náhrada hesla, ktorú vygenerovali starší klienti, ktorí nepodporujú nový algoritmus pre QPWDLVL 2 alebo 3 aj keby boli špecifické znaky správne, nebude akceptovaná. To platí aj pre každé iSeries pre prístup iSeries rovnakej úrovne, ktoré využíva zašifrované hodnoty na autentifikáciu z jedného systému do druhého.

Problém sa komplikuje, pretože niektoré postihnuté produkty (ako napríklad Java Toolbox) sa poskytujú ako midlevér. Produkt tretej strany, ktorý začleňuje predchádzajúcu verziu jedného z týchto produktov nebude fungovať správne, kým sa nanovo nezostaví využitím aktualizovanej verzie daného midlevéru.

Už aj z tohto a z iných scenárov vidieť, prečo je potrebné dôležité plánovanie pred zmenou systémovej hodnoty QPWDLVL.

## Úvahy pre zmenu QPWDLVL z 0 na 1

Úroveň hesiel 1 umožňuje systému, ktorý nepotrebuje komunikovať s produktom Windows 95/98/ME AS/400 Client Support for Windows Network Neighborhood (iSeries NetServer), aby boli heslá iSeries NetServer odstránené zo systému. Elimináciou nepotrebných zašifrovaných hesiel zo systému sa zvyšuje celková bezpečnosť systému.

Pri QPWDLVL 1, všetky súčasné, pred-V5R1 náhrady hesiel a mechanizmy autentifikácie hesiel budú naďalej fungovať. Existuje iba veľmi malá možnosť prelomenia, s výnimkou funkcií a služieb, ktoré vyžadujú heslo iSeries NetServer.

## Úvahy pre zmenu QPWDLVL z 0 alebo 1 na 2

Úroveň hesiel 2 predstavuje použitie hesiel s rozlišovaním veľkosti písmen do 128 znakov (nazývané tiež heslové frázy) a poskytuje maximálnu schopnosť prejsť späť na QPWDLVL 0 alebo 1.

Bez ohľadu na úroveň hesiel systému, heslá úrovne hesiel 2 a 3 sa vytvoria pri každej zmene hesla, alebo keď sa užívateľ prihlási do systému. Vytvorenie hesiel úrovne 2 a 3, keď je systém stále na úrovni hesiel 0 alebo 1 pomôže prípravám na zmenu úrovne hesiel 2 alebo 3.

Pred zmenou QPWDLVL na 2 by ste mali použiť príkazy DSPAUTUSR alebo PRTUSRPRF TYPE(*PWDINFO) na lokalizovanie všetkých užívateľských profilov, ktoré nemajú heslo, ktoré sa dá použiť na úrovni hesiel 2. Podľa toho, ktoré profily tieto príkazy lokalizujú, budete musieť použiť jeden z nasledujúcich mechanizmov, aby sa do týchto profilov pridala úroveň hesiel 2 a 3.

- Zmeniť heslo pre užívateľský profil pomocou CL príkazu CHGUSRPRF alebo CHGPWD alebo API QSYCHGPW. Toto spôsobí, že systém zmení heslo, ktoré je použiteľné na úrovniach hesiel 0 a 1; a systém tiež vytvorí dve rovnaké heslá, rozlišujúce veľkosť písmen, ktoré sú použiteľné na úrovniach hesiel 2 a 3. Verzie hesla s veľkými písmenami a aj malými písmenami sa vytvoria na použitie na úrovni hesiel 2 alebo 3.

  Napríklad, zmena hesla na C4D2RB4Y má za následok, že systém vygeneruje heslá C4D2RB4Y a c4d2rb4y úrovne hesiel 2.
- Prihlásiť sa do systému cez mechanizmus, ktorý poskytuje heslo v čistom textovom tvare (nepoužíva náhradu hesla). Ak je heslo platné a užívateľský profil nemá heslo, ktoré je použiteľné na úrovniach hesiel 2 a 3, systém vytvorí dve rovnaké heslá, rozlišujúce veľkosť

písmen, ktoré sú použiteľné na úrovni hesiel 2 a 3. Verzie hesla s veľkými písmenami a aj malými písmenami sa vytvoria na použitie na úrovni hesiel 2 alebo 3.

Absencia hesla, ktoré je použiteľné na úrovni hesiel 2 alebo 3 môže byť problém bez ohľadu na to, či užívateľský profil má alebo nemá heslo, ktoré je použiteľné na úrovniach hesiel 0 alebo 1, alebo keď sa užívateľ pokúša prihlásiť cez produkt, ktorý používa náhradu hesiel. V takýchto prípadoch sa užívateľ pri zmene úrovne hesiel na 2 nebude môcť prihlásiť.

Ak užívateľský profil nemá heslo, ktoré je použiteľné na úrovniach hesiel 2 a 3, užívateľský profil má heslo, ktoré je použiteľné na úrovniach hesiel 0 a 1 a užívateľ sa prihlási cez produkt, ktorý posiela heslá v čistom textovom tvare, systém vyhodnotí užívateľa s heslom úrovne hesiel 0 a pre užívateľský profil vytvorí dve heslá úrovne hesiel 2 (ako je popísané hore). Následné prihlásenia sa budú validovať pomocou hesiel úrovne hesiel 2.

Ľubovoľný klient/služba, ktorá používa náhradu hesla nebude fungovať správne pri QPWDLVL 2, ak tento klient/služba nebola zaktualizovaná na použitie novej substitučnej schémy hesiel (heslových fráz). Správca by mal skontrolovať, či sa vyžaduje klient/služba, ktorá nebola zaktualizovaná na novú substitučnú schému hesiel.

Ku klientom/službám, ktoré používajú substitúciu hesiel patria:

- TELNET
- iSeries Access
- Hostiteľské servery iSeries
- QFileSrv.400
- Podpora tlače iSeries NetServer
- DDM
- DRDA
- SNA LU6.2

Odporúča sa uložiť bezpečnostné údaje pred zmenou na QPWDLVL 2. Toto môže uľahčiť prechod späť na QPWDLVL 0 alebo 1, ak to bude potrebné.

Odporúča sa nemeniť iné systémové hodnoty hesiel, ako sú QPWDMINLEN a QPWDMAXLEN, kým sa nevykoná otestovanie na QPWDLVL 2. Toto uľahčí prechod späť na QPWDLVL 1 alebo 0, ak to je potrebné. Predtým ako systém povolí zmenu QPWDLVL na 2, systémová hodnota QPWDVLDPGM musí špecifikovať *REGFAC alebo *NONE. Preto, ak používate program na validáciu hesiel, môžete skúsiť napísať nový, ktorý bude zaregistrovaný pre ukončovací bod QIBM_QSY_VLD_PASSWRD pomocou príkazu ADDEXITPGM.

Heslá iSeries NetServer sú stále podporované na QPWDLVL 2, takže všetky funkcie/služby, ktoré vyžadujú heslo iSeries NetServer by stále mali fungovať správne.

Keď je správca spokojný s prevádzkou systému na QPWDLVL 2, môže začať meniť systémové hodnoty hesiel na podporu dlhších hesiel. Administrátor si však musí byť vedomý toho, čo prinášajú tieto dlhšie heslá:

- Ak sa špecifikujú heslá dlhšie ako 10 znakov, úroveň hesiel 0 alebo 1 sa zruší. Tento užívateľský profil sa nebude môcť prihlásiť, ak sa systém vráti späť na úroveň hesiel 0 alebo 1.
- Ak heslá obsahujú špeciálne znaky alebo nevyhovujú pravidlám tvorby hesiel pre jednoduché názvy objektov (vylučujúce rozlišovanie veľkosti písmen), úroveň hesiel 0 a 1 sa zruší.

- Ak sú zadané heslá, dlhšie ako 14 znakov, heslo iSeries NetServer pre užívateľský profil sa vymaže.
- Systémové hodnoty hesiel sa použijú iba pre novú hodnotu úrovne hesiel 2 a nebudú použité pre hodnoty hesiel systémom vygenerovanej úrovne hesiel 0 a 1 alebo pre hodnoty hesiel iSeries NetServer (ak boli vygenerované).

## Úvahy pre zmenu QPWDLVL z 2 na 3

Po prevádzkovaní systému nejaký čas na QPWDLVL 2 sa môže správca rozhodnúť pre prechod na QPWDLVL 3, aby maximalizoval ochranu zabezpečením heslami.

V QPWDLVL 3 sa všetky heslá iSeries NetServer vymažú tak, že systém by sa nemal presunúť do QPWDLVL 3, pokiaľ neprestane existovať potreba používať heslá iSeries NetServer.

Na QPWDLVL 3 sa zrušia všetky heslá úrovne hesiel 0 a 1. Správca môže použiť príkazy DSPAUTUSR alebo PRTUSRPRF na nájdenie užívateľských profilov, ktoré so sebou nemajú spojené heslá úrovne hesiel 2 alebo 3.

## Zmena na nižšiu úroveň hesiel

Návrat na nižšiu hodnotu QPWDLVL je možný, ale nie to úplne bezbolestná operácia. Vo všeobecnosti, majte na pamäti, že prechod z nižších hodnôt QPWDLVL na vyššie hodnoty QPWDLVL je jednosmerný proces. V niektorých prípadoch sa musí opätovne dosadiť nižšia hodnota QPWDLVL.

Nasledovné časti rozoberajú činnosti, potrebné na presun späť na nižšiu úroveň hesiel.

**Úvahy pre zmenu z QPWDLVL 3 na 2:** Táto zmena je relatívne jednoduchá. Akonáhle je QPWDLVL nastavená na 2, správca potrebuje určiť, či sa vyžaduje, aby nejaký užívateľský profil obsahoval heslá iSeries NetServer alebo heslá úrovne 0 alebo 1 a ak áno, aby zmenil heslo užívateľského profilu na prípustnú hodnotu.

Okrem toho môžu byť systémové hodnoty hesiel zmenené späť na hodnoty, ktoré sú kompatibilné s iSeries NetServer a heslami úrovne hesiel 0 alebo 1, ak sú takéto heslá potrebné.

**Úvahy pre zmenu z QPWDLVL 3 na 1 alebo 0:** Z dôvodu vysokj možnosti problémov pre systém (nikto sa nemôže prihlásiť, pretože všetky heslá úrovne hesiel 0 a 1 boli zrušené), táto zmena nie je podporovaná priamo. Ak chcete prejsť z QPWDLVL 3 na QPWDLVL 1 alebo 0, systém musí najprv prejsť na strednú úroveň, QPWDLVL 2.

**Úvahy pre zmenu z QPWDLVL 2 na 1:** Pred zmenou QPWDLVL na 1 by mal správca použiť príkazy DSPAUTUSR alebo PRTUSRPRF TYPE(*PWDINFO) na nájdenie všetkých užívateľských profilov, ktoré nemajú heslo úrovne hesiel 0 alebo 1. Ak bude užívateľský profil vyžadovať po zmene QPWDLVL heslo, správca by mal zaistiť, že heslo úrovne hesiel 0 a 1 sa vytvorí pre profil pomocou jedného z nasledovných mechanizmov:

- Zmeniť heslo pre užívateľský profil pomocou CL príkazu CHGUSRPRF alebo CHGPWD alebo API QSYCHGPW. Toto spôsobí, že systém zmení heslo, použiteľné na úrovni hesiel 2 a 3; a systém tiež vytvorí rovnaké heslo s veľkými písmenami, ktoré je použiteľné na úrovni hesiel 0 a 1. Systém je schopný vytvoriť heslo úrovne 0 a 1 len pri splnení nasledovných podmienok:
  - Heslo má 10 alebo menej znakov.
  - Heslo môže byť skonvertované na veľké EBCDIC znaky A-Z, 0-9, @, #, $ a podčiarkovník.
  - Heslo nezačína číslom ani znakom podčiarkovníka.

Napríklad, zmena hesla na hodnotu RainyDay by spôsobila, že systém vygeneruje heslo úrovne hesiel 0 a 1, RAINYDAY. Ale zmenou hodnoty hesla na Rainy Days In April spôsobí, že systém zruší heslo úrovne hesiel 0 a 1 (pretože heslo je pridlhé a obsahuje medzery).

Ak sa heslo úrovne hesiel 0 alebo 1 nedalo vytvoriť, nezobrazí sa o tom žiadna správa ani oznam.

- Prihlásiť sa do systému cez mechanizmus, ktorý poskytuje heslo v čistom textovom tvare (nepoužíva náhradu hesla). Ak je heslo platné a užívateľský profil nemá heslo, ktoré je použiteľné na úrovniach hesiel 0 a 1, systém vytvorí rovnaké heslo s veľkými písmenami, ktoré je použiteľné na úrovniach hesiel 0 a 1. Systém je schopný vytvoriť heslo úrovne hesiel 0 a 1 len pri splnení podmienok hore.

Správca môže potom zmeniť QPWDLVL na 1. Všetky heslá iSeries NetServer sa vymažú, keď sa zmena na QPWDLVL 1 prejaví (pri ďalšom IPL).

**Úvahy pre zmenu z QPWDLVL 2 na 0:** Úvahy sú rovnaké ako pri zmene z QPWDLVL 2 na 1, okrem toho, že všetky heslá iSeries NetServer zostanú zapamätané, keď sa zmena prejaví.

**Úvahy pre zmenu z QPWDLVL 1 na 0:** Po zmenení QPWDLVL na 0 by mal správca použiť príkazy DSPAUTUSR alebo PRTUSRPRF na lokalizáciu každého užívateľského profilu, ktorý nemá heslo iSeries NetServer. Ak užívateľský profil vyžaduje heslo iSeries NetServer, môže byť vytvorené zmenením užívateľského hesla alebo prihlásením sa prostredníctvom mechanizmu, ktorý heslo uvádza v čisto textovej forme.

Správca môže potom zmeniť QPWDLVL na 0.

## Zmena známych hesiel

Ak chcete zatvoriť niektoré dobre známe vstupy do servera iSeries, ktoré sa môžu nachádzať vo vašom systéme, urobte nasledovné:

__ Krok 1. Presvedčte sa, že užívateľské profily majú stále štandardné heslá (rovnaké ako názov užívateľského profilu). Môžete použiť príkaz ANZDFTPWD (Analyze Default Passwords). (Pozrite si “Vyhýbanie sa štandardným heslám” na strane 23.)

__ Krok 2. Skúste sa prihlásiť do vášho systému pomocou kombinácií užívateľských profilov a hesiel, ktoré sú uvedené v Tabuľka 2 na strane 19. Tieto heslá sú zverejnené a sú prvou voľbou hocikoho, kto sa pokúša dostať do vášho systému. Ak sa môžete prihlásiť, použite príkaz CHGUSRPRF (Change User Profile) a zmeňte heslo na odporúčanú hodnotu.

__ Krok 3. Spustite DST (Dedicated Service Tools) a skúste sa prihlásiť pomocou hesiel, ktoré sa ukážu v Tabuľka 2 na strane 19. Pozrite si Informačné centrum iSeries —>Bezpečnosť—>Servisné nástroje. Pozrite si “Nevyhnutné predpoklady a súvisiace informácie” na strane xii, kde nájdete informácie o sprístupňovaní informačného centra iSeries.

__ Krok 4. Ak sa dokážete do DST prihlásiť pomocou ľubovoľného z týchto hesiel, mali by ste heslá zmeniť. Informačné centrum iSeries—>Bezpečnosť—>Servisné nástroje poskytuje podrobné pokyny o tom, ako zmeniť ID užívateľa a heslo servisných nástrojov. V “Nevyhnutné predpoklady a súvisiace informácie” na strane xii nájdete viac informácií o prístupe na informačné centrum iSeries.

__ Krok 5. Nakoniec sa presvedčte, že sa nemôžete prihlásiť iba pomocou stlačenia klávesu Enter na prihlasovacej obrazovke bez toho, aby ste zadali ID užívateľa a heslo. Skúste niekoľko rôznych obrazoviek. Ak sa môžete prihlásiť bez zadania informácií na prihlasovacej obrazovke, spravte niečo z nasledovného:

- Zmeňte úroveň bezpečnosti na 40 alebo 50 (systémová hodnota QSECURITY).

  **Poznámka:** Vaše aplikácie sa môžu spúšťať inak, keď zvýšite vašu úroveň bezpečnosti na 40 alebo na 50.
- Zmeňte všetky položky pracovnej stanice pre interaktívne podsystémy tak, aby ukazovali na opisy úloh, ktoré špecifikujú USER(*RQD).

*Tabuľka 2. Heslá pre profily dodávané firmou IBM*

| ID užívateľa | Heslo | Odporúčaná hodnota |
|---|---|---|
| QSECOFR | QSECOFR[1] | Netriviálna hodnota známa len správcovi bezpečnosti. **Zaznačte si heslo, ktoré ste vybrali a uložte si ho na bezpečnom mieste.** |
| QSYSOPR | QSYSOPR | *NONE[2] |
| QPGMR | QPGMR | *NONE[2] |
| QUSER | QUSER | *NONE[2, 3] |
| QSRV | QSRV | *NONE[2] |
| QSRVBAS | QSRVBAS | *NONE[2] |

**Poznámky:**

1. Systém prichádza s hodnotou *Nastaviť heslo do ukončenej platnosti* pre QSECOFR, nastavenú na *YES. Keď sa prvýkrát prihlásite do nového systému, musíte zmeniť heslo QSECOFR.
2. Systém potrebuje tieto užívateľské profily pre systémové funkcie, ale nemal by užívateľom umožňovať prihlásiť sa bez nich. Pre nové systémy, nainštalované s V3R1 alebo neskoršími vydaniami, dodané heslo je *NONE.

   Keď spustíte príkaz CFGSYSSEC, systém nastaví tieto heslá na *NONE.
3. Ak chcete spustiť iSeries Access for Windows s použitím TCP/IP, užívateľský profil QUSER musí byť povolený.

*Tabuľka 3. Heslá pre vyhradené servisné nástroje*

| Úroveň DST | ID užívateľa[1] | Heslo | Odporúčaná hodnota |
|---|---|---|---|
| Základná schopnosť | 11111111 | 11111111 | Netriviálna hodnota známa len správcovi bezpečnosti.[2] |
| Úplná schopnosť | 22222222 | 22222222[3] | Netriviálna hodnota známa len správcovi bezpečnosti.[2] |
| Bezpečnostná schopnosť | QSECOFR | QSECOFR[3] | Netriviálna hodnota známa len správcovi bezpečnosti.[2] |
| Schopnosť služieb | QSRV | QSRV[3] | Netriviálna hodnota známa len správcovi bezpečnosti.[2] |

**Poznámky:**

1. ID užívateľa sa vyžaduje iba pre PowerPC AS (RISC) vydania operačného systému.
2. Ak sa váš predstaviteľ servisu hardvéru potrebuje prihlásiť pomocou tohto ID užívateľa a hesla, zmeňte heslo na novú hodnotu, keď predstaviteľ servisu hardvéru odíde.
3. Užívateľský profil servisných nástrojov exspiruje pri prvom použití.

**Poznámka:** Heslá DST sa môžu meniť len autentifikovaným zariadením. Toto tiež platí pre všetky heslá a príslušné ID užívateľov, ktoré sú zhodné. Viac informácií o autentifikovaných zariadeniach nájdete v informáciách o nastavení Operačnej konzoly v informačnom centre iSeries.

## Nastavenie prihlasovacích hodnôt

Tabuľka 4 zobrazuje niekoľko hodnôt, ktoré môžete nastaviť, aby ste sťažili neoprávnenej osobe sa prihlásiť do vášho systému. Ak spustíte príkaz CFGSYSSEC, nastaví tieto systémové hodnoty na odporúčané nastavenia. O týchto systémových hodnotách sa môžete viac dozvedieť v Kapitole 3 knihy *iSeries Security Reference*.

*Tabuľka 4. Prihlasovacie systémové hodnoty*

| Názov systémovej hodnoty | Opis | Odporúčané nastavenie |
|---|---|---|
| QAUTOCFG | Či systém automaticky konfiguruje nové zariadenia. | 0 (Nie) |
| QAUTOVRT | Počet opisov virtuálnych zariadení, ktoré vytvorí systém, ak nie je k dispozícii na použitie žiadne zariadenie. | 0 |
| QDEVRCYACN | Čo spraví systém po opätovnom pripojení zariadenia po chybe.[1] | *DSCMSG |
| QDSCJOBITV | Ako dlho systém čaká pred ukončením odpojenej úlohy. | 120 |
| QDSPSGNINF | Či systém pri prihlasovaní užívateľa zobrazí informácie o predchádzajúcej prihlasovacej aktivite. | 1 (Áno) |
| QINACTITV | Ako dlho systém čaká pred vykonaním akcie, keď je interaktívna úloha neaktívna. | 60 |
| QINACTMSGQ | Čo spraví systém, keď sa dosiahne časová perióda QINACTITV. | *ENDJOB |
| QLMTDEVSSN | Či systém zabráni prihlásiť sa užívateľovi na viac ako jednej pracovnej stanici súčasne. | 1 (Áno) |
| QLMTSECOFR | Či sa používatelia so špeciálnymi oprávneniami *ALLOBJ alebo *SERVICE môžu prihlásiť len na konkrétnych pracovných staniciach. | 1 (Áno)[2] |
| QMAXSIGN | Maximum za sebou nasledujúcich nesprávnych pokusov o prihlásenie (užívateľský profil alebo heslo je nesprávne). | 3 |
| QMAXSGNACN | Čo spraví systém, keď sa dosiahne limit QMAXSIGN. | 3 (Zakázať užívateľský profil aj zariadenie) |

**Poznámky:**

1. Systém môže relácie TELNET odpojiť a opakovane pripojiť, keď je opis zariadenia pre reláciu priradený explicitne.
2. Ak nastavíte systémovú hodnotu na 1(Áno), budete musieť užívateľov so špeciálnymi oprávneniami *ALLOBJ alebo *SERVICE explicitne oprávniť na zariadenia. Najľahší spôsob ako to spraviť je dať užívateľskému profilu QSECOFR oprávnenie *CHANGE na konkrétne zariadenia.

## Zmena správ pri chybnom prihlásení

Hakeri by radi vedeli, ako postupujú v procese dostať sa do systému. Keď chybová správa na Prihlasovacej obrazovke uvádza Nesprávne heslo, haker môže predpokladať, že ID užívateľa je správne. Hakera môžete sklamať použitím príkazu CHGMSGD (Change Message Description) a zmenením textu pre dve správy pri chybnom prihlásení. Tabuľka 5 na strane 21 ukazuje odporúčaný text.

*Tabuľka 5. Správy pri chybnom prihlásení*

| ID správy | Dodaný text | Odporúčaný text |
|---|---|---|
| CPF1107 | CPF1107 – Nesprávne heslo pre užívateľský profil. | Prihlasovacie informácie sú nesprávne **Poznámka:** Do textu správy nedajte ID správy. |
| CPF1120 | CPF1120 – Užívateľ XXXXX neexistuje. | Prihlasovacie informácie sú nesprávne. **Poznámka:** Do textu správy nedajte ID správy. |

## Plánovanie dostupnosti užívateľských profilov

Môžete požadovať, aby sa pomocou niektorých užívateľských profilov dalo prihlásiť len v určitých časoch dňa alebo určitých dní v týždni. Napríklad, ak máte profil nastavený pre audítora bezpečnosti, budete ho chcieť povoliť len počas hodín, kedy má audítor naplánovanú prácu. Tiež možno budete chcieť zakázať užívateľské profily so špeciálnym oprávnením *ALLOBJ (vrátane užívateľského profilu QSECOFR) mimo pracovných hodín.

Pomocou príkazu CHGACTSCDE (Change Activation Schedule Entry) môžete nastaviť užívateľské profily, aby povoľovali a zakazovali automaticky. Pre každý užívateľský profil, ktorý chcete plánovať, vytvoríte položku definujúcu plán užívateľského profilu.

Napríklad, ak chcete, aby profil QSECOFR bol k dispozícii len medzi 7 ráno a 10 večer, na obrazovke CHGACTSCDE by ste mali zadať nasledovné:

```
             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
```

*Obrázok 2. Obrazovka Schedule Profile Activation – Príklad*

V skutočnosti môžete chcieť mať profil QSECOFR k dispozícii len počas veľmi obmedzeného počtu hodín každý deň. Na vykonávanie väčšiny systémových funkcií môžete používať iný užívateľský profil s triedou *SECOFR. Takto sa vyhnete vystaveniu pokusom o prelomenie dobre známeho užívateľského profilu.

Príkaz DSPAUDJRNE (Display Audit Journal Entries) môžete periodicky používať na vytlačenie CP (Change Profile) auditových žurnálových položiek. (Change Profile) auditové žurnálové položky. Tieto položky použite na skontrolovanie, či systém povoľuje a zakazuje užívateľské profily podľa vášho naplánovaného rozvrhu.

Inou metódou na skontrolovanie, či sa užívateľské profily zakazujú vo vašom naplánovanom rozvrhu je použiť príkaz PRTUSRPRF (Print User Profile). Keď špecifikujete *PWDINFO pre typ hlásenia, hlásenie bude obsahovať stav každého vybraného užívateľského profilu. Ak napríklad pravidelne zakazujete všetky užívateľské profily so špeciálnym oprávnením *ALLOBJ, môžete naplánovať, aby sa nasledovný príkaz spustil okamžite po zakázaní profilov:

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

# Odstránenie neaktívnych užívateľských profilov

Váš systém by mal obsahovať len užívateľské profily, ktoré sú potrebné. Ak už ďalej nepotrebujete užívateľský profil, pretože užívateľ odišiel alebo si našiel v organizácii inú prácu, odstráňte tento užívateľský profil. Ak niekto odíde z organizácie na dlhší čas, zakážte (deaktivujte) profil tohto užívateľa. Nepotrebný užívateľský profil môže poskytovať neoprávnený vstup do vášho systému.

## Automatické zakázanie užívateľských profilov

Na pravidelné zakázanie užívateľských profilov, ktoré sú neaktívne určený počet dní, môžete použiť príkaz ANZPRFACT (Analyze Profile Activity). Keď použijete príkaz ANZPRFACT, špecifikujete počet dní neaktivity, ktoré systém vyhľadá. Systém prezerá dátum posledného prihlásenia, obnovenia a vytvorenia užívateľského profilu.

Keď ste špecifikovali hodnotu pre príkaz ANZPRFACT, systém naplánuje týždenné spúšťanie úlohy o 13:00 (od dňa, kedy ste prvýkrát špecifikovali hodnotu). Systém preskúša všetky profily a zakáže neaktívne profily. Príkaz ANZPRFACT nemusíte použiť dovtedy, kým nechcete zmeniť počet neaktívnych dní.

Príkaz CHGACTPRFL (Change Active Profile List) môžete použiť na vylúčenie niektorých profilov zo spracovania príkazom ANZPRFACT. Príkaz CHGACTPRFL vytvorí zoznam užívateľských profilov, ktoré príkaz ANZPRFACT nezakáže, bez ohľadu na dobu neaktivity týchto profilov.

Keď systém spustí príkaz ANZPRFACT, zapíše CP položku v auditovom žurnáli pre každý zakázaný užívateľský profil. Príkaz DSPAUDJRNE môžete použiť na zobrazenie nových užívateľských profilov, ktoré sa zakázali.

**Poznámka:** Systém zapisuje auditové položky len vtedy, ak hodnoty AUDCTL špecifikuje *AUDLVL a systémová hodnoty QAUDLVL špecifikuje *SECURITY.

Inou metódou na skontrolovanie, či sa užívateľské profily zakazujú vo vašom naplánovanom rozvrhu je použiť príkaz PRTUSRPRF (Print User Profile). Keď pre typ hlásenia špecifikujete *PWDINFO, hlásenie bude obsahovať stav každého vybraného užívateľského profilu.

## Automatické odstránenie užívateľských profilov

Príkaz CHGEXPSCDE (Change Expiration Schedule Entry) môžete použiť na riadenie odstránenia alebo zakázania užívateľských profilov. Ak viete, že užívateľ odchádza na dlhší čas, môžete naplánovať odstránenie alebo zakázanie profilu tohto užívateľa.

Keď prvýkrát spustíte príkaz CHGEXPSCDE, vytvorí položku plánovania úlohy, ktorá sa spustí každý deň 1 minútu po polnoci. Úloha si prezrie súbor QASECEXP aby zistila, či je na tento deň naplánované odstránenie nejakých užívateľských profilov.

Príkazom CHGEXPSCDE môžete zakázať alebo vymazať užívateľský profil. Ak vyberiete vymazanie užívateľského profilu, musíte špecifikovať, čo spraví systém s objektmi vlastnenými týmto užívateľom. Pred naplánovaním užívateľského profilu na vymazanie musíte vyhľadať objekty, ktoré tento užívateľ vlastní. Napríklad, ak užívateľ vlastní programy, ktoré adoptujú oprávnenie, chcete aby tieto programy adoptovali vlastníctvo nového vlastníka? Alebo má nový vlastník väčšie oprávnenie, ako je potrebné (ako je napríklad špeciálne oprávnenie)? Možno potrebujete vytvoriť nový užívateľský profil so špeciálnymi oprávneniami, ktorý bude vlastniť programy, ktoré potrebujú adoptovať oprávnenie.

Tiež musíte zistiť, či sa pri vymazaní užívateľského problému neobjavia problémy s aplikáciami. Napríklad, špecifikujú nejaké opisy úloh užívateľský profil ako štandardného užívateľa?

Na zobrazenie profilov, ktoré sú naplánované na vymazanie alebo zakázanie, môžete použiť príkaz DSPEXPSCD (Display Expiration Schedule).

Na zobrazenie všetkých užívateľských profilov na vašom systéme môžete použiť príkaz DSPAUTUSR (Display Authorized Users). Príkaz DLTUSRPRF (Delete User Profile) použite na vymazanie zastaraných profilov.

**Poznámka k bezpečnosti::** Užívateľský profil zakážete nastavením jeho stanu na *DISABLED. Keď zakážete užívateľský profil, stane sa nedostupným pre interaktívne použitie. Pomocou zakázaného užívateľského profilu sa nemôžete prihlásiť ani naň zmeniť svoju úlohu. Pod zakázaným užívateľským profilom môžu byť spúšťané dávkové úlohy.

## Vyhýbanie sa štandardným heslám

Keď vytvoríte nový užívateľský profil, štandardne sa mu dá rovnaké heslo ako názov užívateľského profilu. Toto poskytuje príležitosť niekomu vstúpiť do vášho systému, ak niekto pozná vašu politiku prideľovania názvov profilov a vie, že sa do vašej organizácie pripája nová osoba.

Keď vytvárate nové užívateľské profily, pouvažujte o prideľovaní netriviálneho hesla namiesto použitia štandardného hesla. Toto heslo povedzte dôverne novému užívateľovi, napríklad pomocou písmen “Vitajte v Systéme”, ktoré naznačujú vaše bezpečnostné politiky. Požadujte, aby si užívateľ pri prvom prihlásení sa zmenil heslo a to nastavením užívateľského profilu na PWDEXP(*YES).

Pomocou príkazu ANZDFTPWD (Analyze Default Passwords) môžete skontrolovať všetky užívateľské profily na vašom systéme na prítomnosť štandardných hesiel. Pri tlači hlásenia máte voľbu na špecifikovanie toho, aby systém vykonal akciu (ako je zakázanie užívateľského profilu), ak je heslo rovnaké ako názov užívateľského profilu. Príkaz ANZDFTPWD vytlačí zoznam nájdených profilov a vykonanej akcie.

**Poznámka:** Heslá na vašom systéme sú uložené v jednosmerne zakódovanej forme. Nedajú sa odkódovať. Systém zakóduje špecifikované heslo a porovná ho s uloženým heslom rovnako ako pri kontrole hesla pri prihlasovaní sa do systému. Ak auditujete zlyhania oprávnenia (*AUTFAIL), systém zapíše PW záznam auditovacieho žurnálu pre každý užívateľský profil, ktorý *nemá* štandardné heslo (pre systémy používajúce V4R1 alebo skoršie vydania). Počnúc od V4R2, systém pri spustení príkazu ANZDFTPWD nezapisuje PW auditové žurnálové položky.

## Monitorovanie prihlasovania a aktivity hesiel

Ak sa obávate o neoprávnené pokusy o vstup do vášho systému, použite príkaz PRTUSRPRF, ktorý vám pomôže monitorovať aktivitu prihlasovania a hesiel.

Nasleduje niekoľko návrhov na použitie tejto správy:

- Zistite, či je interval exspirácie hesla pre niektoré užívateľské profily dlhší ako systémová hodnota a či je nastavený dlhší interval exspirácie. Napríklad, v správe má užívateľ USERY interval exspirácie hesla 120 dní.

- Túto správu spúšťajte pravidelne, aby ste monitorovali neúspešné pokusy o prihlásenie. Niekto, kto sa pokúša dostať do vášho systému, si môže byť vedomý toho, že váš systém pri určitom počte neúspešných pokusoch vykoná nejakú akciu. Narušiteľ sa môže každú noc pokúšať prihlásiť menej krát ako je vaša hodnota QMAXSIGN, aby sa vyhol oznámeniu prekročeniu pokusov. Keď spustíte túto správu skoro ráno každý deň a zistíte, že niektoré profily majú často neúspešné prihlasovacie pokusy, môžete za tým predpokladať problém.
- Identifikujte profily, ktoré sa dlho nepoužívali alebo ktorých heslá sa dlho nezmenili.

## Ukladanie informácií o heslách

Pre podporu niektorých sieťových funkcií a komunikačných požiadaviek poskytujú servery iSeries bezpečnú metódu pre ukladanie hesiel, ktoré sa dajú odkódovať. Váš systém používa tieto heslá napríklad na vytvorenie SLIP spojenia s iným systémom. (“Bezpečnosť a relácie volania von” na strane 114 popisuje toto použitie uložených hesiel.)

Servery iSeries ukladajú tieto špeciálne heslá do zabezpečenej oblasti, ktorá nie je prístupná každému užívateľskému programu alebo rozhraniu. Len výlučne oprávnené systémové funkcie môžu nastaviť a obnoviť tieto heslá.

Napríklad, keď použijete uložené heslo pre volajúce SLIP spojenia, nastavíte heslo so systémovým príkazom, ktorý vytvorí konfiguračný profil (WRKTCPPTP). Na použitie tohto príkazu musíte mať oprávnenie *IOSYSCFG. Špeciálne zakódovaný skript spojenia obnovuje heslo a odkóduje ho počas procedúry volania. Odkódované heslo nie je viditeľné pre používateľa, ani v žiadnom protokole úloh.

Ako správca bezpečnosti musíte rozhodnúť, či umožníte, aby vo vašom systéme boli uložené heslá, ktoré môžu byť odkódované. Môžete to našpecifikovať pomocou systémovej hodnoty Retain Server Security Data (QRETSVRSEC). Štandardná hodnota je 0 (Nie). Preto váš systém neuloží heslá, ktoré môžu byť odkódované, kým výlučne nezadáte túto systémovú hodnotu.

Ak máte sieťové alebo komunikačné požiadavky na uložené heslá, mali by ste nastaviť príslušné politiky, a pochopiť politiky a praktiky vašich komunikačných partnerov. Napríklad, keď na komunikácia s iným serverom iSeries používate SLIP, obidva systémy by mali posúdiť nastavenie osobitných užívateľských profilov pre vytvorenie relácií. Určité profily by mali mať obmedzené právomoci v systéme. Toto obmedzí zásah do vášho systému, ak je uložené heslo odhalené v systéme partnera.

# Kapitola 4. Konfigurácia iSeries na používanie Security Tools

Tieto informácie popisujú, ako máte nastaviť váš systém, aby používal bezpečnostné nástroje, ktoré sú súčasťou OS/400. Keď nainštalujete OS/400, nástroje bezpečnostné nástroje sú pripravené na použitie. Nasledujúca téma poskytuje návrhy na vykonávanie postupov s bezpečnostné nástroje.

## Bezpečná práca s Security Tools

Keď nainštalujete OS/400, objekty prislúchajúce bezpečnostné nástroje sú zabezpečené. Pre bezpečnú prácu s bezpečnostné nástroje, predchádzajte vykonávaniu zmien v oprávneniach k akýmkoľvek bezpečnostné nástroje objektom.

Nasledujú bezpečnostné nastavenia a požiadavky pre bezpečnostné nástroje objekty:

- Programy a príkazy bezpečnostné nástroje sú v knižnici produktu QSYS. Príkazy a programy prislúchajú k verejnému oprávneniu *EXCLUDE. Mnoho príkazov bezpečnostné nástroje vytvára súbory v knižnici QUSRSYS. Keď systém vytvorí tieto súbory, verejné oprávnenie pre ne je *EXCLUDE.

  Súbory obsahujúce informácie pre vytváranie zmenených oznámení majú názvy začínajúce s QSEC. Súbory obsahujúce informácie pre riadenie užívateľských profilov majú názvy začínajúce s QASEC. Tieto súbory obsahujú dôverné informácie o vašom systéme. Preto by ste nemali meniť verejné oprávnenie pre súbory.
- bezpečnostné nástroje používajú bežné nastavenie vášho systému pre riadenie tlače výstup. Tieto oznamy obsahujú dôverné informácie o vašom systéme. Aby sa výstup nasmeroval do chráneného frontu výstupov, vykonajte príslušné zmeny v užívateľskom profile, alebo v opise úloh pre užívateľov, ktorí majú spustené bezpečnostné nástroje.
- Kvôli svojim bezpečnostným funkciám, a kvôli tomu, že sprístupňujú mnoho objektov v systéme, príkazy bezpečnostné nástroje vyžadujú špeciálne oprávnenie *ALLOBJ. Niektoré príkazy vyžadujú tiež špeciálne oprávnenia *SECADM, *AUDIT, alebo *IOSYSCFG. Aby ste sa presvedčili, či príkazy prebiehajú úspešne, mali by ste sa prihlásiť ako správca bezpečnosti, keď používate bezpečnostné nástroje. Preto by ste nemali mať povinnosť prideliť súkromné oprávnenie žiadnemu príkazu bezpečnostné nástroje.

## Predchádzanie konfliktom so súbormi

Mnoho príkazov oznámení bezpečnostné nástroje vytvára databázový súbor, ktorý môžete použiť na vytlačenie zmenenej verzie oznámenia. “Príkazy a ponuky pre príkazy bezpečnosti” na strane 26 uvádza názov súboru pre každý príkaz. Naraz je možné pracovať s príkazom iba z jednej úlohy. Väčšina príkazov má zabudovanú kontrolu, ktorá toto zabezpečí. Ak pracujete s príkazom a iná úloha s ním ešte neskončila úlohu, dostanete hlásenie o chybe.

Mnoho tlačových úloh je dlho prebiehajúcimi úlohami. Mali by ste byť opatrný, aby ste predišli konfliktom so súbormi, keď predkladáte oznámenia do dávky, alebo ich pridávate do plánovača úloh. Napríklad by ste mohli chcieť vytlačiť dve verzie oznámenia PRTUSRPRF s rôznymi výberovými kritériami. Ak predkladáte oznámenia do dávky, mali by ste použiť front úloh, ktorá spúšťa len jednu úlohu naraz, aby ste zabezpečili, že úlohy oznámení budú prebiehať postupne za sebou.

Ak používate plánovač úloh, musíte naplánovať dve úlohy v dostatočnom odstupe tak, aby prvá verzia skončila predtým, ako sa začne druhá úloha.

## Uloženie Security Tools

bezpečnostné nástroje programy uložíte vždy, keď spustíte buď príkaz Uložiť systém (SAVSYS), alebo možnosť z ponuky Uložiť, ktorá spustí príkaz SAVSYS.

Súbory bezpečnostné nástroje sú v knižnici QUSRSYS. Uloženie tejto knižnice by ste už mali vykonávať ako súčasť vašich zvyčajných prevádzkových postupov. Knižnica QUSRSYS obsahuje údaje pre mnoho licenčných programov vo vašom systéme. Pozrite si Informačné centrum, kde nájdete viac informácií o tom, ktoré príkazy a voľby ukladajú knižnicu QUSRSYS.

## Príkazy a ponuky pre príkazy bezpečnosti

Táto časť popisuje príkazy a ponuky pre nástroje bezpečnosti. Príklady, ako príkazy používať sa nachádzajú všade v týchto informáciách.

Pre bezpečnostné nástroje sú dostupné dve ponuky:

- Ponuka SECTOOLS (Security Tools) pre interaktívne spustenie príkazov.
- Ponuka SECBATCH (Submit or Schedule Security Reports to Batch) pre spustenie oznamovacích príkazov v dávke. Ponuka SECBATCH má dve časti. Prvá časť ponuky používa príkaz Submit Job (SBMJOB) na predloženie oznámení pre okamžité spracovanie v dávke.

  Druhá časť ponuky používa príkaz ADDJOBSCDE (Add Job Schedule Entry). Použijete ju na naplánovanie bezpečnostných oznámení, aby sa spúšťali pravidelne v danom dni a čase.

### Voľby ponuky Nástroje bezpečnosti

Tabuľka 6 popisuje tieto možnosti ponuky a príslušné príkazy:

*Tabuľka 6. Príkazy nástrojov pre užívateľské profily*

| Voľba Ponuky[1] | Názov príkazu | Opis | Použitý databázový súbor |
|---|---|---|---|
| 1 | ANZDFTPWD | Príkaz Analyze Default Passwords použite na zaznamenanie a spracovanie užívateľských profilov, ktoré majú heslo rovnaké ako názov užívateľského profilu. | QASECPWD[2] |
| 2 | DSPACTPRFL | Príkaz Display Active Profile List použite na zobrazenie alebo vytlačenie zoznamu užívateľských profilov, ktoré sú vyňaté zo spracovania ANZPRFACT. | QASECIDL[2] |
| 3 | CHGACTPRFL | Príkaz Change Active Profile List použite na pridanie a odstránenie užívateľských profilov zo zoznamu vyňatých, pre príkaz ANZPRFACT. Profil užívateľa, ktorý je v zozname aktívnych profilov, je stále aktívny (kým neodstránite profil zo zoznamu). Príkaz ANZPRFACT nevypne profil, ktorý je v zozname aktívnych profilov, bez ohľadu na to, ako dlho bol tento profil neaktívny. | QASECIDL[2] |
| 4 | ANZPRFACT | Príkaz Analyze Profile Activity použite na zablokovanie užívateľských profilov, ktoré neboli používané počas daného počtu dní. Po použití príkazu ANZPRFACT na zadanie počtu dní, systém spustí úlohu ANZPRFACT v noci.<br><br>Príkaz CHGACTPRFL môžete použiť na vyňatie užívateľských profilov pred ich vypnutím. | QASECIDL[2] |

*Tabuľka 6. Príkazy nástrojov pre užívateľské profily (pokračovanie)*

| Voľba Ponuky[1] | Názov príkazu | Opis | Použitý databázový súbor |
|---|---|---|---|
| 5 | DSPACTSCD | Príkaz Display Profile Activation Schedule použite na zobrazenie, alebo vytlačenie informácií o pláne, pre odblokovanie a zablokovanie špecifických užívateľských profilov. Plán môžete vytvoriť s príkazom CHGACTSCDE. | QASECACT[2] |
| 6 | CHGACTSCDE | Príkaz Change Activation Schedule Entry použite na vytvorenie užívateľského profilu, ktorý sa bude môcť prihlásiť len v stanovených časoch dňa alebo týždňa. Pre každý profil užívateľa, ktorý naplánujete, systém vytvorí položky plánu úloh pre čas zapnutia a vypnutia. | QASECACT[2] |
| 7 | DSPEXPSCD | Príkaz Display Expiration Schedule použite na zobrazenie, alebo vytlačenie zoznamu užívateľských profilov, ktoré sú pre budúcnosť naplánované na vypnutie, alebo odstránenie zo systému. Príkaz CHGEXPSCDE použite na nastavenie uplynutia platnosti užívateľských profilov. | QASECEXP[2] |
| 8 | CHGEXPSCDE | Príkaz Change Expiration Schedule Entry použite na naplánovanie odstránenia užívateľského profilu. Môžete ho odstrániť dočasne (jeho vypnutím), alebo ho môžete vymazať zo systému. Tento príkaz používa položku plánu úlohy, ktorá sa spustí každý deň o 00:01 (1 minútu po polnoci). Úloha si prezrie súbor QASECEXP aby zistila, či je na tento deň naplánované uplynutie platnosti nejakých užívateľských profilov.<br><br>Príkaz DSPEXPSCD použite na zobrazenie užívateľských profilov, ktoré majú naplánované uplynutie platnosti. | QASECEXP[2] |
| 9 | PRTPRFINT | Príkaz Print Profile Internals použite na vytlačenie oznámenia, ktoré obsahuje informácie o počte položiek zahrnutých v užívateľskom profile. Počet položiek určuje veľkosť užívateľského profilu. | |

**Poznámky:**

1. Voľby sú z ponuky SECTOOLS.
2. Tento súbor je v knižnici QUSRSYS.

V tejto ponuke môžete posunúť stránku nižšie, aby ste videli ďalšie možnosti. Tabuľka 7 na strane 28 opisuje možnosti ponuky a príslušné príkazy pre revidovanie bezpečnosti:

*Tabuľka 7. Príkazy nástrojov pre auditovanie bezpečnosti*

| Voľba ponuky [1] | Názov príkazu | Opis | Použitý databázový súbor |
|---|---|---|---|
| 10 | CHGSECAUD | Príkaz Change Security Auditing použite na nastavenie revidovania bezpečnosti, a na zmenu systémových hodnôt, ktoré regulujú revidovanie bezpečnosti. Keď spustíte príkaz CHGSECAUD, systém vytvorí žurnál auditovania bezpečnosti (QAUDJRN), ak ešte neexistuje.<br><br>Príkaz CHGSECAUD poskytuje možnosti, ktoré zjednodušujú zadanie systémovej hodnoty QAUDLVL (úroveň auditu). Môžete zadať *ALL pre aktivovanie všetkých možných nastavení úrovne auditu. Alebo môžete zadať *DFTSET pre aktivovanie najbežnejšie používaných nastavení (*AUTFAIL, *CREATE, *DELETE, *SECURITY a *SAVRST).<br>**Poznámka:** Ak použijete bezpečnostné nástroje pre nastavenie auditovania, určite naplánujte riadenie prijímateľov žurnálu auditu. V opačnom prípade môžete rýchlo zachytiť problémy s využitím disku. | |
| 11 | DSPSECAUD | Príkaz Display Security Auditing použite na zobrazenie informácií o žurnáli revidovania bezpečnosti a o systémových hodnotách, ktoré regulujú revidovanie bezpečnosti. | |

**Poznámky:**

1. Voľby sú z ponuky SECTOOLS.

## Použitie ponuky Bezpečnosť dávky

Nasleduje prvá časť ponuky SECBATCH:

```
SECBATCH         Submit or Schedule Security Reports To Batch
                                                                  System:
Vyberte si jednu položku z nasledovných:

  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
```

Keď si z tejto ponuky vyberiete voľbu, uvidíte obrazovku Odovzdať úlohu (SBMJOB). Ak chcete zmeniť štandardné možnosti pre príkaz, môžete stlačiť F4 (Prompt) na riadku *Command to run*.

Aby ste zobrazili Schedule Batch Reports, prejdite na nasledujúcu stranu v ponuke SECBATCH. Pomocou možností v tejto časti ponuky môžete napríklad nastaviť váš systém

tak, aby pravidelne spúšťal zmenené verzie oznámení. Môžete posunúť stránku dole pre ďalšie možnosti ponuky. Keď si vyberiete voľbu z tejto časti ponuky, uvidíte obrazovku Pridať položku rozvrhu úloh (ADDJOBSCDE).

Môžete umiestniť váš kurzor na riadku *Command to run* a stlačiť F4 (Prompt), aby ste vybrali iné nastavenia oznámenia. Mali by ste prideliť názov úlohy s určitým významom, aby ste túto položku mohli rozoznať, keď zobrazíte položky plánu úloh.

## Voľby ponuky Bezpečnosť dávky

Tabuľka 8 popisuje možnosti ponuky a príslušné príkazy pre bezpečnostné oznámenia.

Keď spustíte bezpečnostné oznámenia, systém vytlačí len informácie, ktoré spĺňajú výberové kritériá, ktoré ste zadali, ako aj výberové kritériá pre nástroj. Napríklad, opisom úloh, ktoré špecifikujú názov užívateľského profilu, prislúcha ich zabezpečenie. Preto oznámenie opisu úlohy (PRTJOBDAUT) vytlačí opisy úloh v danej knižnici len vtedy, keď verejné oprávnenie pre opis úlohy nie je *EXCLUDE, *a* keď opis úlohy špecifikuje názov užívateľského profilu v parametri USER.

Podobne, keď tlačíte informácie o podsystéme (príkaz PRTSBSDAUT), systém vytlačí informácie o podsystéme len vtedy, keď opis podsystému má komunikačnú položku, ktorá špecifikuje užívateľský profil.

Ak príslušné oznámenie vytlačí menej informácií ako očakávate, pozrite si informácie v online pomoci, aby ste zistili výberové kritériá pre oznámenie.

*Tabuľka 8. Príkazy pre bezpečnostné správy*

| Voľba ponuky [1] | Názov príkazu | Opis | Použitý databázový súbor |
|---|---|---|---|
| 1, 40 | PRTADPOBJ | Príkaz Print Adopting Objects použite na vytlačenie zoznamu objektov, ktoré preberajú oprávnenie daného užívateľského profilu. Môžete zadať jeden profil, všeobecný názov profilu (ako napríklad všetky profily začínajúce s Q), alebo všetky užívateľské profily v systéme.<br><br>Toto oznámenie má dve verzie. Úplné oznámenie vymenúva všetky prevzaté objekty, ktoré spĺňajú výberové kritériá. Zmenené oznámenie vymenúva rozdiely medzi prevzatými objektmi, ktoré sú v systéme teraz, a prevzatými objektmi, ktoré boli v systéme naposledy, keď ste spustili oznámenie. | QSECADPOLD[2] |
| 2, 41 | DSPAUDJRNE | Príkaz Display Audit Journal Entries použite na zobrazenie, alebo vytlačenie informácií o položkách v žurnáli auditu bezpečnosti. Môžete použiť špecifické typy položiek, špecifických používateľov a časové obdobie. | QASYxxJ4[3] |

*Tabuľka 8. Príkazy pre bezpečnostné správy (pokračovanie)*

| Voľba ponuky [1] | Názov príkazu | Opis | Použitý databázový súbor |
|---|---|---|---|
| 3, 42 | PRTPVTAUT *AUTL | Keď použijete príkaz Print Private Authorities pre objekty *AUTL, získate zoznam všetkých zoznamov oprávnení v systéme. Oznámenie obsahuje používateľov, ktorí majú oprávnenie na každý zoznam, a oprávnenia, ktoré majú používatelia na daný zoznam. Tieto informácie vám pomôžu pri analyzovaní zdrojov objektových oprávnení vo vašom systéme.<br><br>Toto oznámenie má tri verzie. Úplné oznámenie vymenúva všetky zoznamy oprávnení v systéme. Zmenené oznámenie vymenúva doplnky a zmeny v oprávneniach odvtedy, keď ste spustili oznámenie. Vymazané oznámenie vymenúva používateľov, ktorých oprávnenie na zoznam oprávnení bolo vymazané odvtedy, kedy ste naposledy spustili oznámenie.<br><br>Keď vytlačíte úplné oznámenie, máte možnosť vytlačiť zoznam objektov, ktoré zabezpečuje každý zoznam oprávnení. Systém vytvorí oznámenia zvlášť pre každý zoznam oprávnení. | QSECATLOLD[2] |
| 6, 45 | PRTCMNSEC | Príkaz Print Communications Security použite na vytlačenie nastavení dôležitých pre bezpečnosť pre objekty, ktoré ovplyvňujú komunikácie vo vašom systéme. Tieto nastavenia ovplyvnia spôsob vstupu používateľov a úloh do vášho systému.<br><br>Tento príkaz vytvorí dve oznámenia: oznámenie, ktoré zobrazí zoznam nastavení konfigurácií v systéme, a oznámenie, ktoré vymenúva parametre dôležité pre zabezpečenie pre opisy, radiče a opisy zariadení. Každé z týchto oznámení má úplnú aj zmenenú verziu. | QSECCMNOLD[2] |
| 15, 54 | PRTJOBDAUT | Príkaz Print Job Description Authority použite na vytlačenie zoznamu opisov úloh, ktoré špecifikujú užívateľský profil, a majú verejné oprávnenie, ktoré nie je *EXCLUCE. Oznámenie zobrazí špeciálne oprávnenia pre profil používateľa, ktorý je zadaný v opise úlohy.<br><br>Toto oznámenie má dve verzie. Úplné oznámenie vymenúva všetky objekty opisu úloh, ktoré spĺňajú výberové kritériá. Zmenené oznámenie vymenúva rozdiely medzi objektmi opisu úloh, ktoré sú v systéme teraz, a objektmi opisu úloh, ktoré boli v systéme, keď ste naposledy spustili oznámenie. | QSECJBDOLD[2] |

*Tabuľka 8. Príkazy pre bezpečnostné správy (pokračovanie)*

| Voľba ponuky [1] | Názov príkazu | Opis | Použitý databázový súbor |
|---|---|---|---|
| Viď poznámku 4 | PRTPUBAUT | Príkaz Print Publicly Authorized Objects použite na vytlačenie zoznamu objektov, ktorých verejné oprávnenie nie je *EXCLUDE. Keď spustíte príkaz, zadáte typ objektu a knižnicu alebo knižnice pre oznámenie. Príkaz PRTPUBAUT použite na vytlačenie informácií o objektoch, ktoré môže sprístupniť každý používateľ v systéme.<br><br>Toto oznámenie má dve verzie. Úplné oznámenie vymenúva všetky objekty, ktoré spĺňajú výberové kritériá. Zmenené oznámenie vymenúva rozdiely medzi danými objektmi, ktoré sú v systéme teraz, a objektmi (rovnakého typu v rovnakej knižnici), ktoré boli v systéme, keď ste naposledy spustili oznámenie. | QPBxxxxxx[5] |
| Viď poznámku 5. | PRTPVTAUT | Príkaz Print Private Authorities použite na vytlačenie zoznamu súkromných oprávnení na objekty daného typu v danej knižnici. Toto oznámenie vám pomôže pri zisťovaní zdrojov oprávnení na objekty.<br><br>Toto oznámenie má tri verzie. Úplné oznámenie vymenúva všetky objekty, ktoré spĺňajú výberové kritériá. Zmenené oznámenie vymenúva rozdiely medzi danými objektmi, ktoré sú v systéme teraz, a objektmi (rovnakého typu v rovnakej knižnici), ktoré boli v systéme, keď ste naposledy spustili oznámenie. Vymazané oznámenie vymenúva používateľov, ktorých oprávnenie na objekt bolo vymazané odvtedy, kedy ste naposledy vytlačili oznámenie. | QPVxxxxxx[5] |
| 24, 63 | PRTQAUT | Použite Print Queue Report na tlač nastavení bezpečnosti pre výstupné fronty a fronty úloh vo vašom systéme. Tieto nastavenia regulujú, kto môže prezerať a meniť položky vo výstupnom fronte alebo fronte úloh.<br><br>Toto oznámenie má dve verzie. Úplné oznámenie vymenúva všetky výstupné fronty a fronty úloh, ktoré spĺňajú výberové kritériá. Zmenené oznámenie vymenúva rozdiely medzi objektmi výstupných frontov a frontov úloh, ktoré sú v systéme teraz, a objektmi výstupných frontov a frontov úloh, ktoré boli v systéme, keď ste naposledy spustili oznámenie. | QSECQOLD[2] |
| 25, 64 | PRTSBSDAUT | Príkaz Print Subsystem Description použite na vytlačenie položiek komunikácií dôležitých pre bezpečnosť, pre opisy podsystému vo vašom systéme. Tieto nastavenia regulujú, ako môže do vášho systému vstúpiť spracovanie, a ako prebiehajú úlohy. Oznámenie vytlačí opis podsystému len vtedy, keď má komunikačné položky, ktoré špecifikujú názov užívateľského profilu.<br><br>Toto oznámenie má dve verzie. Úplné oznámenie vymenúva všetky objekty opisu podsystému, ktoré spĺňajú výberové kritériá. Zmenené oznámenie vymenúva rozdiely medzi objektmi opisu podsystémov, ktoré sú v systéme teraz, a objektmi opisu podsystémov, ktoré boli v systéme, keď ste naposledy spustili oznámenie. | QSECSBDOLD[2] |

*Tabuľka 8. Príkazy pre bezpečnostné správy (pokračovanie)*

| Voľba ponuky [1] | Názov príkazu | Opis | Použitý databázový súbor |
|---|---|---|---|
| 26, 65 | PRTSYSSECA | Príkaz Print System Security Attributes použite na vytlačenie zoznamu systémových hodnôt a atribútov siete dôležitých pre bezpečnosť. Toto oznámenie zobrazuje súčasnú a odporúčanú hodnotu. | |
| 27, 66 | PRTTRGPGM | Príkaz Print Trigger Programs použite na vytlačenie zoznamu spúšťacích programov, ktoré prislúchajú databázovým súborom vo vašom systéme.<br><br>Toto oznámenie má dve verzie. Úplné oznámenie vymenúva všetky spúšťacie programy, ktoré sú pridelené, a spĺňajú vaše výberové kritériá. Zmenené oznámenie vymenúva spúšťacie programy, ktoré boli pridelené odvtedy, kedy ste naposledy spustili oznámenie. | QSECTRGOLD[2] |
| 28, 67 | PRTUSROBJ | Na tlač zoznamu užívateľských objektov (objekty, ktoré nedodala firma IBM), ktoré sa nachádzajú v knižnici, použite príkaz Print User Objects. Toto oznámenie ste mohli použiť na vytlačenie zoznamu užívateľských objektov, ktoré sú v knižnici (ako napríklad QSYS), ktorá je v zozname knižníc systému.<br><br>Toto oznámenie má dve verzie. Úplné oznámenie vymenúva všetky objekty používateľov, ktoré spĺňajú výberové kritériá. Zmenené oznámenie vymenúva rozdiely medzi objektmi používateľov, ktoré sú v systéme teraz, a objektmi používateľov, ktoré boli v systéme, keď ste naposledy spustili oznámenie. | QSECPUOLD[2] |
| 29, 68 | PRTUSRPRF | Príkaz Print User Profile použite na analýzu užívateľských profilov, ktoré spĺňajú dané kritériá. Profily používateľov môžete vybrať na základe špeciálnych oprávnení, užívateľských tried, alebo nezhôd medzi špeciálnymi oprávneniami a užívateľskými triedami. Môžete vytlačiť informácie o oprávneniach, informácie o prostredí, informácie o heslách a informácie o úrovni hesiel. | |
| 30, 69 | PRTPRFINT | Príkaz Print Profile Internals použite na vytlačenie oznámenia, ktoré obsahuje interné informácie o počte položiek. | |
| 31, 70 | CHKOBJITG | Príkaz Check Object Integrity použite na zistenie, či boli funkčné objekty (napríklad programy) zmenené bez použitia kompilátora. Tento príkaz vám pomôže odhaliť pokusy o zavedenie vírusového programu do vášho systému, alebo o zmenu programu, aby vykonával neoprávnené inštrukcie. Kniha *iSeries Security Reference* poskytuje viac informácií o príkaze CHKOBJITG. | |

*Tabuľka 8. Príkazy pre bezpečnostné správy (pokračovanie)*

| Voľba ponuky [1] | Názov príkazu | Opis | Použitý databázový súbor |
|---|---|---|---|
| **Poznámky:**<br>1. Možnosti sú z ponuky SECBATCH.<br>2. Tento súbor je v knižnici QUSRSYS.<br>3. xx je dvojznakový typ položky žurnálu. Napríklad, modelový výstupný súbor pre záznamy žurnálu AE je QSYS/QASYAEJ4. Modelové výstupné súbory sú popísané v Doplnku F knihy *iSeries Security Reference*.<br>4. Ponuka SECBATCH obsahuje možnosti typov objektov, ktoré sa týkajú väčšinou správcov bezpečnosti. Použite napríklad možnosti 11, alebo 50 na spustenie príkazu PRTPUBAUT oproti objektom *FILE. Použite všeobecné možnosti (18 a 57) pre zadanie typu objektu.<br>5. Ponuka SECBATCH obsahuje možnosti typov objektov, ktoré sa týkajú väčšinou správcov bezpečnosti. Napríklad možnosť 12, alebo 51 spustí príkaz PRTPVTAUT oproti objektom *FILE. Použite všeobecné možnosti (19 a 58) pre zadanie typu objektu.<br>6. Znaky xxxxxx v názve súboru predstavujú typ objektu. Napríklad, súbor pre programové objekty je nazvaný QPBPGM pre verejné oprávnenia, a QPVPGM pre súkromné oprávnenia. Súbory sú v knižnici QUSRSYS.<br>Súbor obsahuje člena pre každú knižnicu, pre ktorú máte vytlačené oznámenie. Názov člena sa zhoduje s názvom knižnice. | | | |

## Príkazy pre prispôsobovanie bezpečnosti

Tabuľka 9 opisuje príkazy, ktoré môžete použiť na prispôsobenie bezpečnosti vo vašom systéme. Tieto príkazy sú v ponuke SECTOOLS:

*Tabuľka 9. Príkazy pre prispôsobovanie vášho systému*

| Voľba ponuky [1] | Názov príkazu | Opis | Použitý databázový súbor |
|---|---|---|---|
| 60 | CFGSYSSEC | Príkaz Configure System Security použite na nastavenie systémových hodnôt dôležitých pre bezpečnosť, na odporúčané nastavenia. Tento príkaz tiež nastavuje revidovanie bezpečnosti vo vašom systéme. "Hodnoty nastavené pomocou príkazu Configure System Security" popisuje, čo tento príkaz vykonáva.<br>**Poznámka:** Ak chcete získať odporúčania pre bezpečnosť prispôsobené vašej situácií, namiesto spustenia tohoto príkazu, spustite Sprievodcu bezpečnosťou iSeries alebo Poradcu bezpečnosti iSeries. Viac informácií o týchto nástrojoch nájdete v Kapitola 2, "Sprievodca bezpečnosťou iSeries a Plánovač bezpečnosti eServer", na strane 9. | |
| 61 | RVKPUBAUT | Príkaz Revoke Public Authority použite na nastavenie verejného oprávnenia na *EXCLUDE pre sadu príkazov vo vašom systéme, citlivých na bezpečnosť. "Funkcie príkazu Revoke Public Authority" na strane 35 vymenúva činnosti, ktoré príkaz RVKPUBAUT vykonáva. | |
| **Poznámky:**<br>1. Voľby sú z ponuky SECTOOLS. | | | |

## Hodnoty nastavené pomocou príkazu Configure System Security

Tabuľka 10 na strane 34 zobrazuje systémové hodnoty, ktoré sa nastavia, keď spustíte príkaz CFGSYSSEC. Príkaz CFGSYSSEC spúšťa program, ktorý sa nazýva QSYS/QSECCFGS.

*Tabuľka 10. Hodnoty nastavené pomocou príkazu CFGSYSSEC*

| Názov systémovej hodnoty | Nastavenie | Opis systémovej hodnoty |
|---|---|---|
| QALWOBJRST | *NONE | Či sa môžu obnovovať stavové programy systému a programy adoptujúce oprávnenie |
| QAUTOCFG | 0 (Nie) | Automatická konfigurácia nových zariadení |
| QAUTOVRT | 0 | Počet opisov virtuálnych zariadení, ktoré vytvorí systém, ak nie je k dispozícii na použitie žiadne zariadenie. |
| QDEVRCYACN | *DSCMSG (Disconnect with message) | Akcia systému pri opätovnom vytvorení komunikácie |
| QDSCJOBITV | 120 | Čas predtým ako systém vykoná na odpojenej úlohe akciu |
| QDSPSGNINF | 1 (Áno) | Či používatelia vidia prihlasovaciu obrazovku |
| QINACTITV | 60 | Čas predtým ako systém vykoná na neaktívnej interaktívnej úlohe akciu |
| QINACTMSGQ | *ENDJOB | Akcia, ktorú systém vykoná na neaktívnej úlohe |
| QLMTDEVSSN | 1 (Áno) | Či sú používatelia obmedzení na prihlásenie do práve jedného zariadenia naraz |
| QLMTSECOFR | 1 (Áno) | Či sú používatelia *ALLOBJ a *SERVICE obmedzení na konkrétne zariadenia |
| QMAXSIGN | 3 | Koľko je povolených za sebou nasledujúcich neúspešných prihlásení |
| QMAXSGNACN | 3 (Oba) | Či systém zablokuje pracovnú stanicu alebo profil používateľ, keď sa dosiahne limit QMAXSIGN. |
| QRMTSIGN | *FRCSIGNON | Ako systém spracúva pokusy o vzdialené (passthrough alebo TELNET) prihlásenie. |
| QRMTSVRATR | 0 (Vypnuté) | Povoľuje vzdialenú analýzu systému. |
| QSECURITY [1 na strane 35] | 50 | Presadená bezpečnostná úroveň |
| QVFYOBJRST | 3 (Pri obnove overiť podpisy) | Pri obnove overiť objekt |
| QPWDEXPITV | 60 | Ako často musia používatelia meniť svoje heslá |
| QPWDMINLEN | 6 | Minimálna dĺžka hesiel |
| QPWDMAXLEN | 8 | Maximálna dĺžka hesiel |
| QPWDPOSDIF | 1 (Áno) | Či sa musí každá pozícia v novom hesle odlišovať od rovnakej pozícii v poslednom hesle |
| QPWDLMTCHR | Pozrite si poznámku 2 na strane 35 | Znaky, ktoré nie sú povolené v heslách |
| QPWDLMTAJC | 1 (Áno) | Či sú v heslách zakázané susedné číslice |
| QPWDLMTREP | 2 (Nemôžu sa za sebou opakovať) | Či sú v heslách zakázané opakujúce sa znaky |
| QPWDRQDDGT | 1 (Áno) | Či musia mať heslá najmenej jednu číslicu |
| QPWDRQDDIF | 1 (32 jedinečných hesiel) | Koľko jedinečných hesiel sa vyžaduje predtým ako sa môže heslo zopakovať |
| QPWDVLDPGM | *NONE | Ukončovací program užívateľa, ktorý systém volá na overenie hesiel |

*Tabuľka 10. Hodnoty nastavené pomocou príkazu CFGSYSSEC (pokračovanie)*

| Názov systémovej hodnoty | Nastavenie | Opis systémovej hodnoty |
|---|---|---|
| **Poznámky:**<br>1. Ak momentálne pracujete s hodnotu 40 pre QSECURITY alebo nižšou, určite si pozrite informácie k Kapitole 2 knihy *iSeries Security Reference* predtým ako prejdete na vyššiu bezpečnostnú úroveň.<br>2. Obmedzené znaky sú uložené v správe s ID CPXB302 v súbore správ QSYS/QCPFMSG. Sú zaslané ako AEIOU@$#. Na zmenenie obmedzených znakov môžete použiť príkaz CHGMSGD (Change Message Description). Systémová hodnota QPWDLMTCHR nie je vnútená na úrovniach hesiel 2 alebo 3. | | |

Príkaz CFGSYSSEC tiež nastaví heslo na *NONE pre nasledovné užívateľské profily dodané od IBM:

QSYSOPR

QPGMR

QUSER

QSRV

QSRVBAS

Na záver, príkaz CFGSYSSEC nastavuje auditovanie bezpečnosti pomocou príkazu CHGSECAUD (Change Security Auditing). Príkaz CFGSYSSEC zapína auditovanie akcií a objektov a tiež špecifikuje štandardnú množinu akcií na auditovanie príkazom CHGSECAUD.

### Prispôsobenie programu

Ak niektoré z týchto nastavení nie sú vhodné pre vašu inštaláciu, vytvoríte si svoju vlastnú verziu programu, ktorý spracúva príkaz. Spravte nasledovné:

__ Krok 1. Použite príkaz RTVCLSRC (Use the Retrieve CL Source) na skopírovanie zdrojového programu, ktorý sa spúšťa keď použijete príkaz CFGSYSSEC. Program na získanie je QSYS/QSECCFGS. Keď ho získate, dajte mu *iný názov*.

__ Krok 2. Zmeny spravte upravením programu. Potom ho skompilujte. Pri kompilácii sa uistite, že *nenahradzujete* program QSYS/QSECCFGS dodaný od IBM. Váš program by mal mať odlišný názov.

__ Krok 3. Použite príkaz CHGCMD (Change Command) na zmenu programu, aby spracoval parameter príkazu (PGM) pre príkaz CFGSYSSEC. Nastavte hodnotu PGM na názov vášho programu. Napríklad, ak vytvoríte program v knižnici QGPL nazvaný MYSECCFG, mali by ste napísať nasledovné:

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

**Poznámka:** Ak zmeníte program QSYS/QSECCFGS, IBM nemôže zaručiť ani implikovať spoľahlivosť, prevádzkyschopnosť, výkon ani funkciu programu. Zahrnuté záruky predajnosti a vhodnosti pre konkrétny účel sú výslovne popreté.

## Funkcie príkazu Revoke Public Authority

Na nastavenie verejného oprávnenia na *EXCLUDE pre množinu príkazov a programov môžete použiť príkaz Revoke Public Authority (RVKPUBAUT). Príkaz RVKPUBAUT spúšťa program, nazývaný QSYS/QSECRVKP. Pri dodaní odoberá QSECRVKP verejné oprávnenie (nastavením verejného oprávnenia na *EXCLUDE) pre príkazy, ktoré sú uvedené v Tabuľka 11 na strane 36 a aplikačným programovým rozhraniam (API), uvedeným v Tabuľka 12 na strane 36. Pri dodaní vášho systému majú tieto príkazy a API nastavené ich verejné oprávnenie na *USE.

Príkazy, ktoré sú uvedené v Tabuľka 11 a API, ktoré sú uvedené v Tabuľka 12, všetky vykonávajú na vašom systéme funkcie, ktoré môžu byť zdrojom nepríjemností. Ako správca bezpečnosti by ste mali explicitne autorizovať používateľov na používanie týchto príkazov a programov a nerobiť ich dostupnými pre všetkých používateľov systému.

Keď spustíte príkaz RVKPUBAUT, špecifikujete knižnicu, ktorá obsahuje príkazy. Štandardne to je knižnica QSYS. Ak máte na vašom systéme viac ako jeden národný jazyk, tento príkaz musíte spustiť pre každú knižnicu QSYSxxx.

*Tabuľka 11. Príkazy, ktoré majú nastavené verejné oprávnenie pomocou príkazu 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 |

API v Tabuľka 12 sú všetky v knižnici QSYS:

*Tabuľka 12. Programy, ktoré majú nastavené verejné oprávnenie pomocou príkazu RVKPUBAUT*

| |
|---|
| QTIENDSUP |
| QTISTRSUP |
| QWTCTLTR |
| QWTSETTR |
| QY2FTML |

Keď spustíte príkaz RVKPUBAUT, systém nastaví verejné oprávnenie pre koreňový adresár na *USE (pokiaľ to už nie je *USE alebo menšie).

## Prispôsobenie programu

Ak niektoré z týchto nastavení nie sú vhodné pre vašu inštaláciu, vytvoríte si svoju vlastnú verziu programu, ktorý spracúva príkaz. Spravte nasledovné:

__ Krok 1. Použite príkaz RTVCLSRC (Use the Retrieve CL Source) na skopírovanie zdrojového programu, ktorý sa spúšťa keď použijete príkaz RVKPUBAUT. Program na získanie je QSYS/QSECRVKP. Keď ho získate, dajte mu *iný názov*.

__ Krok 2. Zmeny spravte upravením programu. Potom ho skompilujte. Pri kompilácii sa uistite, že *nenahradzujete* program QSYS/QSECRVKP, dodaný od IBM. Váš program by mal mať odlišný názov.

__ Krok 3. Použite príkaz CHGCMD (Change Command) na zmenu programu, aby spracoval parameter príkazu (PGM) pre príkaz RVKPUBAUT. Nastavte hodnotu PGM na názov vášho programu. Napríklad, ak vytvoríte program v knižnici QGPL nazvaný MYRVKPGM, mali by ste napísať nasledovné:

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

**Poznámka:** Ak zmeníte program QSYS/QSECRVKP, IBM nemôže zaručiť ani implikovať spoľahlivosť, prevádzkyschopnosť, výkon ani funkciu programu. Zahrnuté záruky predajnosti a vhodnosti pre konkrétny účel sú výslovne popreté.

# Časť 2. Rozšírená bezpečnosť iSeries

# Kapitola 5. Ochrana informačného majetku s oprávnením k objektu

Ako správca bezpečnosti máte na starosť chrániť informácie vašej organizácie bez frustrácie používateľov na vašom systéme. Musíte zabezpečiť, aby používatelia mali dostatočné oprávnenie na vykonávanie ich úloh bez toho, aby ste im dali oprávnenie na prechádzanie cez systém a vykonanie neoprávnených zmien.

**Bezpečnostný tip**

Oprávnenie, ktoré je príliš tesné môže zlyhať. Používatelia môžu zareagovať na príliš silné obmedzenia oprávnení tak, že budú vzájomne zdieľať heslá.

Operačný systém OS/400 podporuje integrovanú ochranu objektov. Používatelia musia na prístup k objektom používať rozhrania poskytované systémom. Napríklad, ak chcete pristupovať na databázový súbor, musíte použiť príkazy alebo programy, ktoré sú určené na prístup k databázovým súborom. Nemôžete použiť príkaz, ktorý je určený na prístup do frontu správ alebo protokolu úlohy.

Kedykoľvek použijete systémové rozhranie na prístup k objektu, systém overí, či máte oprávnenie na objekt, ktoré vyžaduje rozhranie. Oprávnenie objektu je výkonný a flexibilný nástroj pre chránenie majetku na vašom systéme. Ako správca bezpečnosti máte za úlohu nastaviť účinnú schému bezpečnosti objektov, ktorú môžete spravovať a udržiavať.

## Vynútenie si oprávnenia k objektu

Vždy keď sa pokúsiť o prístup na objekt si operačný systém skontroluje vaše oprávnenie k tomuto objektu. Ak je bezpečnostná úroveň na vašom systéme (systémová hodnota QSECURITY) nastavená na 01 alebo 20, každý užívateľ má oprávnenie pristupovať na všetky objekty, pretože každý užívateľský profil má špeciálne oprávnenie *ALLOBJ.

**Tip pre oprávnenie k objektu:** Ak nemáte istotu, či používate bezpečnosť objektov, skontrolujte systémovú hodnotu QSECURITY (úroveň bezpečnosti). Ak je QSECURITY 10 alebo 20, nepoužíva bezpečnosť objektov.

Pred zmenou bezpečnostnej úrovne na 30 alebo vyššiu musíte plánovať a pripraviť sa na to. V opačnom prípade vaši používatelia nebudú môcť pristupovať na informácie, ktoré potrebujú.

Téma **Základná bezpečnosť systému a plánovanie** v Information Center poskytuje metódu pre analyzovanie vašich aplikácií a pre rozhodovanie, ako by ste mali nastaviť bezpečnosť objektov. Ak ešte nepoužívate bezpečnosť objektov alebo, ak je schéma bezpečnosti vašich objektov zastaraná a komplikovaná, prečítajte si túto tému, ktorá vám pomôže začať.

## Bezpečnosť ponúk

Server iSeries bol pôvodne navrhnutý ako nasledujúci produkt pre S/36 a S/38. Mnohé inštalácie servera iSeries boli, kedysi, inštaláciami S/36 alebo inštaláciami S/38. Na riadenie toho, čo môžu vykonávať používatelia, správcovia bezpečnosti na týchto skorších systémoch používali techniku, ktorá sa nazývala **bezpečnosť ponúk** alebo **riadenie prístupu do ponúk**.

Riadenie prístupu do ponúk znamená, že keď sa užívateľ prihlási, užívateľ uvidí ponuku. Užívateľ môže vykonávať len funkcie, ktoré sú v ponuke. Užívateľ sa nemôže dostať do príkazového riadku na systéme, aby vykonal funkcie, ktoré nie sú v ponuke. Teoreticky sa správca bezpečnosti nemusí obávať o oprávnenie na objekty, pretože aktivita užívateľov je riadená ponukami a programami.

Server iSeries poskytuje niekoľko volieb užívateľského profilu pre pomoc s riadením prístupu do ponúk. Môžete použiť:

- Parameter **Úvodná ponuka** (INLMNU) na riadenie toho, akú ponuku užívateľ uvidí ako prvú po prihlásení.
- Parameter **Úvodný program** (INLPGM) na spustenie programu nastavenia predtým, ako užívateľ uvidí ponuku. Alebo parameter INLPGM môžete použiť na obmedzenie spustenia nejakého programu užívateľom.
- Parameter **Schopnosti obmedzenia** (LMTCPB) na zamedzenie prístupu užívateľa k limitovanej sade príkazov. Tiež zabraňuje užívateľovi špecifikovať iný úvodný program alebo ponuku na prihlasovacej obrazovke. (Parameter MTCPB obmedzuje len príkazy zadané z príkazového riadku.)

## Obmedzenia riadenia prístupu do ponúk

Počítače a používatelia počítačov sa za posledných pár rokov veľmi zmenili. Používatelia majú k dispozícii veľa programov, ako sú dotazovacie programy a tabuľkové procesory, pomocou ktorých si môžu samostatne niečo naprogramovať, čím odbremenia oddelenia informačných systémov. Niektoré nástroje, ako je SQL alebo ODBC, poskytujú možnosť prezerania informácií a zmeniť informácie. Umožniť tieto nástroje v štruktúre ponúk je veľmi zložité.

Pracovné stanice s pevnou funkciou (“zelená obrazovka”) sa rýchlo nahradzujú osobnými počítačmi a počítačovými sieťami. Ak sa váš systém nachádza v sieti, používatelia môžu do vášho systému vstúpiť bez toho, aby videli akúkoľvek prihlasovaciu obrazovku alebo ponuku.

Ako správca bezpečnosti, ktorý sa pokúša použiť riadenie prístupu do ponúk, narazíte na dva problémy:

- Ak ste úspešne obmedzili užívateľov na ponuky, vaši používatelia budú pravdepodobne nespokojní, lebo je obmedzená ich možnosť použiť moderné nástroje.
- Ak sa vám to nepodarí, mohli by ste vystaviť nebezpečiu dôverné informácie, ktoré mali byť chránené prístupom do ponúk. Keď sa váš systém nachádza v sieti, vaša možnosť na používanie riadenie prístupu do ponúk je menšia. Napríklad, parameter LMTCPB sa týka len príkazov zadaných z príkazového riadku v interaktívnej relácii. Parameter LMTCPB nemá žiaden vplyv na požiadavky z komunikačných relácií, ako pre prenos súborov PC, FTP alebo vzdialené príkazy.

## Rozšírenie riadenia prístupu do ponúk pomocou bezpečnosti objektov

Pri množstve nových volieb, ktoré sú dostupné na pripojenie do systémov, sa života schopná schéma bezpečnosti servera iSeries nemôže v budúcnosti spoliehať iba na riadenie prístupu do ponúk. Táto téma poskytuje návrhy ako prejsť na prostredie so zabezpečenými objektmi na doplnenie riadenia vášho prístupu do ponúk.

Téma *Základná systémová bezpečnosť a plánovanie* v Informačnom centre opisuje techniku pre analyzovanie oprávnenia, ktoré musia mať používatelia na objekty, aby mohli spúšťať vaše súčasné aplikácie. Užívateľov priradíte do skupín a skupinám dáte vhodné oprávnenie. Tento prístup je primeraný a logický. Ak váš systém funguje mnoho rokov a má veľa aplikácií, úloha analyzovania a nastavenia oprávnenia objektov sa môže zdať zdrvujúca.

**Tip pre oprávnenie k objektu:** vaše aktuálne ponuky v kombinácií s programami, ktoré si adoptujú oprávnenia vlastníkov programov môžu poskytnúť prechod cez riadenie prístupu do ponúk. Presvedčte sa, že chránite programy adoptujúce oprávnenie a užívateľské profily, ktoré ich vlastnia.

Vaše súčasné ponuky môžete použiť na pomoc pri nastavení prechodného prostredia, kým postupne analyzujete vaše aplikácie a objekty. Nasleduje príklad na používanie ponuky Zadanie objednávky (OEMENU) a pridružených súborov a programov.

## Príklad: Nastavenie prechodného prostredia

Tento príklad začína s nasledovnými predpokladmi a požiadavkami:

- Všetky súbory sú v knižnici ORDERLIB.
- Nepoznáte názvy všetkých súborov. Tiež neviete, aké oprávnenie vyžadujú voľby ponuky na rôzne súbory.
- Ponuky a všetky programy, ktoré volá, sú v knižnici pomenovanej ORDERPGM.
- Chcete, aby každý kto sa môže prihlásiť do vášho systému, mohol prezerať informácie vo všetkých súboroch objednávok, súborov zákazníkov a položiek (napríklad, s dotazmi alebo tabuľkami).
- Meniť súbory by mohli len tí používatelia, ktorých súčasná prihlasovacia ponuka je OEMENU. A aby toto mohli vykonať, musia použiť programy v ponuke.
- Systémoví používatelia, iní ako správcovia bezpečnosti, nemajú špeciálne oprávnenie *ALLOBJ alebo or *SECADM.

Vykonajte nasledujúce kroky, na zmenu tohto prostredia riadenia-prístupu-do-ponúk, aby sa vyhovelo potrebe dotazov:

__ Krok 1. Spravte zoznam užívateľov, ktorých úvodná ponuka je OEMENU.

Na zobrazenie prostredia pre každý užívateľský profil na vašom systéme môžete použiť príkaz PRTUSRPRF *ENVINFO (Print User Profile). Výstup bude obsahovať úvodnú ponuku, úvodný program a súčasnú knižnicu. Obrázok 7 na strane 57 ukazuje príklad výstupu.

__ Krok 2. Presvedčte sa, že objekt OEMENU (môže to byť objekt *PGM alebo *MENU) je vlastnený užívateľským profilov, ktorý nie je použitý na prihlásenie. Užívateľský profil by mal byť zakázaný alebo mať heslo *NONE. Pre tento príklad predpokladajme, že OEOWNER vlastní programový objekt OEMENU.

__ Krok 3. Presvedčte sa, že užívateľský profil vlastniaci programový objekt OEMENU nie je skupinový profil. Môžete použiť nasledovný príkaz:

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

__ Krok 4. Zmeňte program OEMENU tak, aby adoptoval oprávnenie užívateľského profilu OEOWNER. (Na zmenenie parametra USRPRF na *OWNER použite príkaz CHGPGM.)

**Poznámka:** Objekty *MENU nemôžu adoptovať oprávnenie. AK je OEMENU objekt *MENU, tento príklad môžete použiť na vykonanie jedného z nasledovného:

- Vytvoriť program na zobrazenie ponuky.
- Použiť adoptované oprávnenie pre programy, ktoré sa spúšťajú keď užívateľ vyberie voľbu z ponuky OEMENU.

__ Krok 5. Nastavte verejné oprávnenie všetkých súborov v ORDERLIB na *USE napísaním nasledovných dvoch príkazov:

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

Nezabudnite, že ak vyberiete oprávnenie *USE, používatelia môžu kopírovať súbor pomocou prenosu súborov PC alebo FTP.

__ Krok 6. Profilu, ktorý vlastní program ponuky, dajte oprávnenie *ALL na všetky súbory napísaním nasledovného:

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

Pre väčšinu aplikácií je oprávnenie *CHANGE postačujúce. Vaše aplikácie však môžu vykonávať funkcie, ako je vyčistenie členov fyzického súboru, ktoré vyžadujú väčšie oprávnenie ako *CHANGE. Prípadne by ste mali zanalyzovať vaše aplikácie a aplikácii poskytnúť len minimálne potrebné oprávnenie. Počas prechodnej doby sa adoptovaním oprávnenia *ALL vyhnete zlyhaniam aplikácií, ktoré by mohli byť spôsobené nedostatočným oprávnením.

__ Krok 7. Obmedzte oprávnenie na programy v inej knižnici napísaním nasledovného:

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

__ Krok 8. Profilu OEOWNER dajte oprávnenie na programy v knižnici napísaním nasledovného:

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

__ Krok 9. Užívateľom identifikovaným v kroku 1 dajte oprávnenie na program ponuky napísaním nasledovného pre každého užívateľa:

```
GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM)
     USER(názov-užívateľského-programu) AUT(*USE)
```

Keď dokončíte tieto kroky, všetci používatelia systému, ktorí nie sú explicitne vylúčení, budú môcť pristupovať (ale nie meniť) súbory v knižnici ORDERLIB. Používatelia s oprávnením na program QEMENU budú môcť používať programy v ponuke na aktualizáciu súborov v knižnici ORDERLIB. Meniť súbory v tejto knižnici budú môcť len používatelia s oprávnením na program OEMENU. Súbory sú chránené kombináciou zabezpečenia objektov a riadením prístupu do ponúk.

Keď dokončíte podobné kroky pre všetky knižnice, ktoré obsahujú údaje užívateľov, vytvoríte jednoduchú schému na riadenie aktualizácií databáz. Táto metóda zabraňuje užívateľom systému aktualizovať databázové súbory okrem prípadu, keď používajú schválené ponuky a programy. Zároveň ste sprístupnili databázové súbory na prezeranie, analyzovanie a kopírovanie pre užívateľov s nástrojmi na podporu rozhodovania alebo s väzbami z iného systému alebo z PC.

**Tip pre oprávnenie k objektu:** Keď sa váš systém nachádza v sieti, oprávnenie *USE môže poskytnúť väčšie oprávnenie ako očakávate. Napríklad, pomocou FTP môžete spraviť kópiu súboru do iného systému (vrátane PC), ak na súborov máte oprávnenie *USE.

## Použitie zabezpečenia knižníc na doplnenie bezpečnosti ponúk

Aby ste mohli pristupovať na objekt v knižnici, musíte mať oprávnenie na objekt aj na knižnicu. Väčšina operácii vyžaduje pre knižnicu oprávnenie *EXECUTE alebo *USE.

V závislosti od vašej situácii by ste mohli používať oprávnenie knižnice ako jednoduchý prostriedok na zabezpečenie objektov. Napríklad, ak budeme uvažovať o príklade ponuky Zadanie objednávky, tak každý s oprávnením na ponuku Zadanie objednávky môže použiť všetky programy v knižnici ORDERPGM. Radšej by ste mali nastaviť verejné oprávnenie pre knižnicu ORDERPGM na *EXCLUDE ako zabezpečovať jednotlivé programy. Takto môžete

poskytnúť oprávnenie *USE na knižnicu konkrétnym užívateľským profilom, ktoré im umožní používať programy v knižnici. (Toto predpokladá, že verejné oprávnenie na programy je *USE alebo väčšie.)

Oprávnenie knižnice môže byť jednoduchá, účinná metóda pre správu oprávnení objektov. Musíte si byť však vedomý obsahu zabezpečovaných knižníc, aby ste neposkytli neplánovaný prístup na objekty.

## Konfigurovanie vlastníctva objektu

Vlastníctvo objektov na vašom systéme je dôležitá časť vašej schémy oprávnenia objektov. Štandardne má vlastník objektu na tento objekt oprávnenie *ALL. Kapitola 5 v knihe *iSeries Security Reference* poskytuje odporúčania a príklady pre plánovanie vlastníctva objektov. Nasleduje niekoľko tipov:

- Vo všeobecnosti by skupinové profily nemali vlastniť objekty. Ak skupinový profil vlastní objekt, všetci členovia skupiny majú na objekt oprávnenie *ALL, ak člen skupiny nie je explicitne vylúčený.
- Ak používate adoptované oprávnenie, pouvažujte o tom, či by mali užívateľské profily vlastniace programy tiež mali vlastniť objekty aplikácií, ako sú súbory. Nemusíte chcieť, aby používatelia spúšťajúci programy adoptujúce oprávnenie mali na súbory oprávnenie *ALL.

Ak používate iSeries Navigator, dá sa to previesť dokončením zmien s použitím funkcie bezpečnostných **politík**. Viac informácií nájdete v Informačnom centre (pozrite si detaily v časti “Nevyhnutné predpoklady a súvisiace informácie” na strane xii).

## Oprávnenie k objektu pre systémové príkazy a programy

Nasleduje niekoľko návrhov týkajúcich sa obmedzovania oprávnenia na objekty dodané IBM:

- Keď máte na svojom systéme viac ako jeden národný jazyk, váš systém má viac ako jednu systémovú knižnicu (QSYS). Váš systém má knižnicu QSYSxxxx pre každý národný jazyk na vašom systéme. Ak používate oprávnenie objektov na riadenie prístupu na systémové príkazy, nezabudnite zabezpečiť príkaz v knižnici QSYS v každej knižnici QSYSxxx na vašom systéme.
- Knižnica System/38 niekedy poskytuje príkaz s funkciou, ktorá je ekvivalentná s príkazmi, ktoré chcete obmedziť. Uistite sa, že obmedzíte príslušný príkaz v knižnici QSYS38.
- Ak máte prostredie System/36, možno budete musieť obmedziť dodatočné programy. Napríklad, program QY2FTML poskytuje prenos súborov na System/36.

## Audit bezpečnostných funkcií

Táto kapitola opisuje techniky pre auditovanie účinnosti bezpečnosti na vašom systéme. Ľudia auditujú bezpečnosť ich systému z niekoľkých dôvodov:

- Na vyhodnotenie, či je ich bezpečnostný plán úplný.
- Na overenie, že všetky naplánované bezpečnostné prvky sú na mieste a fungujú. Tento typ auditovania zvyčajne vykonáva správca bezpečnosti ako súčasť dennej správy bezpečnosti. Tiež sa vykonáva, niekedy oveľa podrobnejšie, ako súčasť pravidelného vyhodnocovania bezpečnosti internými alebo externými audítormi.
- Na overenie, že bezpečnosť systému drží krok so zmenami v systémovom prostredí. K príkladom zmien, ktoré ovplyvňujú bezpečnosť patria:
  - Vytvorenie nových objektov užívateľmi systému
  - Povolenie vstupu nových užívateľov do systému
  - Zmena vlastníctva objektu (nenastavená autorizácia)

- Zmena zodpovedností (zmena skupiny užívateľov)
- Dočasné oprávnenie (včasné neodobratie)
- Inštalácia nových produktov

• Aby ste sa pripravili na budúcu udalosť, ako je inštalácia novej aplikácie, prechodom na vyššiu bezpečnostnú úroveň alebo nastavením komunikačnej siete.

Popísané techniky v tejto kapitole sú vhodné pre všetky tieto situácie. Čo máte auditovať a ako často závisí na veľkosti a bezpečnostných potrebách vašej organizácie. Účelom tejto kapitoly je rozobrať dostupné informácie, ako ich získať a prečo sú potrebné, nie dávať pokyny ku frekvencii auditov.

Tieto informácie majú tri časti:

• Kontrolný zoznam položiek, ktoré sa môžu naplánovať a auditovať.
• Informácie o nastavovaní a používaní auditovacieho žurnálu, poskytovaného systémom.
• Ostatné techniky, ktoré sú dostupné na získanie bezpečnostných informácií na systéme.

Auditovanie bezpečnosti zahŕňa použitie príkazov na iSeries systéme a prístup na protokoly a informácie žurnálov na systéme. Môžete vytvoriť špeciálny profil, ktorý bude používať osoba, vykonávajúca bezpečnostný audit vášho systému. Profil audítora bude potrebovať špeciálne oprávnenie *AUDIT, aby mohol meniť auditovacie charakteristiky vášho systému. Niektoré z odporučených úloh v tejto kapitole vyžadujú užívateľský profil so špeciálnym oprávnením *ALLOBJ a *SECADM. Nezabudnite po skončení auditovania nastaviť heslo pre profil audítora na *NONE.

Viac informácií o auditovaní bezpečnosti nájdete v kapitole 9 príručky *Prehľad bezpečnosťou*.

## Analýza užívateľských profilov

Úplný zoznam všetkých používateľov na vašom systéme môžete zobraziť alebo vytlačiť príkazom DSPAUTUSR (Display Authorized Users). Tento zoznam sa môže usporiadať podľa názvu profilu alebo názvu skupinového profilu. Nasleduje príklad poradia podľa 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       Predaj a Marketing
            DPTWH      08/13/0x    X       Sklad
            RICHARDS   09/05/0x            Janet Richards
            SMITHJ     09/18/0x            John Smith
```

### Tlač vybraných užívateľských profilov

Príkaz DSPUSRPRF (Display User Profile) môžete použiť na vytvorenie výstupného súboru, ktorý môžete spracovať pomocou dotazovacieho nástroja.

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

Dotazovací nástroj môžete použiť na vytvorenie rôznych hlásení analýzy vášho výstupného súboru, ako:

- Zoznam všetkých používateľov, ktorí majú špeciálne oprávnenie *ALLOBJ a *SPLCTL.
- Zoznam všetkých používateľov, usporiadaný podľa poľa užívateľského profilu, ako je úvodný program alebo trieda používateľov.

Môžete vytvoriť dotazovacie programy, ktoré budú produkovať rôzne hlásenia z vášho výstupného súboru. Napríklad:

- Zobrazte všetky užívateľské profily, ktoré majú ľubovoľné špeciálne oprávnenia výberom záznamov, ktorých pole UPSPAU je rovné *NONE.
- Zobrazte všetkých používateľov, ktorí majú povolené zadávať príkazy výberom záznamov, kde pole *Obmedzenie schopností* (nazývané UPLTCP v modelovom výstupnom datazovom súbore) je rovné *NO alebo *PARTIAL.
- Zobrazte všetkých používateľov, ktorí majú konkrétnu úvodnú ponuku alebo úvodný program.
- Zobrazte neaktívnych používateľov prehľadaním poľa s dátumom posledného prihlásenia.

### Preverenie veľkých užívateľských profilov

Užívateľské profily s veľkým počtom oprávnení, ktoré vyzerajú ako náhodne rozprestreté nad väčšinou systému môžu odrážať potrebu plánovania bezpečnosti. Nasleduje metóda nájdenia veľkých užívateľských profilov a ich vyhodnotenia:

1. Príkaz DSPOBJD (Display Object Description) použite na vytvorenie výstupného súboru, ktorý obsahuje informácie o všetkých užívateľských profiloch na systéme:

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

2. Vytvorte dotazový program, ktorý zobrazí názov a veľkosť každého užívateľského profilu v zostupnom poradí podľa veľkosti.
3. Vytlačte detailné informácie o najväčších užívateľských profiloch a vyhodnoťte oprávnenia a vlastnené objekty, či sú primerané:

   ```
   DSPUSRPRF USRPRF(názov-užívateľského-profilu) +
             TYPE(*OBJAUT) OUTPUT(*PRINT)
   DSPUSRPRF USRPRF(názov-užívateľského-profilu) +
             TYPE(*OBJOWN) OUTPUT(*PRINT)
   ```

   Niektoré užívateľské profily od IBM sú veľmi veľké pre počet objektov, ktoré vlastnia. Ich výpisy a analýza je zvyčajne nepotrebná. Mali by ste však skontrolovať programy, adoptujúce oprávnenie užívateľských profilov od IBM, ktoré majú špeciálne oprávnenie *ALLOBJ, ako je QSECOFR a QSYS.

Viac informácií o auditovaní bezpečnosti nájdete v kapitole 9 príručky *Prehľad bezpečnosťou*.

## Analýza oprávnení na objekt

Na zistenie, kto má oprávnenie na knižnice na systéme môžete použiť nasledovnú metódu:

1. Použite príkaz DSPOBJD na vypísanie všetkých knižníc na systéme:

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

   **Poznámka:** Knižnice v nezávislých pomocných oblastiach ukladania, ktoré nie sú v stave AVAILABLE, sa pomocou tohoto príkazu nezobrazia.

2. Príkaz DSPOBJAUT (Display Object Authority) použite na vypísanie oprávnení na špecifickú knižnicu:

   ```
   DSPOBJAUT OBJ(QSYS/názov-knižnice) OBJTYPE(*LIB) +
             ASPDEV(názov-zariadenia-asp) OUTPUT(*PRINT)
   ```

3. Príkaz DSPLIB (Display Library) použite na vypísanie objektov v knižnici:

   ```
   DSPLIB LIB(QSYS/názov-knižnice) ASPDEV(názov-zariadenia-asp) OUTPUT(*PRINT)
   ```

Pomocou týchto hlásení môžete určiť, čo je v knižnici a kto má prístup na knižnicu. Ak to je potrebné, použite tiež príkaz DSPOBJAUT na zobrazenie oprávnenia na vybraté objekty v knižnici.

## Kontrola zmenených objektov

Príkaz CHKOBJITG (Check Object Integrity) môžete použiť na nájdenie objektov, ktoré boli zmenené. Zmenený objekt zvyčajne znamená, že niekto sa pokúša zasahovať do vášho systému. Tieto príkazy môžete spustiť po tom, ako niekto:

- Obnovil programy na vašom systéme
- Použil vyhradené servisné nástroje (DST)

Keď spustíte tento príkaz, systém vytvorí databázový súbor, obsahujúci informácie o všetkých možných problémoch s integritou. Môžete vyhľadať objekty vlastnené jedným profilom, viacerými rôznymi profilmi alebo všetkými profilmi. Môžete vyhľadať objekty, ktorých doména sa zmenila. Môžete tiež prepočítať validačné hodnoty programu, aby sa vyhľadali zmenené objekty typu *PGM, *SRVPGM, *MODULE a *SQLPKG.

Spustenie programu CHKOBJITG vyžaduje špeciálne oprávnenie *AUDIT. Tento príkaz môže trvať dosť dlho, pretože prehľadáva a robí prepočty. Mali by ste ho spustiť v čase, kedy váš systém nie je vyťažený.

**Poznámka:** Profily, ktoré vlastnia veľa objektov s mnohými súkromnými oprávneniami sa môžu stať veľmi veľkými. Veľkosť profilu vlastníka môže ovplyvňovať výkon pri zobrazovaní a práci s oprávnením na vlastnené objekty a pri ukladaní alebo obnove profilov. Môže to tiež ovplyvniť systémové operácie. Aby ste zabránili dopadu na výkon alebo systémové operácie, rozdeľte vlastníctvo objektov medzi viacero profilov. **Nepriraďujte všetky (alebo takmer všetky) objekty len jednému profilu vlastníka.**

## Analýza programov, ktoré si adoptujú oprávnenie

Programy, ktoré adoptujú oprávnenie užívateľa so špeciálnym oprávnením *ALLOBJ predstavujú možné bezpečnostné riziko. Na nájdenie a vyšetrenie takýchto programov sa môže použiť nasledovná metóda:

1. Pre každého užívateľa so špeciálnym oprávnením *ALLOBJ použite príkaz Display Programs That Adopt (DSPPGMADP) na zobrazenie programov, ktoré adoptujú oprávnenie tohto užívateľa:

   ```
   DSPPGMADP
   USRPRF(názov-užívateľského-profilu) +
             OUTPUT(*PRINT)
   ```

   **Poznámka:** Téma “Tlač vybraných užívateľských profilov” na strane 47 ukazuje, ako zobraziť užívateľov s oprávnením *ALLOBJ.

2. Na zistenie, kto je oprávnený na používanie každého adoptujúceho programu a ktoré verejné oprávnenie má program použite príkaz DSPOBJAUT:

   ```
   DSPOBJAUT OBJ(názov-knižnice/názov-programu) +
             OBJTYPE(*PGM) ASPDEV(názov-knižnice/názov-programu) +
             OUTPUT(*PRINT)
   ```

3. Preskúmajte zdrojový kód a opis programu a určite:
   - Či užívateľ programu má zakázané pristupovať na nadbytočnú funkciu, ako je použitie príkazového riadka, počas prevádzky pod adoptovaným profilom.
   - Či program adoptuje minimálnu potrebnú úroveň oprávnenia pre určenú funkciu. Aplikácie, ktoré dokážu využiť zlyhanie programu sa môžu navrhnúť pomocou rovnakého profilu vlastníka pre objekty a programy. Keď sa adoptuje oprávnenie vlastníka programu, užívateľ má na objekty aplikácií oprávnenie *ALL. V mnohých prípadoch profil vlastníka nepotrebuje žiadne špeciálne oprávnenia.
4. Pomocou príkazu DSPOBJD skontrolujte, kedy bol program naposledy zmenený:

```
DSPOBJD OBJ(názov-knižnice/názov-programu) +
        OBJTYPE(*PGM) ASPDEV(názov-knižnice/názov-programu) +
        DETAIL(*FULL)
```

## Riadenie žurnálu auditu a žurnálových prijímačov

Auditovací žurnál, QSYS/QAUDJRN, je určený hlavne pre auditovanie bezpečnosti. Objekty by sa nemali žurnálovať do tohto auditovacieho žurnálu. Riadenie odovzdania zmien by nemalo používať auditovací žurnál. Užívateľské záznamy by sa nemali posielať do tohto žurnálu pomocou príkazu Send Journal Entry (SNDJRNE) alebo API Send Journal Entry (QJOSJRNE).

Na zaistenie toho, aby systém mohol zapisovať auditovacie záznamy do auditovacieho žurnálu sa používa špeciálna ochrana zamykaním. Keď je auditovanie aktívne (systémová hodnota QAUDCTL nie je *NONE), systémová arbitrážna úloha (QSYSARB) drží na žurnáli QSYS/QAUDJRN zámku. Keď je aktívne auditovanie, nemôžete na auditovacom žurnáli vykonávať niektoré operácie ako sú:

- Príkaz DLTJRN
- Príkaz ENDJRNxxx
- Príkaz APYJRNCHG
- Príkaz RMVJRNCHG
- Príkaz DMPOBJ alebo DMPSYSOBJ
- Presun žurnálu
- Obnova žurnálu
- Operácie, ktoré pracujú s oprávnením, ako je príkaz GRTOBJAUT
- Príkaz WRKJRN

Informácie, zaznamenané v záznamoch bezpečnostného žurnálu sú popísané v príručke *Prehľad bezpečnosťou*. Všetky bezpečnostné záznamy v auditovacom žurnáli majú kód žurnálu T. Okrem bezpečnostných záznamov sa v žurnáli QAUDJRN objavia aj systémové záznamy. Toto sú záznamy s kódom žurnálu J, ktoré sa týkajú počiatočného zavedenia programu (IPL) a všeobecných operácií, vykonávaných na žurnálových prijímačoch (napríklad, uloženie prijímača).

Ak sa poškodí žurnál alebo jeho súčasný prijímač a auditovacie záznamy sa nedajú žurnálovať, potrebnú akciu určuje systémová hodnota QAUDENDACN. Obnova poškodeného žurnálu alebo žurnálového prijímača je rovnaká ako pre ostatné žurnály.

Manažment zmien žurnálových prijímačov môžete prenechať systému. Pri vytváraní žurnálu QAUDJRN alebo pri zmene žurnálu na túto hodnotu špecifikujte MNGRCV(*SYSTEM). Ak špecifikujete MNGRCV(*SYSTEM), systém automaticky odpojí prijímač pri dosiahnutí prahovej veľkosti a vytvorí a pripojí nový žurnálový prijímač. Nazýva sa to **Manažment žurnálu-systémových zmien**. Viac informácií nájdete v informačnom centre iSeries—>Riadenie systémov–> Manažment žurnálu–>Manažment lokálneho

žurnálu–>Riadenie žurnálov. V časti “Nevyhnutné predpoklady a súvisiace informácie” na strane xii nájdete viac informácií o prístupe na informačné centrum iSeries.

# Kapitola 6. Riadenie oprávnení

Na zachovanie stopy nastavovaní oprávnenia na vašom systéme máte k dispozícii množinu bezpečnostných správ. Keď tieto správy spúšťate prvýkrát, môžete vytlačiť všetko (napríklad, oprávnenie pre všetky súbory alebo všetky programy).

Keď ste si vytvorili svoju základňu informácií, môžete pravidelne spúšťať zmenené verzie správ. Zmenené verzie vám pomôžu identifikovať zmeny týkajúce sa bezpečnosti na vašom systéme, ktoré vyžadujú vašu pozornosť. Napríklad, každý týždeň môžete spustiť správu, ktoré zobrazuje verejné oprávnenie pre súbory. Môžete požadovať len zmenenú verziu správy. Ukáže vám nové súbory na systéme, ktoré sú dostupné pre každého a existujúce súbory, ktorých verejné oprávnenie sa od poslednej správy zmenilo.

Na spustenie bezpečnostných nástrojov máte dve ponuky:

- Na interaktívne spustenie programov použite ponuku SECTOOLS.
- Na spustenie súborov v dávke použite ponuku SECBATCH. Ponuka SECBATCH má dve časti: jedna je na okamžité predanie úloh do frontu úloh a druhá je na umiestňovanie úloh do plánovača úloh.

Ak používate iSeries Navigator, vykonajte tieto kroky, aby ste mohli spustiť nástroje bezpečnosti:

1. V iSeries Navigator, rozviňte váš Server—>**Bezpečnosť**.
2. Pravým tlačidlom kliknite na **Politiky** a vyberte **Preskúmať**, aby sa zobrazil zoznam politík, ktoré môžete vytvoriť a riadiť.

## Monitorovanie verejného oprávnenia na objekty

Pre jednoduchosť a výkon je väčšina systémov nastavená tak, že väčšina objektov je dostupná pre väčšinu užívateľov. Užívateľom sa radšej explicitne zakáže prístup na určité, dôverné informácie, ktoré treba chrániť, ako by sa mali explicitne oprávňovať na používanie každého objektu. Iný prístup používajú systémy s vysokými nárokmi na bezpečnosť, kde sa objekty oprávňujú na základe známych pravidiel. Na týchto systémoch sa väčšina objektov vytvára s verejným oprávnením nastaveným na *EXCLUDE.

iSeries je objektovo založený systém s mnohými typmi objektov. Väčšina typov objektov neobsahuje dôležité informácie alebo nevykonáva funkcie, ktoré je treba zabezpečovať. Ako správca bezpečnosti na systéme iSeries s typickými požiadavkami na bezpečnosť by ste mali zamerať svoju pozornosť na objekty, ktoré vyžadujú ochranu, ako sú databázové súbory a programy. Pre iné typy objektov môžete nastaviť verejné oprávnenie, ktoré je dostatočné pre vaše aplikácie, čo je pre väčšinu typov objektov oprávnenie *USE.

Informácie o objektoch, na ktoré môžu pristupovať verejní používatelia môžete použiť príkaz PRTPUBAUT (Print Public Authority). (**Verejný užívateľ** je každý s oprávnením na prihlásenie, kto nemá explicitne zakázaný prístup k objektu.) Keď použijete príkaz PRTPUBAUT, môžete špecifikovať typy objektov, knižníc alebo adresárov, ktoré chcete prehliadnuť. Voľby na vytlačenie správ Publicly Authorized Objects pre typy objektov, ktoré sú najčastejšie predmetom bezpečnosti, sú k dispozícii v ponukách SECBATCH a SECTOOLS. Objekty vyžadujúce vašu pozornosť nájdete tak, že budete pravidelne tlačiť zmenené verzie tejto správy.

## Riadenie oprávnenia pre nové objekty

OS/400 poskytuje funkcie, ktoré vám pomôžu riadiť oprávnenie a vlastníctvo pre nové objekty na vašom systéme. Keď užívateľ vytvorí nový objekt, systém zistí nasledovné:

- Kto bude vlastniť objekt
- Aké je verejné oprávnenie pre objekt
- Či má objekt nejaké súkromné oprávnenia
- Kam sa umiestni objekt (ktorý knižnica alebo adresár)
- Či sa bude auditovať prístup na objekt

Na vykonanie týchto rozhodnutí systém používa systémové hodnoty, parametre knižníc a parametre užívateľských profilov. “Pridelenie oprávnenia a vlastníctva novým objektom” v kapitole 5 knihy *iSeries Security Reference* poskytuje niekoľko príkladov dostupných volieb.

Na vytlačenie parametrov užívateľských profilov, ktoré ovplyvňujú vlastníctvo a oprávnenie pre nové objekty, použite príkaz PRTUSRPRF. Obrázok 5 na strane 56 ukazuje príklad tejto správy.

## Monitorovanie autorizačných zoznamov

Objekty s podobnými požiadavkami na bezpečnosť môžete zoskupovať pomocou zoznamov oprávnení. Koncepčne, zoznam oprávnení obsahuje zoznam užívateľov a oprávnenie, ktoré majú používatelia na objekty chránené zoznamom. Zoznamy oprávnení poskytujú účinný spôsob na riadenie oprávnenia pre podobné objekty na systéme. V niektorých prípadoch však môže byť obtiažne zachovať stopu oprávnení na objekty.

Na vytlačenie informácií o oprávneniach zoznamu oprávnení môžete použiť príkaz PRTPVTAUT (Print Private Authority). Obrázok 3 ukazuje príklad správy.

```
                        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
```

*Obrázok 3. Správa Private Authorities pre zoznamy oprávnení*

Táto správa zobrazuje rovnaké informácie ako vidíte na obrazovke EDTAUTL (Edit Authorization List). Výhoda správy je, že poskytuje informácie o všetkých zoznamoch oprávnení na jednom mieste. Ak napríklad nastavujete bezpečnosť pre novú skupinu objektov, môžete správu rýchlo prebehnúť a skontrolovať, či existujúci zoznam oprávnení spĺňa vaše potreby pre tieto objekty.

Môžete vytlačiť zmenenú verziu správy, aby ste si prezreli nové zoznamy oprávnení alebo zoznamy oprávnení so zmenami oprávnenia od posledného vytlačenia správy. Tiež máte možnosť vytlačiť zoznam objektov, ktoré sú chránené každým zoznamom oprávnení. Obrázok 4 na strane 53 ukazuje príklad správy pre jeden zoznam oprávnení:

```
                    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
```

*Obrázok 4. Zobraziť správu o objektoch autorizačného zoznamu*

Túto správu môžete napríklad použiť na to, aby ste si ozrejmili efekt pridania nového užívateľa do zoznamu oprávnení (aké oprávnenia získa užívateľ).

## Použitie autorizačných zoznamov

iSeries Navigator poskytuje bezpečnostné vlastnosti navrhnuté, aby vám pomáhali pri vývoji bezpečnostného plánu a politiky a pri konfigurovaní vášho systému, aby uspokojil potreby vášho podniku. Jednou z dostupných funkcií je použitie autorizačných zoznamov.

Autorizačné zoznamy majú nasledovné vlastnosti.

- Autorizačný zoznam zoskupuje objekty s podobnými bezpečnostnými požiadavkami.
- Autorizačný zoznam konceptuálne obsahuje zoznam užívateľov a skupín a oprávnení, ktoré majú na objekty, zabezpečené zoznamom.
- Každý užívateľ alebo skupina môže mať iné oprávnenie na množinu objektov, ktoré chráni zoznam.
- Oprávnenie sa prideľuje formou zoznamu, nie jednotlivým užívateľom a skupinám.

K úlohám, ktoré sa dajú vykonať pomocou autorizačných zoznamov patria nasledovné.

- Vytvorenie autorizačného zoznamu.
- Zmena autorizačného zoznamu.
- Pridanie užívateľov a skupín.
- Zmena povolení užívateľa.
- Zobrazenie chránených objektov.

Ak chcete použiť túto funkciu, vykonajte nasledujúce kroky:

1. V iSeries Navigator rozviňte váš server—>Bezpečnosť. Uvidíte **Autorizačné zoznamy** a **Politiky**.
2. Pravým tlačidlom kliknite na **Autorizačné zoznamy** a vyberte **Nový autorizačný zoznam**. **Nový autorizačný zoznam** vám umožní vykonávať nasledujúce.
   - **Použiť:** Umožňuje prístup na atribúty objektu a použitie objektu. Verejnosť môže zobraziť, ale nemôže meniť tieto objekty.
   - **Zmeniť:** Umožňuje zmeniť obsah objektu (s niektorými výnimkami).
   - **Všetko:** Umožňuje všetky operácie na objekte, okrem tých, ktoré sú obmedzené na vlastníka. Užívateľ alebo skupina môže riadiť existenciu objektu, špecifikovať bezpečnosť pre objekt, zmeniť objekt a vykonávať na objekte základné funkcie. Užívateľ alebo skupina tiež môže zmeniť vlastníctvo objektu.
   - **Vylúčiť:** Na objekte sú zakázané všetky operácie. Na objekt nemôžu pristupovať ani na ňom vykonávať žiadne operácie používatelia a skupiny, ktoré majú toto oprávnenie. Špecifikuje, že verejnosť nemôže používať daný objekt.

Pri práci s autorizačnými zoznamami budete chcieť poskytovať povolenia na objekty aj na údaje. Dostupné povolenia pre objekty sú uvedené dole.

- **Prevádzka:** Poskytuje povolenie na zobrazenie opisu objektu a použitie objektu podľa povolenia na údaje, ktoré má na objekt daný užívateľ alebo skupina.
- **Manažment:** Poskytuje povolenie na špecifikovanie bezpečnosti pre objekt, presun alebo premenovanie objektu a pridávanie členov do databázových súborov.
- **Existencia:** Poskytuje povolenie na riadenie existencie a vlastníctva objektu. Užívateľ alebo skupina môže vymazať objekt, uvoľniť pamäť objektu, vykonávať pre objekt operácie uloženia a obnovy a prenášať vlastníctvo objektu. Ak má užívateľ alebo skupina špeciálne povolenie na ukladanie, tento užívateľ alebo skupina nepotrebuje povolenie na existenciu objektu.
- **Zmena** (používa sa len pre databázové súbory a SQL balíky): Poskytuje povolenie, potrebné na zmenu atribútov objektu. Ak má užívateľ alebo skupina toto povolenie na databázový súbor, tento užívateľ alebo skupina môžu pridávať a odstraňovať spúšťače, pridávať a odstraňovať referenčné a jedinečné obmedzenia a meniť atribúty databázového súboru. Ak užívateľ alebo skupina má toto povolenie na SQL balík, tento užívateľ alebo skupina môže meniť atribúty SQL balíka. Toto povolenie sa v súčasnosti používa len pre databázové súbory a SQL balíky.
- **Referencia** (používa sa len pre databázové súbory a SQL balíky): Poskytuje povolenie, potrebné na odkaz na objekt z iného objektu, takže operácie na danom objekte sa môžu zakázať iným objektom. Ak má užívateľ alebo skupina toto povolenie na fyzický súbor, tento užívateľ alebo skupina môže pridávať referenčné obmedzenia, v ktorých je tento fyzický súbor rodičom. Toto povolenie sa v súčasnosti používa len pre databázové súbory.

Dostupné povolenia na údaje sú uvedené dole.
- **Čítať:** Poskytuje povolenie, potrebné na získanie a zobrazenie obsahu objektu, ako je prezeranie záznamov v súbore.
- **Pridať:** Poskytuje povolenie na pridávanie záznamov do objektu, ako je pridávanie správ do frontu správ alebo pridávanie záznamov do súboru.
- **Aktualizovať:** Poskytuje povolenie na zmenu záznamov v objekte, ako je zmena záznamov v súbore.
- **Vymazať:** Poskytuje povolenie na odstránenie záznamov z objektu, ako je odstránenie správ z frontu správ alebo vymazanie záznamov zo súboru.
- **Vykonať:** Poskytuje povolenie, potrebné na vykonanie programu, služobného programu alebo SQL balíka. Užívateľ tiež môže vyhľadať objekt v knižnici alebo v adresári.

Keď chcete získať viac informácií o každom procese počas vytvárania alebo úprav vo vašich autorizačných zoznamoch, použite online pomoc dostupnú v aplikácii iSeries Navigator.

## Politiky sprístupňovania v iSeries Navigator

Môžete použiť iSeries Navigator, na prezeranie a riadenie politík pre váš server iSeries. iSeries Navigator má päť oblastí politík:

- **Politika auditu**
  Tá vám umožňuje nastaviť monitorovanie pre špecifické akcie a prístup k špecifickým prostriedkom vo vašom systéme.
- **Politika bezpečnosti**
  Tá vám umožňuje zadať úroveň bezpečnosti a ďalšie voľby, ktoré súvisia so systémovou bezpečnosťou.
- **Politika hesiel**
  Tá vám umožňuje zadať úroveň hesiel pre systém.
- **Politika obnovy**
  Tá vám umožňuje zadať, ako sa majú určité objekty v systéme obnoviť.
- **Politika prihlasovania**
  Tá vám umožňuje zadať, ako sa užívateľ môže prihlásiť do systému.

Ak chcete politiky meniť alebo prezerať pomocou iSeries Navigator, vykonajte tieto kroky:

1. V iSeries Navigator rozviňte váš server—>**Bezpečnosť**.
2. Pravým tlačidlom kliknite na **Politiky** a vyberte **Preskúmať**, aby sa zobrazil zoznam politík, ktoré môžete vytvoriť a riadiť. Špecifické informácie o týchto politikách nájdete v pomoci aplikácie iSeries Navigator.

## Monitorovanie súkromného oprávnenia na objekty

**Voľby ponuky SECBATCH:**
**12** *na okamžité predloženie* **41** *na použitie plánovača úloh*

Príkaz PRTPVTAUT (Print Private Authority) môžete použiť na vytlačenie zoznamu všetkých súkromných oprávnení pre objekty špecifikovaného typu v určenej knižnici.

Tato správa vám pomôže nájsť nové oprávnenia na objekty. Tiež vám pomôže predísť tomu, aby vaša schéma súkromných oprávnení bola zamotaná a neriaditeľná.

## Monitorovanie prístupu na výstupné fronty a fronty úloh

Niekedy si správca bezpečnosti počína skvele pri chránení prístupu k súborom a pri vytlačení obsahu súboru zabudne na to, čo sa stalo. Servery iSeries vám poskytujú funkcie na ochranu citlivých výstupných frontov a frontov úloh. Môžete chrániť výstupný front, aby si neoprávnení používatelia napríklad nemohli prezerať alebo kopírovať dôverné súbory, ktoré čakajú na vytlačenie. Fronty úloh chránite a tak neoprávnení používatelia nemôžu presmerovať dôvernú úlohu do nedôverného výstupného frontu alebo ju úplne zrušiť.

**Voľby ponuky SECBATCH:**
**24 na okamžité predloženie 63** *na použitie plánovača úloh*

Téma *Základná systémová bezpečnosť a plánovanie* v Informačnom centre a príručky *iSeries Security Reference* popisujú, ako chrániť vaše výstupné fronty a fronty úloh.

Na vytlačenie nastavení bezpečnosti pre výstupné fronty a výstupné fronty na vašom systéme môžete použiť príkaz PRTQAUT (Print Queue Authority). Následne môžete vyhodnotiť tlačové úlohy, ktoré tlačia dôverné informácie a zabezpečiť, že idú do chránených výstupných frontov a frontov úloh.

Pre výstupné fronty a fronty úloh, ktoré považujete za potrebné chrániť, môžete porovnať vaše nastavenia bezpečnosti s informáciami v Prílohe D z knihy *iSeries Security Reference*. Tabuľka v Prílohe D hovorí, aké nastavenia sa vyžadujú na vykonávanie rôznych funkcií výstupných frontov a frontov úloh.

## Monitorovanie mimoriadnych oprávnení

Keď používatelia na vašom systéme majú nepotrebné špeciálne oprávnenia, vaša snaha o vytvorenie dobrej schémy oprávnení objektov môže byť zbytočná. Oprávnenie objektov nemá zmysel, keď užívateľský profil má špeciálne oprávnenie *ALLOBJ. Užívateľ so špeciálnym oprávnením *SPLCTL si môže prezerať všetky súbory pripravené na tlač bez ohľadu na to, aké úsilie použijete na chránenie vašich výstupných frontov. Užívateľ so špeciálnym oprávnením *JOBCTL môže ovplyvniť systémové operácie a presmerovať úlohy. Užívateľ so špeciálnym oprávnením *SERVICE môže použiť služobné nástroje na prístup k údajom bez toho, aby šiel cez operačný systém.

**Voľby ponuky SECBATCH:**
**29 na okamžité predloženie 68** *na použitie plánovača úloh*

Na vytlačenie informácií o špeciálnych oprávneniach a tried užívateľov pre užívateľské profily na vašom systéme môžete použiť príkaz PRTUSRPRF (Print User Profile). Keď spúšťate správu, máte niekoľko možností:
- Všetky užívateľské profily
- Užívateľské profily s určenými špeciálnymi oprávneniami
- Užívateľské profily, ktoré majú konkrétne triedy užívateľov
- Užívateľské profily s nezhodou medzi triedou užívateľov a špeciálnymi oprávneniami.

Obrázok 5 ukazuje príklad správy, ktorá zobrazuje špeciálne oprávnenia pre všetky užívateľské 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
```

*Obrázok 5. Správa s informáciami pre užívateľa: Príklad 1*

Okrem špeciálnych oprávnení správa zobrazuje aj nasledovné:
- Či má užívateľský profil obmedzené schopnosti.
- Či užívateľ alebo užívateľova skupiny vlastnia nové objekty, ktoré vytvorí užívateľ.
- Aké oprávnenie automaticky prijme užívateľova skupina na nové objekty, ktoré vytvorí užívateľ.

Obrázok 6 ukazuje príklad správy s nezhodou špeciálnych oprávnení a tried užívateľov:

```
User Profile Information
Report type  . . . . . . . . . . :   *AUTINFO
Select by  . . . . . . . . . . . :   *MISMATCH
-------------------------------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
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
```

*Obrázok 6. Správa s informáciami pre užívateľa: Príklad 2*

V Obrázok 6 si všimnite nasledovné:
- USERX má triedu užívateľa systémový operátor (*SYSOPR), ale má špeciálne oprávnenia *ALLOBJ a *SPLCTL.
- USERY má triedu užívateľov užívateľ (*USER), ale má špeciálne oprávnenie *SECADM.
- USERZ má tiež triedu užívateľ (*USER) a špeciálne oprávnenie *SECADM. Tiež môžete vidieť, že USERZ je členom skupiny QPGMR, ktorá má špeciálne oprávnenia *JOBCTL a *SAVSYS.

Tieto správy môžete spúšťať pravidelne, aby ste si uľahčili monitorovanie správy užívateľských profilov.

## Monitorovanie užívateľských prostredí

Jedna úloha užívateľského profilu je definovať prostredie pre užívateľa, vrátane výstupného frontu, úvodnej ponuky a opisu úlohy. Prostredie užívateľa ovplyvňuje spôsob ako užívateľ vidí systém a do určitej miery aj to, čo má užívateľ povolené vykonávať. Užívateľ musí mať oprávnenie na objekty, ktoré sú špecifikované v užívateľskom profile. Ak je však vaša schéma oprávnení stále vo vývoji alebo nie je veľmi obmedzujúca, prostredie užívateľa definované v užívateľskom profile môže produkovať výsledky, ktoré neboli zamýšľané. Nasleduje niekoľko príkladov:

**Voľby ponuky SECBATCH:**

**29** *na okamžité predloženie* **68** *na použitie plánovača úloh*

- Opis úlohy užívateľa môže špecifikovať užívateľský profil, ktorý má väčšie oprávnenie ako užívateľ.
- Užívateľ môže mať úvodnú ponuku, ale nemusí mať príkazový riadok. Obslužný program upozorňujúceho klávesu užívateľa však môže príkazový riadok poskytovať.
- Užívateľ smie byť oprávnený na spustenie dôverných správ. Užívateľov výstup však môže byť nasmerovaný do výstupného frontu, dostupného užívateľom, ktorí by nemali vidieť správy.

Môžete použiť voľbu *ENVINFO príkazu PRTUSRPRF (Print User Profile), ktorá vám pomôže monitorovať prostredia, ktoré sú definované pre užívateľov systému. Obrázok 7 ukazuje príklad správy:

```
                                    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
```

*Obrázok 7. Príklad tlače prostredia užívateľského profilu*

## Riadenie servisných nástrojov

Servisné nástroje sa používajú na konfigurovanie, riadenie a servis vášho servera. Servisné nástroje sa dajú sprístupniť z DST (dedicated service tools) alebo zo SST (system service tools). ID užívateľa servisných nástrojov sa vyžadujú pre prístup na DST, SST a pre použitie funkcií aplikácie iSeries Navigator pre riadenie LPAR (logical partition) a pre riadenie diskových jednotiek.

DST sú dostupné, keď bol spustený Licensed Internal Code, a to aj vtedy, ak nebol zavedený OS/400. SST sú dostupné z OS/400. Nasledujúca tabuľka naznačuje základné rozdiely medzi DST a SST.

| Charakteristika | DST | SST |
|---|---|---|
| **Ako získať prístup** | Fyzický prístup prostredníctvom konzoly počas manuálneho IPL alebo pomocou výberu voľby 21 na ovládacom paneli. | Prístup prostredníctvom interaktívnej úlohy so schopnosťou prihlásiť sa pomocou QSRV alebo pomocou nasledujúcich autorizácií:<br>• Autorizovaný na CL príkaz STRSST (Start SST).<br>• Servisné mimoriadne oprávnenie (*SERVICE) alebo mimoriadne oprávnenie na všetky objekty (*ALLOBJ).<br>• Funkčné privilégium používať SST. |
| **Kedy je dostupné** | Dostupné aj vtedy, keď má server obmedzené schopnosti. OS/400 sa nevyžaduje pre prístup na DST. | Dostupné po spusteníOS/400. OS/400 sa vyžaduje pre prístup na SST. |
| **Ako autentifikovať** | Vyžaduje ID užívateľa a heslo servisných nástrojov. | Vyžaduje ID užívateľa a heslo servisných nástrojov. |

V informačnom centre iSeries—>Bezpečnosť—>Servisné nástroje nájdete informácie o používaní servisných nástrojov na vykonávanie nasledujúcich úloh :

- Sprístupnenie servisných nástrojov pomocou DST
- Sprístupnenie servisných nástrojov pomocou SST
- Sprístupnenie servisných nástrojov pomocou aplikácie iSeries Navigator
- Vytvorenie ID užívateľa servisných nástrojov
- Zmena funkčného privilégia pre ID užívateľa servisných nástrojov
- Zmena opisu pre ID užívateľa servisných nástrojov
- Zobrazenie ID užívateľa servisných nástrojov
- Povolenie alebo zakázanie ID užívateľa servisných nástrojov
- Vymazanie ID užívateľa servisných nástrojov
- Zmena ID užívateľa a hesiel servisných nástrojov s použitím SST alebo DST
- Zmena hesla ID užívateľa vašich servisných nástrojov s použitím STRSST
- Zmena ID užívateľa a hesiel servisných nástrojov s použitím
- API QSYCHGDS (Change Service Tools User ID)
- Resetovanie QSECOFR hesla užívateľského profilu OS/400
- Resetovanie QSECOFR ID užívateľa a hesla servisných nástrojov
- Uloženie bezpečnostných údajov servisných nástrojov Obnovenie bezpečnostných údajov servisných nástrojov
- Vytvorenie vašich vlastných verzií QSECOFR ID užívateľa servisných nástrojov
- Konfigurovanie servera servisných nástrojov pre DST
- Konfigurovanie servera servisných nástrojov pre OS/400
- Monitorovanie použitia servisných funkcií prostredníctvom DST
- Monitorovanie použitia servisných nástrojov prostredníctvom protokolu auditu bezpečnostiOS/400

Pozrite si “Nevyhnutné predpoklady a súvisiace informácie” na strane xii, kde nájdete informácie o sprístupňovaní informačného centra iSeries.

# Kapitola 7. Použitie bezpečnosti logických oddielov (LPAR)

Existencia viacerých logických oddielov na jednom serveri iSeries sa môže ukázať užitočná v nasledujúcich scenároch.

- **Udržiavanie nezávislých systémov**: Vyhradenie časti prostriedkov (jednotka diskovej pamäte, procesory, pamäť a I/O zariadenia) pre oddiel dosiahne logickú izoláciu softvéru. Logické oddiely majú pri správnej konfigurácii určitú toleranciu pri hardvérových chybách. Interaktívne aj dávkové pracovné zaťaženia, ktoré nemusia na jednom počítači pracovať správne sa môžu izolovať a účinne spúšťať v samostatných oddieloch.
- **Konsolidácia** : Logicky rozdelený systém dokáže zredukovať počet serverových systémov iSeries, ktoré sú potrebné v rámci podniku. Môžete usporiadať niekoľko systémov do jedného logicky rozdeleného systému. Toto eliminuje potrebu a náklady na dodatočné vybavenie. Pri zmene potrieb môžete jednoducho presunúť prostriedky z jedného logického oddielu do iného.
- **Vytvorenie zmiešanej produkcie a testovacieho prostredia:** Môžete vytvoriť kombináciu produkčného a testovacieho prostredia. Produkčný oddiel môžete vytvoriť v primárnom oddiele. Ak chcete viac produkčných oddielov, pozrite si dole *Vytvorenie prostredia s viacerými produkčnými oddielmi*.

  Logický oddiel je buď testovací alebo produkčný oddiel. Produkčný oddiel spúšťa vaše hlavné obchodné aplikácie. Chyba v produkčnom oddiele by mohla podstatne spomaliť obchodné operácie a stáť vás čas a peniaze. Testovací oddiel testuje softvér. Chyba v testovacom oddiele, ktorá nie je nevyhnutne naplánovaná, nepreruší normálne obchodné operácie.
- **Vytvorenie prostredia s viacerými produkčnými oddielmi:** Viacero produkčných oddielov by ste mali vytvoriť iba vo vašich sekundárnych oddieloch. V takejto situácii vyhradíte primárny oddiel na manažment oddielov.
- **Horúca záloha:** Keď sa sekundárny oddiel replikuje do iného logického oddielu v rámci toho istého systému, prepnutie na zálohu počas zlyhania oddielu by zapríčinilo minimálne ťažkosti. Táto konfigurácia tiež minimalizuje efekt dlhých ukladacích okien. Záložný oddiel môžete zabezpečiť vypnutím, pričom iný logický oddiel pokračuje vykonávať produkčnú prácu. Na použitie tejto stratégie horúcej zálohy budete potrebovať špeciálny softvér.
- **Integrovaný klaster:** S použitím OptiConnect/400 a vysoko dostupného aplikačného softvéru sa môže váš rozdelený systém spustiť ako integrovaný klaster. Integrovaný klaster môžete použiť na ochranu vášho systému od najčastejších neplánovaných výpadkov v sekundárnom oddiele.

**Poznámka:** Pri nastavovaní sekundárneho oddielu je potrebné uvážiť dodatočné ohľady pre umiestňovanie kariet. Ak vami vybratý vstupno/výstupný procesor (IOP) pre konzolu má tiež LAN kartu a LAN karta nie je určená na použitie s Operačnou konzolou, aktivuje sa na použitie konzolou a možno ju nebudete môcť používať na vami zamýšľané účely. Viac informácií o práci s Operačnou konzolou nájdete v časti Kapitola 8, “iSeries Operačná konzola”, na strane 61.

Pozrite si ″Logické oddiely″ v Informačnom centre, kde nájdete podrobnejšie informácie k tejto téme.

## Riadenie bezpečnosti pre logické oddiely

S bezpečnosťou súvisiace úlohy, ktoré môžete vykonávať na rozdelenom systéme sú rovnaké ako na systéme bez logických oddielov. Keď vytvoríte logické oddiely, pracujete s viac ako jedným nezávislým systémom. Preto musíte vykonať tie isté úlohy na každom logickom oddiele, namiesto jedného vykonania na systéme bez logických oddielov.

Nasleduje niekoľko základných pravidiel, ktoré treba mať na pamäti pri práci s bezpečnosťou na logických oddieloch:

- Používateľ pridávate do systému naraz len do jedného logického oddielu. Ak na nich chcete pristupovať v inom oddiele, musíte ich pridať do každého takéhoto logického oddielu.
- Obmedzte počet ľudí, ktorí majú oprávnenie používať vyhradené servisné nástroje (DST) a systémové servisné nástroje (SST) na primárnom oddiele. Pozrite si tému ″Riadiť logické oddiely pomocou iSeries Navigator, DST a SST″ v iSeries Information Center, kde nájdete viac informácií o DST a SST. Pozrite si časť “Riadenie servisných nástrojov” na strane 57, kde nájdete informácie o používaní užívateľských profilov servisných nástrojov na riadenie prístupu na aktivity oddielov.

  **Poznámka:** Pred použitím iSeries Navigator na prístup k funkciám LPAR musíte inicializovať server STS (Service Tools Server) . V Informačnom centre iSeries—>Bezpečnosť—>Servisné nástroje nájdete súvisiace informácie. Pozrite si “Nevyhnutné predpoklady a súvisiace informácie” na strane xii, kde nájdete informácie o sprístupňovaní informačného centra iSeries.
- Sekundárne oddiely nemôžu vidieť ani používať hlavnú pamäť a diskové jednotky iného logického oddielu.
- Sekundárne oddiely môžu vidieť len svoje vlastné hardvérové prostriedky.
- Primárny oddiel môže vidieť všetky hardvérové systémové prostriedky na obrazovkách Work with System Partitions z DST a SST.
- Operačný systém na primárnom oddiele vidí len ako dostupné len jeho prostriedky.
- Primárny oddiel je riadený systémovým ovládacím panelom. Keď nastavíte režim panela na Bezpečný, na obrazovke Work with Partition Status z SST sa nemôže vykonať žiadna akcia. Ak chcete vnútiť DST zo systémového ovládacieho panelu, musíte zmeniť režim na Manuálny.
- Keď nastavíte prevádzkový režim sekundárneho oddielu na bezpečný, obmedzíte použitie jeho Work with Partition Status takto:
  - DST na sekundárnom oddiele môžete použiť len na zmenu stavu oddielu; na zmenu stavu oddielu nemôžete použiť SST.
  - DST na sekundárnom oddiele môžete vnútiť len z obrazovky Work with Partition Status primárneho oddielu pomocou DST alebo SST.
  - DST môžete na sekundárnom oddiele použiť len na zmenu režimu sekundárneho oddielu z bezpečného na ľubovoľnú inú hodnotu.

Keď režim sekundárneho oddielu nie je bezpečný, na zmenu stavu oddielu môžete použiť DST a SST na sekundárnom oddiele.

Viac informácií o bezpečnosti na vašom serveri iSeries si pozrite v knihe Security Reference a na stránkach iSeries Information Center s názvom Základná systémová bezpečnosť a plánovanie.

# Kapitola 8. iSeries Operačná konzola

Operačná konzola vám umožňuje použiť vaše PC, na prístup a riadenie vášho servera iSeries. Operačná konzola obsahuje podporu pre vzdialené volanie PC do serverov iSeries, bez zariadení konzoly, pričom umožňuje vzdialeným PC, aby sa stali konzolami. Keď použijete Operačná konzola, všimnite si nasledovné:

- Z Operačnej konzoly môžete vykonávať všetky úlohy, ktoré by ste mohli vykonávať z tradičnej konzoly. Napríklad, užívateľské profily so špeciálnym oprávnením *SERVICE alebo *ALLOBJ sa môžu prihlásiť do relácie Operačnej konzoly, aj keď boli zakázané.
- Operačná konzola používa užívateľské profily a heslá servisných nástrojov na povolenie pripojenia do servera iSeries. Preto je veľmi dôležité zmeniť vaše užívateľské profily servisných nástrojov a heslá. Hakeri sú pravdepodobne dobre oboznámení s ID užívateľov heslami Užívateľských profilov servisných nástrojov a mohli by ich použiť pri pokuse o reláciu vzdialenej konzoly vo vašom serveri iSeries. Pozrite si “Zmena známych hesiel” na strane 18 a “Vyhýbanie sa štandardným heslám” na strane 23, kde nájdete tipy k heslám.
- Ak chcete ochrániť vaše informácie pri používaní Vzdialenej konzoly, používajte voľbu spätného volania z Windows Dial-Up Networking.
- Pri nastavovaní sekundárneho oddielu je potrebné uvážiť dodatočné ohľady pre umiestňovanie kariet. Ak vami vybratý vstupno/výstupný procesor (IOP) pre konzolu má tiež LAN kartu a LAN karta nie je určená na použitie s Operačnou konzolou, aktivuje sa na použitie konzolou a možno ju nebudete môcť používať na vami zamýšľané účely.

Vo V5R1 bola Operačná konzola vylepšená o vykonávanie konzolových aktivít cez miestnu počítačovú sieť (LAN). Konzolové procedúry sú chránené sieťovou bezpečnosťou, realizovanou vylepšenou autentifikáciou a šifrovaním údajov. Ak chcete použiť Operačná konzola so sieťovým pripojením, odporúčame vám nainštalovať nasledovné produkty:

- Cryptographic Access Provider, 5722–AC2 alebo 5722–AC3 vo vašom serveriiSeries
- Client Encryption, 5722–CE2 alebo 5722–CE3 na vaše PC s Operačnou konzolou

Aby mohli byť údaje konzoly zašifrované server iSeries musí mať nainštalovaný jeden z produktov Cryptographic Access Provider **a** PC musí mať nainštalovaný jeden z produktov Client Encryption.

**Poznámka:** Ak nie sú nainštalované žiadne kryptografické produkty, nebude sa vykonávať žiadne šifrovanie údajov.

Tabuľka dole sumarizuje výsledky šifrovania dostupných produktov:

*Tabuľka 13. Výsledky šifrovania*

| **Cryptographic Access Provider vo vašom serveriiSeries** | **Client Encryption na vašom PC s Operačnou konzolou** | **Výsledné šifrovanie údajov** |
|---|---|---|
| Žiadne | Žiadne | Žiadne |
| 5722–AC2 | 5722–CE2 | 56 bitové |
| 5722–AC2 | 5722–CE3 | 56 bitové |
| 5722–AC3 | 5722–CE2 | 56 bitové |
| 5722–AC3 | 5722–CE3 | 128 bitové |

Ďalšie informácie o nastavení a správe iSeries Operačná konzola, nájdete v informačnom centre iSeries.

## Prehľad bezpečnosti Operačná konzola

Bezpečnosť Operačnej konzoly tvorí:

- autentifikácia konzolového zariadenia
- autentifikácia používateľa
- súkromnosť údajov
- integrita údajov

Operačná konzola s priamym pripojením má implicitne autentifikáciu zariadení, súkromnosť údajov a integritu údajov vďaka jej spojeniu point-to-point. Na prihlásenie do obrazovky terminálu sa vyžaduje bezpečnosť cez autentifikáciu používateľov.

### Autentifikácia zariadení konzoly

Autentifikácia konzolového zariadenia zaručuje, že fyzické zariadenie je konzola. Operačná konzola s priamym pripojením používa fyzické spojenie podobné twinaxiálnej konzole. Operačná konzola, používajúca priame pripojenie môže byť fyzicky zabezpečená podobne ako twinaxiálne spojenie, čo umožňuje riadiť prístup na fyzické konzolové zariadenie.

Operačná konzola so sieťovým pripojením používa verziu secure sockets layer (SSL), ktorá podporuje autentifikáciu používateľov a zariadení bez použitia certifikátov. Pre tento druh spojení je autentifikácia zariadení založená na profile zariadenia servisných nástrojov. Viac informácií nájdete v časti 63.

### Autentifikácia užívateľa

Autentifikácia užívateľov poskytuje istotu o tom, kto používa konzolové zariadenie. Všetky úvahy pre autentifikáciu užívateľov sú rovnaké bez ohľadu na typ konzoly.

### Súkromnosť údajov

Súkromnosť údajov poskytuje istotu, že údaje konzoly môže prečítať len určený príjemca. Operačná konzola s priamym pripojením používa pre LAN pripojenie a ochranu údajov konzoly fyzické spojenie, podobné twinaxiálnej konzole alebo bezpečnému sieťovému spojeniu. Operačná konzola, používajúca priame spojenie má rovnakú súkromnosť údajov ako twinaxiálne spojenie. Ak je fyzické spojenie bezpečné, údaje konzoly zostanú chránené.

Operačná konzola so sieťovým pripojením používa bezpečné sieťové spojenie, ak sú nainštalované príslušné kryptografické produkty (ACx a CEx). Relácia konzoly používa najsilnejšie možné šifrovanie v závislosti od nainštalovaných šifrovacích produktov na serveri iSeries a od PC, na ktorom je spustená operačná konzola.

**Poznámka:** Ak nie sú nainštalované žiadne kryptografické produkty, nebude sa vykonávať žiadne šifrovanie údajov.

### Integrita údajov

Integrita údajov poskytuje istotu, že údaje konzoly neboli na ceste k prijímateľovi zmenené. Operačná konzola s priamym pripojením používa pre LAN pripojenie a ochranu údajov konzoly fyzické spojenie, podobné twinaxiálnej konzole alebo bezpečnému sieťovému spojeniu. Operačná konzola, používajúca priame spojenie má rovnakú integritu údajov ako twinaxiálne spojenie. Ak je fyzické spojenie bezpečné, údaje konzoly zostanú chránené.

Operačná konzola so sieťovým pripojením používa bezpečné sieťové spojenie, ak sú nainštalované príslušné kryptografické produkty (ACx a CEx). Relácia konzoly používa najsilnejšie možné šifrovanie v závislosti od nainštalovaných šifrovacích produktov na serveri iSeries a od PC, na ktorom je spustená operačná konzola.

**Poznámka:** Ak nie sú nainštalované žiadne kryptografické produkty, nebude sa vykonávať žiadne šifrovanie údajov.

## Použitie Operačná konzola so sieťovým pripojením

**Poznámka:** Ľubovoľné zariadenie Operačnej konzoly môže byť konzolou, ale užívateľský profil servisných nástrojov používajú len konfigurácie, založené na LAN.

Server iSeries sa dodáva s QCONSOLE štandardným profilom zariadenia servisných nástrojov a štandardným heslom QCONSOLE. Operačná konzola so sieťovým pripojením zmení heslo počas každého úspešného spojenia. Pozrite si "Použitie Sprievodcu nastavovaním Operačná konzola", kde nájdete viac informácií.

Ďalšie informácie o iSeries Operačná konzola so sieťovým pripojením nájdete v téme Konfigurácia operačnej konzoly s pripojiteľnosťou LAN v informačnom centre.

## Ochrana Operačná konzola so sieťovým pripojením

Pri používaní Operačná konzola so sieťovým pripojením sa odporúča nasledovné:

- Vytvorte iný profil zariadenia servisných nástrojov s atribútmi konzoly a informácie profilu odložte na bezpečnom mieste.
- Nainštalujte Cryptographic Access Provider, 5722–AC2 alebo 5722–AC3 do vášho servera iSeries a Client Encryption, 5722–CE2 alebo 5722–CE3 do vášho PC Operačná konzola.
- Vyberte netriviálne heslo pre servisné zariadenie.
- Operačnú konzolu na PC chráňte rovnako, ako by ste chránili twinaxiálnu konzolu alebo Operačnú konzolu s priamym pripojením.

## Použitie Sprievodcu nastavovaním Operačná konzola

Sprievodca nastavením pridá na PC potrebné informácie pri používaní Operačná konzola so sieťovým pripojením. Sprievodca nastavením vás požiada o profil zariadenia servisných nástrojov, heslo profilu zariadenia servisných nástrojov a heslo na ochranu informácií profilu zariadenia servisných nástrojov.

**Poznámka:** Heslo informácií profilu zariadenia servisných nástrojov sa používa na zamknutie a odomknutie informácií profilu zariadenia servisných nástrojov (profil zariadenia servisných nástrojov a heslo) na PC.

Keď vytvoríte sieťové spojenie, sprievodca nastavením Operačnej konzoly vás požiada o zadanie hesla k informáciám servisného zariadenia, aby ste mohli pristúpiť na zašifrovaný profil zariadenia servisných nástrojov a heslo. Budete tiež požiadaný o platnú identifikáciu a heslo užívateľa servisných nástrojov.

# Kapitola 9. Zistenie podozrivých programov

Súčasné trendy v používaní počítačov zvýšili pravdepodobnosť, že váš systém má programy z nedôveryhodných zdrojov alebo programy, ktoré vykonávajú neznáme funkcie. Nasledujú príklady:

- Používateľ osobného počítača môže niekedy získať programy od iných používateľov PC. Ak je k vášmu systému iSeries pripojené PC, tento program môže ovplyvniť váš server iSeries.
- Programy tiež môžu získavať používatelia pripojení do sietí, napríklad z elektronických vývesiek.
- Hakeri sa stali viac aktívnymi a slávnejšími. Často zverejňujú svoje metódy a výsledky. Toto môže viesť k imitácii programátorov, ktorí bežne obchádzajú zákon.

Tieto trendy viedli k problému s bezpečnosťou počítačov, ktorý sa volá **počítačové vírusy**. Vírus je program, ktorý môže zmeniť ostatné programy, aby zahrnul kópiu seba samého. O týchto programoch sa potom hovorí ako o nainfikovaných vírusom. Okrem toho, vírus môže vykonávať iné operácie, ktoré môžu odstraňovať systémové prostriedky alebo ničiť údaje.

Architektúry servera iSeries poskytuje určitú ochranu pre infekčnými charakteristikami počítačového vírusu. Opisuje to "Ochrana proti počítačovým vírusom". Správca bezpečnosti servera iSeries sa musí viac starať o programy, ktoré vykonávajú neautorizované funkcie. Zvyšné témy v tejto kapitole opisujú spôsoby, ako môže niekto so zlými úmyslami nastaviť spustenie škodlivých programov na vašom systéme. Témy poskytujú tipy na vyhnutie sa vykonávaniu neoprávnených funkcií.

**Bezpečnostný tip**

Oprávnenie objektov je vždy vašou prvou líniou v obrane. Ak nemáte dobrý plán na chránenie svojich objektov, váš systém je bezbranný. Tieto informácie prejednávajú spôsoby, ktorými sa neautorizovaný užívateľ mohol pokúsiť o využitie zadných dvierok vo vašej schéme oprávnení k objektom.

## Ochrana proti počítačovým vírusom

Počítač s vírusovou infekciou má program, ktorý môže meniť iné programy. Objektová architektúra iSeries sťažuje záškodníkom vytvárať a šíriť tento typ vírusu, ktorý je v iných architektúrach počítačov. Na serveri iSeries používate špecifické príkazy a inštrukcie pre prácu na každom type objektu. Nemôžete použiť inštrukcie pre súbory na zmenenie objektu programu schopného prevádzky (čo väčšinou robia tvorcovia vírusov). Tiež nemôžete ľahko vytvoriť program, ktorý mení iný programový objekt. Toto vyžaduje značný čas, úsilie, skúsenosti a zároveň vyžaduje prístup na nástroje a dokumentáciu, ktoré nie sú bežne k dispozícii.

Avšak sprístupnením nových funkcií servera iSeries pre účasť v prostredí otvorených systémov sa niektoré z funkcií serverov iSeries pre ochranu na báze objektov už ďalej nepoužívajú. Napríklad, pomocou Integrovaného súborového systému (IFS) môžu používatelia priamo manipulovať s niektorými objektmi v adresároch, ako sú súbory toku.

Hoci architektúra servera iSeries sťažuje rozšírenie vírusu medzi programami servera iSeries, architektúra servera nezabraňuje tomu, aby bol server iSeries prenášačom vírusov. Podobne ako súborový server môže server iSeries ukladať programy, ktoré zdieľa množstvo užívateľov

PC. Ktorýkoľvek z týchto programov môže obsahovať vírus, ktorý server iSeries nezistí. Aby ste zabránili infekcii PC pripojených do vášho servera iSeries týmto typom vírusu, musíte použiť softvér na zistenie vírusov na PC.

Na serveri iSeries sa nachádza niekoľko funkcií, ktoré zabránia cudzím, aby s použitím strojovo orientovaného jazyka so schopnosťami smerníka, zmenil program funkčného objektu:

- Ak je váš systém spustený na bezpečnostnej úrovni 40 alebo vyššej, vstavaná ochrana obsahuje ochranu pred zmenou programových objektov. Napríklad, nemôžete úspešne spustiť program, ktorá obsahuje blokované (chránené) strojové inštrukcie.
- Validačná hodnota programu je tiež určená na ochranu pri obnovovaní programu, ktorý bol uložený (a možno aj zmenený) na iných systémoch. Kapitola 2 v knihe *iSeries Security Reference* popisuje vstavané funkcie na ochranu pre bezpečnostnú úroveň 40 a vyššej, vrátane validačných hodnôt programu.

  **Poznámka:** Validačná hodnota programu nie je jednoduchá a nie je nahradením za opatrnosť v programoch na vyhodnocovanie, ktoré sa obnovujú na vašom systéme.

Na pomoc pri zisťovaní zavádzania zmenených programov do vášho systému máte k dispozícii niekoľko nástrojov:

- Príkaz CHKOBJITG (Check Object Integrity) môžete použiť na prezretie objektov (operačných objektov) splňujúcich vaše hodnoty pre hľadanie aby ste sa presvedčili, že tieto objekty neboli zmenené. Toto je podobné funkcii na hľadanie vírusov.
- Na monitorovanie zmenených alebo obnovených programov môžete použiť funkcie na auditovanie bezpečnosti. Hodnoty *PGMFAIL, *SAVRST a *SECURITY pre systémovú hodnotu bezpečnostnej úrovne poskytujú auditovanie záznamov, ktoré vám môžu pomôcť zistiť pokusy na zavedenie programu vírusu do vášho systému. Kapitola 9 a Príloha F v knihe *iSeries Security Reference* poskytuje viac informácií o auditových hodnotách a položkách auditového žurnálu.
- Môžete použiť parameter FRCCRT (force create) príkazu CHGPGM (Change Program), aby ste opätovne vytvorili každý program, ktorý bol obnovený na vašom systéme. Systém používa vzor programu na opakované vytvorenie programu. Ak bol programový objekt zmenený po jeho kompilácii, systém opätovne vytvorí tento zmenený objekt na nahradí ho. Ak vzor programu obsahuje blokované (chránené) inštrukcie, systém opakovane nevytvorí program úspešne.
- Systémovú hodnotu QFRCCVNRST (vynútiť konverziu v obnove) môžete použiť na opakované vytvorenie ľubovoľného programu do vášho systému, počas jeho obnovy. Systém na opakované vytvorenie programu používa vzor programu. Táto systémová hodnota poskytuje niekoľko volieb, pri ktorých sa program opakovane vytvorí.
- Systémovú hodnotu QVFYOBJRST (verify objects on restore) môžete použiť na obnovu programov, ktoré nemajú digitálny podpis, alebo nemajú platný digitálny podpis. Keď je digitálny podpis neplatný, znamená to, že program bol zmenený od jeho podpísania jeho výrobcom. Existujú API, ktoré vám umožňujú podpisovať vaše vlastné programy, úložné súbory a súbory toku.

Viac informácií o podpisovaní a spôsobe jeho použitia na ochranu vášho systému pred útokmi nájdete v časti “Podpisovanie objektov” na strane 76.

## Použitie monitora adoptovaného oprávnenia

Na serveri iSeries môžete vytvoriť program, ktorý si adoptuje oprávnenie vlastníka programu. Znamená to, že hocijaký užívateľ spúšťajúci program, má rovnaké oprávnenia (súkromné a špeciálne oprávnenia) ako užívateľský profil, ktorý vlastní program.

Adoptované oprávnenie je cenný bezpečnostný nástroj, keď sa používa správne. Napríklad “Rozšírenie riadenia prístupu do ponúk pomocou bezpečnosti objektov” na strane 42 opisuje spôsoby kombinácie adoptovaného oprávnenia a ponúk, ktoré vám pomôžu rozšíriť riadenie prístupu do ponúk. Adoptované oprávnenie môžete použiť na chránenie svojich dôležitých súborov pred zmenou mimo vašich schválených aplikačných programov a súčasne mať povolené dotazy na súbory.

Ako správca bezpečnosti by ste sa mali presvedčiť, či je adoptované oprávnenie použité správne:

- Programy by mali adoptovať oprávnenie užívateľského profilu, ktorý má na vykonanie potrebných funkcií práve dostatočné oprávnenie, nie nadbytočné oprávnenie. Mali by ste dávať obzvlášť pozor pri programoch, ktoré adoptujú oprávnenie užívateľského profilu, ktorá má špeciálne oprávnenie *ALLOBJ alebo vlastní dôležité objekty.
- Programy adoptujúce oprávnenie by mali mať konkrétnu, obmedzenú funkciu a nemali by poskytovať možnosť zadávania príkazov.
- Programy adoptujúce oprávnenie by mali byť správne zabezpečené.
- Nadmerné používanie adoptovaného oprávnenia môže mať negatívny dopad na výkon vášho systému. Aby ste sa vyhli problémom výkonu, pomôže vám pozrieť si diagramy kontroly oprávnenia a návrhy pre používanie adoptovaného oprávnenia v Kapitole 5 knihy *iSeries Security Reference*.

**Voľby ponuky SECBATCH:**
**1** *na okamžité predloženie* **40 na použitie plánovača úloh**

Na pomoc pri monitorovaní použitia adoptovaného oprávnenia na vašom systéme môžete použiť príkaz PRTADPOBJ (Print Adopting Objects) (voľba 21 na ponuke SECTOOLS).

Správa zobrazí mimoriadne oprávnenia zadaného užívateľského profilu, programov, ktoré si adoptujú oprávnenie užívateľského profilu ako aj zariadení ASP, ktoré používajú oprávnenia profilu. Keď vytvoríte základňu informácií, môžete pravidelne tlačiť zmenené verzie správ adoptovaných objektov. Zobrazuje nové programy adoptujúce oprávnenie a programy, ktorým sa zmenilo adoptovanie oprávnenia od posledného spustenia správy.

Ak máte podozrenie, že adoptované oprávnenie sa na vašom systéme zneužíva, môžete nastaviť systémovú hodnotu QAUDLVL tak, aby obsahovala *PGMADP. Keď je táto hodnota aktívna, systém vytvorí položku auditového žurnálu vždy keď niekto spustí alebo ukončí program adoptujúci oprávnenie. Položka obsahuje názov užívateľa, ktorý spustil program a názov programu.

## Obmedzenie použitia adoptovaného oprávnenia

Keď je iSeries program spustený, môže používať prevzaté oprávnenie, aby získal prístup k objektom dvoma rôznymi spôsobmi:

- Program samotný môže prevziať oprávnenie od vlastníka. Je to určené v parametri užívateľského profilu (USRPRF) v programe alebo servisnom programe.
- Tento program môže používať (zdediť) oprávnenie od predchádzajúceho programu, ktorý je stále v skupine volaní úloh. Program môže zdediť prevzaté oprávnenie od predchádzajúcich programov, dokonca i keď tento program samotný neprevezme oprávnenie. Parameter use adopted authority (USEADPAUT) programu alebo servisného programu určuje, či program zdedí prevzaté oprávnenie od predchádzajúcich programov v skupine programov.

Nasleduje príklad, ako funguje používanie prevzatého oprávnenia od predchádzajúcich programov.

Predpokladajme, že užívateľský profil ICOWNER má oprávnenie *CHANGE na súbor ITEM, a že verejné oprávnenie na súbor ITEM je *USE. Žiadne iné užívateľské profily nemajú žiadne výlučne definované oprávnenie na súbor ITEM. Tabuľka 14 zobrazuje atribúty pre tri programy, ktoré používajú súbor ITEM:

*Tabuľka 14. Vzorka Use Adopted Authority (USEADPAUT)*

| Názov programu | Vlastník programu | Hodnota USRPRF | Hodnota USEADPAUT |
|---|---|---|---|
| PGMA | ICOWNER | *OWNER | *YES |
| PGMB | ICOWNER | *USER | *YES |
| PGMC | ICOWNER | *USER | *NO |

**Vzorka 1–Adoptovanie oprávnenia:**
1. USERA spustí program PGMA.
2. Program PGMA sa pokúša otvoriť súbor ITEM so schopnosťou aktualizovania.

**Výsledok:** Pokus je úspešný. USERA má prístup *CHANGE k súboru ITEM, pretože PGMA prevezme oprávnenie ICOWNER.

**Vzorka 2–Použitie prevzatého oprávnenia:**
1. USERA spustí program PGMA.
2. Program PGMA zavolá program PGMB.
3. Program PGMB sa pokúša otvoriť súbor ITEM so schopnosťou aktualizovania.

**Výsledok:** Pokus je úspešný. Hoci program PGMB neprevezme oprávnenie (*USRPRF je *USER), umožní použiť predchádzajúce prevzaté oprávnenie (*USEADPAUT je *YES). Program PGMA je stále v skupine programov. Preto, USERA získa prístup *CHANGE k súboru ITEM, pretože PGMA prevezme oprávnenie ICOWNER.

**Vzorka 3–Nepoužitie prevzatého oprávnenia:**
1. USERA spustí program PGMA.
2. Program PGMA zavolá program PGMC.
3. Program PGMC sa pokúša otvoriť súbor ITEM so schopnosťou aktualizovania.

**Výsledok:** Oprávnenie zlyhá. Program PGMC neprevezme oprávnenie. Program PGMC neumožní ani použitie prevzatého oprávnenia z predchádzajúcich programov. Hoci PGMA je stále v skupine volaní, jeho prevzaté oprávnenie nie je použité.

## Zamedzenie novým programom, aby používali adoptované oprávnenie

Prenechanie prevzatého oprávnenia novším programom v skupine poskytuje príležitosť pre znalého programátora vytvoriť program Trójsky kôň. Program Trójsky kôň môže spoliehať na to, že mu predchádzajúce programy v skupine poskytnú oprávnenie, ktoré potrebuje na vykonanie nezbednosti. Aby sa tomu zabránilo, môžete obmedziť počet používateľov s možnosťou vytvárať programy, ktoré používajú prevzaté oprávnenie predchádzajúcich programov.

Keď vytvárate nový program, systém automaticky nastaví parameter USEADPAUT na *YES. Ak nechcete, aby tento program zdedil prevzaté oprávnenie, musíte použiť príkaz Change Program (CHGPGM), alebo Change Service Program (CHGSRVPGM) pre nastavenie parametra USEADPAUT na *NO.

Autorizačný zoznam a systémovú hodnotu Použiť adoptované oprávnenie (QUSEADPAUT) môžete použiť na riadenie, kto môže vytvoriť programy, ktoré dedia adoptované oprávnenie. Keď zadáte názov zoznamu oprávnení v systémovej hodnote QUSEADPAUT, systém použije tento zoznam oprávnení na stanovenie, ako vytvoriť nové programy.

Keď používateľ vytvorí program alebo servisný program, systém overí oprávnenie používateľa na zoznam oprávnení. Ak má používateľ oprávnenie *USE, parameter USEADPAUT pre nový program je nastavený na *YES. Ak používateľ nemá oprávnenie *USE, parameter USEADPAUT je nastavený na *NO. Oprávnenie používateľa na zoznam oprávnení nemôže pochádzať z prevzatého oprávnenia.

Zoznam oprávnení, ktorý ste uviedli v systémovej hodnote QUSEADPAUT reguluje tiež, či používateľ môže použiť príkaz CHGxxx pre nastavenie hodnoty USEADPAUT pre program, alebo servisný program.

**Poznámky:**

1. Nemusíte volať váš autorizačný zoznam QUESADPAUT. Môžete vytvoriť zoznam oprávnení s iným názvom. Potom špecifikujte zoznam oprávnení v systémovej hodnote QUSEADPAUT. V príkazoch tohto príkladu použite názov vášho zoznamu oprávnení.
2. Systémová hodnota QUSEADPAUT neovplyvňuje existujúce programy na vašom systéme. Na nastavenie parametra USEADPAUT pre existujúce programy použite príkaz CGHPGM alebo CHGSRVPGM.

***Viac obmedzujúce prostredie:*** Ak chcete, aby väčšina používateľov vytvárala nové programy s parametrom USEADPAUT nastaveným na *NO, urobte nasledovné:

1. Pre nastavenie verejného oprávnenia pre zoznam oprávnení na *EXCLUDE, napíšte nasledovné:

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

2. Pre nastavenie možnosti daným používateľom vytvárať programy, ktoré používajú prevzaté oprávnenia predchádzajúcich programov, napíšte nasledovné:

   ```
   ADDAUTLE AUTL(QUSEADPAUT) USER(názov používateľa)
      AUT(*USE)
   ```

***Menej obmedzujúce prostredie:*** Ak chcete, aby väčšina používateľov vytvárala nové programy s parametrom USEADPAUT nastaveným na *YES, urobte nasledovné:

1. Nastavte verejné oprávnenie pre zoznam oprávnení na *USE.
2. Aby sa zabránilo daným používateľom vytvárať programy, ktoré používajú prevzaté oprávnenie predchádzajúcich programov, napíšte nasledovné:

   ```
   ADDAUTLE AUTL(QUSEADPAUT)
      USER(názov používateľa) AUT(*EXCLUDE)
   ```

## Použitie monitora spúšťacích programov

DB2 UDB poskytuje schopnosť spájať spúšťacie programy s databázovými súbormi. Schopnosť spúšťacích programov je bežná pri práci s vysoko funkčnými správcami databáz.

Keď spájate spúšťací program s databázovým súborom, špecifikujete kedy sa má spúšťací program spúšťať. Napríklad, súbor objednávok zákazníka môžete nastaviť tak, aby spustil spúšťací program pri pridaní nového záznamu do tohto súboru. Keď nevybavený zostatok zákazníka prekročí limit pohľadávky, spúšťací program môže vytlačiť zákazníkovi list s upozornením a odoslať oznámenie správcovi pohľadávok.

Spúšťacie programy sú výkonné spôsoby na poskytovanie funkcií aplikácií a riadenie informácií. Spúšťacie programy tiež poskytujú možnosť niekomu s pochybnými úmyslami

vytvoriť na vašom systéme “Trójskeho koňa”. Deštruktívny program môže ticho sedieť a čakať na spustenie, kým sa v databázovom súbore na vašom systéme nevyskytne určitá udalosť.

**Poznámka:** V dejinách je Trójsky kôň známy ako veľký dutý drevený kôň, v ktorom boli grécky vojaci. Keď koňa umiestnili za hradby Tróje, vojaci z neho vyliezli a pobili Trójanov. Vo svete počítačov sa program skrývajúci deštruktívne funkcie často nazýva Trójsky kôň.

**Voľby ponuky SECBATCH:**
**27** *na okamžité predloženie* **66** *na použitie plánovača úloh*

Pri dodaní vášho systému je schopnosť pridania spúšťacieho programu do databázového súboru obmedzená. Ak dôsledne riadite oprávnenie objektov, typický užívateľ nebude mať dostatočné oprávnenie na pridanie spúšťacieho programu do databázového súboru. Príloha D v knihe *iSeries Security Reference* hovorí o oprávnení, ktoré sa vyžaduje pre všetky príkazy, vrátane príkazu ADDPFTRG (Add Physical File Trigger).

Príkaz PRTTRGPGM (Print Trigger Programs) môžete použiť na vytlačenie zoznamu všetkých spúšťacích programov v konkrétnej knižnici alebo vo všetkých knižniciach.

Úvodnú správu môžete použiť ako základ pre vyhodnotenie všetkých spúšťacích programov, ktoré už existujú na vašom systéme. Potom môžete pravidelne tlačiť zmenené správy, aby ste videli, či sa do vášho systému pridali nové spúšťacie programy.

Pri vyhodnocovaní spúšťacích programov uvažujte o nasledovnom:

- Kto vytvoril spúšťací program? Toto zistíte pomocou príkazu DSPOBJD (Display Object Description).
- Čo robí program? Toto zistíte tak, že si pozriete zdrojový program alebo sa porozprávate s tvorcom programu. Napríklad, zisťuje spúšťací program, kto je užívateľ? Spúšťací program možno čaká na konkrétneho užívateľa (QSECOFR), aby získal prístup na systémové prostriedky.

Keď vytvoríte základňu informácií, pravidelne môžete tlačiť zmenené správy, aby ste mohli monitorovať nové spúšťacie programy, ktoré boli pridané do vášho systému.

## Kontrola skrytých programov

Spúšťacie programy nie sú jediný spôsob ako zaviesť trójskeho koňa do vášho systému. Spúšťacie programy sú príkladom **ukončovacieho programu**. Keď sa vyskytne určitá udalosť, ako je v prípade spúšťacieho programu aktualizácia súboru, systém spustí ukončovací program spojený s touto udalosťou.

Tabuľka 15 na strane 71 opisuje iné príklady, ktoré môžu byť na vašom systéme. Na vyhodnotenie použitia a obsahu týchto ukončovacích programov by ste mali použiť rovnaké metódy, ktoré používate pre spúšťacie programy.

**Poznámka:** Tabuľka 15 na strane 71 nie je úplný zoznam možných ukončovacích programov.

.

*Tabuľka 15. Ukončovacie programy poskytnuté systémom*

| Názov programu | Kedy sa program spúšťa |
|---|---|
| Používateľom špecifikovaný názov v sieťovom atribúte DDMACC. | Keď sa používateľ pokúša otvoriť DDM súbor na vašom systéme alebo vytvára DRDA spojenie. |
| Používateľom špecifikovaný názov v sieťovom atribúte PCSACC. | Keď sa používateľ pokúša použiť funkcie Client Access pomocou Original Clients na prístup na objekty na vašom systéme. |
| Používateľom špecifikovaný názov v systémovej hodnote QPWDVLDPGM | Keď používateľ spustí funkciu Change Password. |
| Používateľom špecifikovaný názov v systémovej hodnote QRMTSIGN. | Keď sa používateľ pokúša prihlásiť interaktívne zo vzdialeného systému. |
| QSYS/QEZUSRCLNP | Keď sa spustí funkcia automatického vyčistenia. |
| Používateľom špecifikovaný názov v parametri EXITPGM príkazu CHGBCKUP. | Keď používate funkciu z Operation Assistant na zálohovanie. |
| Používateľom špecifikované názvy v príkaze CRTPRDLOD. | Predtým a potom ako uložíte, obnovíte alebo vymažete produkt, ktorý bol vytvorený príkazom. |
| Používateľom špecifikovaný názov v parametri DFTPGM príkazu CHGMSGD. | Ak je pre správu špecifikovaný štandardný program, systém spustí program pri vydaní správy. Pretože na typickom systéme je veľké množstvo opisov správ, monitorovať použitie štandardných programov je zložité. Ak chcete zabrániť verejným používateľom pridávať štandardné programy pre správy, pouvažujte o nastavení verejného oprávnenia pre súbory správ (objekty *MSGF) na *USE. |
| Používateľom špecifikovaný názov v parametri FKEYPGM príkazu STREML3270. | Keď používateľ stlačí funkčný kláves počas relácie emulácie zariadenia 3270. Po dokončení ukončovacieho programu vráti systém riadenie relácie emulácie zariadenia 3270. |
| Používateľom špecifikovaný názov v parametri EXITPGM príkazov monitora výkonu. | Na spracovanie údajov zhromaždených nasledovnými príkazmi: STRPFRMON, ENDPFRMON, ADDPFRCOL a CHGPFRCOL. Program sa spustí po dokončení zhromaždenia údajov. |
| Používateľom špecifikovaný názov v parametri EXITPGM príkazu RCVJRNE. | Pre každý záznam žurnálu alebo skupinu záznamov žurnálu, ktoré prečíta zo špecifikovaného žurnálu a žurnálových prijímačov. |
| Používateľom špecifikovaný názov v QTNADDCR API. | Počas operácie COMMIT alebo ROLLBACK. |
| Používateľom špecifikované názvy v QHFRGFS API. | Na vykonanie funkcií súborového systému. |
| Používateľom špecifikovaný názov v parametri SEPPGM opisu zariadenia tlačiarne. | Na určenie, čo sa bude tlačiť na oddeľovacích stranách pred alebo po súbore pripravenom na tlač alebo tlačovej úlohe. |
| QGPL/QUSCLSXT | Keď sa zatvorí databázový súbor, aby sa povolilo získanie informácií o použití súboru. |
| Používateľom špecifikovaný názov v parametri FMTSLR logického súboru. | Keď sa záznam zapíše do databázového súboru a názov formátu záznamu nie je obsiahnutý v programe napísaného v jazyku vyššej úrovne. Program na vyberanie prijme záznam ako vstup, určí použitý formát záznamu a vráti ho do databázy. |
| Používateľom špecifikovaný názov, ktorý je určený v systémovej hodnote, parametri ATNPGM v profile používateľa alebo v parametri PGM príkazu SETATNPGM. | Keď používateľ stlačí kláves Attention. |
| Používateľom špecifikovaný názov v parametri EXITPGM príkazu TRCJOB. | Pred spustením procedúry Trace Job. |

Pre príkazy, ktoré vám povoľujú špecifikovať ukončovací program by ste mali zaistiť, aby sa nemohlo zmeniť štandardné nastavenie príkazu tak, aby špecifikovalo ukončovací program. Mali by ste tiež zaistiť, aby verejné oprávnenie pre tieto príkazy nebolo postačujúce na zmenenie štandardného nastavenia príkazu. Príkaz CHGCMDDFT vyžaduje na príkaz oprávnenie *OBJMGT. Na spustenie príkazu nepotrebujete oprávnenie *OBJMGT.

## Vyhodnotenie zaregistrovaných výstupných programov

Registračnú funkciu systému môžete použiť na registráciu ukončovacích programov, ktoré by sa mali spustiť, keď sa vyskytnú určité udalosti. Na zobrazenie informácií o registrácii na vašom systéme, napíšte WRKREGINF OUTPUT(*PRINT). Obrázok 8 ukazuje príklad správy:

```
              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  . . . . . . . . . . . . . . :
```

*Obrázok 8. Work with Registration Information-Príklad*

Pre každý ukončovací bod na systéme správa ukazuje, či sú momentálne zaregistrované nejaké ukončovacie programy. Keď má ukončovací bod programy, ktoré sú súčasne zaregistrované, môžete vybrať voľbu 8 (Display programs) zo zobrazenej verzie WRKREGINF, aby sa zobrazili informácie o programoch:

```
                     Work with Registration Information

Vyberte príslušnú voľbu a stlačte 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
```

Na vyhodnotenie týchto ukončovacích programov použite rovnakú metódu ako pre iné ukončovacie a spúšťacie programy.

## Kontrola naplánovaných programov

iSeries poskytuje niekoľko metód plánovania úloh na spúšťanie v neskoršom čase, vrátane plánovača úloh. Bežne tieto metódy nepredstavujú ohrozenie bezpečnosti, pretože používateľ plánujúci úlohu musí mať rovnaké oprávnenie ako sa vyžaduje na vydanie úlohy do dávky.

Aj tak by ste však mali periodicky kontrolovať naplánované úlohy do budúcnosti. Nespokojný používateľ, ktorý už nie je v organizácii by mohol túto metódu použiť na naplánovanie katastrofy.

## Obmedzenie schopnosti Uložiť a Obnoviť

Väčšina používateľov nepotrebuje ukladať a obnovovať objekty na vašom systéme. Príkazy na uloženie poskytujú možnosť skopírovať dôležité informácie organizácie na médium alebo do iného systému. Väčšina príkazov na ukladanie podporuje uloženie súborov, ktoré môžu byť odoslané do iného systému (pomocou príkazu SNDNETF) bez toho, aby sa pristupovalo na médium alebo na úložné/obnovovacie zariadenie.

Príkazy na obnovenie poskytujú príležitosť na obnovenie neoprávnených objektov na váš systém, ako sú programy, príkazy a súbory. Pomocou úložných súborov tiež môžete obnoviť informácie bez prístupu na médium alebo úložné/obnovovacie zariadenie. Úložné súbory sa môžu poslať z iného systému pomocou príkazu SNDNETF alebo funkciou FTP.

Nasledujú návrhy na obmedzenie operácií na ukladanie a obnovu na vašom systéme:

- Skontrolujte, ktorí používatelia majú špeciálne oprávnenie *SAVSYS. Špeciálne oprávnenie *SAVSYS povoľuje používateľovi ukladať a obnovovať objekty, ak keď používateľ na tieto objekty nemá potrebné oprávnenie.
- Riaďte fyzický prístup na ukladacie a obnovovacie zariadenia.
- Obmedzte prístup na príkazy ukladania a obnovy. Keď nainštalujete licenčné programy OS/400, verejné oprávnenie pre príkazy RSTxxx je *EXCLUDE. Verejné oprávnenie pre príkazy SAVxxx je *USE. Zvážte zmenu verejného oprávnenia pre príkazy SAVxxx na *EXCLUDE. Opatrne obmedzte užívateľov, ktorých oprávnite na príkazy RSTxxx.
- Systémovú hodnotu QALWOBJRST použite na obmedzenie obnovenia systémových stavových programov, ktoré adoptujú oprávnenie a objektov, ktoré majú validačné chyby.
- Na riadenie obnovy podpísaných objektov na vašom systéme použite systémovú hodnotu QVFYOBJRST.
- Systémovú hodnotu QFRCCVNRST použite na riadenie opakovaného vytvárania určitých objektov, ktoré sa obnovujú vo vašom systéme.
- Na monitorovanie operácií obnovy použite auditovanie bezpečnosti. Do systémovej hodnoty QAUDLVL zahrňte *SAVRST a periodicky tlačte záznamy auditovania, ktoré boli vytvorené operáciami obnovy. (Kapitola 9 a Príloha F knihy *iSeries Security Reference* poskytuje viac informácií o operáciách s položkami auditu.)

## Skontrolovanie užívateľských objektov v chránených knižniciach

Každá úloha servera iSeries má zoznam knižníc. Zoznam knižníc určuje poradie, v ktorom bude systém hľadať objekt, ak názov knižnice nie je špecifikovaný s názvom objektu. Napríklad, keď voláte program bez určenia jeho umiestnenia, systém postupne prehľadá váš zoznam knižníc a spustí prvú nájdenú kópiu programu.

Kniha *iSeries Security Reference* poskytuje viac informácií o ohrození bezpečnosti zoznamov knižníc a volaní programov bez názvu knižnice (nazývané **nekvalifikované volanie**). Tiež poskytuje návrhy pre riadenie obsahu knižníc zoznamov knižníc a možnosti menenia zoznamov systémových knižníc.

Aby váš systém fungoval správne, niektoré systémové knižnice, ako sú QSYS a QGPL, musia byť v zozname knižníc pre každú úlohu. Na riadenie toho, kto môže pridávať programy do týchto knižníc, by ste mali používať oprávnenia objektov. Toto pomôže zabrániť tomu, aby niekto umiestnil do jednej z knižníc nesprávny program s rovnakým názvom, s akým sa nachádza tento program ďalej v knižnici.

Tiež by ste mali vyhodnotiť, kto má oprávnenie na príkaz CHGSYSLIBL a monitorovať záznamy SV v žurnáli auditovania bezpečnosti. Zlomyseľný užívateľ by mohol v zozname

knižníc umiestniť knižnicu pred QSYS a spôsobiť tak, že ostatní používatelia budú spúšťať neoprávnené príkazy s rovnakými názvami ako príkazy dodané od IBM.

**Voľby ponuky SECBATCH:**
**28** *na okamžité predloženie* **67** *na použitie plánovača úloh*

Príkaz PRTUSROBJ (Print User Objects) môžete použiť na tlač zoznamu užívateľských objektov (objekty, ktoré nevytvorila firma IBM), ktoré sa nachádzajú v zadanej knižnici. Potom môžete vyhodnotiť programy v zozname a určiť, kto ich vytvoril a akú vykonávajú funkciu.

Užívateľské objekty iné ako programy tiež môžu predstavovať ohrozenie bezpečnosti, keď sa nachádzajú v systémových knižniciach. Napríklad, ak program zapisuje dôverné informácie do súboru, ktorého názov nie je určený, tento program môže byť oklamaný tak, že zo systémovej knižnice otvorí podvrhnutý súbor.

# Kapitola 10. Zamedzenie a zistenie pokusov o prelomenie

Tieto informácie sú zbierkou rôznych tipov, ktoré vám majú pomôcť zistiť potenciálne odhalenia bezpečnosti a záškodníkov.

## Fyzické zabezpečenie

Vaša systémová jednotka predstavuje dôležitý majetok firmy a možné dvere do vášho systému. Niektoré komponenty vnútri systému sú malé a hodnotné. Systémovú jednotku by ste mali umiestniť na kontrolovateľné miesto, aby ste všetkým zabránili odstrániť cenné komponenty systému.

Systémová jednotka má riadiaci panel, ktorá poskytuje možnosť vykonávať základné funkcie bez pracovnej stanice. Napríklad, ovládací panel môžete použiť na vykonanie nasledovného:

- Zastavenie systému.
- Spustenie systému.
- Zavedenie operačného systému.
- Spustenie servisných funkcií.

Všetky tieto aktivity môžu prerušiť vaši používatelia systému. Tiež predstavujú pre váš systém možné bezpečnostné riziko. Na riadenie toho, kedy sú povolené tieto aktivity môžete použiť dodaný uzamykateľný vypínač. Ak chcete zabrániť používaniu ovládacieho panelu, dajte zámku do polohy Secure, vytiahnite kľúč a uložte ho na bezpečnom mieste.

**Poznámky:**

1. Ak musíte na vašom systéme vykonať vzdialené IPL alebo vykonať vzdialenú diagnostiku, možno budete musieť vybrať iné nastavenie pre zámku. Téma Začíname v Informačnom centre poskytuje viac informácií o nastavení zámky (pozrite si podrobnosti v časti “Nevyhnutné predpoklady a súvisiace informácie” na strane xii).
2. Nie všetky modely systémov majú štandardné dodanú zámku.

## Monitorovanie aktivity profilu užívateľa

Profily používateľa poskytujú vstup do vášho systému. Parametre v profile používateľa určujú prostredie a charakteristiky bezpečnosti používateľa. Ako správca bezpečnosti musíte ovládať a auditovať zmeny, ktoré sa objavia v užívateľských profiloch vo vašom systéme.

Audit bezpečnosti môžete nastaviť tak, aby váš systém napísal správu o zmene v užívateľských profiloch. Na vytlačenie a ohlásenie týchto zmien môžete použiť príkaz DSPAUDJRNE.

Môžete vytvoriť výstupné programy na ohodnotenie požadovaných činností do užívateľských profilov. Tabuľka 16 zobrazuje výstupné body, ktoré sú dostupné pre príkazy užívateľského profilu.

*Tabuľka 16. Výstupné body pre aktivitu profilu užívateľa*

| Príkaz užívateľského profilu | Názov výstupného bodu |
|---|---|
| Vytvoriť užívateľský profil (CRTUSRPRF) | QIBM_QSY_CRT_PROFILE |
| Zmeniť užívateľský profil (CHGUSRPRF) | QIBM_QSY_CHG_PROFILE |
| Vymazať užívateľský profil (DLTUSRPRF) | QIBM_QSY_DLT_PROFILE |
| Obnoviť užívateľský profil (RSTUSRPRF) | QIBM_QSY_RST_PROFILE |

Váš výstupný program môže napríklad vyhľadať zmeny, ktoré by mohli zapríčiniť, že užívateľ spustí neoprávnenú verziu programu. Tieto zmeny mohli prideliť buď iný opis úlohy alebo novú aktuálnu knižnicu. Váš výstupný program mohol buď zaznamenať front správ, alebo urobiť nejakú činnosť (ako napríklad zmena alebo vypnutie užívateľského profilu) na základe informácií, ktoré dostane výstupný program.

Kniha *iSeries Security Reference* poskytuje viac informácií o výstupných programoch pre činnosti užívateľského profilu.

## Podpisovanie objektov

Všetky vami vykonané bezpečnostné opatrenia nemajú zmysel, ak ich niekto obíde tak, že systému predloží sfalšované údaje. Server iSeries má mnoho zabudovaných funkcií, ktoré môžete použiť na to, aby sfalšovaný softvér nemohol byť zavedený do vášho systému a na zistenie každého takéhoto softvéru, ktorý už v systéme je. Jednou z techník pridaných vo V5R1 je podpisovanie objektov.

Podpisovanie objektov je na serveri iSeries implementáciou konceptu šifrovania, ktorý poznáme ako ″digitálne podpisy.″ Myšlienka je pomerne jasná: keď je výrobca softvéru pripravený doručiť softvér zákazníkom, výrobca ho ″podpíše″. Tento podpis negarantuje, že softvér vykonáva nejakú konkrétnu funkciu. Poskytuje však spôsob overiť, že softvér prišiel od výrobcu, ktorý ho podpísal a od vytvorenia a podpísania nebol zmenený. Toto je hlavne dôležité, ak sa má softvér prenášať cez internet alebo na médiu, o ktorom si myslíte, že sa mohlo modifikovať.

Používanie digitálnych podpisov vám dáva väčšie riadenie toho, ktorý softvér sa zavedie na váš systém a umožňuje vám účinnejšie detekovať zmeny od jeho zavedenia. Systémová hodnota Verify Object Restore (QVFYOBJRST) poskytuje mechanizmus pre nastavenie reštriktívnej politiky, ktorá vyžaduje, aby bol všetok zavádzaný softvér na systém podpísaný známymi softvérovými zdrojmi. Môžete tiež vybrať otvorenejšiu politiku a jednoducho len kontrolovať podpisy, ak sú prítomné.

Všetok softvér OS/400 ako aj softvér pre voľby a licenčné programy servera iSeries bol podpísaný dôveryhodným systémovým zdrojom. Tieto podpisy pomáhajú systému ochraňovať jeho integritu a kontrolujú sa pri použití opráv do systému, aby sa zaručilo, že oprava pochádza zo spoľahlivého systémového zdroja a že nebola po ceste zmenená. Tieto podpisy sa môžu kontrolovať potom, keď bude tento softvér na systéme. Príkaz CHKOBJITG (Check Object Integrity) bol rozšírený, aby kontroloval podpisy okrem iných funkcií integrity objektov v systéme. Okrem toho, Správca digitálnych certifikátov má panely, ktoré môžete použiť na kontrolu podpisov na objektoch, vrátane objektov v operačnom systéme.

Rovnako, ako je podpísaný operačný systém, digitálne podpisy môžete použiť na ochranu integrity softvéru, ktorý je kritický pre vašu firmu. Môžete si kúpiť softvér, ktorý je podpísaný poskytovateľom softvéru alebo môžete podpísať softvér, ktorý ste si zakúpili alebo napísali. Súčasťou vašej bezpečnostnej politiky by potom mohlo byť pravidelné používanie CHKOBJITG alebo Správcu digitálnych certifikátov na kontrolu, že podpisy na softvéri sú stále platné — že boli zmenené od ich podpísania. Môžete tiež vyžadovať, aby všetok obnovovaný softvér na vašom systéme bol podpísaný vami alebo známym zdrojom. Avšak pretože väčšina iSeries softvéru pre server, ktorý nevyrába firma IBM nie je aktuálne podpísaná, môže to byť pre váš systém príliš obmedzujúce. Nová podpora digitálnych podpisov vám dáva flexibilitu pri rozhodovaní, ako najlepšie chrániť integritu vášho softvéru.

Digitálne podpisy na chránenie softvéru sú len jedným použitím digitálnych certifikátov. Dodatočné informácie o manažovaní digitálnych certifikátov môžete nájsť v téme Manažment

digitálnych certifikátov v Informačnom centre (pozrite si informácie v časti “Nevyhnutné predpoklady a súvisiace informácie” na strane xii).

## Monitorovanie opisov podsystémov

Keď na serveri iSeries spustíte podsystém, systém vytvorí prostredie pre prácu na vstup a spustenie systému. Opis podsystému definuje, ako toto prostredie vyzerá. Opisy podsystémov preto môžu poskytovať príležitosť pre pochybných používateľov. Záškodník môže použiť opis podsystému na automatické spustenie programu alebo ho umožniť na prihlasovanie bez užívateľského profilu.

Keď spustíte príkaz RVKPUBAUT (Revoke Public Authority), systém nastaví verejné oprávnenia na príkazy z opisu podsystému na *EXCLUDE. Toto zabraňuje používateľom, ktorí nie sú konkrétne oprávnení (a ktorí nemajú špeciálne oprávnenie *ALLOBJ), meniť alebo vytvárať opisy podsystémov.

Nasledovné témy poskytujú návrhy pre prezeranie podsystémov, ktoré aktuálne existujú na vašom systéme. Na vytvorenie zoznamu všetkých opisov podsystémov môžete použiť príkaz WRKSBSD (Work with Subsystem Descriptions). Keď zo zoznamu vyberiete 5 (Zobraziť), pre opis systému, ktorý ste vybrali, sa zobrazí ponuka . Ukazuje zoznam častí prostredia podsystému.

Ak si chcete prezrieť detaily o častiach, vyberiete si voľby. Na zmenenie prvých dvoch položiek v menu použite príkaz CHGSBSD (Change Subsystem Description). Ak chcete zmeniť ostatné položky, použite vhodný príkaz na pridanie, odstránenie alebo zmenu pre typ položky. Napríklad, ak chcete zmeniť položku pracovnej stanice, použite príkaz CHGWSE (Change Workstation Entry).

Kniha *Work Management* poskytuje viac informácií o práci s opismi podsystémov. Zároveň zobrazuje dodané hodnoty pre opisy podsystémov dodaných IBM.

## Automatické spustenie položiek úlohy

Položky automatického spustenia úloha obsahuje názov opisu úlohy. Opis úlohy môže obsahovať RQSDTA (request data), ktoré spôsobia spustenie programu alebo príkazu. Napríklad, RQSDTA môže byť CALL LIB1/PROGRAM1. Kedykoľvek sa spustí podsystém, systém spusti program PROGRAM1 v knižnici LIB1.

Pozrite sa na vaše autostart job entries a s nimi súvisiace opisy úloh. Uistite sa, že rozumiete funkcii programu, ktorý sa automaticky spustí pri spustení podsystému.

## Názvy pracovných staníc a typy pracovných staníc

Keď sa spustí podsystém, vyhradí si všetky nevyhradené pracovné stanice, ktoré sú uvedené (konkrétne alebo generický) v jeho položkách pre názvy a typy pracovných staníc. Keď sa užívateľ prihlási, prihlási sa do podsystému, ktorý vyhradil pracovnú stanicu.

Položka pracovnej stanice hovorí, ktorý opis úlohy sa použije pri spustení úlohy na pracovnej stanici. Opis úlohy môže obsahovať údaje požiadavky, ktoré spôsobia spustenie programu alebo príkazu. Napríklad, parameter by mohol byť CALL LIB1/PROGRAM1. Vždy keď sa užívateľ prihlási do pracovnej stanice v tomto podsystéme, systém spustí PROGRAM1 v LIB1.

Pozrite sa na vaše položky pracovnej stanice a s nimi súvisiace opisy úloh. Presvedčte sa, že nikto nepridal alebo neaktualizoval žiadne položky na spúšťanie programov, ktorých si nie ste vedomý.

Položka pracovnej stanice tiež môže špecifikovať štandardný užívateľský profil. Pre určité konfigurácie podsystému toto umožňuje, aby sa do neho dalo prihlásiť jednoducho stlačením klávesu Enter. Ak je bezpečnostná úroveň (systémová hodnota QSECURITY) na vašom systéme menšia ako 40, mali by prezrieť vaše položky pracovnej stanice pre štandardných užívateľov.

## Položky frontu úloh

Keď sa spustí podsystém, vyhradí si všetky nepridelené fronty úloh, ktoré sú uvedené v opise podsystéme. Položky frontu úloh neposkytujú žiadne priame bezpečnostné riziká. Poskytujú však príležitosť pre niekoho, aby sfalšoval výkonnosť systému tým, že spustí úlohy v nesprávnych prostrediach.

Mali by ste pravidelne prezerať položky frontu úloh v opisoch vašich podsystémov aby ste zaistili, že všetky úlohy sú spustené tam, kde ste ich chceli mať.

## Smerovacie položky

Smerovacia položka definuje, čo spraví úloha pri vstupe do podsystému. Podsystém používa smerovacie položky pre všetky typy úloh; dávkové, interaktívne a komunikačné úlohy. Smerovacia položka špecifikuje nasledovné:

- Triedu pre úlohu. Podobne ako položky frontu úloh, trieda spojená s úlohou môže ovplyvniť jej výkon, ale nepredstavuje bezpečnostné riziko.
- Program, ktorý sa spustí pri spustení úlohy. Pozrite sa na smerovacie položky a presvedčte sa, že nikto nepridal alebo neaktualizoval žiadne položky na spúšťanie programov, ktorých si nie ste vedomý.

## Komunikačné položky a názvy vzdialených umiestnení

Keď komunikačná položky vstúpi do vášho systému, systém použije komunikačné položky a položky názvov vzdialeného umiestnenia v aktívnom podsystéme na zistenie, ako sa má spustiť komunikačná úloha. Pozrite si nasledovné pre tieto položky:

- Všetky podsystémy sú schopné spúšťať komunikačné úlohy. Ak podsystém, ktorý ste určili pre komunikácie nie je aktívny, úloha pokúšajúca sa vstúpiť do vášho systému môže nájsť inú položku v inom opise podsystému, ktorá spĺňa jej potreby. Musíte sa pozrieť na položky vo všetkých opisoch podsystémov.
- Komunikačná položka obsahuje opis úlohy. Opis úlohy môže obsahovať údaje s požiadavkou, ktoré spustia príkaz alebo program. Pozrite sa na svoje komunikačné položky a s nimi spojené opisy úloh aby ste sa uistili, že viete ako sa budú spúšťať úlohy.
- Komunikačná položka tiež špecifikuje štandardný profil užívateľa, ktorý systém použije v niektorých situáciách. Uistite sa, že ste porozumeli úlohe štandardných profilov. Ak váš systém obsahuje štandardné profily, mali by ste zabezpečiť, aby mali minimálne oprávnenie. Pozrite si Kapitola 12, “Zabezpečenie komunikácií APPC”, kde je viac informácií o štandardných užívateľských profiloch.

  Na identifikovanie komunikačných položiek, ktoré špecifikujú názov užívateľského profilu môžete použiť príkaz PRTSBSDAUT Print Subsystem Description).

## Položky predspustených úloh

Položky predspustených úloh môžete použiť na pripravenie systému na určité druhy úloh, aby sa tieto úlohy spúšťali oveľa rýchlejšie. Prespustené úlohy sa môžu spustiť pri spustení podsystému alebo keď sú potrebné. Položka predspustených úloh určuje nasledovné:

- Program na spustenie

  Štandardný užívateľský profil

Opis úlohy

Všetko toto poskytuje možné riziká v bezpečnosti. Mali by ste sa uistiť, že položky predspustených úloh vykonávajú len oprávnené a požadované funkcie.

## Úlohy a opisy úloh

Opisy úloh obsahujú údaje s požiadavkou a smerovacie údaje, ktoré môžu spôsobiť spustenie konkrétneho programu, keď sa použije opis úlohy. Keď opis úlohy špecifikuje program v parametri pre údaje s požiadavkou, systém spustí program. Keď opis úlohy špecifikuje smerovacie údaje, systém spustí program, ktorý je špecifikovaný v smerovacej položke, ktorá sa zhoduje so smerovacími údajmi.

Systém používa opisy úloh pre interaktívne aj dávkové súbory. Pre interaktívne úlohy špecifikuje položka pracovnej stanice opis úlohy. Typicky je hodnota položky pracovnej stanice *USRPRF, preto systém používa opis úloh, ktorý je určený v užívateľskom profile. Pre dávkové úlohy špecifikujete opis úlohy pri jej predložení.

Mali by ste pravidelne prezerať opisy úloh aby ste sa uistili, že nespúšťajú nechcené programy. Tiež by ste mali použiť oprávnenie objektu, aby ste zabránili zmenám v opisoch úloh. Na spustenie úlohy s opisom úlohy stačí oprávnenie *USE. Typický užívateľ nepotrebuje na opisy úloh oprávnenie *CHANGE.

**Voľby ponuky SECBATCH:**
**15** *na okamžité predloženie* **54** *na použitie plánovače úloh*

Opisy úloh tiež môžu špecifikovať, pod ktorým užívateľským profilom by sa mala úloha spustiť. S bezpečnostnou úrovňou 40 alebo vyššou musíte mať na opis úlohy a užívateľský profil, ktorý je špecifikovaný v opise úlohy, oprávnenie *USE. S bezpečnostnými úrovňami menšími ako 40 potrebujete oprávnenie *USE len na opis úlohy.

Príkaz PRTJOBDAUT (Print Job Description Authority) môžete použiť na vytlačenie zoznamu opisov úloh, ktoré špecifikujú užívateľské profily a majú verejné oprávnenie *USE.

Správa ukazuje špeciálne oprávnenia užívateľského profilu, ktorý je špecifikovaný v opise úlohy. Správa obsahuje špeciálne oprávnenia všetkých skupinových profilov, ktoré má užívateľský profil. Nasledovný príkaz môžete použiť na zobrazenie súkromných oprávnení užívateľského profilu.

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

Opis úlohy špecifikuje zoznam knižníc, ktoré použije úloha pri svojom behu. Ak niekto môže zmeniť užívateľský zoznam knižníc, tento užívateľ môže spúšťať neželané verzie programu v odlišnej knižnici. Mali by ste periodicky prezerať zoznamy knižníc, ktoré sú špecifikované v opisoch úloh na vašom systéme.

Na záver by ste sa mali presvedčiť, že štandardné hodnoty pre príkazy SBMJOB (Submit Job) a CRTUSRPRF (Create User Profile) sa nezmenili tak, aby ukazovali na neželané opisy úloh.

## Navrhnuté názvy transakčných programov

Niektoré komunikačné požiadavky posielajú vášmu systému konkrétny typ signálu. Táto požiadavka sa volá **architektúra názvu transakčného programu (TPN)**, pretože názov transakčného programu je časťou architektúry APPN pre systém. Žiadosť na žiadosť o passthrough zobrazovaciu stanicu je príkladom architektúry TPN. Architektúra TPN je normálny spôsob pre fungovanie komunikácií a nevyhnutne nepredstavuje riziko v bezpečnosti. Architektúra TPN však môže poskytnúť neočakávaný vstup do vášho systému.

Niektoré TPN nepredávajú v žiadosti profil. Ak sa požiadavka bude spojená s komunikačnou položkou, ktorej štandardný užívateľ je *SYS, požiadavka sa môže iniciovať na vašom systéme. Profil *SYS však môže spúšťať len systémové funkcie, nie užívateľské aplikácie.

Ak nechcete spúšťať architektúru TPN so štandardným profilom, môžete zmeniť v komunikačných položkách štandardného užívateľa z *SYS na *NONE. “Navrhnuté požiadavky TPN” zobrazuje architektúru TPN a ňou spojené užívateľské profily.

Ak nechcete na vašom systéme vôbec spúšťať konkrétny TPN, spravte nasledovné:

1. Vytvorte program pre príkazový riadok, ktorý akceptuje niekoľko parametrov. Program by nemal vykonávať žiadnu funkciu. Mal by mať len príkazy DCL (Declare) pre parametre a potom skončiť.
2. Pridajte smerovaciu položku pre TPN do každého podsystému, ktorý má komunikačné položky alebo položky názvov vzdialených umiestnení. Smerovacia položka by mala špecifikovať nasledovné:
   - Hodnotu *Compare value* (CMPVAL) rovnú názvu programu pre TPN (pozrite si Navrhnuté požiadavky TPN) so začiatočnou pozíciou 37.
   - Hodnotu *Program to call* (PGM) rovnú názvu programu, ktorý ste vytvorili v kroku 1. Týmto sa zabráni tomu, aby TPN našiel inú smerovaciu položku, ako je *ANY.

Niekoľko TPN už má svoje vlastné smerovacie položky v podsystéme QCMN. Tieto boli pridané z výkonnostných dôvodov.

### Navrhnuté požiadavky TPN

*Tabuľka 17. Programy a používatelia pre požiadavky TPN*

| Požiadavka TPN | Program | Užívateľský profil | Opis |
|---|---|---|---|
| X'30F0F8F1' | AMQCRC6A | *NONE | Zaraďovanie správ do frontu |
| X'06F3F0F1' | QACSOTP | QUSER | APPC prihlasovací transakčný program |
| X'30F0F2D1' | QANRTP | QADSM | ADSM/400 APPC konfigurácia |
| X'30F0F1F9' | QCNPCSUP | *NONE | Zdieľané zložky |
| X'07F0F0F1' | QCNTEDDM | QUSER | DDM |
| X'07F6C4C2' | QCNTEDDM | QUSER | Vzdialený SQL–DRDA1 |
| X'30F0F7F7' | QCQNRBAS | QSVCCS | SNA CC_Server |
| X'30F0F1F4' | QDXPRCV | QUSER | DSNX–PC príjemca |
| X'30F0F1F3' | QDXPSEND | QUSER | DSNX–PC odosielateľ |
| X'30F0F2C4' | QEVYMAIN | QUSER | ENVY**/400 Server |
| X'30F0F6F0' | QHQTRGT | *NONE | Front údajov PC |
| X'30F0F8F0' | QLZPSERV | *NONE | Client Access licenčný manažér |
| X'30F0F1F7' | QMFRCVR | *NONE | príjemca správ PC |
| X'30F0F1F8' | QMFSNDR | *NONE | odosielateľ správ PC |

*Tabuľka 17. Programy a používatelia pre požiadavky TPN (pokračovanie)*

| Požiadavka TPN | Program | Užívateľský profil | Opis |
|---|---|---|---|
| X'30F0F6F6' | QND5MAIN | QUSER | APPN 5394 radič pracovnej stanice |
| DB2DRDA | QCNTEDDDM | QUSER | DB2DRDA |
| APINGD | QNMAPINGD | QUSER | APINGD |
| X'30F0F5F4' | QNMEVK | QUSER | Funkčnosti systémového manažmentu |
| X'30F0F2C1' | QNPSERVR | *NONE | PWS-I sieťový tlačový server |
| X'30F0F7F9' | QOCEVOKE | *NONE | Systémový kalendár |
| X'30F0F6F1' | QOKCSUP | QDOC | Tieňovanie adresára |
| X'20F0F0F7' | QOQSESRV | QUSER | DIA verzia 2 |
| X'20F0F0F8' | QOQSESRV | QUSER | DIA verzia 2 |
| X'30F0F5F1' | QOQSESRV | QUSER | DIA verzia 2 |
| X'20F0F0F0' | QOSAPPC | QUSER | DIA verzia 1 |
| X'30F0F0F5' | QPAPAST2 | QUSER | S/36—S/38 pass-through |
| X'30F0F0F9' | QPAPAST2 | QUSER | Pass-through tlačiarne |
| X'30F0F4F6' | QPWFSTP0 | *NONE | Zdieľané zložky Typ 2 |
| X'30F0F2C8' | QPWFSTP1 | *NONE | Client Access súborový server |
| X'30F0F2C9' | QPWFSTP2 | *NONE | Windows** Client Access súborový server |
| X'30F0F6F9' | QRQSRVX | *NONE | Vzdialený SQL–konvergovaný server |
| X'30F0F6F5' | QRQSRV0 | *NONE | Vzdialený SQL bez záväzku |
| X'30F0F6F4' | QRQSRV1 | *NONE | Vzdialený SQL bez záväzku |
| X'30F0F2D2' | QSVRCI | QUSER | SOC/CT |
| X'21F0F0F8' | QS2RCVR | QGATE | príjemca SNADS FS2 |
| X'21F0F0F7' | QS2STSND | QGATE | odosielateľ SNADS FS2 |
| X'30F0F1F6' | QTFDWNLD | *NONE | prenosová funkcia PC |
| X'30F0F2F4' | QTIHNPCS | QUSER | funkcia TIE |
| X'30F0F1F5' | QVPPRINT | *NONE | virtuálna tlač PC |
| X'30F0F2D3' | QWGMTP | QWGM | Ultimedia Mail/400 Server |
| X'30F0F8F3' | QZDAINIT | QUSER | PWS-I server prístupu k údajom |
| X'21F0F0F2' | QZDRCVR | QSNADS | príjemca SNADS |
| X'21F0F0F1' | QZDSTSND | QSNADS | odosielateľ SNADS |
| X'30F0F2C5' | QZHQTRG | *NONE | PWS-I server frontu údajov |
| X'30F0F2C6' | QZRCSRVR | *NONE | PWS-I server vzdialených príkazov |
| X'30F0F2C7' | QZSCSRVR | *NONE | PWS-I centrálny server |

## Metódy pre monitorovanie bezpečnostných udalostí

Nastavenie bezpečnosti nie je jednorazová aktivita. Musíte neustále vyhodnocovať zmeny na vašom systéme a vaše zlyhania bezpečnosti. Následne musíte spraviť úpravy do bezpečnostného prostredia podľa toho, čo ste zistili.

Bezpečnostné správy vám pomáhajú monitorovať zmeny na vašom systéme, ktoré sa týkajú bezpečnosti. Nasledujú iné funkcie systému, ktoré môžete použiť pri určovaní zlyhaní bezpečnosti alebo možných rizík:

- Auditovanie bezpečnosti je výkonný nástroj, ktorý môžete použiť na pozorovanie rôznych typov udalostí týkajúcich sa bezpečnosti, ktoré sa vyskytnú na vašom systéme. Napríklad, môžete nastaviť systém tak, aby zapisoval auditový záznam vždy keď používateľ otvorí konkrétny databázový súbor na aktualizáciu. Môžete auditovať všetky zmeny v systémových hodnotách. Môžete auditovať akcie, ktoré sa stanú, keď používateľ obnovuje objekty.

  Kapitola 9 v knihe *iSeries Security Reference* poskytuje úplné informácie o funkcii auditovania bezpečnosti. Na nastavenie auditovania bezpečnosti na vašom systéme môžete použiť príkaz CHGSECAUD (Change Security Auditing). Na vytlačenie vybraných informácií z auditového žurnálu tiež môžete použiť príkaz DSPAUDJRNE (Display Audit Journal Entries).
- Môžete vytvoriť front správ QSYSMSG na zachytávanie dôležitých správ pre systémového operátora. Front správ QSYSOPR prijíma správy rôzneho významu počas bežného pracovného dňa. Kritické správy týkajúce sa bezpečnosti sa môžu prehliadnuť kvôli množstvu objemu správ vo fronte správ QSYSOPR.

  Ak vytvoríte front správ QSYSMSG v knižnici QSYS na vašom systéme, systém automaticky smeruje určité kritické správy do frontu správ QSYSMSG namiesto frontu správ QSYSOPR.

  Môžete vytvoriť program na monitorovanie frontu správ QSYSMSG alebo ju môžete prideliť v prerušenom móde vám alebo inému dôveryhodnému používateľovi.

# Časť 3. Aplikácie a sieťové komunikácie

# Kapitola 11. Použitie Integrovaného súborového systému na zabezpečenie súborov

Integrovaný súborový systém vám poskytuje viacero spôsobov ukladania a prezerania informácií o serveri iSeries. Integrovaný súborový systém je časť operačného systému OS/400, ktorý podporuje vstupné a výstupné operácie toku. Poskytuje metódy riadenia ukladania, ktoré sú podobné (a kompatibilné s) operačným systémom osobných počítačov a operačným systémom UNIX.

Pomocou Integrovaného súborového systému sa môžu všetky objekty na systéme prezerať z pohľadu hierarchickej štruktúry adresárov. Vo väčšine prípadov si však používatelia prezerajú objekty spôsobom, ktorý je pre konkrétny súborový systém najbežnejší. Napríklad, ″tradičné″ objekty iSeries sú v súborovom systéme QSYS.LIB. Poväčšine si budú používatelia prezerať tieto objekty z pohľadu knižníc. Objekty v súborovom systéme QDLS si používatelia typicky prezerajú z pohľadu dokumentov v zložkách. Priestor (/), QOpenSys a užívateľom definovaný súborový systém predstavuje štruktúru hierarchických (vložených) adresárov.

Ako správca bezpečnosti musíte porozumieť nasledovnému:

- Ktoré súborové systémy sú použité na vašom systéme
- Jedinečné bezpečnostné charakteristiky každého súborového systému

Nasledovné témy poskytujú všeobecné úvahy pre bezpečnosť Integrovaného súborového systému.

## Prístup Integrovaného súborového systému k bezpečnosti

Koreňový súborový systém sa chová ako dáždnik (alebo základ) pre všetky ostatné súborové systémy na serveroch iSeries. Na vyššej úrovni poskytuje integrované zobrazenie všetkých objektov na systéme. Ostatné súborové systémy, ktoré sa nachádzajú na serveroch iSeries, poskytujú rôzne prístupy k riadeniu objektov a integrácii, v závislosti od základného zamerania každého súborového systému. Napríklad, súborový (optický) systém QOPT umožňuje, aby aplikácie a servery iSeries (vrátane súborového servera iSeries Access for Windows) mali prístup na jednotku CD-ROM na serveri iSeries. Podobne súborový systém QFileSvr.400 umožňuje, aby aplikácie mali prístup na údaje Integrovaného súborového systému na vzdialených serveroch iSeries. Súborový server QLANSrv umožňuje pristupovať na súbory, uložené na Integrated xSeries Server for iSeries alebo na iných pripojených serveroch v sieti.

Postoj k bezpečnosti pre každý súborový systém závisí na údajoch, ktoré sprístupňuje súborový systém. Súborový systém QOPT napríklad neposkytuje bezpečnosť na úrovni objektov, pretože neexistuje žiadna technológia na zapísanie informácií o oprávnení na CD-ROM. Pre súborový systém QFileSvr.400, riadenie prístupu sa vykonáva na vzdialenom systéme (kde sú súbory fyzicky uložené a riadené). Pre súborové systémy ako je QLANSrv poskytuje Integrated xSeries Server for iSeries riadenie prístupu. Napriek odlišným bezpečnostným súborom, veľa súborových systémov podporuje konzistentné riadenie kontroly prístupu prostredníctvom integrovaným príkazov súborového systému, ako napr. Zmeniť autoritu (CHGAUT) a Zmeniť vlastníka (CHGOWN).

Nasleduje niekoľko typov, súvisiacich so zákutiami a trhlinami bezpečnosti integrovaného súborového systému. Integrovaný súborový systém je navrhnutý tak, aby spĺňal čo najlepšie štandardy POSIX. To vedie k určitému zaujímavému správaniu, pri ktorom sa oprávnenie servera iSeries a povolenia POSIX ″zmiešajú″:

1. Neodstraňujte súkromné oprávnenie pre užívateľa na adresár, ktorý tento užívateľ vlastní, ani vtedy, ak má tento užívateľ oprávnenie prostredníctvom verejného oprávnenia, skupiny alebo zoznamu oprávnení. Pri práci s knižnicami alebo zložkami v štandardnom bezpečnostnom modeli servera iSeries by sa odstránením súkromného oprávnenia vlastníka znížilo množstvo informácií o oprávnení, ktoré sú uložené pre užívateľský profil a neovplyvnili by sa ostatné operácie. Ale pre spôsob, akým štandard POSIX definuje povoľovacie dedičstvo pre adresáre, bude mať majiteľ novovytvoreného adresára oprávnenia na rovnaké objekty v tom adresári, na aké má oprávnenie majiteľ rodičovského adresára, aj keby mal majiteľ novovytvoreného adresára iné súkromné oprávnenia na hlavný adresár. To môže byť dosť ťažké na pochopenie, takže nasleduje príklad: USERA vlastní adresár /DIRA, ale súkromné oprávnenia USERA boli odstránené. USERB má súkromné oprávnenia na /DIRA. USERB vytvorí adresár /DIRA/DIRB. Keďže USERA nemá žiadne oprávnenia na objekty na /DIRA, USERB nebude mať žiadne oprávnenia na objekty na /DIRA/DIRB. USERB nebude môcť premenovať ani vymazať /DIRA/DIRB bez ďalšieho kroku na zmenu oprávnení na objekty USERB. Toto prichádza do hry, keď sa vytvárajú súbory s otvoreným () API pomocou návestia O_INHERITMODE. Ak USERB vytvoril súbor /DIRA/FILEB, USERB by nemal žiadne oprávnenie na objekty a údaje. USERB by nemohol písať do nového súboru.
2. Adoptované oprávnenie nie je uznávané väčšinou fyzických súborových systémov. To zahŕňa kmeň (/), QOpenSys, QDLS, ako aj užívateľom definované súborové systémy.
3. Ľubovoľné objekty vlastní užívateľský profil, ktorý objekty vytvoril, aj keď je pole OWNER užívateľského profilu nastavené na *GRPPRF.
4. Mnohé operácie súborového systému vyžadujú oprávnenie na údaje *RX na každý komponent cesty, vrátane kmeňového (/) adresára. Pri problémoch s oprávneniami, si skontrolujte oprávnenie užívateľa na samotný kmeňový adresár.
5. Zobrazenie alebo načítanie aktuálneho pracovného adresára (DSPCURDIR, getcwd(), atď.) vyžaduje oprávnenie na údaje *RX na každý komponent cesty. Zmena aktuálneho pracovného adresára (CD, chdir(), atď.) však vyžaduje iba oprávnenie na údaje *X na každý komponent. Užívateľ preto môže zmeniť aktuálny pracovný adresár na určitú cestu a potom sa môže stať, že nebude môcť túto cestu zobraziť.
6. Zámerom príkazu COPY je zduplikovať objekt. Nastavenie oprávnenia na novom súbore bude rovnaké ako na pôvodnom s výnimkou majiteľa. Zámerom príkazu CPYTOSTMF však je jednoducho zduplikovať údaje. Nastavenie oprávnenia na novom súbore nemôže riadiť užívateľ. Tvorca/majiteľ bude mať oprávnenie na údaje *RWX, ale skupinové alebo verejné oprávnenia budú *EXCLUDE. Užívateľ musí použiť ďalší prostriedok (CHGAUT, chmod(), atď.) na priradenie želaných oprávnení.
7. Užívateľ musí byť majiteľom alebo mať oprávnenie na objekty *OBJMGT, aby mohol z uvedeného objektu načítať informácie o oprávnení. Toto roluje na niektoré nečakané miesta, ako je napríklad COPY, čo musí načítať informácie o oprávnení na zdrojovom objekte na nastavenie ekvivalentných oprávnení na cieľovom objekte.
8. Keď sa mení majiteľ alebo skupina objektu, užívateľ musí mať nielen príslušné oprávnenie na objekt, ale tiež oprávnenie na údaje *ADD na nový užívateľský profil majiteľa/skupiny a údajové oprávnenie *DELETE na starý profil majiteľa/skupiny. Tieto oprávnenia na údaje sa netýkajú údajových oprávnení na súborové systémy. Tieto údajové oprávnenia sa dajú zobraziť pomocou príkazu DSPOBJAUT a zmeniť pomocou príkazu EDTOBJAUT. To niekedy roluje nečakane na COPY, keď sa pokúša nastaviť skupinový ID pre nový objekt.
9. Príkaz MOV je náchylný na pomiešanie chýb oprávnení, zvlášť keď sa presúva jeden fyzický súborový systém do druhého, alebo keď sa vykonáva konverzia údajov. V takýchto prípadoch sa presun vlastne stáva operáciou kopírovať-a-vymazávať. Preto môže byť príkaz MOV okrem iných špecifických úvah o MOV ovplyvnený všetkými úvahami o rovnakom oprávnení, ako aj príkaz COPY (viď vyššie uvedený 7 a 8) a príkaz RMVLNK.

Nasledujúca časť vám poskytne určité úvahy pre niektoré reprezentatívne súborové systémy. Keď chcete získať viac informácií o špecifickom súborovom systéme vo vašom serveri iSeries, musíte ich vyhľadať v dokumentácii pre licenčný program, ktorý používa súborový systém.

# Koreňový (/), QOpenSys a užívateľom definované súborové systémy

Nasledujú predpoklady bezpečnosti priestoru, QOpenSys a užívateľom definované súborové systémy.

## Ako funguje oprávnenie

Koreňový, QOpenSys a užívateľom definované súborové systémy poskytujú zmes funkcií servera iSeries, PC a UNIX** pre riadenie objektov i pre bezpečnosť. Keď používate príkazy Integrovaného súborového systému z relácie servera iSeries (WRKAUT a CHGAUT), môžete nastaviť všetky bežné oprávnenia na objekty servera iSeries. Patria sem oprávnenia *R, *W a *X, ktoré sú kompatibilné so Spec 1170 (typ UNIX operačného systému).

**Poznámka:** Priestor, QOpenSys a užívateľom definované súborové systémy sú funkčne ekvivalentné. Súborový systém QOpenSys zohľadňuje veľkosť písmen. Koreňový súborový systém nie. Užívateľom definované súborové systémy sú nadefinované tak, že zohľadňujú veľkosť. Pretože oba tieto súborové systémy majú rovnaké bezpečnostné charakteristiky, môžete v nasledovných témach názvy oboch súborových systémov vzájomne zamieňať.

Keď pristupujete na koreňový súborový systém ako správca z relácie PC, môžete nastaviť atribúty objektov, ktoré používa PC na obmedzenie určitých typov prístupu:
- Systém
- Skrytý
- Archív
- Iba-na-čítanie

Tieto atribúty PC sú doplnkom, nie náhradou za, hodnoty oprávnenia na objekt servera iSeries.

Keď sa užívateľ pokúša pristúpiť na objekt v koreňovom súborovom systéme, OS/400 použije všetky hodnoty oprávnení objektov a atribútov pre objekt bez ohľadu na to, či sú tieto atribúty ″viditeľné″ z užívateľského rozhrania. Napríklad, predpokladajme, že je pre objekt nastavený read-only atribút. PC užívateľ nemôže vymazať objekt cez rozhranie iSeries Access. Ani užívateľ servera iSeries so stálou funkciou pracovnej stanice nemôže vymazať objekt, aj keby mal užívateľ servera iSeries mimoriadne oprávnenie *ALLOBJ. Predtým ako sa môže objekt vymazať, oprávnený užívateľ musí použiť funkciu PC na vynulovanie hodnoty read-only na vypnutú. Podobne, užívateľ PC nemusí mať dostatočné oprávnenie OS/400, aby mohol zmeniť bezpečnostné atribúty objektu týkajúce sa PC.

Aplikácie typu UNIX, ktoré sa spúšťajú na serveroch iSeries, používajú podobné rozhrania na programovanie aplikácií (API) ako má UNIX, aby mali prístup k údajom v koreňovom súborovom systéme. Pomocou API podobných UNIXu môžu aplikácie rozpoznať a udržovať nasledovné bezpečnostné informácie:
- Object owner
- Group owner (oprávnenie primárnej skupiny servera iSeries)
- Read (súbory)
- Write (meniť obsah)
- Execute (spúšťať programy alebo prehľadávať adresáre)

Systém mapuje tieto oprávnenia na údaje do existujúcich oprávnení na objekty a údaje servera iSeries:

- Read (*R) = *OBJOPR a *READ

- Write (*W) = *OBJOPR, *ADD, *UPD, *DLT
- Execute (*X) = *OBJOPR a *EXECUTE

Koncepcia iných oprávnení na objekty (*OBJMGT, *OBJEXIST, *OBJALTER, a *OBJREF) v prostrediach typu UNIX neexistuje.

Tieto oprávnenia na objekt však existujú pre všetky objekty v základnom súborovom systéme. Keď vytvárate objekt pomocou API-UNIX, zdedí tieto oprávnenia z rodičovského adresára, čo má za následok:

- Nový vlastník objektu má tie isté oprávnenia na objekt ako vlastník rodičovského adresára.
- Nová primárna skupina objektu má tie isté oprávnenia na objekt ako primárna skupina rodičovského adresára.
- Noví používatelia objektu majú tie isté oprávnenia ako používatelia rodičovského adresára.

Nové oprávnenia na údaje objektu pre vlastníka, primárnu skupinu a užívateľov sú špecifikované v parametri režimu na API. Keď sú nastavené všetky oprávnenia na objekty, máte právo na taký typ oprávnených činností, aký by ste očakávali v prostredí UNIX. Je najlepšie, ak ich necháte nastavené, pokiaľ chcete vykonávať činnosti ako v prostredí POSIX.

Keď spúšťate aplikácie používajúce API podobné UNIXu, systém použije všetky oprávnenia na objekty bez ohľadu na to, či sú ″viditeľné″ aplikáciám typu UNIX. Napríklad, systém použije oprávnenie zoznamov oprávnení aj vtedy, keď koncepcia zoznamov oprávnení v operačných systémoch typu UNIX neexistuje.

Keď máte prostredia so zmiešanými aplikáciami musíte zaistiť, aby ste nespravili zmeny v oprávnení v jednom prostredí, ktoré narušia vaše aplikácie v inom prostredí.

## Práca s bezpečnosťou pre Koreňový (/), QOpenSys a užívateľom definované súborové systémy

Uvedenie Integrovaného súborového systému, serverov iSeries poskytlo aj novú sadu príkazov pre prácu s objektmi vo viacerých súborových systémoch. Táto množina príkazov obsahuje príkazy na prácu s bezpečnosťou:

- Change Auditing (CHGAUD)
- Change Authority (CHGAUT)
- Change Owner (CHGOWN)
- Change Primary Group (CHGPGP)
- Display Authority (DSPAUT)
- Work with Authority (WRKAUT)

Tieto príkazy zoskupujú základné oprávnenia na údaje a objekty do podmnožím oprávnení podobných UNIXu:

***RWX** Read/write/execute
***RW** Read/write
***R** Read
***WX** Write/execute
***W** Write
***X** Execute

Okrem toho sú na prácu s bezpečnosťou k dispozícii API príbuzné prostrediu UNIX.

## Verejné oprávnenie na koreňový adresár

Pri dodaní vášho systému je verejné oprávnenie pre koreňový adresár *ALL (všetky oprávnenia na objekty a údaje). Toto nastavenie poskytuje flexibilitu a kompatibilitu pre očakávania aplikácií podobných UNIXu a pre očakávania užívateľov typického servera iSeries. Užívateľ servera iSeries s funkciou príkazového riadku dokáže vytvoriť v súborovom systéme QSYS.LIB novú knižnicu, iba s použitím príkazu CRTLIB. Oprávnenie na typickom

serveri iSeries to normálne umožňuje. Podobne aj pre dodané nastavenie pre koreňový súborový systém, typický užívateľ môže v koreňovom súborovom systéme vytvoriť adresár (rovnako ako vytvoríte nový adresár na vašom PC).

Ako správca bezpečnosti musíte vysvetliť svojim užívateľom ako si majú adekvátne chrániť vytvorené objekty. Keď užívateľ vytvorí knižnicu, pravdepodobne by verejné oprávnenie na knižnicu nemalo byť *CHANGE (štandardná hodnota). Užívateľ by mal verejné oprávnenie nastaviť na *USE alebo *EXCLUDE, v závislosti od obsahu knižnice.

Ak vaši používatelia potrebujú vytvoriť nové adresáre v koreňovom priestore (/), QOpenSys alebo v užívateľom definovanom súborovom systéme, máte niekoľko bezpečnostných možností:

- Môžete vysvetliť svojim užívateľom, aby pri vytvorení nových adresárov nahradili štandardné oprávnenie. Štandardne sa oprávnenie dedí z priameho rodičovského adresára. V prípade novovytvoreného adresára v koreňovom adresári sa použije verejné oprávnenie *ALL.
- V koreňovom adresári môžete vytvoriť ″hlavný″ adresár. Na hlavnom adresári nastavte verejné oprávnenie vhodné pre vašu organizáciu. Potom oznámte užívateľom, aby si vytvárali nové osobné adresáre v hlavnom podadresári. Ich nové adresáre zdedia jeho oprávnenie.
- Môžete pouvažovať o zmene verejného oprávnenia pre koreňový adresár, aby ste zabránili užívateľov vytvárať objekty v tomto adresári. (Odstrániť oprávnenia *W, *OBJEXIST, *OBJALTER, *OBJREF a *OBJMGT). Musíte však vyhodnotiť, či zmenou tohto nevzniknú problémy vo vašich aplikáciách. Napríklad, môžete mať aplikácie typu UNIX, ktoré predpokladajú možnosť vymazávania objektov z koreňového adresára.

## Príkaz PRTPVTAUT (Print private authorities objects)

Príkaz PRTPVTAUT (Print Private Authorities) vám umožňuje vytlačiť správu o všetkých súkromných oprávneniach pre objekty špecifikovaného typu v špecifikovanej knižnici, zložke alebo adresári. Správa zobrazuje všetky objekty špecifikovaného typu a užívateľov, ktorí majú oprávnenie na objekt. Toto je spôsob ako skontrolovať rozdielne zdroje oprávnení na objekty.

Tento príkaz vytlačí pre vybrané objekty tri správy. Prvá správa (Full Report) obsahuje všetky súkromné oprávnenia pre každý z vybraných objektov. Druhá správa (Changed Report) obsahuje dodatky a zmeny v súkromných oprávneniach na vybrané objekty, ak sa príkaz PRTPVTAUT už niekedy predtým spustil na určené objekty v špecifikovanej knižnici, zložke alebo adresári. Všetky nové objekty vybraného typu, nové oprávnenia na existujúce objekty alebo zmeny v existujúcich oprávneniach sú zobrazené v 'Changed Report'. Ak príkaz PRTPVTAUT ešte nebol spustený na vybrané objekty v určenej knižnici, zložke alebo adresári, nevytvorí sa žiaden 'Changed Report'. Ak sa príkaz už niekedy predtým spustil, ale v oprávneniach na objekty neboli spravené žiadne zmeny, 'Changed Report' sa vytlačí, ale nebudú v ňom uvedené žiadne objekty.

Tretia správa (Deleted Report) obsahuje vymazania súkromne oprávnených užívateľov z určených objektov do posledného spustenia príkazu PRTPVTAUT. Všetky objekty, ktoré boli vymazané alebo všetci odstránení používatelia, ktorí boli súkromne oprávnenými užívateľmi, sú uvedení v 'Deleted Report'. Ak príkaz PRTPVTAUT ešte nebol spustený, nevytvorí sa žiaden 'Deleted Report'. Ak sa príkaz už predtým niekedy spustil, ale na objektoch sa nevykonala žiadna operácia vymazania, 'Deleted Report' sa vytlačí, ale nebudú v ňom uvedené žiadne objekty.

**Obmedzenie:** Na použitie tohto príkazu musíte mať špeciálne oprávnenie *ALLOBJ.

**Príklady:**

Tento príkaz vytvára úplné, pozmenené a zrušené hlásenia pre všetky súborové objekty v PAYROLLLIB:

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

Tento príkaz vytvára úplné, pozmenené a zrušené hlásenia pre všetky kontinuálne súborové objekty v adresári:

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

Tento príkaz vytvára úplné, pozmenené a zrušené hlásenia pre všetky kontinuálne súborové objekty v štruktúrach podadresárov, ktoré sú spustené z adresára:

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

## Príkaz PRTPUBAUT (Print publicly authorized objects)

Príkaz PRTPUBAUT (Print Publicly Authorized Objects) vám umožňuje vytlačiť správu so špecifikovanými objektmi, ktoré nemajú verejné oprávnenie *EXCLUDE. Pre objekty *PGM sa do správy zahrnú len programy, ktoré nemajú verejné oprávnenie *EXCLUDE, ktoré môže volať užívateľ (program je buď v doméne užívateľa alebo má hodnotu systémovej bezpečnosti (systémová hodnota QSECURITY) je 30 alebo menšia). Toto je spôsob na vyhľadanie objektov, na ktoré majú povolený prístup všetci používatelia na systéme.

Tento príkaz vytlačí dve hlásenia. Prvé hlásenie (Full Report) bude obsahovať všetky zo špecifikovaných objektov, ktoré nemajú verejné oprávnenie *EXCLUDE. Druhé hlásenie (Changed Report) bude obsahovať objekty, ktoré momentálne nemajú verejné oprávnenie *EXCLUDE, ktoré mali verejné oprávnenie *EXCLUDE alebo neexistovali pri poslednom spustení príkazu PRTPUBAUT. Ak príkaz PRTPUBAUT ešte nebol predtým spustený na špecifikované objekty v knižnici, zložke alebo adresári, nevytvorí sa žiaden 'Changed Report'. Ak už bol príkaz predtým spustený, ale žiadne ďalšie objekty nemajú verejné oprávnenie *EXCLUDE, 'Changed Report' sa vytlačí, ale nebudú v ňom uvedené žiadne objekty.

**Obmedzenia:** Na použitie tohto príkazu musíte mať špeciálne oprávnenie *ALLOBJ.

**Príklady:**

Tento príkaz vytvára úplné, pozmenené a zrušené hlásenia pre všetky súborové objekty v knižnici GARRY, ktorá nemá verejné oprávnenie *EXCLUDE:

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

Tento príkaz vytvára úplné, pozmenené a zrušené hlásenia pre všetky kontinuálne súborové objekty v štruktúrach podadresárov, ktoré štartujú v adresári, ktorý nemá verejné oprávnenie *EXCLUDE:

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

## Obmedzenie prístupu k súborovému systému QSYS.LIB

Pretože koreňový súborový systém je dáždnik súborových systémov, súborový systém QSYS.LIB sa objavuje ako podadresár v koreňovom adresári. Z toho dôvodu môže každý užívateľ PC s prístupom na váš server iSeries manipulovať s objektmi, ktoré sú uložené v knižniciach servera iSeries (súborový systém QSYS.LIB) pomocou normálnych príkazov a akcií PC. Užívateľ PC by napríklad mohol presunúť objekt QSYS.LIB (ako je knižnica s vašimi dôležitými údajovými súbormi) do koša.

Ako ste sa dozvedeli v "Koreňový (/), QOpenSys a užívateľom definované súborové systémy" na strane 87, systém použije najvyššie oprávnenie na objekty bez ohľadu na to, či je viditeľné

pre rozhranie. Preto užívateľ nemôže vymazať objekt, pokiaľ užívateľ nemá na objekt oprávnenie *OBJEXIST. Ak ale vášmu iSeries viac závisí na bezpečnosti prístupu do ponúk ako na bezpečnosti objektov, užívateľ PC môže objaviť objekty v súborovom systéme QSYS.LIB, ktoré sa dajú vymazať.

Ak rozšírite použitie vášho systému a rôzne metódy prístupu, ktoré poskytujete, čoskoro zistíte, že bezpečnosť prístupu do ponúk nie je dostatočná. Kapitola 5, “Ochrana informačného majetku s oprávnením k objektu”, na strane 41 rozoberá stratégie pre doplnenie riadenia prístupu do ponúk o zabezpečenie objektov. Servery iSeries však tiež poskytujú jednoduchý spôsob, aby ste mohli obmedziť prístup do súborového systému QSYS.LIB prostredníctvom štruktúry adresára koreňového súborového systému. Na riadenie užívateľov, ktorí môžu pristúpiť do súborového systému QSYS.LIB, môžete použiť zoznam oprávnení QPWFSERVER.

Keď je užívateľove oprávnenie na QPWFSERVER zoznam oprávnení je *EXCLUDE, užívateľ nemôže vstúpiť do adresára QSYS.LIB zo štruktúry kmeňového adresára. Keď je oprávnenie užívateľa *USE, užívateľ môže vstúpiť do knižnice. Keď má užívateľ oprávnenie na vstup do adresára, pre všetky akcie, ktoré sa užívateľ pokúsi vykonať na objekte v súborovom systéme QSYS.LIB, sa použije normálne oprávnenie na objekt. Inými slovami, oprávnenie na zoznam oprávnení QPWFSERVER slúži ako dvere do celého súborového systému QSYS.LIB. Pre užívateľ s oprávnením *EXCLUDE sú tieto dvere zamknuté. Pre používateľa s oprávnením *USE (alebo ľubovoľným väčším oprávnením) sú dvere otvorené.

Vo väčšine situácií používatelia nepotrebujú použiť rozhranie adresára na prístup k objektom v súborovom systéme QSYS.LIB. Možno budete chcieť nastaviť verejné oprávnenie pre zoznam oprávnení QPWFSERVER na *EXCLUDE. Nezabudnite, že oprávnenie na zoznam oprávnení otvára alebo zatvára dvere ku knižniciam v súborovom systéme QSYS.LIB, vrátane užívateľských knižníc. Ak narazíte na užívateľov, ktorí sú predmetom tohto vylúčenia, ich požiadavky môžete vyhodnotiť jednotlivo. Ak to je vhodné, jednotlivých užívateľov môžete autorizovať na zoznam oprávnení explicitne. Musíte ale zabezpečiť, aby mal užívateľ vhodné oprávnenie na objekty v súborovom systéme QSYS.LIB. V opačnom prípade môže užívateľ neúmyselne vymazať objekty alebo celé knižnice.

**Poznámky:**

1. Pri dodaní vášho systému má verené oprávnenie na zoznam oprávnení QPWFSERVER hodnotu *USE.
2. Ak výslovne oprávnite konkrétneho užívateľa, autorizačný zoznam riadi prístup iba s obsluhou súborov iSeries Access, obsluhou súborov NetServer a obsluhou súborov medzi servermi iSeries. Toto nezabraňuje pristupovať do rovnakých adresárov cez FTP, ODBC a iné siete.

## Bezpečné adresáre

Ak pristupujete na objekt v koreňovom súborovom systéme, čítate celú cestu k tomuto objektu. Aby ste mohli prehľadať adresár, musíte mať na tento adresár oprávnenie *X (*OBJOPR a *EXECUTE). Napríklad predpokladajme, že chcete pristúpiť na nasledovný objekt:

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

Musíte mať oprávnenie *X na adresár companya a na adresár customers.

V koreňovom súborovom systéme môžete vytvoriť symbolický odkaz na objekt. Symbolický odkaz je koncepčne alias pre názov cesty. Zvyčajne je kratší a pamätá sa ľahšie, ako názov celej cesty. Symbolický odkaz ale nevytvára odlišnú fyzickú cestu k objektu. Užívateľ stále potrebuje oprávnenie *X na každý adresár a podadresár vo fyzickej ceste k objektu.

Pre objekty v koreňovom súborovom systéme môžete použiť zabezpečenie adresárov rovnako ako zabezpečenie knižníc v súborovom systéme QSYS.LIB. Napríklad, môžete nastaviť verejné oprávnenie adresára na *EXCLUDE, aby ste verejným užívateľom zabránili prístup na objekty v tomto strome.

## Bezpečnosť pre nové objekty

Je možné vytvoriť nový objekt v koreňovom súborovom systéme, rozhranie ktorého používate na vytvorenie jeho oprávnení. Napríklad, ak použijete príkaz CRTDIR a jeho štandardné vlastnosti, nový adresár zdedí všetky vlastnosti oprávnenia rodičovského adresára, vrátane súkromných oprávnení, oprávnení na primárnu skupinu a autorizačný zoznam priradení. Nasledovná časť popisuje, ako sú povolenia vyznačené pre každý typ rozhraní.

Oprávnenie sa berie z priameho rodičovského adresára, nie z vyšších adresárov tohto stromu. Preto ako správca bezpečnosti sa musíte na oprávnenie pridelené adresárom v hierarchii pozerať z dvoch pohľadov:

- Ako oprávnenie ovplyvňuje prístup na objekty v strome (ako je oprávnenie knižníc).
- Ako oprávnenie ovplyvňuje novovytvorené objekty (ako je hodnota CRTAUT pre knižnice).

**Odporúčanie:** Je možné, že budete chcieť dať užívateľom, ktorí pracujú v integrovanom súborovom systéme domáci adresár (napríklad /home/usrxxx), a potom vhodne nastaviť bezpečnosť (ako je PUBLIC *EXCLUDE). Všetky adresáre, ktoré užívateľ vytvorí v domácom adresári, budú dediť oprávnenia.

Nasledujú opisy dedenia oprávnení pre rôzne rozhrania:

### Použitie príkazu Create Directory

Keď vytvárate nový adresár pomocou príkazu CRTDIR, máte dve možnosti na špecifikovanie oprávnenia:

- Môžete špecifikovať verejné oprávnenie (oprávnenie na údaje, oprávnenie na objekty alebo oboje).
- Môžete špecifikovať *INDIR pre oprávnenie na údaje, oprávnenie na objekty alebo oboje. Keď špecifikujete *INDIR pre oba typy oprávnení, systém vytvorí presnú kópiu informácií o oprávnení z rodičovského adresára do nového objektu, vrátane zoznamu oprávnení, primárnej skupiny, verejného oprávnenia a súkromných oprávnení. (Systém neskopíruje súkromné oprávnenie, ktoré má profil QSYS alebo QSECOFR na objekt.)

### Vytvorenie adresára cez API

Keď vytvárate adresár pomocou mkdir() API, špecifikujete oprávnenie na údaje pre vlastníka, primárnu skupinu a verejné oprávnenie (pomocou mapy oprávnení *R, *W a *X). Systém na nastavenie oprávnení na objekt pre vlastníka, primárnu skupinu a verejné použije informácie z rodičovského adresára.

Pretože operačné systémy typu UNIX nemajú koncepciu oprávnení objektov, mkdir() API nepodporuje špecifikovanie oprávnení objektu. Ak chcete iné oprávnenia na objekty, môžete použiť príkaz servera iSeries (CHGAUT). Aj keď odstránite niektoré oprávnenia objektu, aplikácie typu UNIX nemusia pracovať podľa očakávaní.

### Vytvorenie súboru toku pomocou API open() alebo creat()

Keď vytvárate prúdový súbor pomocou creat() API, môžete špecifikovať oprávnenia na údaje pre vlastníka, primárnu skupinu a verejnosť (pomocou oprávnení prostredia UNIX *R, *W a *X). Systém na nastavenie oprávnení na objekt pre vlastníka, primárnu skupinu a verejné použije informácie z rodičovského adresára.

Takisto je možné špecifikovať tieto oprávnenia, keď nastavujete open() API na vytvorenie súboru toku. Je iná možnosť, keď nastavujete open() API, je možné špecifikovať, že objekt zdedí všetky oprávnenia od rodičovského adresára. Toto sa nazýva režim dedenia. Keď špecifikujete mód dedenia, systém vytvorí úplnú zhodu pre oprávnenia rodiča, vrátane zoznamu oprávnení, primárnej skupiny, verejného oprávnenia a súkromných oprávnení. Táto voľba pracuje podobne ako špecifikovanie *INDIR v príkaze CRTDIR.

### Vytvorenie objektu s použitím rozhrania PC

Keď používate aplikáciu PC na vytvorenie objektu v koreňovom súborovom systéme, systém automaticky dedí všetky oprávnenia z rodičovského adresára. Patrí sem zoznam oprávnení, primárna skupina, verejné oprávnenie a súkromné oprávnenia. Aplikácie pre PC nemajú pri vytváraní objektu žiaden ekvivalent na špecifikovanie oprávnenia.

## Súborový systém QFileSvr.400

Pomocou súborového systému QFileSvr.400 môže užívateľ (USERX) na jednom systéme iSeries (SYSTEMA) pristupovať na údaje na inom pripojenom systéme iSeries (SYSTEMB). USERX má rozhranie, ktorá sa presne podobá rozhraniu Client Access. Vzdialený server iSeries (SYSTEMB) sa objaví ako adresár so všetkými svojimi súborovými systémami ako podadresármi.

Keď sa USERX pokúša pristupovať do SYSTEMB pomocou tohto rozhrania, SYSTEMA odošle do SYSTEMB názov užívateľského profilu užívateľa USERX a zakódované heslo. Rovnaký užívateľský profil musí existovať na SYSTEMB, lebo ináč SYSTEMB odmietne požiadavku.

Ak SYSTEMB prijme požiadavku, USERX sa javí systému SYSTEMB ako každý užívateľ Client Access. Na všetky akcie, o ktoré sa pokúsi USERX, sa použije rovnaké pravidlo na kontrolu oprávnenia.

Ako správca bezpečnosti si musíte byť vedomý, že súborový systém QFileSvr.400 predstavuje ďalšie možné dvere do vášho systému. Nemôžete predpokladať, že vzdialených užívateľov obmedzíte interaktívnym prihlásením na passthrough zobrazovacej stanici. Ak máte spustený podsystém QSERVER a váš systém je pripojený do iného systému iSeries, vzdialený používatelia môžu pristupovať na váš systém, ako keby mali na lokálnom PC spustený Client Access. Je viac ako pravdepodobné, že váš systém bude mať pripojenie, ktorý vyžaduje spustený podsystém QSERVER. Toto je ďalší dôvod, prečo je podstatná dobrá schéma oprávnení objektov.

## Sieťový súborový systém

Sieťový súborový systém (NFS) poskytuje prístup do a zo systémov, ktoré majú implementácie NFS. NFS je metóda priemyselného štandardu na zdieľanie informácií medzi užívateľmi na systémoch prepojených sieťou. Väčšina operačných systémov (vrátane operačných systémov pre PC) poskytuje NFS. Pri systémoch UNIX je NFS primárnou metódou na sprístupnenie údajov. Servery iSeries sa môžu správať aj ako klient NFS client aj ako server NFS.

Keď ste správca bezpečnosti systému iSeries, ktorý vystupuje ako NFS server, musíte porozumieť a riadiť bezpečnostné aspekty NFS. Nasledujú návrhy a úvahy:

- Musíte explicitne spustiť funkciu NFS servera pomocou príkazu STRNFSSVR. Skontrolujte, kto má oprávnenie použiť tento príkaz.
- Spravte adresár alebo objekt dostupnými klientom NFS tak, že ho vyexportujete. Takto máte veľmi podrobné riadenie nad tým, ktoré časti vášho systému budú dostupné klientom NFS vo vašej sieti.
- Keď exportujete môžete špecifikovať, ktorí klienti majú prístup na objekty. Klienta identifikujete názvom systému alebo IP adresou. Klientom môže byť samostatné PC alebo celý server iSeries alebo systém UNIX. V terminológii NFS sa klient (IP adresa) nazýva stroj.
- Keď exportujete môžete špecifikovať prístup len na čítanie alebo na čítanie/zápis pre každý stroj, ktorý má prístup na vyexportovaný adresár alebo objekt. Vo väčšine prípadov budete chcieť poskytovať prístup len na čítanie.
- NFS neposkytuje ochranu hesiel. Je navrhnutý a určený na zdieľanie údajov v spoľahlivej komunite systémov. Keď užívateľ požaduje prístup, server prijme uid užívateľa. Nasledujú nejaké úvahy o uid:
  - Server iSeries sa pokúsi lokalizovať užívateľský profil s tým istým uid. Ak nájde zhodujúce sa uid, použije osobné doklady užívateľského profilu. Osobné doklady je výraz z NFS, ktorý popisuje použitie oprávnenia užívateľa. Podobá sa to na odkladanie profilu v iných aplikáciách servera iSeries.
  - Keď exportujete adresár alebo objekt môžete špecifikovať, či umožníte prístup pomocou profilu s oprávnením root. Server NFS na serveroch iSeries považuje oprávnenie root za rovnaké ako mimoriadne oprávnenie *ALLOBJ. Ak špecifikujete, že neumožníte oprávnenie root, užívateľ NFS s uid, ktoré mapuje do užívateľského profilu so špeciálnym oprávnením *ALLOBJ, nebude môcť pristupovať na objekt. A naopak, ak bude povolený anonymný prístup, žiadateľ bude zmapovaný do anonymného profilu.
  - Keď exportujete adresár alebo objekt môžete špecifikovať, či umožníte anonymné požiadavky. Anonymná požiadavka je požiadavka s uid, ktoré sa nezhoduje so žiadnym uid na vašom systéme. Ak vyberiete povolenie anonymných požiadaviek, systém mapuje anonymného užívateľa do užívateľského profilu QNFSANON dodaného IBM. Tento užívateľský profil nemá žiadne špeciálne oprávnenia alebo explicitné oprávnenie. (Pri exportovaní môžete špecifikovať iný užívateľský profil pre anonymné požiadavky, ak chcete.)
- Keď sa váš server iSeries nachádza v sieti NFS (alebo v nejakej sieti so systémami UNIX, ktoré závisia od uid), pravdepodobne namiesto povolenia systému, aby uid priradil automaticky, budete musieť riadiť svoje vlastné uid. Budete musieť skoordinovať uid s inými systémami vo vašej sieti.

  Možno zistíte, že musíte zmeniť uid (dokonca aj pre užívateľské profily dodané od IBM), aby ste zachovali kompatibilitu s ostatnými systémami vo vašej sieti. Program sa dá využiť na zjednodušenie zmenenia uid pre užívateľský profil. (Keď zmeníte uid pre profil užívateľa, musíte tiež zmeniť uid pre všetky objekty, ktoré vlastní profil v koreňovom adresári alebo adresári QOpenSrv.) Program QSYCHGID automaticky zmení uid v užívateľskom profile a všetkých vlastnených objektoch. Informácie o tom, ako sa má tento program používať nájdete v knihe *iSeries System API Reference*.

# Kapitola 12. Zabezpečenie komunikácií APPC

Keď používate váš systém v sieti s inými systémami, do vášho systému sa otvoria nové dvere a okná. Ako správca bezpečnosti by ste si mali byť vedomý možností, ktoré môžete použiť na riadenie vstupov do vášho systému v prostredí APPC.

Rozšírená medziproduktová komunikácia (APPC) je bežný spôsob, ktorým vzájomne komunikujú počítače, vrátane osobných počítačov. Prechod zobrazovacou stanicou, riadenie distribuovaných údajov a iSeries Access for Windows dokážu používať komunikácie APPC.

Nasledovné témy poskytujú niektoré základné informácie o tom, ako fungujú APPC komunikácie a ako ich môžete vhodne zabezpečiť. Tieto témy sa zameriavajú hlavne na časti konfigurácie APPC, ktoré sa týkajú bezpečnosti. Ak si chcete tento príklad prispôsobiť na vašu situáciu, budete musieť spolupracovať s ľuďmi, ktorí riadia vašu komunikačnú sieť a možno aj s poskytovateľom aplikácií. Tieto informácie použite ako základ k porozumeniu otázkam bezpečnosti a možností dostupných pre APPC.

Bezpečnosť nie je nikdy "zadarmo". Niektoré návrhy pre uľahčenie bezpečnosti siete môžu sťažiť správu siete. Napríklad, tieto informácie nekladú dôraz na APPN (Advanced Peer-to-Peer Networking), pretože bezpečnosť sa ľahšie chápe a riadi bez APPN. Avšak bez APPN musí správca siete vytvoriť konfiguračné informácie manuálne, ktoré inak APPN vytvára automaticky.

**PC tiež používajú komunikácie**

Veľa metód pre pripojenie PC k vašim serverom iSeries závisí od komunikácií, ako napríklad APPC alebo TCP/IP. Keď budete čítať nasledovné témy, určite pouvažujte o otázkach bezpečnosti pri pripájaní pomocou oboch spomenutých možností do iných systémoch a PC. Keď plánujete ochranu vašej siete presvedčte sa, že nepriaznivo neovplyvníte PC, ktoré sú pripojené do vášho systému.

## Terminológia APPC

APPC poskytuje možnosť používateľovi na jednom systéme vykonávať prácu na inom systéme. Systém, z ktorého sa spustí požiadavka sa nazýva ľubovoľne z nasledovného:

- **Zdrojový systém**
- **Lokálny systém**
- **Klient**

Systém, ktorý prijme požiadavku sa nazýva ľubovoľne z nasledovného:

- **Cieľový systém**
- **Vzdialený systém**
- **Server**

## Základné prvky komunikácií APPC

Z pohľadu správcu bezpečnosti sa musí najprv vykonať nasledovné, aby používateľ na jednom systéme (SYSTEMA) mohol vykonávať zmysluplnú prácu na inom systéme (SYSTEMB):

- Zdrojový systém (SYSTEMA) musí poskytnúť cestu do cieľového systému (SYSTEMB). Táto cesta sa nazýva **APPC relácia**.

- Cieľový systém musí identifikovať používateľa a spojiť ho s užívateľským profilom. Cieľový systém musí podporovať šifrovací algoritmus zdrojového systému (pozrite si informácie v časti “Úrovne hesla” na strane 14).
- Cieľový systém musí spustiť úlohu pre používateľa s vhodným prostredím (hodnoty riadenia práce).

Nasledovné témy rozoberajú tieto časti a ako súvisia s bezpečnosťou. Správca bezpečnosti na cieľovom systéme má hlavnú zodpovednosť za zabezpečenie toho, aby používatelia APPC nenarušili bezpečnosť. Keď správcovia bezpečnosti na oboch systémoch pracujú spolu, úloha správa bezpečnosti APPC je oveľa ľahšia.

## Príklad: Základná relácia APPC

V prostredí APPC, keď užívateľ alebo aplikácia na jednom systéme požaduje prístup na ďalší systém, tieto dva systémy vytvoria reláciu. Aby sa vytvorila relácia, systémy musia spojiť dva zhodujúce sa opisy zariadení APPC. Parameter názov vzdialeného umiestnenia (RMTLOCNAME) v opise zariadenia na SYSTEMA sa musí zhodovať s parametrom názov lokálneho umiestnenia (LCLLOCNAME) v opise zariadenia na SYSTEMB a naopak.

Aby dva systémy vytvorili APPC reláciu, heslá umiestnení v opisoch zariadení APPC na SYSTEMA a SYSTEMB musia byť identické. Obe musia špecifikovať *NONE alebo rovnakú hodnotu.

Ak majú heslá inú hodnotu ako *NONE, ukladajú a prenášajú sa v zakódovanom formáte. Ak sa heslá zhodujú, systémy vytvoria reláciu. Ak sa heslá nezhodujú, požiadavky užívateľa sa odmietne. Keď systémy špecifikujú na vytvorenie relácie heslá umiestnení, nazýva sa to **bezpečná väzba**.

**Poznámka:** Nie všetky počítačové systémy poskytujú funkciu bezpečnej väzby.

### Obmedzenie relácií APPC

Ako správca bezpečnosti na zdrojovom systéme môžete použiť oprávnenia objektu na riadenie toho, kto sa môže pokúšať pristupovať na iné systémy. Nastavte verejné oprávnenie pre opisy zariadení APPC na *EXCLUDE a konkrétnym užívateľom dajte oprávnenie *CHANGE. Aby ste zabránili užívateľom so špeciálnym oprávnením *ALLOBJ používať APPC komunikácie, použite systémovú hodnotu QLMTSECOFR.

Ako správca bezpečnosti na cieľovom systéme tiež môžete použiť oprávnenie na zariadenia APPC, aby ste zakázali užívateľom spúšťať APPC relácia na vašom systéme. Musíte porozumieť, aké ID užívateľa sa bude pokúšať pristupovať na opis zariadenia APPC. “Prístup užívateľa APPC na cieľový systém” na strane 97 opisuje, ako servery iSeries pridružujú ID užívateľa k požiadavke na reláciu APPC.

**Poznámka:** Ak chcete zistiť, kto má oprávnenie na opisy zariadenia vašom systéme, môžete použiť príkazy PRTPUBAUT *DEVD (Print Publicly Authorized Objects) a PRTPVTAUT *DEVD (Print Private Authorities).

Keď váš systém používa APPN, automaticky vytvorí nové APPC zariadenie , keď pre cestu vybranú systémom neexistuje žiadne dostupné zariadenie. Jedna metóda pre obmedzenie prístupu na APPN zariadenia na systéme je použitie APPN na vytvorenie autorizačného zoznamu. Zoznam oprávnení obsahuje zoznam užívateľov, ktorí by mali byť oprávnení na zariadenia APPC. Použite príkaz CHGCMDDFT (Change Command Default) na zmenu príkazu CRTDEVAPPC. Pre parameter oprávnenia (AUT) v príkaze CRTDEVAPPC nastavte štandardnú hodnotu na zoznam oprávnení, ktorý ste vytvorili.

**Poznámka:** Ak váš systém má iný jazyk ako anglický, musíte zmeniť štandardné nastavenie príkazu v knižnici QSYSxxxx pre každý národný jazyk, ktorý je na vašom systéme.

Parameter heslo umiestnenia (LOCPWD) v opise zariadenia APPC použite na overenie identity iného systému, ktorý požaduje reláciu na vašom systéme (pre užívateľa alebo aplikáciu). Heslo umiestnenia vám pomôže zistiť falošný systém.

Keď používate heslá umiestnení, musíte spolupracovať so správcami bezpečnosti iných systémov v sieti. Tiež musíte riadiť, kto môže vytvárať alebo meniť opisy zariadení APPC a konfiguračné zoznamy. Systém vyžaduje špeciálne oprávnenie *IOSYSCFG, aby mohol používať príkazy, ktoré pracujú so zariadeniami APPC a konfiguračnými zoznamami.

**Poznámka:** Keď používate APPN, umiestnenia hesiel sa ukladajú v konfiguračnom zozname QAPPNRMT, nie v opisoch zariadení.

## Prístup užívateľa APPC na cieľový systém

Keď systémy vytvárajú APPC reláciu, vytvoria cestu pre žiadajúceho užívateľa k dverám cieľového systému. Niekoľko iných častí určí, čo musí užívateľ spraviť, aby získal vstup do iného systému.

Nasledovné témy opisujú časti určujúce ako užívateľ APPC získa vstup do cieľového systému.

### Systémové metódy pre odosielanie informácií o užívateľovi

Architektúra APPC poskytuje tri metódy pre odoslanie bezpečnostných informácií o užívateľovi zo zdrojového systému do cieľového systému. Na tieto metódy sa odvoláva ako na **naprojektované bezpečnostné hodnoty**. Tabuľka 18 ukazuje tieto metódy:

**Poznámka:** Kniha *APPC Programming* poskytuje o naprojektovaných bezpečnostných hodnotách viac informácií.

*Tabuľka 18. Bezpečnostné hodnoty v architektúre APPC*

| Navrhnutá bezpečnostná hodnota | ID užívateľa odoslané do cieľového systému | Heslo odoslané do cieľového systému |
|---|---|---|
| Žiadne | Nie | Nie |
| Rovnaké | Áno[1] | Viď poznámku 2. |
| Program | Áno | Áno[3] |

**Poznámky:**

1. Zdrojový systém pošle ID užívateľa, ak cieľový systém špecifikuje SECURELOC(*YES) alebo SECURELOC(*VFYENCPWD).
2. Užívateľ v žiadosti nezadáva heslo, pretože heslo je už overené zdrojovým systémom. Pre SECURELOC(*YES) a SECURELOC(*NO), zdrojový systém neposiela heslo. Pre SECURELOC(*VFYENCPWD), zdrojový systém získa uložené zakódované heslo a odošle ho (v zakódovanej forme).
3. Ak zdrojový i cieľový systém podporuje šifrovanie hesla, systém odošle heslo v zašifrovanom formáte. V opačnom prípade sa heslo nezakóduje.

Požadovaná aplikácia užívateľov zistí naprojektované bezpečnostné hodnoty. Napríklad, SNADS vždy používa SECURITY(NONE). DDM používa SECURITY(SAME). Pomocou passthrough zobrazovacej stanice užívateľ špecifikuje bezpečnostnú hodnotu pomocou parametrov príkazu STRPASTHR.

Vo všetkých prípadoch systém vyberá pomocou bezpečnostnej hodnoty špecifikovanej na systéme, či prijme požiadavku. V niektorých situáciách môže cieľový systém úplne odmietnuť požiadavku. V iných situáciách môže vnútiť inú bezpečnostnú hodnotu. Napríklad, keď užívateľ špecifikuje ID užívateľa aj heslo v príkaze STRPASTHR, požiadavka použije SECURITY(PGM). Ak systémová hodnota QRMTSIGN na cieľovom systéme *FRCSIGNON, užívateľ vidí prihlasovaciu obrazovku. S nastavením *FRCSIGNON systém vždy používa SECURITY(NONE), čo je ekvivalent zadania ID užívateľa a hesla užívateľom v príkaze STRPASTHR.

**Poznámky:**

1. Zdrojové a cieľové systémy si pred odoslaním údajov potvrdzujú bezpečnostnú hodnotu. V situácii, keď cieľový systém špecifikuje SECURELOC(*NO) a požiadavka je SECURITY(SAME), napríklad cieľový systém hovorí zdrojovému systému, aby použil SECURITY(NONE). Zdrojový systém nepošle ID užívateľa.
2. Keď užívateľskému heslu na cieľovom systéme skončila platnosť, cieľový systém odmietne požiadavku na reláciu. Toto sa týka len pripojení posielajúcich heslá, vrátane nasledovného:
   - Požiadavky na reláciu typu SECURITY(PROGRAM).
   - Požiadavky na reláciu typu SECURITY(SAME), keď hodnota SECURELOC je *VFYENCPWD.

## Voľby pre delenie zodpovednosti za bezpečnosť siete

Keď sa váš systém nachádza v sieti, musíte sa rozhodnúť, či sa na overenie identity užívateľov, ktorí sa pokúšajú vstúpiť do vášho systému, spoľahnete na iné systémy. Uveríte, že SYSTEMA zaručí, že USERA je skutočne USERA (alebo QSECOFR je skutočne QSECOFR)? Alebo budete znovu požadovať od užívateľa jeho ID a heslo?

Parameter bezpečné umiestnenie (SECURELOC) v opise zariadenia APPC na cieľovom systéme určuje, či je zdrojový systém bezpečné (dôveryhodné) umiestnenie.

Keď majú obidva systémy spustené vydanie, ktoré podporuje *VFYENCPWD, potom SECURELOC(*VFYENCPWD) poskytuje dodatočnú ochranu, keď aplikácie používajú SECURITY(SAME). Hoci požadovateľ nezadá v požiadavke heslo, zdrojový systém získa heslo užívateľa a pošle ho s požiadavkou. Aby bola požiadavka úspešná, užívateľ musí mať rovnaké ID užívateľa a heslo na oboch systémoch.

Keď cieľový systém špecifikuje SECURELOC(*VFYENCPWD) a zdrojový systém túto hodnotu nepodporuje, cieľový systém spracuje požiadavku ako SECURITY(NONE).

Tabuľka 19 ukazuje, ako spolu pracujú naprojektované bezpečnostné hodnoty a hodnota SECURELOC:

*Tabuľka 19. Ako spolu fungujú bezpečnostná hodnota APPC a hodnota SECURELOC*

| **Zdrojový systém** | **Cieľový systém** | |
|---|---|---|
| **Navrhnutá bezpečnostná hodnota** | **Hodnota SECURELOC** | **Užívateľský profil pre úlohu** |
| Žiadne | Ľubovoľný | Štandardný užívateľ[1] |

*Tabuľka 19. Ako spolu fungujú bezpečnostná hodnota APPC a hodnota SECURELOC (pokračovanie)*

| Zdrojový systém | Cieľový systém | |
|---|---|---|
| **Navrhnutá bezpečnostná hodnota** | **Hodnota SECURELOC** | **Užívateľský profil pre úlohu** |
| Rovnaké | *NO | Štandardný užívateľ[1] |
| | *YES | Rovnaký názov užívateľského profilu ako požadovateľ zo zdrojového systému. |
| | *VFYENCPWD | Rovnaký názov užívateľského profilu ako požadovateľ zo zdrojového systému. Užívateľ musí mať na oboch systémoch rovnaké heslo. |
| Program | Ľubovoľný | Užívateľský profil, ktorý je špecifikovaný v požiadavke zo zdrojového systému. |

**Poznámky:**

1. Štandardný užívateľ sa určí komunikačnou položkou v opise podsystému. Toto opisuje "Pridelenie užívateľských profilov cieľového systému pre úlohy".

## Pridelenie užívateľských profilov cieľového systému pre úlohy

Keď užívateľ požaduje na inom systéme úlohu APPC, požiadavka má so sebou spojený názov módu. Názov módu môže prísť z požiadavky užívateľa alebo to môže byť štandardná hodnota zo sieťových atribútov zdrojového systému.

Cieľový systém používa názov módu a názov zariadenia APPC na určenie spôsobu spustenia úlohy. Cieľový systém pohľadá v aktívnych podsystémoch komunikačnú položku, ktorá najlepšie vyhovuje názvu zariadenia APPC a názvu módu.

Komunikačná položka špecifikuje, ktorý užívateľský profil bude systém používať pre požiadavky SECURITY(NONE). Nasleduje príklad komunikačnej položky v opise 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
```

Tabuľka 20 zobrazuje možné hodnoty pre parameter štandardného užívateľa v komunikačnej položke:

*Tabuľka 20. Možné hodnoty pre parameter štandardného užívateľa*

| Hodnota | Výsledok |
|---|---|
| ***NONE** | Nie je k dispozícii žiaden štandardný užívateľ. Ak zdrojový systém neposkytne v požiadavke ID užívateľa, úloha sa nespustí. |
| ***SYS** | Spustia sa len programy (systémové úlohy) od IBM. Nespustia sa žiadne užívateľské aplikácie. |
| *meno-užívateľa* | Ak zdrojový systém nepošle ID užívateľa, úloha sa spustí pod týmto užívateľským profilom. |

Na vytlačenie všetkých komunikačných podsystémov, ktoré majú položky so štandardným užívateľským profilom, môžete použiť príkaz PRTSBSDAUT (Print Subsystem Description).

## Voľby passthrough zobrazovacej stanice

Passthrough zobrazovacia stanica je príkladom aplikácie, ktorá používa APPC komunikáciu. Passthrough zobrazovaciu stanicu môžete použiť na prihlásenie sa do iného systému, ktorý je k vášmu systému pripojený cez sieť.

Tabuľka 21 ukazuje príklady passthrough požiadaviek (príkaz STRPASTHR) a ako ich cieľový systém spracováva. Pre passthrough zobrazovaciu stanicu používa systém základné časti APPC komunikácií a systémovú hodnotu pre vzdialené prihlasovanie (QRMTSIGN).

**Poznámka:** Požiadavky passthrough zobrazovacej stanice už nie sú smerované cez podsystémy QCMN alebo QBASE. Počínajúc s V4R1 sú smerované cez podsystém QSYSWRK. Mohli by sme predpokladať, že ak nemáme spustené podsystémy QCMD alebo QBASE, passthrough zobrazovacia stanica nebude fungovať. Toto neplatí. Je možné presmerovať túto funkciu na použitie QCMN (alebo QBASE, ak je aktívny), a to zmenením systémovej hodnoty QPASTHRSVR na 0.

*Tabuľka 21. Vzorové pass-through požiadavky na prihlásenie*

| **Hodnoty v príkaze STRPASTHR** | | **Cieľový systém** | | |
|---|---|---|---|---|
| **ID užívateľa** | **Heslo** | **Hodnota SECURELOC** | **Hodnota QRMTSIGN** | **výsledok** |
| *NONE | *NONE | Ľubovoľný | Ľubovoľný | Používateľ sa musí prihlásiť na cieľovom systéme. |
| Názov užívateľského profilu | Nezadané | Ľubovoľný | Ľubovoľný | Požiadavka zlyhá. |
| *CURRENT | Nezadané | *NO | Ľubovoľný | Požiadavka zlyhá |
| | | *YES | *SAMEPRF | Interaktívna úloha sa spúšťa s rovnakým názvom užívateľského profilu ako má užívateľský profil v zdrojovom systéme. Heslo nie je posielané na vzdialený systém. Názov užívateľského profilu musí existovať na cieľovom systéme. |
| | | | *VERIFY | |
| | | | *FRCSIGNON | Používateľ sa musí prihlásiť na cieľovom systéme. |
| | | *VFYENCPWD | *SAMEPRF | Interaktívna úloha sa spúšťa s rovnakým názvom užívateľského profilu ako má užívateľský profil v zdrojovom systéme. Zdrojový systém získa heslo používateľa a odošle ho do vzdialeného systému. Názov užívateľského profilu musí existovať na cieľovom systéme. |
| | | | *VERIFY | |
| | | | *FRCSIGNON | Používateľ sa musí prihlásiť na cieľovom systéme. |

*Tabuľka 21. Vzorové pass-through požiadavky na prihlásenie (pokračovanie)*

| Hodnoty v príkaze STRPASTHR | | Cieľový systém | | |
|---|---|---|---|---|
| **ID užívateľa** | **Heslo** | **Hodnota SECURELOC** | **Hodnota QRMTSIGN** | **výsledok** |
| *CURRENT (alebo názov súčasného užívateľského profilu pre úlohu) | Zadaná | Ľubovoľný | *SAMEPRF | Interaktívna úloha sa spúšťa s rovnakým názvom užívateľského profilu ako má užívateľský profil v zdrojovom systéme. Heslo *je* posielané na vzdialený systém. Názov užívateľského profilu musí existovať na cieľovom systéme. |
| | | | *VERIFY | |
| | | | *FRCSIGNON | Používateľ sa musí prihlásiť na cieľovom systéme. |
| Názov užívateľského profilu (názov odlišný od súčasného užívateľského profilu pre úlohu) | Zadaná | Ľubovoľný | *SAMEPRF | Požiadavka zlyhá. |
| | | | *VERIFY | Interaktívna úloha sa spúšťa s rovnakým názvom užívateľského profilu ako má užívateľský profil v zdrojovom systéme. Heslo *je* posielané na vzdialený systém. Názov užívateľského profilu musí existovať na cieľovom systéme. |
| | | | *FRCSIGNON | Interaktívna úloha sa spustí so špecifikovaným názvom užívateľského profilu. Heslo je zaslané do cieľového systému. Názov užívateľského profilu musí existovať na cieľovom systéme. |

## Predchádzanie neočakávaných priradení zariadenia

Keď sa na aktívnom zariadení vyskytne zlyhanie, systém sa ho pokúsi opraviť. V niektorých prípadoch pri prerušení pripojenia môže iný užívateľ mimovoľne opätovne vytvoriť reláciu, ktorá zlyhala. Napríklad predpokladajme, že USERA vypol pracovnú stanicu bez toho, aby sa odhlásil. USERB by mohol zapnúť pracovnú stanicu a opätovne spustiť reláciu užívateľa USERA bez toho, aby sa prihlásil.

Aby ste tejto možnosti zabránili, nastavte systémovú hodnotu QDEVRCYACN (Device I/O Error Action) na *DSCMSG. Keď zariadenie zlyhá, systém ukončí úlohu užívateľa.

## Riadenie vzdialených príkazov a dávkových úloh

Na riadenie toho, čo na vašom systéme môžu spúšťať vzdialené príkazy a úlohy, vám pomôže niekoľko volieb, vrátane nasledovných:

- Ak váš systém používa DDM, môžete obmedziť prístup na súbory DDM tak, že zakážete užívateľom použiť príkaz SBMRMTCMD (Submit Remote Command) z iného systému. Aby sa dal použiť príkaz SBMRMTCMD, užívateľ musí vedieť otvoriť súbor DDM. Musíte tiež obmedziť schopnosť vytváranie súborov DDM.
- Pre systémovú hodnotu DDM request access (DDMACC) môžete špecifikovať ukončovací program. V ukončovacom programe môžete vyhodnotiť všetky požiadavky DDM predtým ako ich povolíte.
- Sieťový atribút JOBACN (network job action) môžete použiť na zabránenie vydania sieťových úloh alebo zabránenie ich automatického spúšťania.

- Aké požiadavky na programy sa môžu spustiť v komunikačnom prostredí môžete explicitne špecifikovať odstránením smerovacej položky PGMEVOKE z opisov podsystému. Smerovacia položka PGMEVOKE umožňuje požadovateľovi špecifikovať program, ktorý sa má spustiť. Keď odstránite túto smerovaciu položku z opisov podsystému, ako je opis podsystému QCMN, musíte pridať smerovacie položky pre komunikačné požiadavky, ktoré sa musia spustiť úspešne.

  "Navrhnuté požiadavky TPN" na strane 80 zobrazuje názvy programov pre komunikačné požiadavky aplikácií dodaných IBM. Pre každú požiadavku, ktorú chcete povoliť, môžete pridať položku s hodnotou na porovnanie a názvom programu, pričom obe sa rovnajú názvu programu.

  Keď používate túto metódu, musíte porozumieť prostrediu riadenia prác na vašom systéme a typy komunikačných požiadaviek, ktoré sa vyskytujú na vašom systéme. Ak to je možné, mali by ste otestovať všetky typy komunikačných požiadaviek aby ste sa uistili, že pracujú správne po vami vykonanej zmene smerovacích položiek. Keď komunikačná požiadavka nenájde dostupnú smerovaciu položku, dostanete správu CPF1269. Inou alternatívou (menej chybovou, ale možno menej efektívnou) je nastavenie verejného oprávnenia na *EXCLUDE pre transakčné programy, ktoré nechcete spúšťať na svojom systéme.

  **Poznámka:** Kniha *Work Management* poskytuje viac informácií o smerovacích položkách a ako systém spracováva požiadavky na spustenie programov.

## Zhodnotenie konfigurácie vášho APPC

Na vytlačenie hodnôt týkajúcich sa bezpečnosti vo vašej konfigurácii APPC môžete použiť príkaz PRTCMNSEC (Print Communications Security) alebo voľby ponuky. Nasledovné témy popisujú informácie v správach.

### Príslušné parametre pre zariadenia APPC

Obrázok 9 ukazuje príklad správy s informáciami o komunikácii pre opisy zariadení. Obrázok 10 na strane 103 ukazuje príklad správy pre konfiguračné zoznamy. Za správami sú uvedené vysvetlenia jednotlivých polí správ.

```
                          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
```

*Obrázok 9. Príklad správy opisov APPC zariadení*

```
                  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
```

*Obrázok 10. Správa konfiguračný zoznam-Príklad*

## Pole Secure location

Pole SECURELOC (secure location) určuje, či sa lokálny systém spolieha na overenie hesiel pre lokálny systém vzdialeným systémom. Pole SECURELOC sa používa len pre aplikácie, ktoré používajú hodnotu SECURITY(SAME), ako sú DDM a aplikácie používajúce CPI-komunikačné API.

SECURELOC(*YES) robí lokálny systém zraniteľný pre možné slabiny vo vzdialenom systéme. Každý používateľ, ktorý existuje na oboch systémoch, môže volať programy na lokálnom systéme. Toto je obzvlášť nebezpečné, pretože užívateľský profil QSECOFR (security officer) existuje na všetkých systémoch iSeries a má špeciálne oprávnenie *ALLOBJ. Ak systém v sieti sa dobre nestará o chránenie hesla QSECOFR, iné systémy považujúce tento systém za bezpečné umiestnenie sú ohrozené.

Keď použijete SECURELOC(*VFYENCPWD), váš systém je menej zraniteľný inými systémami, ktoré si primerane nechránia heslá. Používateľ požadujúci aplikáciu, ktorá používa SECURITY(SAME), musí mať na oboch systémoch rovnaké užívateľské ID a heslo. SECURELOC(*VFYENCPWD) vyžaduje vo vašej sieti politiky na správu hesiel, aby mali používatelia rovnaké heslo na všetkých systémoch.

**Poznámka:** SECURELOC(*VFYENCPWD) je podporovaný len medzi systémami, ktoré na ktorých je V3R2, V3R7 alebo V4R1. Ak cieľový systém špecifikuje SECURELOC(*VFYENCPWD) a zdrojový systém túto funkciu nepodporuje, požiadavka sa berie ako SECURITY(NONE).

Ak systém špecifikuje SECURELOC(*NO), aplikácie používajúce SECURITY(SAME) budú na spustenie programov vyžadovať štandardného používateľa. Štandardný používateľ závisí na opise zariadenia aj móde, ktoré sú spojené s požiadavkou. (Pozrite si “Pridelenie užívateľských profilov cieľového systému pre úlohy” na strane 99.)

## Pole Location password

Toto pole určuje, či si dva systémy vymenia heslá za účelom overenia, že žiadajúci systém nie je falošný. “Príklad: Základná relácia APPC” na strane 96 poskytuje viac informácií o heslách umiestnení.

### Pole APPN Capable

Pole APPN-capable (APPN) zadáva, či vzdialený systém dokáže podporovať rozšírené funkcie sieťovania alebo je obmedzený na jednoskokové pripojenia. APPN(*YES) znamená nasledovné:

- Ak je vzdialený systém sieťový uzol, môže vedieť pripájať lokálny systém k iným systémom. Toto sa nazýva **smerovanie prostredným uzlom**. Znamená to, že používatelia na vašom systéme môže použiť vzdialený systém ako cestu do väčšej siete.
- Ak je lokálny systém sieťový uzol, vzdialený systém môže použiť lokálny systém na pripojenie k iným systémom. Používatelia na vzdialenom systéme môžu používať váš systém ako cestu do väčšej siete.

**Poznámka:** Či je systém sieťový alebo koncový uzol zistíte pomocou príkazu DSPNETA.

### Pole Single session

Pole SNGSSN (single session) určuje, či vzdialený systém môže naraz spustiť viac ako jednu reláciu pomocou rovnakého opisu APPC zariadenia. Bežne sa používa SNGSSN(*NO), pretože odstraňuje potrebu vytvorenia viacerých opisov zariadení pre vzdialený systém. Napríklad, používateľ PC chce často viac ako jednu reláciu emulácie 5250 a reláciu pre funkcie súborového a tlačového servera. Pomocou SNGSSN(*NO) môžete poskytnúť túto funkciu s jedným opisom zariadenia pre PC na systéme iSeries.

SNGSSN(*NO) znamená, že sa musíte spoľahnúť na bezpečné operačné procedúry od používateľov PC a iných používateľov APPC. Váš systém je zraniteľný každým na vzdialenom systéme, kto spustí neoprávnenú reláciu používajúcu rovnaký opis zariadenia ako existujúca relácia. (Táto praktika sa niekedy nazýva **piggy-backing**.)

### Pole Pre-establish session

Pole PREESTSSN (pre-establish session) pre jednu reláciu zariadenia riadi, či lokálny systém spustí reláciu so vzdialeným systémom, keď vzdialený systém prvýkrát kontaktuje lokálny systém. PREESTSSN(*NO) znamená, že lokálny systém čaká na spustenie relácie, kým aplikácia nepožiada o reláciu so systémom. PREESTSSN(*YES) je užitočný pre minimalizovanie čakania aplikačného programu na dokončenie pripojenia.

PREESTSSN(*YES) zabraňuje systému odpojiť prepínanú linku (telefonickú), ak sa už ďalej nepoužíva. Aplikácia alebo používateľ musia linku vypnúť explicitne. PREESTSSN(*YES) môže predĺžiť čas, počas ktorého je zraniteľný cez piggy-backing na reláciu.

### Pole SNUF Program start

Pole SNUF program start field určuje, či má vzdialený systém povolené spúšťať programy na lokálnom systéme. *YES znamená, že schéma oprávnenia objektov na lokálnom systéme musí byť primeraná na ochranu objektov, keď používatelia na vzdialenom systéme spustia úlohy a spustia programy na lokálnom systéme.

## Parametre pre radiče APPC

Obrázok 11 na strane 105 ukazuje príklad správy s informáciami o komunikácii pre opisy radičov. Keď budete prechádzať správou, nájdete vysvetlené všetky polia v správe.

```
                          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
```

*Obrázok 11. Príklad správy opisov APPC radičov*

### Pole Auto-create

V opise linky pole auto-create (AUTOCRTCTL) určuje, či lokálny systém automaticky vytvorí opis radiča, keď prichádzajúca požiadavka nemôže nájsť vyhovujúci opis radiča. V opise radiča pole auto-create (AUTOCRTDEV) určuje, či lokálny systém automaticky vytvorí opis zariadenia, keď prichádzajúca požiadavka nemôže nájsť vyhovujúci opis zariadenia.

Pre radiče vhodné pre APPN nemá pole auto-create žiaden význam. Systém automaticky vytvorí opisy zariadení podľa potreby bez ohľadu na to, ako ste nastavili pole auto-create field.

Keď špecifikujete *YES pre opis linky, do vášho systému sa môže pripojiť hocikto s prístupom na linku. Patria sem miesta, ktoré sú mosty a smerovače.

### Pole Control point sessions

Pre radiče vyhovujúce APPN pole control point session (CPSSN) určuje, či systém vytvorí APPC pripojenie so vzdialeným systémom automaticky. Systém používa CP reláciu na výmenu informácií o sieti a stave so vzdialeným systémom. Výmena najnovších informácie medzi sieťovými uzlami APPN je hlavne dôležitá pre bezchybnú činnosť siete.

Keď špecifikujete *YES, nečinnosť na prepájanej linke nespôsobí automatické odpojenie. Toto robí váš systém zraniteľnejší pre vykonanie piggy-back na reláciu.

### Pole Disconnect timer

Pre APPC radič pole disconnect timer určuje ako dlho musí byť radič nepoužívaný (žiadne aktívne relácie), aby systém odpojil linku do vzdialeného systému. Toto pole má dve hodnoty. Prvá hodnota špecifikuje, ako dlho zostane radič aktívny od času, keď bol prvýkrát skontaktovaný. Druhá hodnota určuje, ako dlho čaká systém po dokončení poslednej relácie predtým ako preruší linku.

Systém používa časovač pre odpojenie len vtedy, keď pole switched disconnect (SWTDSC) je *YES.

Ak spravíte tieto hodnoty veľkými, systém je zraniteľnejší na vykonanie piggy-back na reláciu.

## Parametre pre opisy liniek

Obrázok 12 na strane 106 ukazuje príklad správy s informáciami o komunikácii pre opisy liniek. Keď budete prechádzať správou, nájdete vysvetlené všetky polia v správe.

```
                          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
```

*Obrázok 12. Príklad správy opisov APPC liniek*

## Pole Auto answer

Pole AUTOANS (auto answer) určuje, či prepájaná linka bude akceptovať prichádzajúce volania bez zásahu operátora.

Keď špecifikujete *YES, váš systém je menej bezpečný, pretože sa naň dá ľahšie pristupovať. Aby ste minimalizovali ohrozenie bezpečnosti pri špecifikovaní *YES, mali by ste vypnúť linku, keď ju nepotrebujete.

## Pole Auto dial

Pole AUTODIAL (auto dial) určuje, či prepájaná linka môže uskutočňovať odchádzajúce volania bez zásahu operátora. Keď špecifikujete *YES, umožníte lokálnym užívateľom bez fyzického prístupu na komunikačné linky a modemov pripájať sa do iných systémov.

# Kapitola 13. Zabezpečenie komunikácií TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) je bežný spôsob, ktorým vzájomne komunikujú počítače všetkých typov. TCP/IP aplikácie sú dobre známe a značne používané na "informačnej diaľnice".

Táto kapitola poskytuje tipy pre nasledovné:

- Zabránenie spusteniu TCP/IP aplikáciám na vašom systéme.
- Chránenie systémových prostriedkov, keď na vašom systéme umožníte spúšťanie TCP/IP aplikácií.

Webová stránka iSeries Information Center—>Networking—>TCP/IP je kompletným zdrojom pre informácie o všetkých aplikáciách TCP/IP. *SecureWay: iSeries a Internet* (Informačné centrum iSeries —>Bezpečnosť—>SecureWay popisuje úvahy o bezpečnosti v prípade, keď váš server iSeries pripojíte buď na internet (veľmi veľká sieť TCP/IP) alebo k intranetu. Pozrite si "Nevyhnutné predpoklady a súvisiace informácie" na strane xii, kde nájdete informácie o sprístupňovaní informačného centra iSeries.

Pamätajte si, že servery iSeries podporujú mnoho možných použití TCP/IP. Keď sa rozhodnete na svojom systéme povoliť jednu TCP/IP aplikáciu, možno tiež povolíte aj iné TCP/IP aplikácie. Ako správca bezpečnosti si musíte byť vedomý rozsahu TCP/IP aplikácií a bezpečnostných implikácií týchto aplikácií.

## Zabránenie spracovaniu TCP/IP

Úlohy TCP/IP servera sa spúšťajú v podsystéme QSYSWRK. Na spustenie TCP/IP na vašom systéme použite príkaz STRTCP (Start TCP/IP). Ak nechcete žiadne spracovanie TCP/IP alebo spúšťať aplikácie, nepoužite príkaz STRTCP. Váš systém je dodaný s verejným oprávnením pre príkaz STRTCP nastaveným na *EXCLUDE.

Ak máte podozrenie, že niekto s prístupom na príkaz spúšťa TCP/IP (napríklad mimo pracovných hodín), nastavte auditovanie objektu pre príkaz STRTCP. Systém zaznačí auditovú žurnálovú položku pri každom spustení príkazu užívateľom.

## Komponenty bezpečnosti TCP/IP

Môžete využiť niekoľko komponentov bezpečnosti TCP/IP, ktoré rozširujú bezpečnosť vašej siete a pridávajú jej flexibilitu. Hoci niektoré z týchto technológií nájdete aj v produktoch firewall, tieto komponenty bezpečnosti TCP/IP pre OS/400 nie sú určené, aby sa používali ako firewall. Aj keď v niektorých prípadoch môžete použiť niektoré z týchto funkcií na odstránenie potreby samostatného firewall produktu. Tieto funkcie TCP/IP tiež môžete použiť na poskytnutie dodatočnej bezpečnosti v prostrediach, kde už používate firewall.

Na vylepšenie bezpečnosti TCP/IP sa môžu využiť nasledovné komponenty:

- Packet Rules
- HTTP Proxy Server
- VPN (virtual private networking)
- SSL (secure sockets layer)

## Packet rules použite na zabezpečenie premávky TCP/IP

Packet rules, ktoré sú kombináciou filtrovania IP a NAT (network address translation) sa správajú ako firewall, aby ochránili vašu internú sieť pred votrelcami. Filtrovanie IP vám umožňuje riadiť premávku IP, ktorú môžete dovoliť do a z vašej siete. V zásade vašu sieť chráni pomocou filtrovania paketov podľa pravidiel, ktoré zadefinujete. NAT vám na druhej strane umožňuje skryť vaše nezaregistrované súkromné adresy IP za sadu zaregistrovaných adries IP. To pomáha chrániť vašu internú sieť pred externými sieťami. NAT tiež pomáha zmierniť problém s vyčerpaním adries IP, pretože mnoho súkromných adries môže byť zastúpených malou množinou zaregistrovaných adries. Viac informácií nájdete v informačnom centre iSeries .

## HTTP proxy server

HTTP proxy server sa dodáva s IBM HTTP Server pre server iSeries. HTTP Server je súčasťou OS/400. Proxy server prijíma HTTP požiadavky z webových prehliadačov a rozposiela ich webovým serverom. Webové servery, ktoré prijmú požiadavky vidia len IP adresu proxy servera a nemôžu určiť názvy alebo adresy PC, ktoré vydali požiadavky. Proxy server môže spracovať požiadavky URL pre HTTP, FTP, Gopher a WAIS.

Proxy server si uchováva vrátené webové stránky z požiadaviek všetkých používateľov proxy servera. Preto keď používatelia pošlú požiadavku na stránku, proxy server skontroluje, či je v stránka vo vyrovnávacej pamäti. Ak je, proxy server vráti stránku z tejto pamäte. Použitím stránok z vyrovnávacej pamäte môže proxy server poskytovať webové stránky oveľa rýchlejšie, čím sa odstraňujú možné dlhotrvajúce požiadavky na webový server.

Proxy server tiež zaznamenáva všetky požiadavky URL za účelom sledovania. Protokoly si môžete prezrieť za účelom monitorovania a nesprávneho používania prostriedkov siete.

Podporu HTTP proxy môžete použiť v IBM HTTP Server na zabezpečenie prístupu z WWW. Adresy PC klientov sa pred webovými servermi, na ktoré pristupujú, skrývajú; známa je len IP adresa proxy servera. Použitie vyrovnávacej pamäte pre webové stránky redukuje šírku pásma požiadaviek a zaťaženie firewallu. Pozrite si domovskú stránku IBM HTTP Server for iSeries, kde nájdete viac informácií: http://www-1.ibm.com/servers/eserver/iseries/software/http/index.html

## VPN (Virtual Private Networking)

VPN (virtual private network) umožňuje vášmu podniku bezpečne rozšíriť svoj súkromný intranet v existujúcom rámci verejnej siete, ako je napríklad internet. S VPN môže váš podnik riadiť premávku siete pričom budú poskytované dôležité funkcie bezpečnosti, ako napríklad autentifikácia a súkromnosť údajov.

OS/400 VPN je voliteľne inštalovateľný komponent iSeries Navigator, grafického užívateľského rozhrania (GUI) pre OS/400. Umožňuje vám vytvoriť bezpečnú cestu medzi ľubovoľnou kombináciou hostiteľa a brány po celej dĺžke. OS/400 VPN používa autentifikačné metódy, šifrovacie algoritmy a iné opatrenia na zabezpečenie, že údaje posielané medzi dvoma koncovými bodmi jeho pripojenia zostávajú bezpečné.

VPN sa spúšťa na sieťovej vrstve modelu zásobníka vrstvovej komunikácie TCP/IP. Presnejšie, VPN používa otvorený rámec IPSec (IP Security Architecture). IPSec poskytuje funkcie základnej bezpečnosti pre internet, a rovnako predkladá flexibilné stavebné bloky, z ktorých môžete vytvoriť robustné, bezpečné virtuálne súkromné siete.

VPN tiež podporuje riešenia VPN L2TP (Layer 2 Tunnel Protocol). Pripojenia L2TP, ktoré sa nazývajú aj virtuálne linky, poskytujú finančne nenáročný prístup pre vzdialených užívateľov

tým, že umožňujú serveru podnikovej siete, aby riadil adresy IP, priradené k svojim vzdialeným užívateľom. Ďalej pripojenia L2TP poskytujú zabezpečený prístup na váš systém alebo do vašej siete, keď ich chránite s IPSec.

Je dôležité, aby ste pochopili, aký dopad bude mať VPN na vašu celú sieť. Správne plánovanie a implementácia sú pre váš úspech najdôležitejšie. Tému VPN by ste si mali prezrieť v informačnom centre iSeries, aby ste sa presvedčili, že poznáte ako VPN pracuje a ako ich môžete používať. Viac informácií nájdete v iSeries Informačné centrum—>Bezpečnosť—>Budovanie virtuálnych súkromných sietí. Pozrite si “Nevyhnutné predpoklady a súvisiace informácie” na strane xii, kde nájdete informácie o sprístupňovaní informačného centra iSeries.

### Secure Sockets Layer (SSL)

SSL (Secure Sockets Layer) sa stal štandardom odvetvia pre povoľovanie aplikácií pre bezpečné komunikačné relácie cez nechránenú sieť, ako je aj internet. Protokol SSL vytvára a zabezpečuje pripojenia medzi aplikáciami klientov a servera, ktoré poskytujú autentifikáciu jedného alebo obidvoch koncových bodov komunikačnej relácie. SSL poskytuje aj súkromnosť a integritu údajov, ktoré si aplikácie klienta a servera vymieňajú. Viac informácií nájdete v Informačnom centre iSeries–>Bezpečnosť—>SSL (Secure Sockets Layer). Pozrite si “Nevyhnutné predpoklady a súvisiace informácie” na strane xii, kde nájdete informácie o sprístupňovaní informačného centra iSeries.

## Zabezpečenie vášho prostredia TCP/IP

Táto téma poskytuje všeobecné návrhy pre kroky, ktoré môžete podniknúť na zredukovanie odkrytia bezpečnosti v prostredí TCP/IP na vašom systéme. Tieto tipy sa týkajú viac celého vášho prostredia TCP/IP ako len určitých aplikácií, ktorými sa zaoberajú nasledujúce témy.

- Keď píšete aplikáciu pre port TCP/IP, uistite sa, že aplikácia je správne zabezpečená. Mali by ste predpokladať, že niekto cudzí sa môže snažiť dostať sa na túto aplikáciu cez tento port. Informovaná nepovolaná osoba sa môže snažiť použiť TELENET na túto aplikáciu.
- Monitorujte použitie portov TCP/IP na vašom systéme. Užívateľská aplikácie, ktorá je priradená k portu TCP/IP môže poskytovať položku “zadných dvierok” do vášho systému bez ID používateľa alebo hesla. Niekto s dostatočným oprávnením na vašom systéme môže priradiť aplikácií port TCP alebo UDP.
- Ako správca bezpečnosti by ste si mali byť vedomý techniky nazývanej *spoofovanie IP*, ktorú používajú hakeri. Každý systém v sieti TCP/IP má IP adresu. Ten, kto používa spoofovanie IP nastaví systém (obvykle PC) tak, aby tento predstieral, že je existujúcou IP adresou alebo dôvernou IP adresou. Takže podvodník sa môže pripojiť na váš systém tak, že predstiera, že je systémom, ku ktorému sa normálne pripájate.

  Ak na vašom systéme beží TCP/IP a váš systém sa zúčastňuje na sieti, ktorá nie je fyzicky chránená (všetky nevypnuté pripojenia sú preddefinovanými pripojeniami), ste zraniteľný voči spoofingu. Aby ste chránili váš systém pred poškodením “spooferom”, začnite s návrhmi, ktoré sú v tejto kapitole, ako je ochrana prihlasovania a bezpečnosť objektu. Tiež by ste mali zabezpečiť, aby mal váš systém rozumne nastavené limity pomocnej pamäte. Toto zabraňuje spooferovi zaplaviť váš systém poštou alebo spoolovými súbormi až po bod, kedy sa váš systém stáva nefunkčným.

  Navyše by ste mali pravidelne monitorovať činnosť TCP/IP na vašom systéme. Ak objavíte spoofovanie IP, môžete sa snažiť odhaliť slabiny vo vašom nastavení TCP/IP a urobiť úpravy.
- Pre váš intranet (sieť systémov, ktoré sa nepotrebujú priamo pripájať na vonkajší svet), používajte IP adresy, ktoré sa dajú znovu použiť. Adresy, ktoré sa dajú znovu použiť sú vytvorené na použitie v súkromnej sieti. Chrbtica internetu nesmeruje pakety, ktoré majú IP adresy, ktoré sa dajú znovu použiť. Takže adresy, ktoré sa dajú znovu použiť vytvárajú pridanú vrstvu ochrany vnútri vášho firewall.

Informačné centrum iSeries —>Networking—> webová stránka TCP/IP poskytuje viac informácií o tom, ako sú priraďované adresy IP a o rozsahoch adries IP ako aj o bezpečnostných informáciách o TCP/IP.

- Ak rozmýšľate nad pripojením vášho systému k internetu alebo k intranetu, prezrite si bezpečnostné informácie v *SecureWay: iSeries a v internetovom informačnom centre* (iSeries—>Bezpečnosť—>SecureWay). Pozrite si "Nevyhnutné predpoklady a súvisiace informácie" na strane xii, kde nájdete informácie o sprístupňovaní informačného centra iSeries.

## Riadenie serverov TCP/IP, ktoré sa majú spustiť automaticky

Ako správca bezpečnosti musíte riadiť, ktoré aplikácie TCP/IP sa spustia automaticky pri spustení TCP/IP. Pre spustenie TCP/IP sú dostupné dva príkazy. Pre každý príkaz, systém používa inú metódu určenia, ktoré aplikácie (servery) budú spustené.

Tabuľka 22 zobrazuje dva príkazy a bezpečnostné odporúčania pre ne. Tabuľka 23 zobrazuje štandardné hodnoty automatického spustenia pre servery. Na zmenu hodnoty automatického spustenia pre server použite príkaz pre server CHGxxxA (Change xxx Attributes). Napríklad príkaz pre TELNET je CHGTELNA.

*Tabuľka 22. Ako príkazy TCP/IP určujú, ktoré servery sa majú spustiť*

| Príkaz | Ktoré servery sa spustia | Bezpečnostné odporúčania |
|---|---|---|
| Spustiť TCP/IP (STRTCP) | Systém spustí každý server, ktorý určuje AUTOSTART(*YES). Tabuľka 23 zobrazuje dodávanú hodnotu pre každý server TCP/IP. | • Obozretne priraďte špeciálne oprávnenie *IOSYSCFG, aby ste mohli riadiť, kto môže meniť nastavenia automatického spustenia.<br>• Opatrne riaďte, kto má oprávnenie používať príkaz STRTCP. Štandardným verejným oprávnením pre tento príkaz je *EXCLUDE.<br>• Nastavte auditovanie objektu pre príkazy Change *server-name* Attributes (ako je CHGTELNA), na monitorovanie užívateľov, ktorí sa snažia zmeniť hodnotu AUTOSTART pre server. |
| Spustiť server TCP/IP (STRTCPSVR) | Použite parameter na určenie, ktoré servery sa majú spustiť. Štandard pri dodaní tohto príkazu je spustiť všetky servery. | • Použite príkaz CHGCMDDFT (Change Command Default) na nastavenie príkazu STRTCPSVR, aby sa spustil len určitý server. Toto nezabráni užívateľom v spustení iných serverov. Avšak zmenou štandardu príkazu urobíte menej pravdepodobným to, že používatelia budú spúšťať všetky servery náhodou. Napríklad použite nasledujúci príkaz na nastavenie štandardu na spustenie len serveru TELNET:CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*TELNET)')<br>**Poznámka:** Keď zmeníte štandardnú hodnotu, môžete špecifikovať len jeden server. Vyberte si buď server, ktorý používate pravidelne, alebo server, ktorý bude najmenej pravdepodobne zapríčiňovať odkrytie bezpečnosti (ako je TFTP).<br>• Opatrne riaďte, kto má oprávnenie používať príkaz STRTCPSVR. Štandardným verejným oprávnením pre tento príkaz je *EXCLUDE. |

Nasledujúca tabuľka obsahuje hodnoty automatického spustenia pre servery TCP/IP. Viac informácií o každom z týchto serverov nájdete v Informačnom centre iSeries (**Networking—>TCP/IP**). Pozrite si "Nevyhnutné predpoklady a súvisiace informácie" na strane xii, kde nájdete podrobnosti o sprístupňovaní informačného centra iSeries.

*Tabuľka 23. Hodnoty automatického spustenia pre servery TCP/IP*

| Server | Predvolená hodnota | Vaša hodnota |
|---|---|---|
| TELNET | AUTOSTART(*YES) | |

*Tabuľka 23. Hodnoty automatického spustenia pre servery TCP/IP (pokračovanie)*

| Server | Predvolená hodnota | Vaša hodnota |
|---|---|---|
| FTP (protokol prenosu súborov) | AUTOSTART(*YES) | |
| BOOTP (Samozavádzací protokol) | AUTOSTART(*NO) | |
| TFTP (protokol triviálneho prenosu súborov) | AUTOSTART(*NO) | |
| REXEC (Remote EXECution server) | AUTOSTART(*NO) | |
| RouteD (Smerový démon) | AUTOSTART(*NO) | |
| SMTP (protokol jednoduchého prenosu pošty) | 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 (systém názvu domény) | AUTOSTART(*NO) | |
| DDM | AUTOSTART(*NO) | |
| DHCP (protokol dynamickej konfigurácie hostiteľa) | AUTOSTART(*NO) | |
| NSMI | AUTOSTART(*NO) | |
| INETD | AUTOSTART(*NO) | |

**Poznámky:**

1. Pomocou IBM HTTP Server pre server iSeries použijete príkaz CHGHTTPA, aby ste nastavili hodnotu AUTOSTART.

## Úvahy o bezpečnosti pri používaní SLIP

Podpora TCP/IP servera iSeriesobsahuje Serial Interface Line Protocol (SLIP). SLIP poskytuje spojenie medzi dvoma bodmi s nízkymi nákladmi. Používateľ SLIP sa môže spojiť na LAN alebo WAN vytvorením spojenia medzi dvoma bodmi so systémom, ktorý je časťou LAN alebo WAN.

SLIP prebieha v asynchrónnom spojení. SLIP môžete použiť pre telefonické pripojenie na a zo serverov iSeries. Môžete ho použiť napríklad na nadviazanie spojenia z vášho PC na systém iSeries. Po vytvorení spojenia môžete použiť aplikáciu TELNET vo vašom PC na spojenie s iSeries TELNET serverom. Alebo môžete použiť aplikáciu FTP na prenos súborov medzi dvoma systémami.

Vo vašom systéme na nenachádza žiadna konfigurácia SLIP pri jej dodávke. Preto, ak nechcete spustiť SLIP (a TCP/IP na volanie) vo vašom systéme, nekonfigurujte žiadne konfiguračné profily pre SLIP. Použite príkaz WRKTCPPTP (Work with TCP/IP Point-to-Point) na vytvorenie konfigurácií SLIP. Musíte mať špeciálne oprávnenie *IOSYSCFG, aby ste mohli použiť príkaz WRKTCPPTP.

Ak chcete SLIP spustiť vo vašom systéme, vytvorte jeden alebo viac konfiguračných profilov SLIP (point-to-point). Konfiguračné profily môžete vytvoriť s nasledovnými prevádzkovými režimami:

- Volaný (*ANS)
- Volajúci (*DIAL)

Nasledujúce témy pojednávajú o tom, ako môžete nastaviť bezpečnosť pre konfiguračné profily SLIP.

**Poznámka:** **Užívateľský profil** je objekt servera iSeries, ktorý umožňuje prihlásenie sa. Každá úloha servera iSeries musí mať užívateľský profil, aby mohla byť spustená. **Konfiguračný profil** ukladá informácie, ktoré sa používajú na vytvorenie spojenia SLIP so systémom iSeries. Keď spustíte pripojenie SLIP na serveroch iSeries, jednoducho vytvárate spojenie. Zatiaľ ste sa neprihlásili a nespustili ste úlohu servera iSeries. Preto na spustenie pripojenia SLIP k serverom iSeries nevyhnutne nepotrebujete užívateľský profil. Ako však uvidíte v nasledujúcich rozpravách, konfiguračný profil SLIP môže vyžadovať užívateľský profil, aby mohol určiť, či má pripojenie povoliť alebo nie.

## Riadenie pripojení SLIP pomocou vytáčania

Predtým ako niekto bude môcť vytvoriť volané spojenie s vaším systémom so SLIP, musíte spustiť konfiguračný profil SLIP *ANS. Pre vytvorenie alebo zmenu konfiguračného profilu SLIP použite príkaz WRKTCPPTP (Work with TCP/IP Point-to-Point). Pre spustenie konfiguračného profilu použite buď príkaz Start TCP/IP Point-to-Point (STRTCPPTP) alebo možnosť WRKTCPPTP na obrazovke. Pri dodaní vášho systému je verejné oprávnenie pre STRTCPPTP a ENDTCPPTP: *EXCLUDE. Možnosti na pridávanie, zmenu a vymazanie konfiguračných profilov SLIP sú dostupné len vtedy, keď máte špeciálne oprávnenie *IOSYSCFG. Ako správca bezpečnosti môžete použiť oprávnenie príkazu, aj špeciálne oprávnenie, aby ste zistili, kto môže nastaviť váš systém na povolenie volaných spojení.

### Zabezpečenie telefonického pripojenia SLIP

Ak chcete overiť systémy, ktorá volajú váš systém, potom chcete, aby volajúci systém poslal ID používateľa a heslo. Váš systém potom môže overiť ID a heslo používateľa. Ak ID a heslo používateľa nie sú platné, váš systém môže zamietnuť požiadavku relácie.

Pre nastavenie overovania volania urobte nasledovné:

__ Krok 1. Vytvorte užívateľský profil, ktorý bude môcť volajúci systém použiť na vytvorenie spojenia. ID a heslo používateľa, ktoré žiadateľ odošle, sa musia zhodovať s názvom a heslom tohto užívateľského profilu.

**Poznámka:** Pre systém, ktorý má overiť platnosť hesla, musí byť systémová hodnota QSECURITY nastavená na 20, alebo viac.

Ako dodatočnú ochranu možno budete chcieť vytvoriť užívateľské profily špeciálne na vytvorenie spojení SLIP. Užívateľské profily by mali mať limitované oprávnenie na systém. Ak neplánujete použiť profily pre žiadne funkcie, okrem vytvorenia spojení SLIP, v užívateľských profiloch môžete nastaviť nasledovné funkcie:

- Východisková ponuka (INLMNU) na *SIGNOFF
- Východiskový program (INLPGM) na *NONE.
- Možnosti obmedzenia (LMTCPB) na *YES

Tieto hodnoty zabránia každému prihlásiť sa interaktívne s užívateľským profilom.

__ Krok 2. Vytvorte pre systém zoznam oprávnení pre kontrolu, keď sa žiadateľ pokúsi vytvoriť spojenie SLIP.

**Poznámka:** Tento zoznam oprávnení zadajte v poli *Zoznam oprávnení k prístupu na systém*, keď vytvárate alebo meníte SLIP profil. (Pozrite krok 4.)

__ Krok 3. Použite príkaz ADDAUTLE (Add Authorization Entry) na pridanie užívateľského profilu, ktorý ste vytvorili v kroku 1, do zoznamu oprávnení.

Môžete vytvoriť jedinečný zoznam oprávnení pre každý konfiguračný profil point-to-point, alebo môžete vytvoriť zoznam oprávnení, ktoré bude zdieľať niekoľko konfiguračných profilov.

__ Krok 4. Použite príkaz WRKTCPPTP pre nastavenie TCP/IP point-to-point *ANS profilu, ktorý má nasledovné charakteristiky:

- Konfiguračný profil musí použiť dialógový skript spojenia, ktorý obsahuje funkciu overovania používateľa. Overovanie používateľa zahŕňa akceptovanie a potvrdenie ID a hesla používateľa od žiadateľa. So systémom sa dodáva niekoľko vzorových dialógových skriptov, ktoré poskytujú túto funkciu.
- Konfiguračný profil musí zadať názov zoznamu oprávnení, ktorý ste vytvorili v kroku 2. ID používateľa, ktorý dialógový skript spojenia príjme, musí byť v zozname oprávnení.

Pamätajte si, že hodnota nastavenia bezpečnosti volaného je podmienená bezpečnostnými praktikami a schopnosťami systémov, ktoré sa dovolávajú. Ak vyžadujete ID a heslo používateľa, dialógový skript spojenia v dožadovacom systéme musí tento ID a heslo používateľa odoslať. Niektoré systémy, ako napríklad servery iSeries poskytujú bezpečnú metódu pre ukladanie ID užívateľa a hesiel. ( “Bezpečnosť a relácie volania von” na strane 114 popisuje túto metódu.) Iné systémy ukladajú ID a heslo používateľa v skripte, ktorý môže sprístupniť ktokoľvek, kto vie, kde nájsť tento skript v systéme.

Z dôvodu odlišných bezpečnostných praktík a schopností vašich komunikačných partnerov, budete možno chcieť vytvoriť rôzne konfiguračné profily pre rôzne dožadujúce sa prostredia. Použite príkaz STRTCPPTP pre nastavenie vášho systému tak, aby akceptoval reláciu pre špecifický konfiguračný profil. Môžete napríklad spustiť relácie pre niekoľko konfiguračných profilov len v určitých časových obdobiach dňa. Môžete použiť auditovanie bezpečnosti na zaprotokolovanie činnosti pre príslušné užívateľské profily.

### Zabránenie užívateľom vytáčania v prístupe na ostatné systémy

V závislosti od vašej systémovej a sieťovej konfigurácii, používateľ, ktorý spustí SLIP spojenie, môže byť schopný sprístupniť ďalší systém vo vašej sieti bez prihlásenia sa na váš systém. Napríklad, používateľ by mohol vytvoriť spojenie SLIP k vášmu systému. Potom by tento používateľ mohol vytvoriť spojenie FTP k ďalšiemu systému vo vašej sieti, ktorý nepovoľuje prichádzajúce volanie.

Používateľovi SLIP môžete zabrániť, aby sprístupnil ďalšie systémy vo vašej sieti, a to zadaním N (Nie) v poli *Povoliť postúpenie IP datagramu* v konfiguračnom profile. Toto zamedzí používateľovi prístup do vašej siete predtým, ako sa používateľ prihlási do vášho systému. Avšak po úspešnom prihlásení používateľa do vášho systému, hodnota postúpenia datagramu nemá žiadny vplyv. Neobmedzuje schopnosť používateľa používať TCP/IP aplikáciu na vašom iSeries systéme (ako je FTP alebo TELNET), ani vytvoriť spojenie s iným systémom vo vašej sieti.

## Riadenie relácií volania von

Predtým ako niekto bude môcť použiť SLIP na vytvorenie volajúceho spojenia z vášho systému, musíte spustiť konfiguračný profil SLIP *DIAL. Pre vytvorenie alebo zmenu konfiguračného profilu SLIP môžete použiť príkaz WRKTCPPTP. Pre spustenie konfiguračného profilu použite buď príkaz Start TCP/IP Point-to-Point (STRTCPPTP), alebo možnosť WRKTCPPTP na obrazovke. Pri dodaní vášho systému je verejné oprávnenie pre STRTCPPTP a ENDTCPPTP: *EXCLUDE. Možnosti na pridávanie, zmenu a vymazanie konfiguračných profilov SLIP sú dostupné len vtedy, keď máte špeciálne oprávnenie *IOSYSCFG. Ako správca bezpečnosti môžete použiť oprávnenie príkazu, aj špeciálne oprávnenie, aby ste zistili, kto môže nastaviť váš systém na povolenie volajúcich spojení.

### Bezpečnosť a relácie volania von

Používatelia vášho iSeries systému možno chceli vytvoriť volajúce spojenia so systémami, ktoré vyžadujú overenie používateľa. Skript dialógu pripojenia na vašom serveri iSeries musí odoslať ID užívateľa a heslo do vzdialeného systému. Servery iSeries poskytujú bezpečnú metódu pre ukladanie takého hesla. Toto heslo nemusí byť uložené v dialógovom skripte spojenia.

**Poznámky:**

1. Dokonca i keď váš systém uloží heslo spojenia v zakódovanej forme, pred odoslaním ho odkóduje. Heslá SLIP-u, podobne ako heslá FTP a TELNET-u, sa odošlú odkódované ("jasné"). Avšak heslo SLIP sa, odlišne ako heslo FTP a TELNET-u, odošle predtým, ako systémy vytvoria režim TCP/IP.

   Pretože SLIP používa spojenie point-to-point v asynchrónnom režime, odhalenie bezpečnosti pri odosielaní odkódovaných hesiel je iné, ako odhalenie hesiel FTP a TELNET-u. Odkódované heslá FTP a TELNET-u mohli byť odoslané ako IP premávka v sieti, a preto sú napadnuteľné elektronickým snorením. Prenos vášho hesla SLIP je také bezpečné, ako telefonické spojenie medzi dvoma systémami.
2. Štandardným súborom na uloženie dialógových skriptov spojenia SLIP je QUSRSYS/QATOCPPSCR. Verejné oprávnenie pre tento súbor je *USE, ktoré bráni verejným používateľom zmeniť štandardné dialógové skriptá spojenia.

Keď vytvoríte profil spojenia pre vzdialenú reláciu, ktorá vyžaduje overenie, urobte nasledovné:

__ Krok 1. Overte, či je v systéme Retain Server Security Data (QRETSVRSEC) nastavená na 1 (Áno). Táto systémová hodnota určuje, či umožníte, aby heslá, ktoré môžu byť odkódované, boli uložené v chránenej oblasti vášho systému.

__ Krok 2. Príkaz WRKTCPPTP použite na vytvorenie konfiguračného profilu, ktorý má nasledovné charakteristiky:

- Pre režim konfiguračného profilu zadajte *DIAL.
- Pre *Názov prístupu k vzdialenej službe* zadajte ID používateľa, ktoré vzdialený systém očakáva. Napríklad, ak sa pripájate k inému serveru iSeries, názov užívateľského profilu zadajte na tomto serveri iSeries.
- Pre *Heslo prístupu k vzdialenej službe* zadajte heslo, ktoré vzdialený systém očakáva pre tento ID používateľa. Vo vašom serveri iSeries je toto heslo uložené v chránenej oblasti v podobe, ktorá sa dá odkódovať. Názvy a heslá, ktoré ste pridelili konfiguračným profilom, sú spojené s užívateľským profilom QTCP. Názvy a heslá sa nedajú sprístupniť žiadnymi užívateľskými príkazmi alebo rozhraniami. Len registrované systémové programy môžu sprístupniť tieto informácie o hesle.

  **Poznámka:** Pamätajte si, že sa heslá pre vaše profily spojenia neuložia pri ukladaní konfiguračných súborov TCP/IP. Aby ste uložili heslá SLIP, musíte použiť príkaz Save Security Data (SAVSECDTA) pre uloženie užívateľského profilu QTCP.
- Pre dialógový skript spojenia zadajte skript, ktorý odosiela ID a heslo používateľa. So systémom sa dodáva niekoľko vzorových dialógových skriptov, ktoré poskytujú túto funkciu. Po spustení skriptu systém obnoví heslo, odkóduje ho a odošle ho vzdialenému systému.

## Úvahy o bezpečnosti pre point-to-point protokol

Protokol PPP (Point-to-point) je dostupný ako súčasť TCP/IP. PPP je priemyselným štandardnom pre spojenia z bodu do bodu poskytujúci dodatočné funkcie, cez ktoré je dostupný so SLIP.

S PPP môže mať váš server iSeries vysokorýchlostné pripojenia priamo k poskytovateľovi služieb internetu alebo k ostatným systémom v intranete alebo extranete. Vzdialené LAN môžu realisticky vytvoriť volané pripojenia do vášho servera iSeries.

Pamätajte si, že PPP podobne ako SLIP poskytuje sieťové pripojenie k vášmu serveru iSeries. Spojenie PPP hlavne prinesie dotazník ku dverám vášho systému. Dotazník stále potrebuje ID a heslo používateľa na vstup do vášho systému a pripojenie k serveru TCP/IP, ako napríklad TELNET alebo FTP. Nasledujú úvahy o bezpečnosti s touto novou schopnosťou spojenia:

**Poznámka:** PPP nakonfigurujete s použitím iSeries Navigator v pracovnej stanici IBM iSeries Access for Windows.

- PPP poskytuje schopnosť mať vyhradené spojenia (kde ten istý používateľ vždy má tú istú IP adresu). S vyhradenou adresou ste potenciálnym terčom pre znevažovanie IP (podvodnícky systém, ktorý predstiera, že je dôveryhodný systém so známou IP adresou). Avšak rozšírené schopnosti autentifikácie, ktoré poskytuje PPP, pomáhajú chrániť pred znevažovaním IP.
- S PPP podobne ako so SLIP, môžete vytvárať profily spojenia, ktoré majú názov používateľa a príslušné heslo. Avšak, na rozdiel od SLIP užívateľ nepotrebuje mať platný užívateľský profil a heslo. Meno užívateľa a heslo nie sú priradené k užívateľskému profilu. Namiesto toho, sa pri PPP autentifikácii používajú overovacie zoznamy. Navyše PPP nevyžaduje skript spojenia. Overovanie (výmena názvu a hesla používateľa) je súčasťou PPP architektúry a uskutočňuje sa na nižšej úrovni ako so SLIP-om.
- S PPP máte možnosť použiť CHAP (challenge handshake authentication protocol). Nebudete sa musieť obávať tajných pozorovateľov, ktorí snoria za vaším heslom, pretože CHAP zakóduje názvy a heslá používateľov.

  Vaše PPP spojenie používa CHAP len keď ho obe strany podporujú. Počas výmenných signálov na nastavenie komunikácií medzi dvoma modemami sa oba systémy dohadujú. Napríklad, ak SYSTEMA podporuje CHAP a SYSTEMB nie, SYSTEMA môže buď zrušiť reláciu, alebo použiť odkódovaný názov a heslo používateľa. Súhlas na použitie odkódovaného názvu a hesla používateľa, sa považuje za potvrdenie dohody. Rozhodnutie o potvrdení dohody je možnosťou konfigurácie. Napríklad, ak viete, že vo vašom intranete majú všetky vaše systémy schopnosť CHAP, mali by ste profil vášho spojenia nakonfigurovať tak, aby nepotvrdil dohodu. Vo verejnom spojení, kde volajúcim systémom je váš systém, budete možno ochotný potvrdiť dohodu.

  Profil spojenia pre PPP poskytuje možnosť zadať platné IP adresy. Môžete napríklad vyjadriť, že očakávate špecifickú adresu alebo rozsah adries pre špecifických používateľov. Táto schopnosť spolu so schopnosťou odkódovania hesiel poskytuje ďalšiu ochranu pred znevažovaním.

  Ako dodatočnú ochranu pred znevažovaním aktívnej relácie, môžete nakonfigurovať PPP na znovuvyzvanie v určitých intervaloch. Napríklad, zatiaľ čo je relácia PPP, váš server iSeries mohol vyzvať ostatné systémy na zadanie užívateľa a hesla. Bude tak robiť každých 15 minút, aby sa ubezpečil, či je to ten istý profil spojenia. (Konečný používateľ si ani neuvedomí túto znovuvyzývaciu činnosť. Systémy si vymieňajú názvy a heslá pod úrovňou, ktorú vidí konečný používateľ.)

  S PPP môžete realisticky očakávať, že vzdialené LAN mohli vytvoriť volané pripojenie do vášho servera iSeries a do vašej rozšírenej siete. V tomto prostredí je zapnutie postúpenia IP pravdepodobne žiadosťou. Postúpenie IP je potenciálnym prvkom, ktorý môže umožniť votrelcovi prechádzať sa vo vašej sieti. Avšak PPP má silnejšie ochrany (ako napríklad zakódovanie hesiel a kontrola platnosti IP adries). Preto je menej pravdepodobné, že si nejaký votrelec pri prvej príležitosti vytvorí spojenie na sieť.

Viac informácií o PPP nájdete v informačnom centre iSeries.

# Úvahy o bezpečnosti pre používanie servera Samozavádzací protokol

Samozavádzací protokol (BOOTP) poskytuje dynamickú metódu pre priraďovanie pracovných staníc k serverom a pre priraďovanie IP adries pracovným staniciam a zdrojom IPL (inicial program load).

BOOTP je protokol TCP/IP používaný na povolenie menej mediálnej pracovnej stanici (klient), vyžiadať si súbor, obsahujúci iniciačný kód od servera na sieti. BOOTP server počúva na známom porte BOOTP servera 67. Keď je prijatá požiadavka klienta, server vyhľadá IP adresu definovanú pre klienta a vráti odpoveď klientovi s IP adresou klienta a názvom súboru načítania. Klient potom iniciuje požiadavku TFTP serveru pre súbor načítania. Mapovanie medzi adresou klientskeho hardvéru a adresou IP sa uchováva v tabuľke BOOTP na serveri iSeries.

## Zamedzenie prístupu BOOTP

Ak k vašej sieti nie sú pripojení žiadni tenkí klienti, nepotrebujete vo vašom systéme spustiť server BOOTP. Môže byť použitý pri iných zariadeniach, ale uprednostňované riešenie pre tieto zariadenia je používanie DHCP. Aby ste zabránili spusteniu servera BOOTP, urobte nasledujúce:

__ Krok 1. Aby ste zabránili automatickému spusteniu úloh servera BOOTP pri spustení TCP/IP, napíšte nasledovné:

```
CHGBPA AUTOSTART(*NO)
```

**Poznámky:**

a. AUTOSTART(*NO) je štandardná hodnota.

b. “Riadenie serverov TCP/IP, ktoré sa majú spustiť automaticky” na strane 110 poskytuje viac informácií o riadení toho, ktoré TCP/IP sa spúšťajú automaticky.

__ Krok 2. Aby ste zabránili priradeniu užívateľskej aplikácie, akou je napríklad soketová aplikácia, k portu, ktorý systém normálne používa pre BOOTP, urobte nasledovné:

**Poznámka:** Pretože DHCP aj BOOTP používajú to isté číslo portu, bude to spomaľovať port používaný DHCP. Neobmedzujte port, ak chcete používať DHCP.

__ Krok a. Na obrazovku ponuky Configure TCP/IP napíšte GO CFGTCP.

__ Krok b. Vyberte voľbu 4 (Work with TCP/IP port restrictions).

__ Krok c. Na obrazovke Work with TCP/IP Port Restrictions špecifikujte voľbu 1 (Add).

__ Krok d. Pre port nižšieho rozsahu špecifikujte 67.

__ Krok e. Pre port vyššieho rozsahu špecifikujte *ONLY.

**Poznámky:**

1) Obmedzenie portov sa stane účinné pri nasledovnom spustení TCP/IP. Ak je TCP/IP aktívne pri nastavení obmedzení portov, TCP/IP by ste mali ukončiť a opätovne ho spustiť.

2) RFC1700 poskytuje informácie o bežne priradených číslach portov.

__ Krok f. Pre protokol špecifikujte *UDP.

__ Krok g. V poli pre užívateľský profil špecifikujte názov, ktorý je na vašom systéme chránený. (Chránený užívateľský profil je užívateľský profil, ktorý nevlastní programy adoptujúce oprávnenie a nemá

heslo, ktoré poznajú iní používatelia.) Obmedzením portu na konkrétneho používateľa automaticky vylúčite všetkých ostatných používateľov.

### Zabezpečenie servera BOOTP

BOOTP server neposkytuje priamy prístup na váš systém iSeries a preto predstavuje len obmedzené riziko odkrytia zabezpečenia. Vašou primárnou starosťou ako správcu bezpečnosti je zaistiť, aby boli správne informácie pridružené ku správnemu tenkému klientovi. Inak povedané, záškodník by mohol pozmeniť tabuľku BOOTP a spôsobiť, že by vaši tenkí klienti pracovali nesprávne alebo by nepracovali vôbec.

Na spravovanie BOOTP servera tabuľky BOOTP musíte mať špeciálne oprávnenie *IOSYSCFG. Musíte starostlivo riadiť užívateľské profily, ktoré majú na vašom systéme špeciálne oprávnenie *IOSYSCFG.

## Úvahy o bezpečnosti pre používanie servera DHCP

Protokol dynamickej konfigurácie hostiteľa (DHCP) poskytuje rámec pre posúvanie informácií k hostiteľom na sieti TCP/IP. Pre vaše klientske pracovné stanice, DHCP môže poskytovať funkciu podobnú automatickej konfigurácií. Program s umožneným DHCP na klientskej pracovnej stanici vysiela požiadavku o konfiguračné informácie. Ak je na vašom serveri iSeries spustený server DHCP, server odpovie na požiadavku odoslaním informácií, ktoré klientská pracovná stanica potrebuje pre správne nakonfigurovanie TCP/IP.

DHCP môžete použiť na zjednodušenie prvého pripojenia užívateľov k vášmu serveru iSeries. To preto, lebo používateľ nepotrebuje zadať konfiguračné informácie TCP/IP. DHCP môžete tiež používať na redukovanie počtu interných adries TCP/IP, ktoré potrebujete v podsieti. Server DHCP môže dočasne prideľovať IP adresy aktívnym používateľom (zo svojej spoločnej oblasti IP adries).

Pri tenkých klientoch môžete namiesto BOOTP použiť DHCP. DHCP poskytuje viac funkcií ako BOOTP a dokáže podporovať dynamickú konfiguráciu tenkých klientov i PC.

### Zamedzenie prístupu DHCP

Ak *nechcete*, aby niekto používal DHCP na získanie prístupu na váš systém, mali by ste urobiť nasledujúce:

1. Aby ste zabránili automatickému spusteniu úloh servera DHCP pri spustení TCP/IP, napíšte nasledovné:

   ```
   CHGDHCPA AUTOSTART(*NO)
   ```

   **Poznámky:**

   a. AUTOSTART(*NO) je štandardná hodnota.

   b. “Riadenie serverov TCP/IP, ktoré sa majú spustiť automaticky” na strane 110 poskytuje viac informácií o riadení toho, ktoré TCP/IP sa spúšťajú automaticky.

2. Aby ste zabránili priradeniu užívateľskej aplikácie, akou je napríklad soketová aplikácia, k portu, ktorý systém normálne používa pre DHCP, urobte nasledovné:

   a. Na obrazovku ponuky Configure TCP/IP napíšte GO CFGTCP.

   b. Vyberte voľbu 4 (Work with TCP/IP port restrictions).

   c. Na obrazovke Work with TCP/IP Port Restrictions špecifikujte voľbu 1 (Add).

   d. Pre port nižšieho rozsahu špecifikujte 67.

   e. Pre port vyššieho rozsahu špecifikujte 68.

**Poznámky:**

1) Obmedzenie portov sa stane účinné pri nasledovnom spustení TCP/IP. Ak je TCP/IP aktívne pri nastavení obmedzení portov, TCP/IP by ste mali ukončiť a opätovne ho spustiť.
2) RFC1700 poskytuje informácie o bežne priradených číslach portov.

f. Pre protokol špecifikujte *UDP.

g. V poli pre užívateľský profil špecifikujte názov, ktorý je na vašom systéme chránený. (Chránený užívateľský profil je užívateľský profil, ktorý nevlastní programy adoptujúce oprávnenie a nemá heslo, ktoré poznajú iní používatelia.) Obmedzením portu na konkrétneho používateľa automaticky vylúčite všetkých ostatných používateľov.

## Zabezpečenie servera DHCP

Nasledujú úvahy o bezpečnosti pre prípad, keď si vyberiete na vašom systéme iSeries spustiť DNS:

- Obmedzte počet používateľov, ktorí majú oprávnenie spravovať DHCP. Spravovanie DHCP si vyžaduje nasledujúce oprávnenie:
  - špeciálne oprávnenie *IOSYSCFG
  - oprávnenie *RW k nasledujúcim súborom:

    ```
    /QIBM/UserData/OS400/DHCP/dhcpsd.cfg
    /QIBM/UserData/OS400/DHCP/dhcprd.cfg
    ```
- Zhodnoťte, ako je fyzicky prístupná vaša LAN. Mohol by niekto cudzí jednoducho vojsť do vášho umiestnenia s laptopom a fyzicky sa pripojiť na vašu LAN? Ak toto je odkrytie, DHCP poskytuje schopnosť vytvárať zoznam klientov (adresy hardvéru), ktorý bude server DHCP konfigurovať. Keď používate túto vlastnosť, odstraňujete časť z úžitku produktivity, ktorú poskytuje DHCP vašim správcom siete. Avšak zabraňujete systému konfigurovať neznáme pracovné stanice.
- Ak je to možné, použite spoločnú oblasť IP adries, ktorá sa dá opätovne použiť (nie je vytvorená pre internet). Toto pomáha zabrániť pracovným staniciam mimo vašej siete získať použiteľné konfiguračné informácie zo servera.
- Použite body ukončenia DHCP, ak potrebujete dodatočnú bezpečnostnú ochranu. Nasleduje prehľad bodov ukončenia a ich schopností. *iSeries System API Reference* opisuje, ako používať tieto ukončovacie body.

  **Položka portu**
  Systém volá váš ukončovací program vždy, keď číta paket údajov z portu 67 (port DHCP). Váš ukončovací program prijíma úplný paket údajov. Môže rozhodnúť, či by systém mal tento paket spracovať alebo znehodnotiť. Tento bod ukončenia môžete použiť, keď existujúce skríningové vlastnosti DHCP nie sú pre vaše potreby dostatočné.

  **Priradenie adresy**
  Systém volá váš ukončovací program vždy, keď DHCP formálne priradí klientovi adresu.

  **Vydanie adresy**
  Systém volá váš ukončovací program vždy, keď DHCP formálne vydá adresu a umiestni ju späť do spoločnej oblasti adries.

## Úvahy o bezpečnosti pre používanie servera TFTP

Protokol triviálneho prenosu súborov (TFTP) poskytuje základný prenos súboru bez autentifikácie používateľa. TFTP pracuje s Samozavádzací protokol (BOOTP) alebo Dynamic Host Configuration Protocol (DHCP).

Klient sa na začiatku pripája k serveru BOOTP alebo k serveru DHCP. Server BOOTP alebo DHCP odpovedá s IP adresou klienta a názvom súboru načítania. Klient potom iniciuje požiadavku TFTP serveru pre súbor načítania. Keď klient dokončí sťahovanie súboru načítania, toto skončí TFTP reláciu.

## Zamedzenie prístupu TFTP

Ak k vašej sieti nie sú pripojení žiadni tenkí klienti, pravdepodobne nepotrebujete vo vašom systéme spustiť server TFTP. Aby ste zabránili spusteniu servera TFTP, urobte nasledujúce:

__ Krok 1. Aby ste zabránili automatickému spusteniu úloh servera TFTP pri spustení TCP/IP, napíšte nasledovné:

```
CHGTFTPA AUTOSTART(*NO)
```

**Poznámky:**

a. AUTOSTART(*NO) je štandardná hodnota.

b. “Riadenie serverov TCP/IP, ktoré sa majú spustiť automaticky” na strane 110 poskytuje viac informácií o riadení toho, ktoré TCP/IP sa spúšťajú automaticky.

__ Krok 2. Aby ste zabránili priradeniu užívateľskej aplikácie, akou je napríklad soketová aplikácia, k portu, ktorý systém normálne používa pre TFTP, urobte nasledovné:

__ Krok a. Na obrazovku ponuky Configure TCP/IP napíšte GO CFGTCP.

__ Krok b. Vyberte voľbu 4 (Work with TCP/IP port restrictions).

__ Krok c. Na obrazovke Work with TCP/IP Port Restrictions špecifikujte voľbu 1 (Add).

__ Krok d. Pre port nižšieho rozsahu špecifikujte 69.

__ Krok e. Pre port vyššieho rozsahu špecifikujte *ONLY.

**Poznámky:**

1) Obmedzenie portov sa stane účinné pri nasledovnom spustení TCP/IP. Ak je TCP/IP aktívne pri nastavení obmedzení portov, TCP/IP by ste mali ukončiť a opätovne ho spustiť.

2) RFC1700 poskytuje informácie o bežne priradených číslach portov.

__ Krok f. Pre protokol špecifikujte *UDP.

__ Krok g. V poli pre užívateľský profil špecifikujte názov, ktorý je na vašom systéme chránený. (Chránený užívateľský profil je užívateľský profil, ktorý nevlastní programy adoptujúce oprávnenie a nemá heslo, ktoré poznajú iní používatelia.) Obmedzením portu na konkrétneho používateľa automaticky vylúčite všetkých ostatných používateľov.

## Zabezpečenie servera TFTP

Server TFTP štandardne poskytuje veľmi obmedzený prístup k vášmu systému iSeries. Je špecificky nakonfigurovaný, aby poskytoval iniciačný kód pre tenkých klientov. Ako správca bezpečnosti, by ste si mali byť vedomý nasledujúcich charakteristík servera TFTP:

- Server TFTP nevyžaduje autentifikáciu (ID používateľa a heslo). Všetky úlohy TFTP bežia pod užívateľským profilom QTFTP. Užívateľský profil QTFTP nemá heslo. Preto nie je dostupný pre interaktívne prihlasovanie. Užívateľský profil QTFTP nemá žiadne špeciálne oprávnenia ani nie je explicitne oprávnený pre zdroje systému. Používa verejné oprávnenie na prístup k prostriedkom, ktoré potrebuje pre tenkých klientov.
- Server TFTP sa dodáva s nakonfigurovaným prístupom do adresára, ktorý obsahuje informácie o tenkých klientoch. Musíte mať oprávnenia *PUBLIC alebo QTFTP, aby ste mohli čítať alebo zapisovať v tomto adresári. Na zapisovanie do adresára musíte mať v

parametri ″Allow file writes″ špecifikované *CREATE pre príkaz CHGTFTPA. Ak chcete zapisovať do existujúceho súboru, musíte mať v príkaze CHGTFTPA v parametri ″Allow file writes″ špecifikované *REPLACE. *CREATE umožňuje nahrádzať existujúce súbory alebo vytvárať nové súbory. *REPLACE len umožňuje nahrádzať existujúce súbory.

Klient TFTP sa nemôže dostať do žiadneho iného adresára, pokým vy explicitne nedefinujete adresár príkazom CHGTFTPA (Change TFTP Attributes). Preto, ak sa lokálny alebo vzdialený používateľ pokúsi spustiť reláciu TFTP k vášmu systému, schopnosť používateľa dostať sa k informáciám alebo zapríčiniť škodu je veľmi obmedzená.

- Ak sa rozhodnete nakonfigurovať váš server TFTP, aby poskytoval aj iné služby, okrem spracovávania tenkých klientov, môžete zadefinovať výstupný program, aby vyhodnotil a autorizoval každú požiadavku TFTP. Server TFTP poskytuje ukončenie overenia platnosti požiadavky, ktoré je podobné ukončeniu dostupnému pre server FTP. Viac informácií nájdete v Informačnom centre iSeries—> Networking—>TCP/IP—>TFTP. Pozrite si “Nevyhnutné predpoklady a súvisiace informácie” na strane xii, kde nájdete informácie o sprístupňovaní informačného centra iSeries.

# Úvahy o bezpečnosti pre používanie servera REXEC

Remote EXECution server (REXEC) prijíma a spúšťa príkazy od klienta REXEC. Klient REXEC je typicky PC alebo aplikácia UNIX, ktorá podporuje odosielanie príkazov REXEC. Podpora, ktorú tento server podporuje je podobná schopnosti, ktorá je dostupná, keď používate podpríkaz RCMD (Remote Command) pre server FTP.

## Zamedzenie prístupu REXEC

Ak nechcete, aby váš server iSeries akceptoval príkazy od klienta REXEC, urobte nasledujúce, aby ste zabránili spusteniu servera REXEC:

__ Krok 1. Aby ste zabránili automatickému spusteniu úloh servera REXEC pri spustení TCP/IP, napíšte nasledovné:

```
CHGRXCA AUTOSTART(*NO)
```

**Poznámky:**

a. AUTOSTART(*NO) je štandardná hodnota.

b. “Riadenie serverov TCP/IP, ktoré sa majú spustiť automaticky” na strane 110 poskytuje viac informácií o riadení toho, ktoré TCP/IP sa spúšťajú automaticky.

__ Krok 2. Aby ste zabránili priradeniu užívateľskej aplikácie, akou je napríklad soketová aplikácia, k portu, ktorý systém normálne používa pre REXEC, urobte nasledovné:

__ Krok a. Na obrazovku ponuky Configure TCP/IP napíšte GO CFGTCP.

__ Krok b. Vyberte voľbu 4 (Work with TCP/IP port restrictions).

__ Krok c. Na obrazovke Work with TCP/IP Port Restrictions špecifikujte voľbu 1 (Add).

__ Krok d. Pre port nižšieho rozsahu špecifikujte 512.

__ Krok e. Pre port vyššieho rozsahu špecifikujte *ONLY.

__ Krok f. Pre protokol špecifikujte *TCP.

__ Krok g. V poli pre užívateľský profil špecifikujte názov, ktorý je na vašom systéme chránený. (Chránený užívateľský profil je užívateľský profil, ktorý nevlastní programy adoptujúce oprávnenie a nemá heslo, ktoré poznajú iní používatelia.) Obmedzením portu na konkrétneho používateľa automaticky vylúčite všetkých ostatných používateľov.

**Poznámky:**

a. Obmedzenie portov sa stane účinné pri nasledovnom spustení TCP/IP. Ak je TCP/IP aktívne pri nastavení obmedzení portov, TCP/IP by ste mali ukončiť a opätovne ho spustiť.
b. RFC1700 poskytuje informácie o bežne priradených číslach portov.

## Zabezpečenie servera REXEC

Nasledujú úvahy o prípade, keď si vyberiete spustiť na vašom systéme Remote EXECution server:

- Požiadavka REXCD zahŕňa ID používateľa, heslo a príkaz na spustenie. Autentifikácia a kontrola oprávnení normálneho servera iSeries sa použije:
  - Užívateľský profil a kombinácia hesla musia byť platné.
  - Systém vnucuje hodnotu *Limit capabilities* (LMTCPB) pre užívateľský profil.
  - Používateľ musí mať oprávnenie pre príkaz a pre všetky zdroje, ktoré tento príkaz používa.
- Server REXEC poskytuje body ukončenia, ktoré sú podobné dostupným bodom pre server FTP. Bod ukončenia Validation môžete použiť na zhodnotenie platnosti príkazu a rozhodnutie, či ho povolíte. Viac informácií nájdete v Informačnom centre iSeries—>Networking—>TCP/IP—>REXEC. Pozrite si “Nevyhnutné predpoklady a súvisiace informácie” na strane xii, kde nájdete informácie o sprístupňovaní informačného centra iSeries.
- Keď si vyberiete spustenie servera REXEC, bežíte mimo všetkých ponúk riadenia prístupu, ktoré máte na vašom systéme. Musíte zaistiť, že schéma oprávnenia objektov je adekvátna pre ochranu vašich zdrojov.

# Úvahy o bezpečnosti pre používanie RouteD

Server Smerový démon (RouteD) poskytuje podporu pre RIP (Routing Information Protocol) na serveroch iSeries. RIP je navyše používaným protokolom smerovania. Je to Interior Gateway Protocol, ktorý pomáha TCP/IP v smerovaní IP paketov v rámci autonómneho systému.

RouteD je určený na zvýšenie efektívnosti premávky siete povolením systémov, v rámci dôvernej siete, aktualizovať jeden druhého aktuálnymi informáciami smerovania. Keď u vás beží RouteD, váš systém môže prijímať aktualizácie od iných zúčastňujúcich sa systémov o tom, ako by mali byť prenosy (pakety) smerované. Preto, ak váš server RouteD je dostupný hakerovi, tento by ho mohol použiť na presmerovanie vašich paketov cez systém, ktorý môže snoriť alebo modifikovať tieto pakety. Nasledujú návrhy pre zabezpečenie RouteD:

- Servery iSeries používajú RIPv1, ktorý neposkytuje žiadnu metódu pre autentifikovanie smerovačov. Je určený na použitie v rámci dôvernej siete. Ak je váš systém v sieti s inými systémami, ktorým ″nedôverujete″, nemali by ste server RouteD spúšťať. Na zaistenie toho, aby sa server RouteD nespustil automaticky, napíšte nasledujúce:

  ```
  CHGRTDA AUTOSTART(*NO)
  ```

  **Poznámky:**

  1. AUTOSTART(*NO) je štandardná hodnota.
  2. “Riadenie serverov TCP/IP, ktoré sa majú spustiť automaticky” na strane 110 poskytuje viac informácií o riadení toho, ktoré TCP/IP sa spúšťajú automaticky.
- Zaistite, že riadite, kto môže zmeniť konfiguráciu RouteD, čo si vyžaduje špeciálne oprávnenie *IOSYSCFG.

- Ak sa váš systém zúčastňuje vo viac ako v jednej sieti (napríklad intranet a internet), môžete konfigurovať RouteD server na odosielanie a prijímanie aktualizácií len z bezpečnej siete.

# Úvahy o bezpečnosti pre používanie servera DNS

Server Systém názvu domény (DNS) poskytuje preklad názvu hostiteľa do IP adresy a naopak. Na serveroch iSeries je server DNS určený na poskytovanie prekladov adries pre internú, zabezpečenú sieť (intranet).

## Zamedzenie prístupu DNS

Ak *nechcete*, aby niekto používal DNS na získanie prístupu na váš systém, mali by ste urobiť nasledujúce:

1. Aby ste zabránili automatickému spusteniu úloh servera DNS pri spustení TCP/IP, napíšte nasledovné:

   ```
   CHGDNSA AUTOSTART(*NO)
   ```

   **Poznámky:**

   a. AUTOSTART(*NO) je štandardná hodnota.

   b. “Riadenie serverov TCP/IP, ktoré sa majú spustiť automaticky” na strane 110 poskytuje viac informácií o riadení toho, ktoré TCP/IP sa spúšťajú automaticky.

2. Aby ste zabránili priradeniu užívateľskej aplikácie, akou je napríklad soketová aplikácia, k portu, ktorý systém normálne používa pre DNS, urobte nasledovné:

   a. Na obrazovku ponuky Configure TCP/IP napíšte GO CFGTCP.

   b. Vyberte voľbu 4 (Work with TCP/IP port restrictions).

   c. Na obrazovke Work with TCP/IP Port Restrictions špecifikujte voľbu 1 (Add).

   d. Pre port nižšieho rozsahu špecifikujte 53.

   e. Pre port vyššieho rozsahu špecifikujte *ONLY.

      **Poznámky:**

      1) Obmedzenie portov sa stane účinné pri nasledovnom spustení TCP/IP. Ak je TCP/IP aktívne pri nastavení obmedzení portov, TCP/IP by ste mali ukončiť a opätovne ho spustiť.

      2) RFC1700 poskytuje informácie o bežne priradených číslach portov.

   f. Pre protokol špecifikujte *TCP.

   g. V poli pre užívateľský profil špecifikujte názov, ktorý je na vašom systéme chránený. (Chránený užívateľský profil je užívateľský profil, ktorý nevlastní programy adoptujúce oprávnenie a nemá heslo, ktoré poznajú iní používatelia.) Obmedzením portu na konkrétneho používateľa automaticky vylúčite všetkých ostatných používateľov.

   h. Zopakujte kroky 2c až 2g pre protokol *UDP (User datagram).

## Zabezpečenie servera DNS

Nasledujú bezpečnostné úvahy, keď na vašom iSeries systéme chcete používať DNS:

- Funkcia, ktorú poskytuje server DNS je preklad IP adresy a preklad názvu. Neposkytuje žiadny prístup k objektom na vašom systéme iSeries. Vašim rizikom, keď sa niekto cudzí dostane na váš server DNS je, že server poskytuje jednoduchý spôsob zobrazenia topológie vašej siete. Váš DNS by mohol hakerovi ušetriť čas v určovaní adries potenciálnych cieľov. Avšak váš DHS neposkytuje informácie, ktoré môžu pomôcť preniknúť do týchto cieľových systémov.
- Server DNS iSeries obvykle používate pre váš intranet. Preto pravdepodobne nemusíte obmedzovať schopnosť dotazovania DNS. Avšak by ste napríklad mohli mať niekoľko

podsietí v rámci vášho intranetu. Možno nebudete chcieť, aby používatelia z iných podsietí dokázali dotazovať DNS vo vašom serveri iSeries. Voľba zabezpečenia DNS vám umožňuje obmedzovať prístup k primárnej doméne. iSeries Navigator používajte na zadanie adries IP, na ktoré by mal server DNS odpovedať.

Iná voľba zabezpečenia vám umožní určiť, ktoré druhotné servery môžu kopírovať informácie z vášho primárneho servera DNS. Keď použijete túto možnosť, váš server bude akceptovať požiadavky zónového prenosu (požiadavku na kopírovanie informácií) len od druhotných serverov, ktoré explicitne určíte.

- Uistite sa, že ste pozorne obmedzili schopnosť meniť konfiguráciu súboru pre váš server DNS. Niekto so škodlivým zámerom by napríklad mohol zmeniť váš súbor DNS na ukazovanie na IP adresu mimo vašej siete. Mohli by simulovať server vo vašej sieti a možno by tak mohli získať prístup k dôverným informáciám od používateľov, ktorí navštevujú server.

## Úvahy o bezpečnosti pre používanie servera HTTP pre iSeries

Server HTTP poskytuje klientom internetového prehliadača pristúp k multimediálnym objektom serveru iSeries, ako sú dokumenty HTML (Hypertext Markup Language). Tiež podporuje špecifikáciu *Common Gateway Interface (CGI)*. Programátori aplikácií môžu písať programy CGI na rozšírenie funkčnosti servera.

Správca môže použiť Internet Connection Server alebo IBM HTTP server for iSeries, aby súbežne spustil viacero serverov na rovnakom serveri iSeries. Každý server, ktorý je spustený, sa nazýva **inštancia servera**. Každá inštancia servera má unikátny názov. Správca riadi, ktoré inštancie sa spustia a ktoré nie.

**Poznámka:** Musíte mať spustenú inštanciu *ADMIN HTTP servera, keď na konfigurovanie hocičoho z nasledovného používate webový prehliadač:

- Firewall pre iSeries
- Internet Connection Server
- Internet Connection Secure Server
- IBM HTTP Server for iSeries

Užívateľ (návštevník webovej stránky) nikdy nevidí prihlasovaciu obrazovku servera iSeries. Avšak správca servera iSeries musí všetky dokumenty HTML a programy CGI explicitne autorizovať pomocou ich definovania v direktívach HTTP. Navyše správca môže nastaviť bezpečnosť zdroja a autentifikáciu užívateľa (ID užívateľa a heslo) pre niektoré alebo pre všetky požiadavky.

Útok hakera by mohol spôsobiť odmietnutie služby vášmu webovému serveru. Váš server môže zistiť tento druh útoku prostredníctvom odkladu určitých požiadaviek klienta. Ak server nedostáva požiadavku od klienta, potom je možné, že ide o útok založený na odmietaní služieb. Stáva sa to po prvom pripojení klienta na váš server. Štandardne je server nastavený tak, že zistí a postihne takýto útok.

### Zamedzenie prístupu HTTP

Ak *nechcete*, aby niekto používal program na získanie prístupu na váš systém, mali by ste zabrániť spusteniu servera HTTP. Spravte nasledovné:

__ Krok 1. Aby ste zabránili automatickému spusteniu úloh servera HTTP pri spustení TCP/IP, napíšte nasledovné:

```
CHGHTTPA AUTOSTART(*NO)
```

**Poznámky:**

a. AUTOSTART(*NO) je štandardná hodnota.

b. “Riadenie serverov TCP/IP, ktoré sa majú spustiť automaticky” na strane 110 poskytuje viac informácií o riadení toho, ktoré TCP/IP sa spúšťajú automaticky.

__ Krok 2. Štandard je, že úloha servera HTTP používa užívateľský profil QTMHHTTP. Aby ste zabránili spusteniu servera HTTP, nastavte stav užívateľského profilu QTMHHTTP na *DISABLED.

## Riadenie prístupu do servera HTTP

Primárnym účelom servera HTTP je poskytovať prístup návštevníkov na webovú stránku vášho systému iSeries. Toho, kto navštevuje vašu webovú stránku si môžete predstaviť ako niekoho, kto si prezerá váš inzerát v obchodnom časopise. Návštevník nepozná hardvér a softvér webovej stránky, ako napr. aký typ servera používate a kde je fyzicky lokalizovaný. Obvykle nechcete medzi vašu webovú stránku a potenciálneho návštevníka umiestniť nejakú bariéru (akou je obrazovka Prihlasovania). Avšak mohli by ste chcieť obmedziť prístup k niektorým dokumentom alebo programom CGI, ktoré poskytuje vaša webová stránka.

Tiež by ste mohli chcieť, aby jeden systém iSeries poskytoval viaceré logické webové stránky. Napríklad váš systém iSeries by mohol podporovať odlišné odvetvia vášho podniku, ktoré majú odlišných zákazníkov. Pre každé odvetvie, budete chcieť webovú stránku, ktorá sa bude objavovať návštevníkovi úplne nezávisle. Navyše by ste mohli chcieť poskytovať interné webové stránky (intranet) s dôvernými informáciami o vašom podniku.

Ako správca bezpečnosti potrebujete ochrániť obsah vašej webovej stránky a zároveň zaistiť, že vaše bezpečnostné praktiky nebudú negatívne ovplyvňovať hodnotu vašej webovej stránky. Navyše musíte zaistiť, že činnosť HTTP neohrozí integritu vášho systému alebo vašej siete. Nasledujúce témy poskytujú tipy na zabezpečenie pri použití programu.

### Úvahy o správe

Nasleduje niekoľko úvah o bezpečnosti pre spravovanie vášho serveru internetu.

- Tiež môžete vykonávať nastavenie a konfigurovanie funkcií s použitím webového prehliadača a inštancie *ADMIN. Pre niektoré funkcie ako je vytváranie dodatočných inštancií na servere *musíte* používať server *ADMIN.
- Štandardný URL pre domácu stránku správy (domáca stránka pre server *ADMIN) je zverejnený v dokumentácií pre produkty, ktoré poskytujú funkcie správy prehliadača. Preto bude štandardné URL pravdepodobne známe hakerom a publikované na hakerských fórach, tak ako sú známe a publikované štandardné heslá pre užívateľské profily dodávané IBM. Môžete sa chrániť pred týmto odhalením niekoľkými spôsobmi:
  - Ak potrebujete vykonávať správcovské funkcie, pracujte iba s inštanciou *ADMIN servera HTTP. Nenechávajte bežať inštanciu *ADMIN po celý čas.
  - Aktivujte podporu SSL pre inštanciu *ADMIN (použitím Správcu digitálneho certifikátu). Inštancia *ADMIN používa direktívy ochrany HTTP na vyžiadanie si ID užívateľa a hesla. Keď používate SSL, vaše ID užívateľa a heslo sú kódované (spolu s ostatnými informáciami o konfigurácií, ktoré sa objavujú vo formulároch správy).
  - Používajte firewall na zabraňovanie prístupu na server *ADMIN z internetu a skryte svoj systém a názvy domén, ktoré sú súčasťou URL.
- Keď vykonávate funkcie správy, musíte sa prihlásiť užívateľským profilom, ktorý má špeciálne oprávnenie *IOSYSCFG. Tiež môžete potrebovať oprávnenie pre určité objekty na systéme, ako sú nasledujúce:
  - Knižnice a adresáre, ktoré obsahujú vaše dokumenty HTML a programy CGI.
  - Ľubovoľné užívateľské profily, ktoré plánujete vymieňať v rámci direktív pre server.
  - Zoznamy riadenia prístupu (ACL) pre ľubovoľné adresáre, ktoré používajú vaše direktívy.
  - Objekt overenia platnosti pre vytváranie a zachovávanie ID a hesiel.

So serverom *ADMIN a s TELNET, máte možnosť vykonávať funkcie správy na diaľku, napríklad prostredníctvom pripojenia internetu. Uvedomte si, že ak vykonávate správu prostredníctvom verejného spojenia (internetu) môžete odkrývať silné ID užívateľa a heslo pre snorenie. Snorič potom môže použiť toto ID užívateľa a heslo a pokúsiť sa získať prístup na váš systém s použitím napríklad TELNET alebo FTP.

**Poznámky:**

1. Pomocou TELNET sa obrazovka prihlasovania správa ako každá iná obrazovka. Hoci sa heslo nezobrazuje pri písaní, systém ho prenáša bez kódovania alebo šifrovania.
2. So serverom *ADMIN je heslo kódované, ale nie je zašifrované. Schéma kódovania je priemyselne štandardná a preto je všeobecne známa v komunite hakerov. Hoci bežný snorič nerozumie bez problémov kódovaniu, ale sofistikovaný snorič pravdepodobne má nástroje na to, aby sa pokúsil dekódovať heslo.

**Bezpečnostný tip**

Ak plánujete vykonávať vzdialené spravovanie prostredníctvom internetu, mali by ste používať inštanciu *ADMIN so SSL tak, aby vaše prenosy boli šifrované. Nepoužívajte nezabezpečené aplikácie ako napr. verzie TELNET pred V4R4 (TELNET podporuje SSL až od V4R4). Ak používate server *ADMIN na intranete *dôverných* užívateľov, môžete pravdepodobne bezpečne používať túto správu.

- Direktívy HTTP poskytujú základ pre celú činnosť na vašom systéme. Dodaná konfigurácia poskytuje schopnosť obsluhovať štandardnú uvítaciu stránku. Klient si nemôže prezerať žiadne dokumenty okrem uvítacej stránky, pokým správca serveru nedefinuje direktívy pre server. Na definovanie direktív používajte webový prehliadač a server *ADMIN alebo príkaz WRKHTTPCFG (Work with HTTP Configuration). Obe metódy si vyžadujú špeciálne oprávnenie *IOSYSCFG. Keď svoj server iSeries pripojíte k internetu, bude pre vás ešte oveľa dôležitejšie, aby sa prehodnotil a riadil počet užívateľov vo vašej organizácii, ktorí majú mimoriadne oprávnenie *IOSYSCFG.

## Ochrana prostriedkov

IBM HTTP server for iSeries obsahuje direktívy HTTP, ktoré môžu poskytnúť podrobné riadenie informačného majetku, ktorý používa server. Direktívy môžete použiť na riadenie toho, z ktorých adresárov má webový server obsluhovať URL pre súbory HTML i pre programy CGI, na odklad do ostatných užívateľských profilov a na požadovanie autentifikácie pre niektoré prostriedky.

**Poznámka:** Dokumentácia pod názvom ″Web serving″ v Information Center poskytuje úplné opisy dostupných direktív HTTP a to, ako sa majú používať. Nasleduje niekoľko návrhov na použitie tejto podpory:

- Server HTTP sa spúšťa zo základu ″explicitného oprávnenia″. Server neprijíma požiadavky, pokým požiadavka nie je explicitne definovaná v direktívach. Inými slovami server okamžite odmieta každú požiadavku pre URL, pokým toto URL nie je definované v direktívach (buď názvom alebo generický).
- Môžete použiť direktívy ochrany na získanie užívateľského ID a hesla ešte pred prijatím požiadavky pre niektoré alebo všetky vaše prostriedky.
  - Keď si užívateľ (klient) vyžaduje chránený zdroj, server vyzve prehliadač, aby mu poskytol ID užívateľa a heslo. Prehliadač upozorní užívateľa, aby zadal ID užívateľa a heslo a potom informácie odošle na server. Niektoré prehliadače ukladajú ID užívateľa a heslo a automaticky ich posielajú s nasledujúcimi požiadavkami. Toto odbremeňuje užívateľa od opakovaného zadávania ID užívateľa a hesla pri každej požiadavke.

    Pretože niektoré prehliadače ukladajú ID užívateľa a heslo, stojí pred vami rovnaká úloha vo výchove užívateľov, akú máte vtedy, keď používatelia zadajú váš systém

prostredníctvom prihlasovacej obrazovky servera iSeries alebo prostredníctvom smerovača. Neobsluhovaná relácia prehliadača predstavuje potenciálne odkrytie zabezpečenia.

– Máte tri možnosti pre to, ako bude systém obsluhovať ID užívateľa a heslá (určené v direktívach ochrany):

1. Môžete použiť validáciu užívateľského profilu a hesla normálneho servera iSeries. Toto sa najbežnejšie používa na ochranu zdrojov na intranete (bezpečná sieť).
2. Môžete vytvoriť ″užívateľov internetu″: užívateľov, ktorí môžu byť validovaní, ale nemajú užívateľský profil na serveri iSeries. Používatelia internetu sa implementujú prostredníctvom objektu servera iSeries, ktorý sa nazýva ″validačný zoznam″. Objekt ″preverovací zoznam″ obsahuje zoznam užívateľov a hesiel, ktoré sú špecificky definované iba na použitie určitej aplikácie.

   Vy sa rozhodujete, ako budú ponúkané užívateľské heslá a ID (napríklad, aplikáciou alebo správcom, ktorý bude odpovedať na emailovú požiadavku) a taktiež, ako ovládať užívateľov internetu. Používajte rozhranie HTTP servera založené na prehliadači pri nastavovaní tejto funkcie.

   Pri nezabezpečených sieťach (internet) používanie užívateľov internetu poskytuje lepšiu celkovú ochranu, ako používanie normálnych užívateľských profilov a hesiel. Jedinečná zostava užívateľských ID a hesiel vytvára zabudované obmedzenie toho, čo títo používatelia môžu robiť. ID užívateľov a heslá nie sú dostupné pre normálne prihlasovanie (ako je s TELNET alebo FTP). Okrem toho nevystavujete normálne ID užívateľa a heslá snoreniu.
3. Lightweight directory access protocol (LDAP) je protokol adresárových služieb, ktorý poskytuje prístup na adresár cez Transmission Control Protocol (TCP). Umožňuje vám ukladať informácie v danej adresárovej službe a dotazovať ich. LDAP je v súčasnosti podporované ako možnosť autentifikácie užívateľa.

**Poznámky:**

1. Keď prehliadač odosiela ID užívateľa a heslo (či už pre užívateľský profil alebo pre užívateľa internetu), tieto sú zakódované nie zašifrované. Schéma kódovania je priemyselne štandardná a preto je všeobecne známa v komunite hakerov. Hoci bežný snorič nerozumie bez problémov kódovaniu, ale sofistikovaný snorič pravdepodobne má nástroje na to, aby sa pokúsil dekódovať heslo.
2. Server iSeries ukladá validačný objekt do chránenej systémovej oblasti. Môžete na neho získať prístup len s definovanými rozhraniami systému (API) a vlastnou autorizáciou.

– Môžete použiť DCM (Digital Certificate Manager) na vytvorenie vašej vlastnej CA (Certificate Authority). Digitálny certifikát automaticky pridruží certifikát k užívateľskému profilu vlastníka. Certifikát má niektoré oprávnenia a povolenia ako priradený profil.

- Keď server akceptuje požiadavku, riadenie preberá bezpečnosť prostriedkov normálneho servera iSeries. Užívateľský profil, ktorý požaduje prostriedok musí mať oprávnenie k prostriedku (ako napríklad zložka alebo zdrojový fyzický súbor, ktorý obsahuje dokument HTML). Všetka činnosť serveru štandardne beží pod užívateľským profilom QTMHHTTP. Na odklad do iného užívateľského profilu môžete použiť direktívu. Systém potom používa oprávnenie toho užívateľského profilu pre prístup na objekty. Nasledujú návrhy a úvahy pre použitie tejto novej podpory:
  – Vymieňanie užívateľských profilov môže byť užitočné hlavne vtedy, keď váš server poskytuje viac ako jednu logickú webovú stránku. K inému užívateľskému profilu môžete priradiť direktívy pre každú webovú stránku, a tak použiť bezpečnosť prostriedkov normálneho servera iSeries na ochranu dokumentov pri každej stránke.
  – Môžete používať schopnosť vymieňať užívateľské profily v kombinácií s objektom overenia platnosti. Server používa jedinečné ID užívateľa a heslo (oddelené od vášho

normálneho ID užívateľa a hesla) na zhodnotenie počiatočnej požiadavky. Po autentifikácii užívateľa serverom, systém potom bude odkladať do iného užívateľského profilu, a tak využije výhodu bezpečnosti prostriedkov. Užívateľ tak nevie skutočný názov užívateľského profilu a nemôže sa pokúsiť použiť ho iným spôsobom (ako FTP).

- Niektoré požiadavky HTTP servera potrebujú program na HTTP serveri. Napríklad program, ktorý umožňuje prístup k údajom vo vašom systéme. Pred spustením programu, správca servera musí mapovať požiadavku (URL) na špecifický užívateľom definovaný program, ktorý vyhovuje štandardom užívateľského rozhrania CGI. Nasledujú návrhy a úvahy pre programy CGI:
  - Môžete používať direktívy ochrany pre programy CGI rovnako ako ich používate pre dokumenty HTML. Takže môžete si vyžadovať ID užívateľa a heslo pred spustením programu.
  - Všetky programy CGI bežia štandardne pod užívateľským profilom QTMHHTP1. Do iného užívateľského profilu môžete odkladať pred spustením programu. Preto môžete nastaviť bezpečnosť prostriedkov normálneho servera iSeries pre prostriedky, na ktoré majú vaše programy CGI prístup.
  - Ako správca bezpečnosti, by ste mali vykonať prehľad zabezpečenia pred oprávnením použitia ľubovoľného programu CGI na vašom systéme. Mali by ste vedieť, odkiaľ program prišiel a ktoré funkcie program CGI vykonáva. Tiež by ste mali monitorovať schopnosti užívateľských profilov pod ktorými spúšťate programy CGI. Tiež by ste mali vykonávať testovanie s programami CGI na určenie napríklad toho, či môžete získať prístup na príkazový riadok. Správajte sa k programom CGI rovnako opatrne ako sa správate k programom, ktoré prijímajú oprávnenie.
  - Navyše si určite zhodnoťte, ktoré citlivé objekty by mohli mať nevhodné verejné oprávnenie. Zle navrhnutý program CHI vy mohol v zriedkavých prípadoch dovoliť informovanému užívateľovi pokúsiť sa prehliadať si váš systém.
  - Použite špecifickú knižnicu užívateľa, akou napr. je CGILIB, na uchovávanie všetkých vašich programov CGI. Použite oprávnenie objektu na riadenie toho, kto môže umiestňovať nové objekty v tejto knižnici. Použite direktívy na to, aby ste obmedzili HTTP server na spúšťanie programov CGI, ktoré sú v tejto knižnici.

    **Poznámka:** Ak váš server poskytuje viaceré logické webové stránky, mohli by ste chcieť nastaviť oddelenú knižnicu pre programy CGI pre každú stránku.

### Ostatné úvahy o bezpečnosti

Nasledujú dodatočné úvahy o bezpečnosti:

- HTTP poskytuje prístup len na čítanie na váš systém iSeries. Požiadavky HTTP servera nemôžu priamo vymazávať alebo aktualizovať údaje na vašom systéme. Avšak môžete mať programy CGI, ktoré aktualizujú údaje. Okrem toho môžete povoliť, aby Net.Data program CGI mal prístup na databázu vášho servera iSeries. Systém používa skript (ktorý je podobný ukončovaciemu programu) na vyhodnotenie požiadaviek pre program Net.Data. Takto môže správca systému riadiť, ktoré akcie môže program Net.Data vykonávať.
- HTTP server poskytuje protokol prístupu, ktorý môžete používať na monitorovanie prístupov a pokusov o prístup cez server.

## Úvahy o bezpečnosti pre používanie SSL s IBM HTTP Server for iSeries

IBM HTTP Server for iSeries dokáže poskytovať bezpečné webové pripojenia na váš server iSeries. **Bezpečná webová stránka** znamená, že prenosy medzi klientom a serverom (v obidvoch smeroch) sú zašifrované. Tieto kryptované prenosy sú bezpečné pred pokusmi snoričov a pred tými, ktorí sa snažia buď zachytiť alebo pozmeniť prenosy.

**Poznámka:** Zapamätajte si, že bezpečná webová stránka sa týka informácií, ktoré prechádzajú medzi klientom a serverom. Jej zámerom nie je redukovať zraniteľnosť vášho servera hakermi. Avšak určite to obmedzuje informácie, ktoré by potenciálny haker mohol ľahko získať snorením.

Témy o SSL a Webserving (HTTP) v informačnom centre poskytujú kompletné informácie pre inštaláciu, konfiguráciu a riadenie procesu šifrovania. Tieto témy poskytujú prehľad vlastností servera a niektoré úvahy o použití servera.

Internet Connection Server poskytuje podporu HTTP a HTTPS, keď sa nainštaluje jeden z nasledujúcich licenčných programov:

- 5722–NC1
- 5722–NCE

Ak ste nainštalovali niektorú s týchto volieb, produkt sa bude teraz hlásiť ako zabezpečený server internetového pripojenia.

IBM HTTP Server for iSeries (5722–DG1) poskytuje podporu http i https. Musíte nainštalovať niektorý z nasledovných kryptografických produktov, aby bolo umožnené SSL:

- 5722–AC2
- 5722–AC3

Bezpečnosť, ktorá závisí od šifrovania, má niekoľko požiadaviek:

- Odosielateľ i prijímateľ (server a klient) musia ″chápať″ mechanizmus kryptovania a byť schopní vykonávať kryptovanie a dekryptovanie. Server HTTP požaduje klienta s umožneným SSL. (Najpopulárnejšie webové prehliadače sú SSL umožnené.) Licenčné programy kryptovania iSeries podporujú niekoľko priemyselne štandardných metód kryptovania. Keď sa klient snaží nadviazať bezpečnú reláciu, server a klient komunikujú, aby našli najbezpečnejšiu metódu kryptovania, ktorú oba podporujú.
- Prenos sa nesmie dať dekryptovať niekým, kto ho odpočúva. Takže metódy kryptovania si vyžadujú, aby obe strany mali **súkromný kľúč** kryptovania/dekryptovania, ktorý poznajú len ony. Ak chcete mať bezpečnú *externú* webovú stránku, mali by ste používať nezávislú certifikačnú autoritu (CA) na vytvorenie a vydanie digitálnych certifikátov užívateľom a serverom. Certifikačná autorita je známa ako dôveryhodná strana.

Kódovanie chráni dôvernosť prenášaných informácií. Avšak pre citlivé informácie ako sú finančné informácie chcete integritu a autenticitu spolu s dôvernosťou. Inými slovami klient a (voliteľne) server musí dôverovať strane na druhom konci (prostredníctvom nezávislej referencie) a musia si byť istí, že prenos nebol pozmenený. Digitálny podpis, ktorý poskytuje certifikačná autorita (CA) poskytuje potvrdenie autenticity a integrity. Protokol SSL zabezpečuje autentifikáciu overovaním platnosti digitálneho podpisu certifikátu servera (a voliteľne i certifikátu klienta).

Kryptovanie a dekryptovanie si vyžadujú čas na spracovanie a ovplyvnia výkon vašich prenosov. Preto servery iSeries poskytujú schopnosť spustiť programy aj pre zabezpečenú aj pre nezabezpečenú prevádzku servera v rovnakom čase. Môžete použiť nezabezpečený server HTTP na obsluhu dokumentov, ktoré nevyžadujú zabezpečenie, ako napríklad katalóg produktov. Tieto dokumenty budú mať URL, ktoré sa spúšťa s http://. Zabezpečený server HTTP môžete používať pre citlivé informácie ako je formulár, kde zákazník zadáva informácie o svojej kreditnej karte. Program môže poskytovať dokumenty, ktorých URL začína s http:// alebo https://.

**Pripomienka**

Dobrá internetová etika vraví, že vaši klienti majú byť informovaní o tom, kedy sú prenosy zabezpečené a nezabezpečené, zvlášť vtedy, keď vaša webová stránka používa pre niektoré dokumenty len zabezpečený server.

Pamätajte, že kryptovanie si vyžaduje zabezpečeného klienta a zabezpečený server. Zabezpečené prehliadače (klienti HTTP) sa stali celkom bežnými.

## Úvahy o bezpečnosti pre LDAP

K bezpečnostným vlastnostiam Lightweight Directory Access Protocol (LDAP) patrí Secure Sockets Layer (SSL), zoznamy riadenia prístupu a šifrovanie CRAM-MD5 pre heslá. Do úrovne V5R1, boli pre vylepšenie bezpečnosti LDAP pridané pripojenia Kerberos a podpora auditovania bezpečnosti.

Viac informácií o týchto témach nájdete v Informačnom centre iSeries—> Networking–>TCP/IP–>Adresárové služby (LDAP). V “Nevyhnutné predpoklady a súvisiace informácie” na strane xii nájdete informácie o získaní prístupu na Informačné centrum iSeries.

## Úvahy o bezpečnosti pre LPD

LPD (line printer daemon) poskytuje schopnosť distribuovať výstup tlačiarne vášmu systému. Systém nevykonáva žiadne spracovávanie prihlasovania pre LPD.

### Zamedzenie prístupu LPD

Ak *nechcete*, aby niekto používal LPD na získanie prístupu na váš systém, mali by ste zabrániť spusteniu servera LPD. Spravte nasledovné:

__ Krok 1. Aby ste zabránili automatickému spusteniu úloh servera LPD pri spustení TCP/IP, napíšte nasledovné:

```
CHGLPDA AUTOSTART(*NO)
```

**Poznámky:**

a. AUTOSTART(*YES) je štandardná hodnota.

b. “Riadenie serverov TCP/IP, ktoré sa majú spustiť automaticky” na strane 110 poskytuje viac informácií o riadení toho, ktoré TCP/IP sa spúšťajú automaticky.

__ Krok 2. Aby ste zabránili priradeniu užívateľskej aplikácie, akou je napríklad soketová aplikácia, k portu, ktorý systém normálne používa pre LPD, urobte nasledovné:

__ Krok a. Na obrazovku ponuky Configure TCP/IP napíšte GO CFGTCP.

__ Krok b. Vyberte voľbu 4 (Work with TCP/IP port restrictions).

__ Krok c. Na obrazovke Work with TCP/IP Port Restrictions špecifikujte voľbu 1 (Add).

__ Krok d. Pre port nižšieho rozsahu špecifikujte 515.

__ Krok e. Pre port vyššieho rozsahu špecifikujte *ONLY.

**Poznámky:**

1) Obmedzenie portov sa stane účinné pri nasledovnom spustení TCP/IP. Ak je TCP/IP aktívne pri nastavení obmedzení portov, TCP/IP by ste mali ukončiť a opätovne ho spustiť.

2) RFC1700 poskytuje informácie o bežne priradených číslach portov.

__ Krok f. Pre protokol špecifikujte *TCP.

__ Krok g. V poli pre užívateľský profil špecifikujte názov, ktorý je na vašom systéme chránený. (Chránený užívateľský profil je užívateľský profil, ktorý nevlastní programy adoptujúce oprávnenie a nemá heslo, ktoré poznajú iní používatelia.) Obmedzením portu na konkrétneho používateľa automaticky vylúčite všetkých ostatných používateľov.

__ Krok h. Zopakujte kroky 2c až 2g pre protokol *UDP.

## Riadenie prístupu LPD

Ak chcete povoliť klientom LPD prístup na váš systém, buďte si vedomý nasledujúcich bezpečnostných problémov:

- Aby ste zabránili používateľovi v zavalení vášho systému nechcenými objektmi, uistite sa, že ste nastavili adekvátne prahové limity pre vaše oblasti pomocnej pamäte (ASP). Môžete zobrazovať a nastavovať prahy pre ASP používaním buď SST (systémových nástrojov služieb) alebo DST (vyhradených nástrojov služieb). Kniha *Backup and Recovery* poskytujte ďalšie informácie o prahoch ASP.
- Môžete používať oprávnenie k výstupným frontom na obmedzovanie toho, kto môže posielať spoolové súbory na váš systém. Používatelia LPD bez ID užívateľa používajú užívateľský profil QTMPLPD. Môžete povoliť prístup tomuto užívateľskému profilu len na niekoľko málo výstupných frontov.

# Úvahy o bezpečnosti pre SNMP

Server iSeries sa môže v sieti chovať ako agent SNMP (simple network management protocol). SNMP poskytuje prostriedky na riadenie brán, smerovačov a hostiteľov v sieťovom prostredí. Agent SNMP zbiera informácie o systéme a vykonáva funkcie, ktoré si vyžadujú vzdialení správcovia siete SNMP.

## Zamedzenie prístupu SNMP

Ak *nechcete*, aby niekto používal SNMP na získanie prístupu na váš systém, mali by ste zabrániť spusteniu servera SNMP. Spravte nasledovné:

__ Krok 1. Aby ste zabránili automatickému spusteniu úloh servera SNMP pri spustení TCP/IP, napíšte nasledovné:

```
CHGSNMPA AUTOSTART(*NO)
```

**Poznámky:**

a. AUTOSTART(*YES) je štandardná hodnota.

b. “Riadenie serverov TCP/IP, ktoré sa majú spustiť automaticky” na strane 110 poskytuje viac informácií o riadení toho, ktoré TCP/IP sa spúšťajú automaticky.

__ Krok 2. Aby ste zabránili priradeniu užívateľskej aplikácie, akou je napríklad soketová aplikácia, k portu, ktorý systém normálne používa pre SNMP, urobte nasledovné:

__ Krok a. Na obrazovku ponuky Configure TCP/IP napíšte GO CFGTCP.

__ Krok b. Vyberte voľbu 4 (Work with TCP/IP port restrictions).

__ Krok c. Na obrazovke Work with TCP/IP Port Restrictions špecifikujte voľbu 1 (Add).

__ Krok d. Pre port nižšieho rozsahu špecifikujte 161.

__ Krok e. Pre port vyššieho rozsahu špecifikujte *ONLY.

**Poznámky:**

1) Obmedzenie portov sa stane účinné pri nasledovnom spustení TCP/IP. Ak je TCP/IP aktívne pri nastavení obmedzení portov, TCP/IP by ste mali ukončiť a opätovne ho spustiť.
2) RFC1700 poskytuje informácie o bežne priradených číslach portov.

__ Krok f. Pre protokol špecifikujte *TCP.

__ Krok g. V poli pre užívateľský profil špecifikujte názov, ktorý je na vašom systéme chránený. (Chránený užívateľský profil je užívateľský profil, ktorý nevlastní programy adoptujúce oprávnenie a nemá heslo, ktoré poznajú iní používatelia.) Obmedzením portu na konkrétneho používateľa automaticky vylúčite všetkých ostatných používateľov.

__ Krok h. Zopakujte kroky 2c až 2g pre protokol *UDP.

## Riadenie prístupu SNMP

Ak chcete povoliť managerom SNMP prístup na váš systém, buďte si vedomí nasledujúcich bezpečnostných problémov:

- Ten, kto môže získať prístup na vašu sieť so SNMP, môže zbierať informácie o vašej sieti. Informácie, ktoré máte skryté s použitím aliasov a servera názvu domény sa stávajú dostupnými pre potenciálneho votrelca cez SNMP. Navyše votrelec by mohol použiť SNMP na zmenu konfigurácie vašej siete a na prerušenie vašich komunikácií.
- SNMP sa spolieha na názov komunity pre prístup. Koncepčne je názov komunity podobný heslu. Názov komunity nie je kryptovaný. Preto je zraniteľný pre snifovanie. Použite ADDCOMSNMP (Add Community for SNMP). Príkaz na nastavenie parametra managera INTNETADR (internet address) na jednu alebo viac určitých IP adries namiesto *ANY. Takisto môžete nastaviť parameter OBJACC príkazov ADDCOMSNMP alebo CHGCOMSNMP na hodnotu *NONE, a zabrániť tak správcom komunity, aby mohli pristupovať na objekty MIB. Tento krok bol plánovaný iba za účelom dočasného odmietnutia prístupu správcov komunity bez toho, aby bola odstránená komunita.

# Úvahy o bezpečnosti pre server INETD

Na rozdiel od väčšiny serverov TCP/IP server INETD neposkytuje klientom jednotnú službu. Namiesto toho ponúka množstvo rôznych služieb, ktoré môže správca prispôsobovať. Z tohto dôvodu sa server INETD niekedy nazýva aj ″super server″. Server INETD obsahuje niektoré zabudované služby:

- čas
- deň
- echo
- výmaz
- zmenené

Tieto služby sú podporované TCP aj UDP. Pre UDP odozva, čas, čas dňa a zmenené služby dostávajú UDP pakety a potom ich posielajú späť pôvodcovi. Odozvový server zasiela späť pakety, ktoré dostáva, servery času a času dňa generujú čas v špecifickom formáte a zasielajú ho späť a zmenený server generuje paket vytlačiteľných znakov ASCII a zasiela ho späť.

Podstata týchto UDP služieb robí systém zraniteľný voči útoku, ktorý spočíva v odopretí služby. Napríklad, predpokladajme, že máte dva servery iSeries: SYSTEMA a SYSTEMB. Šikovný programátor sa môže prepracovať k IP hlavičke, k UDP hlavičke so zdrojovou adresou systému SYSTEMA a k číslu portu UDP príslušného pre server času. Potom bude schopný odosielať tieto pakety na server času systému SYSTEMB, ktorý bude odosielať čas

do SYSTEMA, ktorý bude následne odpovedať späť SYSTEMB, atď. - takto sa vytvorí nepretržitá slučka, ktorá spotrebuje prostriedky CPU na oboch systémoch a takisto sieťovú šírku pásma.

Preto by ste mali uvážiť riziko takéhoto útoku na váš iSeries systém a tieto služby spúšťať len na bezpečnej sieti. Server INETD, ktorý ste dostali, nie je nastavený tak, aby sa spustil automaticky, keď spustíte TCP/IP. Je možné ho nakonfigurovať na spustenie (alebo nespustenie) služieb pri spustení INETD. Štandardne sa TCP a UDP servery času a dňa obidva spúšťajú zároveň so spustením servera INETD.

Existujú dva konfiguračné súbory pre server INETD:

```
/QIBM/UserData/OS400/inetd/inetd.conf
/QIBM/ProdData/OS400/inetd/inetd.conf
```

Tieto súbory určujú, ktoré programy sa spustia zároveň so spustením servera INETD. Taktiež určujú, pod ktorým užívateľským profilom tieto programy bežia, keď ich INETD spúšťa.

**Poznámka:** Konfiguračný súbor v adresári proddata by nemal byť nikdy modifikovaný. Tento sa nahrádza zakaždým, keď sa znova zavádza systém. Zákaznícke konfiguračné zmeny by mali byť iba umiestnené do súboru v strome adresárov užívateľských údajov, keďže tento súbor sa **neaktualizuje** počas prechodov vydaní na vyššiu úroveň.

Ak niektorý programátor získa prístup k týmto súborom, môže ich prekonfigurovať na spustenie hociktorého programu spolu so spustením servera INETD. Preto je veľmi dôležitá ochrana týchto súborov. Na vykonávanie zmien štandardne vyžadujú oprávnenie QSECOFR. Nemali by ste rozširovať pôsobnosť tohto oprávnenia.

**Poznámka:** Nemodifikujte konfiguračný súbor v adresári ProdData. Tento súbor je premiestňovaný vždy, keď sa opätovne zavádza systém. Konfiguračné zmeny zákazníka sa môžu vykonať iba v adresárovom strome UserData, pretože tento súbor nebýva aktualizovaný.

## Úvahy o bezpečnosti pre obmedzenie roamingu TCP/IP

Ak je váš systém pripojený na sieť, môžete chcieť obmedziť schopnosť vašich používateľov ' roamingovať vašu sieť s aplikáciami TCP/IP. Jedným zo spôsobov, ako to vykonať, je obmedziť prístup na nasledujúce klientske príkazy TCP/IP:

**Poznámka:** Tieto príkazy môžu existovať v niekoľkých knižniciach na vašom systéme. Minimálne sú v knižniciach QSYS a QTCP. Uistite sa, že ste našli a zabezpečili všetky výskyty.

- STRTCPFTP
- FTP
- STRTCPTELN
- TELNET
- LPR
- SNDTCPSPLF
- RUNRMTCMD (REXEC client)

Možné ciele vašich používateľov sú determinované nasledovným:

- Položkami vo vašej tabuľke hostiteľa TCP/IP.
- Položkou *DFTROUTE v tabuľke smeru TCP/IP. Toto umožňuje používateľom zadávať IP adresy systému ďalšieho skoku, keď je ich cieľ neznámy sieti. Používateľ môže dosiahnuť alebo kontaktovať vzdialenú sieť použitím štandardného smeru.

- Konfigurácie servera vzdialeného názvu. Táto podpora umožňuje inému serveru v sieti nájsť názvy hostiteľov pre vašich používateľov.
- Tabuľka vzdialeného systému.

Potrebujete riadiť, kto môže pridávať položky do týchto tabuliek a meniť vašu konfiguráciu. Tiež musíte porozumieť implikáciám vašich položiek v tabuľkách a vašej konfigurácií.

Buďte si vedomý toho, že informovaný používateľ s prístupom na kompilujúci program ILE C môže vytvoriť soketový program, ktorý môže pridať k TCP alebo k portu UDP. Môžete mu to sťažiť obmedzením prístupu k nasledujúcim súborom rozhrania soketov v knižnici QSYSINC:
- SYS
- NETINET
- H
- ARPA
- sokety a SSL

Pri servisných programoch môžete obmedziť použitie soketov a aplikácií SSL, ktoré sú už skompilované pomocou obmedzenia použitia týchto servisných programov:
- QSOSRV1
- QSOSRV2
- QSOSKIT(SSL)
- QSOSSLSR(SSL)

Programy služieb sú dodávané s verejným oprávnením *USE, ale oprávnenie sa dá zmeniť na *EXCLUDE (alebo na iné hodnoty podľa potreby).

# Kapitola 14. Bezpečný prístup na pracovnú stanicu

Mnohí z užívateľov vášho systému majú na svojich stoloch, ako svoje pracovné stanice, osobné počítače (PC). Používajú nástroje, ktoré sa spúšťajú na PC a PC používajú na pripojenie sa k serveru iSeries.

Väčšina metód pre pripojenia PC k serverom iSeries poskytuje viac funkcií, ako len emuláciu pracovnej stanice. PC môže vyzerať ako obrazovka pre iSeries a poskytuje používateľovi interaktívne prihlasovacie relácie. Okrem toho sa môže PC javiť serverom iSeries ako ďalší počítač a poskytovať funkcie, ako je prenos súborov a volanie vzdialených procedúr.

Ako bezpečnostný správca servera iSeries si musíte byť vedomý nasledujúceho:

- Funkcie, ktoré sú k dispozícii používateľom PC, ktorí sú pripojení do vášho systému
- Prostriedky servera iSeries, ku ktorým môžu mať používatelia PC prístup.

Ak chcete, môžete zabrániť rozšíreným funkciám PC (ako je prenos súborov a volanie vzdialených procedúr), ak bezpečnostná schéma vášho servera iSeries ešte nie je pre tieto funkcie pripravená. Pravdepodobne je váš dlhotrvajúci cieľ umožniť rozšírené funkcie PC a zároveň chrániť informácie na vašom systéme. V nasledovných témach sú rozobrané otázky bezpečnosti, ktoré sa týkajú prístupu PC.

## Zabránenie vírusov pracovnej stanice

Tieto informácie navrhujú spôsoby, ktorými môžu správcovia bezpečnosti ochrániť systém pred PC vírusmi.

## Bezpečný prístup k údajom pracovnej stanice

Softvér niektorých klientov PC používa na ukladanie informácií o serveri zdieľané zložky. Na prístup k databázovým súborom iSeries má používateľ PC obmedzenú, dobre definovanú množinu rozhraní. Pomocou funkcie prenosu súborov, ktorá je súčasťou väčšiny klient/server softvéru môžu používatelia PC kopírovať súbory medzi serverom a PC. Pomocou funkcie prístup do databázy; ako je napríklad súbor DDM, vzdialené SQL alebo ovládač ODBC; môžu používatelia PC získať prístup k údajom na serveri.

V tomto prostredí môžete vytvárať programy pre zastavenie a vyhodnotenie požiadaviek užívateľa PC na prístup k prostriedkom servera. Keď požiadavky používajú súbor DDM, môžete špecifikovať ukončovací program v atribúte siete DDMACC (distributed data management access). Pre niektoré metódy prenosu súborov PC môžete špecifikovať ukončovací program v atribúte siete PCSACC (client request access). Alebo, môžete špecifikovať PCSACC(*REGFAC), aby sa použila registračná funkcia. Keď požiadavka na prístup k údajom používa iné funkcie servera, môžete použiť príkaz WRKREGINF na zaregistrovanie ukončovacieho programu pre tieto funkcie servera.

Ukončovacie programy sa ťažko navrhujú a zriedkavo sú spoľahlivé. Ukončovacie programy nie sú nahradením oprávnením objektov, ktoré je navrhnuté na chránenie vašich objektov pred neoprávneným prístupom z ľubovoľného zdroja.

Softvér niektorých klientov PC, ako napríklad IBM iSeries Access for Windows, používa Integrovaný súborový systém na ukladanie a prístup k údajom na serveroch iSeries. Pomocou Integrovaného súborového systému sa stane celý server ľahšie dostupnejším pre užívateľov PC. Oprávnenie na objekt sa stáva dôležitejšie. Prostredníctvom Integrovaného súborového

systému si môže užívateľ s dostatočným oprávnením prezerať knižnicu servera, ako keby to bol adresár PC. Jednoduché príkazy presunúť a kopírovať dokážu ihneď presunúť údaje z knižnice servera iSeries do adresára PC alebo naopak. Systém automaticky vykoná vhodné zmeny do formátu údajov.

**Poznámky:**

1. Na riadenie použitia objektov v súborovom systéme QSYS.LIB môžete použiť zoznamy oprávnení. Pozrite si “Obmedzenie prístupu k súborovému systému QSYS.LIB” na strane 90, kde nájdete viac informácií.
2. Kapitola 11, “Použitie Integrovaného súborového systému na zabezpečenie súborov”, na strane 85 poskytuje viac informácií o bezpečnostných otázkach k Integrovanému súborovému systému.

Sila Integrovaného súborového systému je v jeho jednoduchosti pre používateľov a vývojárov. S jedným rozhraním môže používateľ pracovať s objektmi vo viacerých prostrediach. Používateľ PC nepotrebuje na prístup k objektom žiaden špeciálny softvér alebo API. Namiesto toho môže používateľ PC používať na priamu prácu s objektmi známe príkazy alebo metódou “ukáž a klikni”.

Pre všetky systémy, ktoré majú pripojené PC, ale hlavne systémy so softvérom klienta, ktorý používa Integrovaný súborový systém, je dôležitá dobrá schéma oprávnenia objektov. Pretože bezpečnosť je integrovaná do produktu OS/400, každá požiadavka na prístup k údajom musí prejsť procesom kontroly oprávnenia. Kontrola oprávnenia sa týka požiadaviek z každého zdroja a prístupu na údaje pomocou ľubovoľnej metódy.

## Oprávnenie k objektu s prístupom na pracovnú stanicu

Keď nastavíte oprávnenie pre objekty, musíte vyhodnotiť, aké oprávnenia poskytnúť používateľovi PC. Napríklad, keď má používateľ na súbor oprávnenie *USE, používateľ si môže prezerať a tlačiť údaje v tomto súbore. Používateľ nemôže meniť informácie v súbore ani ho vymazať. Pre používateľa PC je prezeranie ekvivalentné “čítaniu”, ktoré poskytuje dostatočné oprávnenie pre používateľa na spravenie kópie súboru na PC. Nemusí to byť to, čo ste zamýšľali.

Niektorým dôležitým súborom možno budete musieť nastaviť verejné oprávnenie na *EXCLUDE, aby sa zabránilo ich sťahovaniu. Potom môžete poskytnúť inú metódu pre “prezeranie” súboru na serveri, ako napríklad používanie ponúk a programov, ktoré si oprávnenie adoptujú.

Ďalšou voľbou na zabránenie sťahovania je použitie výstupného programu, ktorý sa spustí vždy, keď užívateľ PC spustí funkciu servera (inú ako je interaktívne prihlásenie). Ukončovací program môžete špecifikovať pomocou atribútu siete PCSACC pomocou príkazu CHGNETA (Change Network Attribute). Alebo, ukončovací program môžete zaregistrovať príkazom WRKREGINF (Work with Registration Information). Metóda, ktorú použijete, záleží na spôsobe prístupu PC k údajom na vašom systéme a ktorý program klienta PC používajú. Ukončovací program (QIBM_QPWFS_FILE_SERV) sa používa na prístup iSeries Access a Net Server do IFS. Nezabraňuje prístupu z PC pomocou iného mechanizmu, ako je FTP alebo ODBC.

Softvér PC tiež typicky poskytuje funkciu odosielania, takže užívateľ môže kopírovať údaje z PC do databázového súboru servera. Ak ste správne nenastavili svoju schému oprávnenia, používatelia PC môžu prekryť všetky údaje v súbore s údajmi z PC. Budete musieť pozorne prideliť oprávnenie *CHANGE. Pozrite si Prílohu D v knihe *iSeries Security Reference*, ktorá vám vysvetlí, aké oprávnenie sa vyžaduje na operácie so súbormi.

iSeries Information Center poskytuje informácie o oprávnení pre PC funkcie a o používaní ukončovacích programoch. Pozrite detaily v časti “Nevyhnutné predpoklady a súvisiace informácie” na strane xii.

## Správa aplikácií

Správa aplikácií je voliteľne inštalovateľný komponent grafického užívateľského rozhrania (GUI) pre server iSeries aplikácie iSeries Navigator. Správa aplikácií umožňuje správcom systému riadiť funkcie alebo aplikácie, ktoré sú dostupné užívateľom a skupinám na špecifickom serveri. Sem patrí riadenie funkcií, ktoré sú dostupné pre užívateľov, ktorí pristupujú na ich server prostredníctvom klientov. Je dôležité, aby ste si tu všimli, že ak pristúpite na server z klienta Windows, užívateľ servera iSeries, a nie užívateľ Windows, určí funkcie, ktoré sú dostupné pre správu.

Kompletnú dokumentáciu k iSeries Navigator Application Administration, nájdete v iSeries Information Center–>Connecting to iSeries—>What to connect with—>iSeries Navigator (../html/as400/v5r2/ic2924/info/rzaj3/rzaj3overview.htm).

### Správa politiky

Politika je nástrojom správcov, ktorý ho používajú pri konfigurácii softvéru na svojich klientskych PC. Politika môže obmedziť, ku ktorým funkciám a aplikáciám má užívateľ na PC prístup. Politika môže tiež navrhnúť alebo určiť, ktoré konfigurácie majú určití používatelia alebo PC použiť.

**Poznámka:** Politiky neponúkajú riadenie nad prostriedkami servera. Politiky nie sú náhradou za bezpečnosť servera. Politiky sa môžu použiť na ovplyvnenie toho, ako iSeries Access dokáže získať prístup na server z určitého PC pomocou určitého užívateľa. Nezmenia však to, ako sa dá získať prístup na prostriedky servera cez ostatné mechanizmy.

Politika je uložená na súborovom serveri. Pri každom prihlásení užívateľa na jeho pracovnú stanicu Windows sa politiky, ktoré sa aplikujú na tohto užívateľa Windows, stiahnu zo súborového servera. Skôr, než bude môcť užívateľ čokoľvek na pracovnej stanici vykonať, použije táto politika register.

Politiky **Microsoft verzus správa aplikácií**

iSeries Access Express podporuje dve rôzne stratégie pre implementáciu administratívneho riadenia vo vašej sieti: systémové politiky Microsoft a iSeries Navigator Application Administration. Keď sa budete rozhodovať, ktorá stratégia je najlepšia pre vaše potreby, zvážte nasledovné:

**Systémové politiky Microsoft**

Politiky sú riadené osobným počítačom, nezávisia na vydaniach OS/400. Politiky sa môžu aplikovať na PC, ako aj na užívateľov Windows. To znamená, že používatelia odkazujú na užívateľský profil Windows, nie na užívateľský profil servera. Politika sa môže použiť na ″konfiguráciu″, ako aj na reštrikciu. Politika zvyčajne ponúkne viac granularity, než Správa aplikácie a tiež aj väčšie množstvo funkcií. Je to spôsobené tým, že pripojenie na server nie je potrebné na určenie, či môže užívateľ funkciu použiť alebo nie. Implementácia politík je oveľa zložitejšia ako implementácia Správy aplikácií, pretože sa vyžaduje použitie editora systémovej politiky od Microsoft a PC sa musia individuálne nastaviť na sťahovanie politík.

**Správa aplikácií iSeries Navigator**

Správa aplikácií pridružuje údaje s užívateľskému profilu, a nie k profilu Windows, ku ktorému sa pridružujú systémové politiky Microsoft. Zatiaľ čo servery iSeries, ktoré majú

spustenú V4R3 alebo novšiu produktu OS/400 sú povinné pre používanie Správy aplikácií, niektoré funkcie sú k dispozícii iba v úrovni V4R4 alebo vyššej. Správa aplikácií používa na správu grafické užívateľské rozhranie aplikácie iSeries Navigator, ktoré sa používa oveľa ľahšie ako editor politík. Informácie Správy aplikácií sa týkajú užívateľa, bez ohľadu na to, z ktorého PC sa prihlasuje. Určité funkcie v rámci iSeries Navigator sa dajú obmedziť. Správa aplikácií sa uprednostňuje vtedy, ak Správa aplikácií podporuje všetky funkcie, ktoré chcete obmedziť a ak použitá verzia OS/400 podporuje Správu aplikácií.

## Použitie SSL s iSeries Access for Windows

Informácie o používaní iSeries Access Express s SSL, poskytujú témy iSeries Information Center *Administrácia Secure Sockets Layer, Zabezpečenie iSeries Access Express a iSeries Navigator, iSeries Developer Kit for Java a iSeries Java Toolbox* pod hlavnou témou Java. Tieto informácie si tiež môžete pozrieť na CD, dodanom s vašim systémom.

## Bezpečnosť iSeries Navigator

iSeries Navigator poskytuje jednoduché rozhranie k vášmu serveru pre užívateľov, ktorí majú iSeries Access. S každým novým vydaním produktu OS/400 sa prostredníctvom iSeries Navigator sprístupňuje stále viac funkcií servera. Ľahko použiteľné užívateľské rozhranie poskytuje veľa výhod vrátane znížených nákladov na technickú podporu a vylepšený imidž pre váš systém. Prezentuje tiež bezpečnostné výzvy.

Ako správca bezpečnosti sa už ďalej nemôžete pri chránení prostriedkov spoliehať na ignoráciu vašimi užívateľmi. iSeries Navigator uľahčuje a zviditeľňuje pre vašich užívateľov veľa funkcií. Aby ste splnili vaše všetky bezpečnostné potreby, presvedčte sa, že máte navrhnuté a implementované bezpečnostné politiky pre užívateľské profily a zabezpečenie objektov.

V4R4 a novšie verzie IBM e(logo)server iSeries Access for Windows poskytujú nasledujúce metódy na riadenie funkcií, ktoré môžu používatelia vykonávať prostredníctvom iSeries Navigator:

- Selektívna inštalácia
- Správa aplikácií
- Podpora systémových politík Windows NT

iSeries Navigator je zbalený do viacerých komponentov, ktoré môžete nainštalovať osobitne. Toto vám umožňuje nainštalovať len funkcie, ktoré požadujete. Správa aplikácií správcovi umožňuje riadiť funkcie, na ktoré môže mať prístup užívateľ alebo skupina prostredníctvom iSeries Navigator. Správa aplikácie triedi aplikácie do týchto kategórií:

**iSeries Navigator**
Obsahuje iSeries Navigator a všetky doplnkové komponenty.

**Klientske aplikácie**
Zahŕňa všetky ostatné klientske aplikácie vrátane iSeries Access, ktoré poskytujú funkcie na klientoch, ktorí sú spravovaní cez administráciu aplikácie.

**Hostiteľské aplikácie**
Obsahujú všetky aplikácie, ktoré sú celé trvalo umiestnené na vašom serveri a poskytujú funkcie, ktoré sa spravujú prostredníctvom Správy aplikácií.

Na obmedzenie funkcií aplikácie iSeries Navigator, ku ktorým má prístup užívateľ, môžete použiť selektívnu inštaláciu, správu aplikácií a politiky. Na zabezpečenie prostriedkov by ste však nemali používať nič z uvedeného.

Počnúc od V4R4, IBM e(logo)server iSeries Access for Windows tiež podporuje použitie Editora systémovej politiky Windows NT na riadenie funkcií, ktoré sa môžu vykonávať z konkrétneho PC klienta, bez ohľadu na to, kto používa dané PC.

Pozrite si iSeries Information Center, kde nájdete dodatočné informácie o selektívnej inštalácii, Správe aplikácií a Správe politík. Sekcia “Obmedzenie prístupu k funkciám programu” na strane 5 v tejto príručke taktiež obsahuje bližšiu rozpravu o správe aplikácií.

## Zamedzenie prístupu ODBC

Open database connectivity (ODBC) je nástroj, ktorý môžu používať PC aplikácie na prístup k údajom iSeries, ako keby to boli údaje na PC. Programátor ODBC môže urobiť fyzické umiestnenie údajov jasné pre používateľa PC aplikácie. Viac informácií ohľadne úvah o bezpečnosti ODBC získate v informáciách ″iSeries Access for Windows ODBC security″ (/rzaii/rzaiiodbc09.HTM), ktoré sú umiestnené v informačnom centre iSeries.

## Úvahy o bezpečnosti o heslách relácií pracovnej stanice

Za normálnych okolností, keď užívateľ PC spustí softvér pre pripojenie, ako napríklad iSeries Access, užívateľ raz napíše ID užívateľa a heslo pre server. Heslo sa zakóduje a uloží sa do pamäte PC. Keď následne užívateľ vytvára novú reláciu do rovnakého servera, PC odošle ID užívateľa a heslo automaticky.

Niektorý softvér typu klient/server tiež povoľuje voľbu obídenia prihlasovacej obrazovky pre interaktívne relácie. Pri spustení interaktívnej relácie (emulácia 5250) softvér odošle ID užívateľa a zakódované heslo. Ak chcete podporu tejto voľby, systémová hodnota QRMTSIGN na serveri sa musí nastaviť na *VERIFY.

Keď umožníte obídenie prihlasovacej obrazovky, musíte zvážiť kompromisy v bezpečnosti.

**Odhalenie bezpečnosti:** Pri emulácii 5250 alebo nejakom inom type interaktívnej relácie je prihlasovacia obrazovka rovnaká ako každá iná obrazovka. Hoci sa heslo pri písaní na obrazovke nezobrazuje, posiela cez pripojenie v nezakódovanej forme ako iné údajové polia. Pri niektorých typoch pripojení toto môže umožniť možnému narušiteľovi monitorovať pripojenie a zistiť ID užívateľa a heslo. Monitorovanie pripojenia elektronickým zariadením sa často nazýva **snorenie**. Od verzie V4R4 môžete používať SSL (secure sockets layer) na šifrovanie komunikácie medzi iSeries Access a serverom iSeries. Takto ochránite svoje údaje (aj heslá) pred zverejnením.

Keď vyberiete voľbu obídenia prihlasovacej obrazovky, PC zakóduje heslo pred jeho odoslaním. Zakódovanie bráni možnosti ukradnutia hesla pomocou snorenia. Musíte však zaistiť, že vaši používatelia PC vykonávajú operačnú bezpečnosť. Neobsluhované PC s aktívnou reláciu do systému iSeries poskytuje hocikomu príležitosť na spustenie ďalšej relácie bez toho, aby poznal ID užívateľa a heslo. PC by mali byť nastavené na zamykanie pri dlhej nečinnosti systému a na obnovenie relácie by mali vyžadovať heslo.

Dokonca aj keď nevyberiete obídenie prihlasovacej obrazovky, neobsluhované PC s aktívnou reláciou predstavuje bezpečnostné riziko. Pomocou softvéru PC môže znovu ktokoľvek spustiť reláciu do servera a pristupovať na údaje bez toho, aby poznal ID užívateľa a heslo. Riziko pri emulácii 5250 je o niečo väčšie, pretože na spustenie relácie a začatie pristupovania na údaje stačí aj menej vedomostí.

Musíte tiež svojich užívateľov poučiť o účinkoch odpojenia ich relácie iSeries Access. Mnoho užívateľov predpokladá (logicky, ale nesprávne), že voľba odpojenia celkom zastaví ich pripojenie k serveru. V skutočnosti, keď užívateľ vyberie voľbu pre odpojenie, server sprístupní reláciu (licenciu) užívateľa pre druhého užívateľa. Klientske pripojenie k serveru je

však stále otvorené. Ďalší užívateľ by mohol vstúpiť do nechráneného PC a získať prístup na prostriedky servera bez toho, aby musel zadať ID užívateľa a heslo.

Svojim užívateľom môžete na odpojenie ich relácie navrhnúť dve metódy:

- Presvedčte sa, že ich PC majú funkciu na zamykanie vyžadujúcu heslo. Týmto sa stane neobsluhované PC nedostupné pre každého, kto nepozná heslo.
- Aby ste úplne odpojili reláciu, odhláste sa z Windows alebo reštartujte PC. Toto ukončí reláciu do iSeries.

Tiež musíte svojich užívateľov poučiť o potenciálnom odhalení bezpečnosti pri používaní iSeries Access for Windows. Keď užívateľ zadá UNC (universal naming convention) na identifikáciu prostriedku iSeries, klient Win95 alebo NT vytvorí sieťové pripojenie tak, aby odkazovalo na server. Pretože užívateľ špecifikuje UNC, nevidí ho ako Sieťovú jednotku. Často si užívateľ nie je vedomý existencie sieťového pripojenia. Toto sieťové pripojenie však na neobsluhovanom PC predstavuje odhalenie bezpečnosti, pretože server sa v PC objavuje v strome adresárov. Ak má relácia užívateľa silný užívateľský profil, prostriedky servera môžu byť na neobsluhovanom PC odhalené. Podobne ako v predchádzajúcom príklade pomôže, ak používatelia porozumejú rizikám a na svojich PC budú používať funkciu na zamykanie.

## Ochrana servera pred vzdialenými príkazmi a procedúrami

Informovaný užívateľ PC so softvérom, ako je napríklad iSeries Access, dokáže na serveri spustiť príkazy bez toho, aby prešiel cez prihlasovaciu obrazovku. Nasleduje niekoľko metód, ktoré sú k dispozícii užívateľom PC na spustenie príkazov servera. Dostupné metódy pre užívateľov PC určuje softvér typu klient/server.

- Na spustenie príkazu môže užívateľ otvoriť súbor DDM a použiť funkciu vzdialeného príkazu.
- Niektorý softvér, ako napríklad optimalizovaní klienti iSeries Access, poskytuje prostredníctvom API pre DPC (Distributed Program Call) funkciu vzdialených príkazov bez použitia DDM.
- Niektorý softvér, ako je vzdialené SQL a ODBC, poskytuje funkciu vzdialeného príkazu bez DDM alebo DPC.

Pre softvér typu klient/server, používajúci DDM na podporu vzdialených príkazov, môžete na úplné zabránenie vzdialeným príkazom použiť sieťový atribút DDMACC . Pre softvér typu klient/server, ktorý používa podporu iného servera, môžete pre server zaregistrovať ukončovacie programy. Ak chcete umožniť vzdialené príkazy musíte zaručiť, aby vaša schéma oprávnenia objektov adekvátne chránila vaše údaje. Funkcia vzdialeného príkazu je rovnaká, ako keby ste užívateľovi dali k dispozícii príkazový riadok. Okrem toho, keď iSeries prijme vzdialený príkaz cez DDM, systém nevykoná nastavenie Limited capability (LMTCPB) v užívateľských profiloch.

## Ochrana pracovných staníc pred vzdialenými príkazmi a procedúrami

IBM iSeries Access for Windows poskytuje funkcie pre prijímanie vzdialených príkazov na PC. Príkaz RUNRMTCMD (Run Remote Command) môžete použiť na serveri, aby ste spustili procedúru na pripojenom PC. Funkcia RUNRMTCMD je cenný nástroj pre správcov systémov a personálu z oddelenia pomoci užívateľom. Poskytuje však tiež príležitosť na poškodenie údajov na PC, či už úmyselné alebo náhodné.

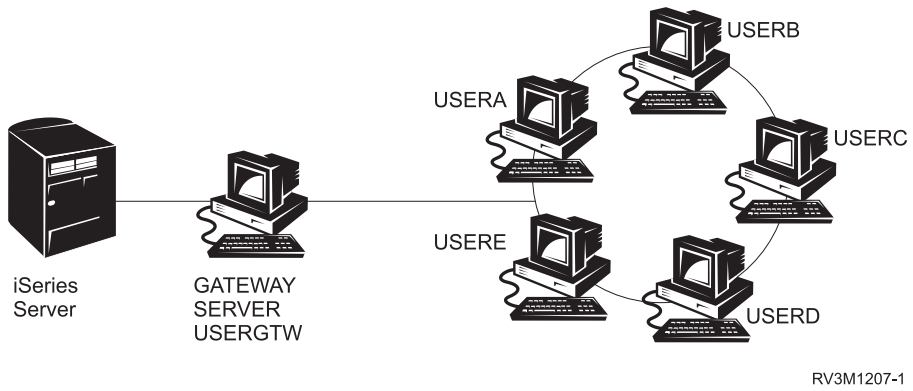
PC nemajú rovnaké funkcie oprávnenia na objekty ako majú servery iSeries. Vašou najlepšou ochranou proti problémom s príkazom RUNRMTCMD je dôsledné obmedzenie užívateľov systému, ktorí majú prístup k tomuto príkazu. IBM iSeries Access for Windows poskytuje funkcie pre registráciu užívateľov, ktorí dokážu spustiť vzdialené príkazy na špecifickom PC. Keď je pripojenie vytvorené pomocou TCP/IP, na riadenie prístupu ku vzdialeným príkazom

môžete použiť vlastnosti ovládacieho panelu na klientovi. Užívateľov môžete autorizovať pomocou ID užívateľa alebo názvom vzdialeného systému. Keď je pripojenie vytvorené pomocou SNA, niektorý softvér klienta poskytuje funkciu na nastavenie zabezpečenia konverzácie. Pri inom softvéri klienta jednoducho určíte, či sa nastaví alebo nenastaví funkcia prichádzajúceho príkazu.

Pre každú kombináciu softvéru klienta a typu pripojenia (ako je TCP/IP alebo SNA) si musíte prezrieť možnosti pre prichádzajúce príkazy do pripojených PC. V dokumentácii klienta pohľadajte "prichádzajúci príkaz" alebo "RUNRMTCMD". Buďte pripravený na poradenie sa s užívateľmi PC a správcami siete o správnom (bezpečnom) spôsobe nakonfigurovania klientov na povolenie alebo zakázanie tejto funkcie.

## Bránové servery

Váš systém sa môže nachádzať v sieti s prostredným alebo bránovým serverom, ktorý je medzi systémom iSeries a PC. Napríklad, váš systém iSeries môže byť pripojený do LAN pomocou PC servera, ktorý má pripojené PC. Otázky ohľadne bezpečnosti v tejto situácii záležia na funkciách softvéru, ktorý je spustený na bránovom serveri. Obrázok 13 ukazuje príklad konfigurácie bránového servera:




*Obrázok 13. Systém iSeries s bránovým serverom*

Ak použijete nejaký softvér, váš systém iSeries nebude vedieť nič o žiadnych užívateľoch (ako sú USERA alebo USERC), ktorí sú za bránovým serverom. Server sa do systému prihlási ako samostatný užívateľ (USERGTW). Na spracovanie všetkých požiadaviek užívateľov, nachádzajúcich sa za ním, použije USERGTW pre ID užívateľa. Požiadavka od USERA bude pre server vyzerať ako požiadavka od užívateľa USERGTW.

V tomto prípade sa na poskytnutie bezpečnosti musíte spoľahnúť na bránový server. Bezpečnostným funkciám bránového servera musíte porozumieť a riadiť ich. Z perspektívy servera iSeries má každý užívateľ rovnaké oprávnenie ako ID užívateľa, ktoré bránový server používa na spustenie relácie. Toto môžete považovať za ekvivalent spustenia programu, ktorý adoptuje oprávnenie a poskytuje príkazový riadok.

Pri inom softvére bránový server posiela požiadavky od jednotlivých užívateľov do serverov iSeries. Server iSeries vie, že USERA požaduje prístup k určitému objektu. Brána je pre systém takmer prehľadná.

Ak je váš systém v sieti s bránovými servermi, musíte vyhodnotiť, aké veľké oprávnenie poskytnete pre ID užívateľov, ktoré používajú bránové servery. Tiež musíte porozumieť nasledovnému:
- Mechanizmus, ktorý používajú bránové servery pre zabezpečenie.
- Ako sa užívatelia za bránovými servermi objavia na vašom systéme iSeries.

# Komunikácie bezdrôtovej LAN

Niektorí klienti môžu používať Bezdrôtovú LAN iSeries na komunikáciu s vaším systémom bez drôtov. iSeries Bezdrôtový LAN používa technológiu na komunikácie s rádiovou frekvenciou. Ako správca bezpečnosti by ste mali dávať pozor na nasledovné charakteristiky produktov iSeries Bezdrôtového LAN:

- Tieto produkty bezdrôtového LAN používajú široké spektrum technológií. Tú istú technológiu používala vláda v minulosti na zabezpečenie rádiových prenosov. Pre niekoho, kto sa pokúša elektronicky monitorovať prenosy údajov, sa môže zdať tento prenos rušnejší, ako aktuálny prenos.
- Bezdrôtové spojenie má tri konfiguračné parametre dôležité pre bezpečnosť:
  - Rozsah údajov (dva možné rozsahy údajov)
  - Frekvencia (päť možných frekvencií)
  - Identifikátor systému (8 miliónov možných identifikátorov)

  Kombinácia týchto konfiguračných prvkov poskytuje 80 miliónov možných konfigurácií, čo znamená, že pravdepodobnosť odhalenia správnej konfigurácie hackermi je veľmi nepatrná.
- Podobne ako pri iných komunikačných metódach, bezpečnosť bezdrôtových komunikácií je ovplyvnená zabezpečenosťou klientskeho zariadenia. Informácie o systémovom ID a o ďalších konfiguračných parametroch sú v súbore v klientskom zariadení, a mali by byť chránené.
- Ak sa bezdrôtové zariadenie stratí alebo ho ukradnú, bezpečnostné opatrenia normálneho servera, ako sú prihlasovacie heslá a bezpečnosť objektov, poskytnú ochranu pri pokusoch neautorizovaného užívateľa o použitie stratenej alebo ukradnutej jednotky na prístup do vášho systému.
- Ak sa stratí, alebo ukradne bezdrôtová klientska jednotka, mali by ste uvážiť zmenu informácií o systémovom ID pre všetkých používateľov, prístupové body a systémy. Uvažujte o tom podobne, ako keby ste mali vymeniť zámky na vašich dverách, keď vám ukradnú sadu kľúčov.
- Možno budete chcieť rozdeliť váš systém medzi skupiny klientov, ktorí majú jedinečné ID systému. Toto limituje zásah, ak sa jednotka stratí, alebo ukradne. Táto metóda funguje len v prípade, keď môžete obmedziť skupinu používateľov na určitú časť vašej inštalácie.
- Bezdrôtová LAN technológia je na rozdiel od drôtovej súkromná. Preto tieto produkty bezdrôtového LAN nie sú verejne dostupné žiadnym elektronickým snoričom. Snorič je elektronické zariadenie, ktoré vykonáva neautorizované monitorovanie prenosu.

# Kapitola 15. Bezpečnostné výstupné programy

Niektoré funkcie servera iSeries poskytujú výstup, takže váš systém môže spustiť užívateľom vytvorený program na vykonanie ďalšej kontroly a validácie. Môžete napríklad nastaviť váš systém tak, aby spustil výstupný program vždy, keď sa niekto pokúsi otvoriť súbor DDM (riadenie distribuovaných údajov) vo vašom systéme. Pri špecifikovaní ukončovacích výstupných programov, ktoré operujú za určitých podmienok, môžete použiť registračnú funkciu.

Niektoré iSeries publikácie obsahujú vzorky výstupných programov, ktoré vykonávajú bezpečnostné funkcie. Tabuľka 24 poskytuje zoznam týchto výstupných programov a zdrojov vzorových programov.

*Tabuľka 24. Zdroje vzorových výstupných programov*

| **Typ výstupného programu** | **Účel** | **Kde sa dajú nájsť príklady** |
|---|---|---|
| Overovanie hesla | Systémová hodnota QPWDVLDPGM môže špecifikovať názov programu alebo označovať, že zaregistrované validačné programy pre ukončovací bod QIBM_QSY_VLD_PASSWRD sa môžu použiť na kontrolu nového hesla pre dodatočné požiadavky, ktoré nespracúvajú systémové hodnoty QPWDxxx. Používanie tohto programu by malo byť opatrne monitorované, pretože prijíma nezakódované heslá. Tento program **by nemal** ukladať heslá do súboru alebo ich predávať inému programu. | • *Sprievodca pre implementáciu bezpečnosti a auditovania iSeries, GG24–4200*<br>• *iSeries Security Reference*, SC41-5302-07 |
| PC Support/400 alebo prístup Client Access[1] | Názov tohto programu môžete zadať v parametri Client request access (PCSACC) atribútov siete pre ovládanie nasledujúcich funkcií:<br>• Funkcia virtuálnej tlačiarne<br>• Funkcia prenosu súborov<br>• Funkcia zdieľaných zložiek Typ 2<br>• Funkcia správ Client Access<br>• Fronty údajov<br>• Funkcia vzdialeného SQL | *Sprievodca pre implementáciu pre bezpečnosť a auditovanie iSeries, GG24–4200* |
| Prístup k Distributed Data Management (DDM) | Názov tohto programu môžete zadať v parametri DDM request access (DDMACC) atribútov siete pre ovládanie nasledujúcich funkcií:<br>• Funkcia zdieľaných zložiek Typ 0 a 1<br>• Funkcia predloženia vzdialeného príkazu | *Sprievodca pre implementáciu pre bezpečnosť a auditovanie iSeries, GG24–4200* |
| Vzdialené odhlásenie | Môžete zadať program v systémovej hodnote QRMTSIGN na reguláciu, ktorí používatelia sa budú môcť automaticky prihlásiť, a z ktorého miesta (pass-through). | *Sprievodca pre implementáciu pre bezpečnosť a auditovanie iSeries, GG24–4200* |

*Tabuľka 24. Zdroje vzorových výstupných programov (pokračovanie)*

| **Typ výstupného programu** | **Účel** | **Kde sa dajú nájsť príklady** |
|---|---|---|
| ODBC (Open Database Connectivity) s iSeries Access[1] | Ovláda nasledujúce funkcie ODBC:<br>• Či je vôbec ODBC povolený.<br>• Ktoré funkcie sú povolené pre iSeries databázové súbory.<br>• Ktoré SQL príkazy sú povolené.<br>• Ktoré informácie môžu byť obnovené o objektoch databázového servera.<br>• Ktoré funkcie katalógu SQL sú povolené. | Žiadne nie sú k dispozícii. |
| Program na obsluhu prerušenia QSYSMSG | Môžete vytvoriť program na monitorovanie frontu správ QSYSMSG a vykonať príslušné činnosti (ako napríklad upovedomiť správcu bezpečnosti) v závislosti od typu správy. | *Sprievodca pre implementáciu pre bezpečnosť a auditovanie iSeries, GG24–4200* |
| TCP/IP | Niektoré TCP/IP servery (ako napríklad FTP, TFTP, TELNET a REXEC) poskytujú výstupné body. Môžete pridať výstupné programy na ovládanie prihlasovania a na overovanie užívateľských požiadaviek, ako napríklad požiadavky na získanie alebo vloženie určitého súboru. Tieto výstupy môžete použiť aj na poskytovanie anonymných FTP vo vašom systéme. | "TCP/IP User Exits v knihe *iSeries System API Reference*" |
| Zmeny užívateľských profilov | Môžete vytvoriť výstupné programy pre nasledovné príkazy užívateľských profilov:<br>CHGUSRPRF<br>CRTUSRPRF<br>DLTUSRPRF<br>RSTUSRPRF | • *iSeries Security Reference*, SC41-5302-07<br>• "TCP/IP User Exitsv knihe *iSeries System API Reference* " |

**Poznámky:**

1. Dodatočné informácie k tejto téme nájdete v Informačnom centre iSeries. Pozrite si časť "Nevyhnutné predpoklady a súvisiace informácie" na strane xii, kde nájdete viac informácií.

# Kapitola 16. Úvahy o bezpečnosti pre internetové prehliadače

Veľa používateľov PC vo vašej organizácií má na svojich pracovných staniciach prehliadače. Môžu sa pripájať do internetu. Môžu sa tiež pripojiť k vášmu serveru. Nasledujú niektoré úvahy o bezpečnosti pre PC i pre váš server.

## Riziko: poškodenie pracovnej stanice

Webová stránka, ktorú navštívi váš používateľ môže mať so sebou spojený ″program″, ako je Java aplet, ovládací prvok Active-X alebo niektorý iný typ doplnkového komponentu. Hoci to je zriedkavé, pri spustení tohto ″programu″ na PC je možné poškodenie informácií na PC. Ako správca bezpečnosti by ste mali pri chránení PC vo vašej organizácii zohľadniť nasledovné:

- Porozumejte bezpečnostným voľbám rôznych prehliadačov, ktoré majú vaši používatelia. Napríklad, niektorými prehliadačmi môžete riadiť prístup, ktorý majú Java aplety mimo prehliadača (obmedzené prevádzkové prostredie Java sa nazýva *sandbox*). Toto môže zabrániť poškodeniu údajov PC apletmi.

  **Poznámka:** Koncept sandboxu a s ním spojených bezpečnostných obmedzení neexistuje pre Active-X a iné komponenty plug-in.
- Navrhnite svojim používateľom nejaké odporúčania ohľadne nastavenia ich prehliadačov. Pravdepodobne nemáte čas alebo prostriedky na zaistenie toho, aby používatelia akceptovali vaše odporúčania. Preto im musíte vysvetliť možné riziká plynúce z nesprávneho nastavenia.
- Zvážte štandardizáciu webových prehliadačov, ktoré vám poskytujú potrebné bezpečnostné voľby.
- Dajte pokyn svojim používateľom, aby vás informovali pri akomkoľvek podozrivom správaní alebo symptómoch, ktoré môžu byť spojené s konkrétnymi webovými stránkami.

## Riziko: prístup do adresárov iSeries cez zmapované jednotky

Predpokladajme, že k vášmu serveru je pripojené PC pomocou relácie IBM iSeries Access for Windows. Relácia nastaví namapované jednotky tak, aby odkazovali na iSeries Integrovaný súborový systém. Napríklad, jednotka **G** z PC sa môže v sieti mapovať do Integrovaného súborového systému servera SYSTEM1.

Teraz predpokladajme, že používateľ tohto PC má prehliadač a môže pristupovať na internet. Používateľ požaduje webovú stránku, ktorá spustí škodlivý ″program″, ako je Java aplet alebo ovládací prvok Active-X. Je možné, aby sa program mohol pokúsiť z jednotky G na PC všetko vymazať.

Máte k dispozícii niekoľko ochrán proti poškodeniu namapovaných jednotiek:

- Vašou najdôležitejšou ochranou je bezpečnosť zdrojov na vašom serveri. Aplet jazyka Java alebo ovládací prvok Active-X sa serveru javí ako užívateľ, ktorý vytvoril reláciu PC. Potrebujete starostlivo riadiť, čo sú používatelia PC autorizovaní vykonávať na vašom serveri.
- Poraďte vašim užívateľom PC, aby svoje prehliadače nastavili na zamedzenie pokusov o prístup na zmapované jednotky. Toto funguje pre Java aplety, ale nie pre ovládacie prvky Active-X, ktoré nemajú koncept sandboxu.

- Poučte vašich užívateľov o nebezpečenstvách pripojenia k vášmu serveru a k internetu v tej istej relácii. Tiež sa presvedčte, či vaši používatelia PC (napríklad s klientmiWindows 95) porozumeli tomu, že jednotky zostávajú zmapované aj vtedy, keď sa relácia iSeries Access javí ako ukončená.

## Riziko: dôveryhodné podpísané aplety

Vaši používatelia mohli realizovať vaše rady a nastaviť si svoje prehliadače na zabránenie zápisu apletmi na ľubovoľné jednotky PC. Vaši používatelia PC si aj tak musia byť vedomí, že *podpísaný aplet* môžete nahradiť nastavenie ich prehliadačov.

Podpísaný aplet má so sebou spojený číslicový podpis, ktorý vytvára jeho autenticitu. Keď používateľ pristupuje na webovú stránku, ktorá má podpísaný aplet, používateľ uvidí správu. Správa určuje, že aplet má podpis (kým a kedy bol podpísaný). Keď váš používateľ bude tento aplet akceptovať, poskytne mu možnosť nahradenia bezpečnostných nastavení prehliadača. Podpísaný aplet môže zapisovať na lokálne jednotky PC, aj keď to štandardné nastavenie prehliadača zakazuje. Podpísaný aplet dokáže tiež zapisovať do zmapovaných jednotiek na vašom serveri, pretože pre PC sa objavujú ako lokálne jednotky.

Pri vašich vlastných apletoch jazyka Java, ktoré pochádzajú z vášho servera, budete možno potrebovať použiť podpísané aplety. Mali by ste inštruovať svojich používateľov, aby aj tak neprijímali podpísané aplety z neznámych zdrojov.

# Kapitola 17. Súvisiace informácie

Príručky

- *APPC Programming*, SC41-5443-00popisuje podporu APPC (advanced program-to-program communications) pre systém iSeries. Táto kniha asistuje pri rozvoji aplikačných programov, ktoré používajú APPC a pri definovaní komunikačného prostredia pre APPC komunikácie. Zahŕňa hľadiská aplikačného programu, požiadavky konfigurácie a príkazy, riadenie problémov pre APPC a všeobecné sieťové hľadiská. Pozrite si iSeries Information Center CD-ROM.
- *AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet* Redbook, SG24-4929 sa zaoberá bezpečnostnou problematikou a rizikami súvisiacimi s pripojením vášho iSeries do internetu. Poskytuje príklady, odporúčania, tipy a techniky pre TCP/IP aplikácie.
- *Backup and Recovery*, SC41-5304-07 poskytuje informácie o plánovaní a stratégií pre zálohovanie a obnovu, ukladaní informácií z vášho systému a obnove vášho systému. Pozrite si Informačné centrum iSeries. Dodatočné informácie k týmto témam môžete nájsť v Informačnom centre. Pozrite si časť “Nevyhnutné predpoklady a súvisiace informácie” na strane xii, kde nájdete viac informácií.
- *CL Programming*, SC41-5721-06 poskytuje podrobné opisy zakódovania špecifikácií opisu údajov (DDS) pre súbory, ktoré môžu byť popísané externe. Tieto súbory sú fyzické, logické, obrazovkové, tlačové a súbory medzisystémových komunikačných funkcií (ICF). Pozrite si Informačné centrum iSeries.
- Téma CL v Informačnom centre (pozrite si “Nevyhnutné predpoklady a súvisiace informácie” na strane xii, kde nájdete viac podrobností) poskytuje opis riadiaceho jazyka (CL) iSeries a jeho príkazov OS/400. Príkazy OS/400 sa používajú na vyžadovanie funkcií licenčného programu Operating System/400 (5722-SS1). Všetky príkazy, ktoré nie sú súčasťou CL z OS/400--pridružené k iným licenčným programom, vrátane všetkých rôznych jazykov a pomocných programov--sú opísané v iných knihách, ktoré podporujú tieto licenčné programy.
- *Implementing iSeries Security, 3. vydanie*, autori Wayne Madden a Carol Woodbury. Loveland, Colorado: 29th Street Press, a division of Duke Communications International, 1998. Poskytuje návody a praktické návrhy pre plánovanie, nastavovanie a riadenie bezpečnosti iSeries.

  Objednávacie číslo ISBN:

  1-882419-78-2
- Viac informácií o serveri HTTP nájdete na nasledujúcej webovej stránke:

  `http://www.ibm.com/eserver/iseries/software/http/docs/doc.htm`
- *iSeries Security Reference*, SC41-5302-07 poskytuje kompletné informácie o hodnotách bezpečnostného systému, užívateľských profiloch, bezpečnosti zdrojov a auditovaní bezpečnosti. Táto príručka nepopisuje bezpečnosť pre špecifické licenčné programy, jazyky a užitočnosti. Pozrite si Informačné centrum iSeries.
- Téma ″Základné systémové operácie″ v Informačnom centre poskytuje informácie o niektorých kľúčových konceptoch a úlohách, ktoré sa vyžadujú pre základné operácie iSeries. Pozrite si časť “Nevyhnutné predpoklady a súvisiace informácie” na strane xii, kde nájdete viac informácií.
- Informačné centrum popisuje, ako sa má popisovať a konfigurovať TCP/IP a niekoľko aplikácií TCP/IP, ako napríklad FTP, SMTP a TELNET. Pozrite si časť “Nevyhnutné predpoklady a súvisiace informácie” na strane xii, kde nájdete viac informácií.

- *TCP/IP File Server Support for OS/400 Installation and User's Guide*, SC41-0125, poskytuje úvodné informácie, inštrukcie k inštalácii a postupy nastavovania pre ponuku File Server Support licenčného programu. Vysvetľuje funkcie dostupné v produkte a zahŕňa príklady a pokyny, ktoré môžete použiť s inými systémami.
- *Trusted Computer Systems Evaluation Criteria* DoD 5200.28.STD, popisuje kritériá pre úrovne dôvery pre počítačové systémy. TCSEC je publikáciou vlády Spojených štátov. Kópie sa môžu získať v:

  Office of Standards and Products
  National Computer Security Center
  Fort Meade, Maryland 20755-6000 USA
  Pozor: Šéf, štandardy počítačovej bezpečnosti
- Informačné centrum obsahuje niekoľko tém, ktoré sa týkajú Riadenie systému a Riadenia práce na iSeries. Niektoré z týchto tém sú zbierka údajov o výkone, riadenie systémových hodnôt a riadenie ukladania. Podrobnosti o prístupe do Informačného centra si pozrite v "Nevyhnutné predpoklady a súvisiace informácie" na strane xii. Riadenie práce, SC41-5306-03 poskytuje informácie o tom, ako vytvoriť a zmeniť prostredie riadenia práce. Pozrite si Informačné centrum iSeries.

Okrem týchto tém informačného centra a Doplnkových príručiek môžete ako pomôcku použiť nasledujúce prostriedky:

- **IBM SecureWay**
  IBM SecureWay poskytuje spoločné označenie pre široké portfólio bezpečnostných ponúk IBM, hardvér, softvér, konzulting a služby na pomoc zákazníkom pri zabezpečení ich informačných technológií. Či riešite individuálne potreby alebo vytvárate celopodnikové riešenie, ponuky IBM SecureWay poskytujú odborné znalosti potrebné na plánovanie, návrh, implementáciu a používanie bezpečných riešení pre podniky. Viac informácií o ponukách IBM SecureWay nájdete na domácej stránke IBM SecureWay:

  `http://www.ibm.com/secureway`
- **Ponuky služieb**
  Nainštalovanie nového hardvéru alebo softvéru môže naozaj vylepšiť vašu efektívnosť a podnikové operácie. Ale tiež to predstavuje hrozbu prerušenia podnikania a odstávky a môže to preťažiť vaše cenné interné prostriedky. IBM Global Services poskytujú služby, ktoré súvisia s bezpečnosťou iSeries. Nasledujúca webová stránka vám umožňuje vyhľadávanie úplných výpisov služieb pre váš iSeries:

  `http://www.as.ibm.com/asus`

# Poznámky

Tieto informácie boli pripravené pre produkty a služby ponúkané v USA

IBM nemusí ponúkať produkty, služby alebo funkcie uvedené v tomto dokumente v ostatných krajinách. Obráťte sa miestneho predstaviteľa firmy IBM, ktorý vám poskytne informácie o produktoch a službách, ktoré sú aktuálne dostupné v oblasti, v ktorej sa nachádzate. Žiadny odkaz na produkt, program alebo službu firmy IBM nemá za úlohu vyhlasovať alebo tvrdiť, že sa môže použiť iba tento produkt, program alebo služba firmy IBM. Miest toho sa môže použiť každý produkt, program alebo služba s rovnakou funkčnosťou, ktorý neporušuje žiadne práva duševného vlastníctva firmy IBM. Avšak vyhodnotenie a overenie funkčnosti akéhokoľvek produktu, programu alebo služby, ktoré nepochádzajú od IBM je na zodpovednosti používateľa.

IBM môže vlastniť patenty alebo patenty v schvaľovacom konaní pokrývajúce predmetné záležitosti opísané v tomto dokumente. Predloženie tohto dokumentu vám nedáva žiadnu licenciu na tieto patenty. Otázky týkajúce sa licencií môžete zasielať v písomnej forme na adresu:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
USA

Informácie o licenciách, týkajúcich sa dvojbajtových informácií (DBCS), vám poskytne oddelenie intelektuálneho vlastníctva IBM vo vašej krajine alebo písomné žiadosti o informácie pošlite na adresu:

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

**Nasledujúci odsek sa netýka Spojeného kráľovstva alebo akejkoľvek inej krajiny, v ktorej sú takéto ustanovenia nezlučiteľné s miestnym zákonom:** INTERNATIONAL BUSINESS MACHINES CORPORATION POSKYTUJE TÚTO PUBLIKÁCIU “AKO JE” BEZ AKÝCHKOĽVEK GARANCIÍ, ČI UŽ VYJADRENÝCH ALEBO IMPLIKOVANÝCH, VRÁTANE, ALE NEOBMEDZENÝCH NA IMPLIKOVANÉ GARANCIE NEPORUŠENIA, SCHOPNOSTI UVEDENIA NA TRH ALEBO SPÔSOBILOSTI NA URČITÝ ÚČEL. Niektoré štáty nedovoľujú zrieknutie sa zodpovednosti za vayjadrené alebo implikované záruky v určitých transakciách, preto sa vás toto vyhlásenie nemusí týkať.

Tieto informácie by mohli zahŕňať technické nepresnosti alebo typografické chyby. Tu uvádzané informácie sa periodicky menia; tieto zmeny budú včleňované do nových vydaní publikácie. IBM môže vykonávať zlepšenia a/alebo zmeny v produkte (produktoch) a/alebo programe (programoch) popísaných v tejto publikácií kedykoľvek a bez oznámenia.

Všetky odkazy v týchto informáciách na webové stránky, ktoré nepatria IBM, sú poskytnuté len pre vaše pohodlie a v žiadnom prípade neslúžia ako potvrdenie týchto webových stránok. Materiály na týchto webových stránkach nie sú súčasťou materiálov pre tento produkt IBM a používanie týchto webových stránok je na vaše vlastné riziko.

IBM môže používať alebo distribuovať akékoľvek informácie, ktoré jej poskytnete, ľubovoľným spôsobom, ktorý považuje za primeraný bez toho, aby vznikol voči vám akýkoľvek záväzok.

Držitelia licencie pre tento program, ktorí si želajú mať o ňom informácie za účelom umožnenia: (i) výmeny informácií medzi nezávisle vytvorenými programami a inými programami (spolu s týmto programom) a (ii) vzájomného použitia informácií, ktoré boli vymenené, by mali kontaktovať:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
USA

Takéto informácie môžu byť dostupné. Sú predmetom príslušných termínov a podmienok, ktoré môžu v niektorých prípadoch zahŕňať aj zaplatenie poplatku.

Licenčný program popísaný v týchto informáciách a všetky preň dostupné licenčné materiály poskytuje IBM podľa podmienok zmluvy IBM Customer Agreement, IBM International License Agreement alebo podľa ľubovoľnej rovnocennej zmluvy medzi nami uzavretej.

Všetky údaje o výkone, ktoré sú tu uvedené, boli určené v riadenom prostredí. Preto sa výsledky dosiahnuté v iných operačných prostrediach môžu od nich významne líšiť. Určité merania sa uskutočňovali na systémoch vývojovej úrovne a neexistuje žiadna záruka, že tieto namerané hodnoty budú také isté aj na bežne dodávaných systémoch. Okrem toho mohli byť niektoré merania odhadnuté extrapoláciou. Skutočné výsledky sa môžu líšiť. Používatelia tohto dokumentu by si mali overiť aplikovateľné údaje pre ich špecifické prostredie.

Informácie o produktoch iných dodávateľov ako IBM boli získané od dodávateľov týchto produktov z ich uverejnených oznámení alebo z iných, verejne prístupných zdrojov. IBM netestovalo tieto produkty a nemôže potvrdiť ich presnosť výkonu, kompatibility alebo všetkých ostatných vyhlásení, ktoré sa týkajú produktov od iných výrobcov ako IBM. Otázky súvisiace s možnosťami produktov od iných dodávateľov ako IBM je potrebné adresovať priamo dodávateľom týchto produktov.

Všetky vyhlásenia týkajúce sa budúceho smerovania firmy IBM alebo jej zámerov môžu byť zmenené bez predchádzajúceho oznámenia a predstavujú jedine jej ciele.

Tieto informácie sú iba pre plánovacie účely. Tu uvedené informácie sú predmetom zmeny predtým, než sa popisované produkty stanú dostupnými.

Tieto informácie obsahujú príklady údajov a správy používané v denných obchodných operáciách. Na ich čo najucelenejšiu ilustráciu obsahujú uvedené príklady mená osôb, spoločností, značiek tovarov a produktov. Všetky tieto názvy sú fiktívne a akákoľvek podobnosť s názvami a adresami použitými skutočnou obchodnou spoločnosťou sú úplne náhodné.

LICENCIA NA AUTORSKÉ PRÁVA:

Tieto informácie obsahujú vzorové aplikačné programy v zdrojovom jazyku, ktoré ilustrujú programovacie techniky na rôznych operačných platformách. Tieto vzorové programy môžete kopírovať, modifikovať a rozširovať v akejkoľvek forme bez poplatku firme IBM, za účelom vývoja, používania, marketingu alebo distribúcie aplikačných programov, ktoré vyhovujú rozhraniu pre programovanie aplikácií pre operačnú platformu, pre ktorú boli vzorové programy napísané. Tieto príklady neboli dôkladne otestované pri všetkých podmienkach. IBM z tohto dôvodu nemôže zaručiť alebo implikovať spoľahlivosť, prevádzkyschopnosť alebo

funkciu týchto programov. Tieto vzorové programy môžete kopírovať, modifikovať a rozširovať v akejkoľvek forme bez poplatku firme IBM, za účelom vývoja, používania, marketingu alebo distribúcie aplikačných programov, ktoré vyhovujú IBM rozhraniam pre programovanie aplikácií.

Ak si tieto informácie prezeráte v skrátenej podobe, nemusia tu byť zobrazené fotografie a farebné ilustrácie.

## Ochranné známky

Nasledujúce termíny sú ochrannými známkami spoločnosti International Business Machines Corporation v Spojených štátoch alebo iných krajinách alebo oboch:

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 sú ochranné známky alebo registrované ochranné známky spoločnosti Intel Corporation v Spojených štátoch, iných krajinách alebo oboch.

Microsoft, Windows, Windows NT a logo Windows sú ochranné známky spoločnosti Microsoft Corporation v Spojených štátoch, iných krajinách alebo oboch.

Java a všetky ochranné známky založené na Java, sú ochrannými známkami spoločnosti Sun Microsystems, Inc. v Spojených štátoch, iných krajinách alebo oboch.

UNIX je registrovaná ochranná známka spoločnosti The Open Group v Spojených štátoch a iných krajinách.

Ostatné mená obchodných spoločností, produktov a služieb môžu byť ochrannými známkami alebo servisnými známkami iných.

# Index

## Špeciálne znaky



## A



## B

## C



## D



## E



## F



## G



## H



## CH



## I

# J



# K



# L



# M



# N



# O

# P

# Q



# R



# S

# Š



# T



# U

# Ú



# V



# Z

# Ž

# Pripomienky čitateľa

**iSeries**
**Tipy a nástroje pre zabezpečenie vášho iSeries**
**Verzia 5**

**Číslo publikácie: SA12-6235-07**

Vážime si vaše pripomienky k tomuto vydaniu. V prípade špeciálnych chýb, vynechaní alebo v prípade nesprávnosti alebo neúplnosti informácií, uvedených v tejto knihe, uvítame vaše pripomienky. Vaše pripomienky by sa mali týkať iba informácií z tejto publikácie a spôsobu, akým boli prezentované.

Ak chcete získať technické informácie o výrobkoch a cenách, kontaktujte IBM Slovensko alebo obchodného partnera IBM.

Ak chcete všeobecné informácie, volajte tel. číslo: ″IBM Slovensko″ (02/49291 111).

Po zaslaní vašich pripomienok si vyhradzuje IBM neexkluzívne právo vaše pripomienky používať alebo rozširovať v akejkoľvek vhodnej forme, bez toho, aby vznikli voči vám akékoľvek záväzky.

Pripomienky:

Ďakujeme vám za pomoc.

Vaše pripomienky môžete:
- Zaslať na adresu uvedenú na druhej strane tohto formulára.
- Zaslat faxom na číslo: Spojené štáty a Kanada: 1-800-937-3430
- Zaslať cez e-mail na adresu: RCHCLERK@us.ibm.com

Ak by ste chceli odpoveď zo strany IBM, prosíme vás, vyplňte nasledujúce informácie:

| | |
|---|---|
| Meno | Adresa |
| Spoločnosť | |
| Tel. číslo | E-mail adresa |

IBM

IBM CORPORATION
ATTN DEPT 542 IDCLERK
3605 Highway 52 N
ROCHESTER MN

Vytlačené v USA

SA12-6235-07