IBM

eserver

iSeries

Savjeti i alati za osiguranje vašeg iSeriesa

Verzija 5

SA12-6294-07

IBM

@server

iSeries

Savjeti i alati za osiguranje vašeg iSeriesa

Verzija 5

SA12-6294-07

Napomena

Prije korištenja ovih informacija i proizvoda koji podržavaju, pročitajte informacije u “Napomene” na stranici 147.

Osmo izdanje (travanj, 2004)

Ovo izdanje se primjenjuje na verziju 5, izdanje 3, modifikaciju 0 IBM Operating System/400 (broj proizvoda 5722-SS1) i na sva naredna izdanja i modifikacije dok ne bude drugačije naznačeno u novim izdanjima. Ova verzija ne radi na svim modelima računala smanjenog seta instrukcija (RISC), niti ne radi na CISC modelima.

Ovo izdanje zamjenjuje SC41-5300-06.

© Autorsko pravo International Business Machines Corp. 1996, 2004. Sva prava pridržana.

Sadržaj

© Autorska prava IBM Corp. 1996, 2004

Slike

© Autorska prava IBM Corp. 1996, 2004

Tablice

© Autorska prava IBM Corp. 1996, 2004

O Savjetima i alatima za osiguranje vašeg iSeriesa (SC41-5300-07)

Uloga računala u organizaciji se brzo mijenja. IT upravitelji, dobavljači softvera, administratori sigurnosti sad trebaju drugačije gledati na mnoga područja koja su u prošlosti uzimali zdravo za gotovo. iSeries sigurnost treba biti na toj listi.

Sistemi omogućuju razne nove funkcije koje su bitno različite od tradicionalnih aplikacija za knjigovodstvo. Korisnici ulaze u sisteme na nove načine: LAN-ovima, preklopljenim linijama (biranjem), bežično, mrežama različitih tipova. Često, korisnici niti ne vide ekran za prijavu. Mnoge organizacije se proširuju da postanu "proširena poduzeća" ili pomoću vlastitih mreža ili pomoću Interneta.

Odjednom, sistemi kao da imaju čitav novi skup vrata i prozora. Sistemski upravitelji i administratori sigurnosti su opravdano zabrinuti za to kako da zaštite informacije u ovom brzo mijenjajućem okruženju.

Ove informacije daju skup praktičnih prijedloga za upotrebu značajki sigurnosti iSeriesa i za uspostavu operacijskih procedura koje su svjesne sigurnosti. Preporuke se u ovim informacijama odnose na instalaciju s prosječnim sigurnosnim zahtjevima i izlaganjima. Ove informacije ne daju potpun opis dostupnih iSeries sigurnosnih značajki. Ako želite čitati o dodatnim opcijama ili trebate potpunije pozadinske informacije posavjetujte se u publikacijama koje su opisane u Poglavlje 17, "Povezane informacije", na stranici 145.

Ove informacije također opisuju uspostavu i upotrebu sigurnosnih alata koji su dio OS/400. Poglavlje 4, "Konfiguriranje iSeriesa za upotrebu Alata za sigurnost", na stranici 25 i "Naredbe i izbornici za sigurnosne naredbe" na stranici 26 daju referentne informacije o sigurnosnim alatima. Ove informacije daju i primjere za upotrebu alata.

Tko bi trebao čitati ovu knjigu

Službenik sigurnosti ili **administrator sigurnosti** je odgovoran za sigurnost sistema. Ta odgovornost uobičajeno uključuje sljedeće zadatke:

- Uspostava i upravljanje korisničkim profilima
- Postavljanje vrijednosti za cijeli sistem koje utječu na sigurnost
- Administracija ovlaštenja za objekte
- Utvrđivanje i nadgledanje politika sigurnosti

Ako ste vi odgovorni za administraciju sigurnosti za jedan ili više iSeries sistema, ove se informacije tiču vas. Upute u ovim informacijama pretpostavljaju sljedeće:

- Poznate su vam osnovne iSeries operacijske procedure, kao što je prijavljivanje i upotreba naredbi.
- Poznati su vam osnovni elementi iSeries sigurnosti: razine sigurnosti, sigurnosne sistemske vrijednosti, korisnički profili i sigurnost objekata.

  Bilješka: Poglavlje 1, "Osnovni elementi iSeries sigurnosti", na stranici 3 daje pregled ovih elemenata. Ako su vam ovi osnovni elementi nepoznanica, tad pročitajte poglavlje *Osnovna sigurnost i planiranje* u iSeries Informacijski Centar. Pogledajte "Preduvjeti i povezane informacije" na stranici xii za više detalja.
- Sigurnost ste na vašem sistemu aktivirali postavljanjem sistemske vrijednosti sigurnosne razine (QSECURITY) bar na 30.

© Autorska prava IBM Corp. 1996, 2004

IBM kontinuirano poboljšava sigurnosna svojstva za iSeries. Da bi iskoristili ova poboljšanja, trebali bi redovito procjenjivati kumulativni paket popravaka koji je trenutno dostupan za vaše izdanje. Pogledajte da li on sadržava popravke koji se odnose na sigurnost.

Kako koristiti ove informacije

Ako niste postavili vaš sistem za korištenje sigurnosnih alata ili ste imali instalirano Oprema za sigurnost za OS/400 za ranije izdanje, učinite sljedeće:

1. Počnite sa Poglavlje 2, “iSeries čarobnjak sigurnosti i eServer planer sigurnosti”, na stranici 9. On opisuje upotrebu ovih značajki za izbor koji alati za sigurnost se preporučuju i kako startati s njima.
2. Za više osnovnih informacija o sigurnosti, možete ponovo pregledati informacije Upute za sigurnost, online locirane u iSeries Informacijski Centar.

Napomena

Ove informacije imaju *mnogo* savjeta za sigurnost iSeriesa. Vaš sistem možda treba zaštitu u samo nekim područjima. Koristite informacije da naučite o mogućim izlaganjima sigurnosti i poboljšanjima. Zatim se fokusirajte na područja koja su najkritičnija za vaš sistem.

Preduvjeti i povezane informacije

Koristite iSeries Informacijski Centar kao polaznu točku za pretraživanje iSeries tehničkih informacija.

Možete pristupiti Informacijskom Centru na dva načina:

- Iz sljedeće Web stranice:

  `http://www.ibm.com/eserver/iseries/infocenter`
- Iz *iSeries Informacijski Centar*, SK3T-4091-04 CD-ROM-a. Ovaj CD-ROM se isporučuje s vašom narudžbom za nadogradnju novog iSeries hardvera ili IBM Operating System/400 softvera. CD-ROM možete naručiti i iz IBM Publikacijskog centra:

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

iSeries Informacijski Centar sadrži nove i ažurirane iSeries informacije kao što je nadogradnja softvera i hardvera, Linux, WebSphere, Java, visoka dostupnost, baza podataka, logičke particije, CL naredbe i sučelje programiranja sistemske aplikacije (API-ji). Osim toga, sadrži savjetnike i pronalazače kao pomoć u planiranju, rješavanju problema i konfiguriranju vašeg iSeries hardvera i softvera.

Sa svakom novom narudžbom hardvera, primate *iSeries CD-ROM za postav i operacije*, SK3T-4098-02. Ovaj CD-ROM sadrži IBM **@server** IBM e(logo)server iSeries Access za Windows i EZ-Setup čarobnjaka. iSeries Access obitelj nudi moćan skup sposobnosti klijenta i poslužitelja za povezivanje PC-eva na iSeries poslužitelje. EZ-Setup čarobnjak automatizira mnogo zadataka iSeries postava.

Kako slati vlastite komentare

Povratna veza s vama je važna da bi se omogućile najtočnije visoko kvalitetne informacije. Ako imate ikakve komentare o ovoj knjizi ili bilo kojoj drugoj iSeries dokumentaciji, ispunite obrazac komentara čitatelja na kraju ove knjige.

- Ako preferirate slanje komentara putem pošte, koristite obrazac komentara čitatelja s adresom koja je ispisana otraga. Ako šaljete poštom obrazac s komentarima čitatelja iz bilo koje zemlje osim Sjedinjenih Država, možete predati obrazac lokalnoj IBM podružnici ili IBM predstavniku za plaćeno slanje poštom.
- Ako preferirate slanje komentara putem FAX-a, koristite bilo koji od sljedećih brojeva:
  - Sjedinjene Države, Kanada i Portoriko: 1-800-937-3430
  - Ostale zemlje: 1-507-253-5192
- Ako preferirate elektroničko slanje komentara, koristite jednu od ovih adresa e-pošte:
  - Komentari o knjigama:

    RCHCLERK@us.ibm.com
  - Komentari o iSeries Informacijskom Centru:

    RCHINFOC@us.ibm.com

Obavezno uključite sljedeće:

- Ime knjige ili poglavlje iSeries Informacijskog Centra.
- Broj izdavanja knjige.
- Broj stranice ili poglavlje knjige na koje se odnosi vaš komentar.

Dio 1. Osnovna iSeries sigurnost

© Autorska prava IBM Corp. 1996, 2004

Poglavlje 1. Osnovni elementi iSeries sigurnosti

Ovo poglavlje daje kratak pregled osnovnih elemenata koji zajedno rade na pružanju iSeries sigurnosti. U drugim dijelovima ove knjige idemo iznad osnova da bi vam dali savjete za upotrebu sigurnosnih elemenata da zadovoljite potrebe vaše organizacije.

Sigurnosne razine

Možete izabrati koliko sigurnosti želite da sistem forsira postavljanjem sistemske vrijednosti sigurnosne razine (QSECURITY). Sistem nudi pet razina sigurnosti:

Razina 10:

Sistem ne forsira nikakvu sigurnost. Nije potrebna nikakva lozinka. Ako specificirani korisnički profil ne postoji na sistemu kad se netko prijavljuje, sistem ga kreira.

PAŽNJA:

Počevši od V4R3 i budućih izdanja, ne možete postaviti QSECURITY sistemsku vrijednost na 10. Ako je vaš sistem trenutno na sigurnosnoj razini 10, ostati će na razini 10 iako vi instalirate Verziju 4 Izdanje 3. Ako promijenite sigurnosnu razinu u neku drugu vrijednost, ne možete je vratiti natrag na razinu 10. Zbog toga što razina 10 ne daje nikakvu sigurnosnu zaštitu, sigurnosna razina 10 nije preporučena od IBM-a. **IBM neće omogućiti nikakvu podršku za bilo kakve probleme koji se mogu desiti na sigurnosnoj razini 10, osim ako problem također ne može nastati na višoj sigurnosnoj razini.**

Razina 20:

Sistem treba korisnički ID i lozinku za prijavu. Sigurnosna razina 20 se često naziva **sigurnost prijave**.Po defaultu, svi korisnici imaju pristup svim objektima jer svi korisnici imaju *ALLOBJ posebno ovlaštenje.

Razina 30:

Sistem treba korisnički ID i lozinku za prijavu. Korisnici moraju imati ovlaštenje da koriste objekte jer po defaultu korisnici nemaju nikakvo ovlaštenje. Ovo se zove **sigurnost resursa**.

Razina 40:

Sistem treba korisnički ID i lozinku za prijavu. Dodatno, uz sigurnost resursa, sistem omogućuje funkcije **zaštite integriteta**. Funkcije zaštite integriteta, kao što je provjera valjanosti parametara za sučelja operativnog sistema, namijenjene su zaštiti i vašeg sistema i objekata na vašem sistemu od uplitanja iskusnih korisnika sistema. Za većinu instalacija, razina 40 je preporučena sigurnosna razina. Kad primite novi iSeries sistem s V4R5 ili kasnijim izdanjem, sigurnosna razina je postavljena na 40.

Razina 50:

Sistem treba korisnički ID i lozinku za prijavu. Sistem forsira i sigurnost resursa i zaštitu integriteta razine 40,ali dodaje **povećanu zaštitu integriteta**, kao što je ograničenje rukovanja porukama između programa stanja sistema i programa stanja korisnika. Sigurnosna je razina 50 namjeravana za iSeries sisteme s visokim zahtjevima za sigurnost.

Bilješka: Razina 50 je potrebna razina za C2 certifikaciju (i FIPS-140 certifikaciju).

© Autorska prava IBM Corp. 1996, 2004

Poglavlje 2 *Uputa iSeries sigurnosti* knjige daje još informacija o sigurnosnim razinama i opisuje kako se premještati iz jedne sigurnosne razine na drugu.

Globalne postavke

Vaš sistem posjeduje globalne postavke koje utječu na to kako posao ulazi u sistem i kako sistem izgleda drugim korisnicima sistema. Ove postavke uključuju sljedeće:

Sigurnosne sistemske vrijednosti:
Sigurnosne se sistemske vrijednosti koriste za kontrolu sigurnosti na vašem sistemu. Ove su vrijednosti razvrstane u četiri grupe:
- Općenite sigurnosne sistemske vrijednosti
- Druge sistemske vrijednosti koje se odnose na sigurnost
- Sistemske vrijednosti koje kontroliraju lozinke
- Sistemske vrijednosti koje kontroliraju revizije

Nekoliko poglavlja u ovoj Knjiga raspravljaju o sigurnosnim implikacijama specifičnih sistemskih vrijednosti. Poglavlje 3 u knjizi *Uputa iSeries sigurnosti* opisuje sve sigurnosno-relevantne sistemske vrijednosti.

Mrežni atributi:
Mrežni atributi kontroliraju kako vaš sistem sudjeluje (ili bira da ne sudjeluje) u mreži s drugim sistemima. O mrežnim atributima možete pročitati više u knjizi *Upravljanje poslom*.

Opisi podsistema i drugi elementi upravljanja poslom:
Elementi upravljanja poslom određuju kako posao ulazi u sistem i u kojem se okruženju posao izvodi. Nekoliko poglavlja u ovim informacijama raspravljaju o sigurnosnim implikacijama nekih vrijednosti upravljanja poslom. Knjiga *Upravljanje poslom* daje potpune informacije.

Konfiguracija komunikacija:
Vaša konfiguracija komunikacija također utječe kako posao ulazi u vaš sistem. Nekoliko poglavlja u ovoj informaciji daje prijedloge za zaštitu vašeg sistema kad on sudjeluje u mreži.

Korisnički profili

Svaki korisnik sistema **mora** imati korisnički profil. Vi morate kreirati korisnički profil prije no što se korisnik može prijaviti. Korisnički profili se mogu koristiti i za kontrolu pristupa servisnim alatima kao što je DASD i dumpovima glavne memorije. Pogledajte “Upravljanje servisnim alatima” na stranici 55 za još informacija.

Korisnički profil je moćan i fleksibilan alat. On kontrolira što korisnik može raditi i prilagođava način prikaza sistema korisniku. Knjiga *Uputa iSeries sigurnosti* opisuje sve parametre u korisničkom profilu.

Profili grupe

Profil grupe je poseban tip korisničkog profila. Možete koristiti profil grupe da definirate ovlaštenje grupe korisnika, rađe nego da dajete ovlaštenje svakom korisniku pojedinačno. Također možete koristiti profil grupe kao obrazac pri kreiranju pojedinačnih korisničkih profila upotrebom funkcije kopiranje-profila ili ako koristite iSeries Navigator možete koristiti izbornik politika sigurnosti da uredite ovlaštenja korisnika.

Poglavlje 5 i Poglavlje 7 u knjizi *Uputa iSeries sigurnosti* daju još informacija o planiranju i upotrebi profila grupe.

Sigurnost resursa

Sigurnost resursa na sistemu omogućuje vam definiranje tko može koristiti objekte i kako se ti objekti mogu koristiti. Sposobnost pristupa objektu naziva se **ovlaštenje**. Kad postavite objektno ovlaštenje, trebate biti pažljivi da date vašim korisnicima dovoljno ovlaštenja da rade svoj posao bez da im date ovlaštenje da pregledavaju i mijenjaju sistem. Objektno ovlaštenje daje dozvole korisnicima za određen objekt i mogu specificirati što korisnik može raditi s objektom. Objektni resurs može biti ograničen kroz specifična detaljna korisnička ovlaštenja, kao što je dodavanje zapisa ili promjena zapisa. Sistemski se resursi mogu koristiti da omoguće korisniku pristup specifičnim sistem-definiranim podskupovima ovlaštenja: *ALL, *CHANGE, *USE i *EXCLUDE.

Datoteke, programi, knjižnice i direktoriji najčešći su sistemski objekti koji trebaju zaštitu sigurnosti resursa, ali vi možete specificirati ovlaštenja za bilo koji pojedinačan objekt na sistemu.

Poglavlje 5, “Zaštita informacijskih sredstava s objektnim ovlaštenjem” raspravlja o važnosti postavljanja objektnog ovlaštenja na vašem sistemu. Poglavlje 5 u knjizi *Uputa iSeries sigurnosti* opisuje opcije postavljanja sigurnosti resursa.

Ograničenje pristupa funkcijama programa

Ograničenje pristupa funkcijama programa vam omogućuje osiguravanje sigurnosti programa kad nemate iSeries objekt za sigurnost programa. Prije nego je dodana podrška ograničenja pristupa funkcijama programa u V4R3, ovo ste mogli postići kreiranjem autorizacijske liste ili drugog objekta i provjeravanjem ovlaštenja na objektu za kontrolu pristupa programskim funkcijama. Sad možete koristiti ograničenje pristupa funkcijama programa da još lakše kontrolirate pristup aplikaciji, dijelovima aplikacije ili funkcijama unutar programa.

Postoje dva načina koja možete koristiti za upravljanje korisničkog pristupa funkcijama aplikacije kroz iSeries Navigator. Prvi koristi podršku Administracije aplikacije:

1. Desno kliknite sistem koji sadržava funkcije čije postavke pristupa želite promijeniti.
2. Izaberite **Administracija aplikacija**.
3. Ako ste na administracijskom sistemu, izaberite **Lokalne postavke**. Inače, nastavite sa sljedećim korakom.
4. Izaberite administrativnu funkciju.
5. Izaberite **Defaultni pristup**, ako je primjenljiv. Ovim izborom dozvoljavate svim korisnicima da po defaultu pristupaju funkciji.
6. Izaberite **Pristup svim objektima**, ako je primjenljiv. Ovim izborom dozvoljavate svim korisnicima sa svim objektnim sistemskim privilegijama pristupaju ovoj funkciji.
7. Izaberite **Prilagodba**, ako je primjenljiva. Upotrebite gumbe **Dodavanje** i **Uklanjanje** u dijalogu **Prilagodba pristupa** da dodate ili uklonite korisnike ili grupe u popisima **Pristup dozvoljen** i **Pristup zabranjen**.
8. Izaberite **Uklanjanje prilagodbe**, ako je primjenljivo. Ovim izborom brišete svaki prilagođeni pristup za izabranu funkciju.
9. Kliknite **OK** da zatvorite dijalog **Administracija aplikacija**.

Drugi način upravljanja korisničkim pristupom uključuje iSeries Navigator podršku Korisnika i Grupa:

1. U iSeries Navigatoru, proširite **Korisnici i Grupe**.
2. Izaberite **Svi korisnici**, **Grupe** ili **Korisnici koji nisu u grupi** za prikaz liste korisnika i grupa.
3. Desno kliknite korisnika ili grupu i izaberite **Svojstva**.

4. Kliknite **Sposobnosti**.
5. Kliknite karticu **Aplikacije**.
6. Ovu stranicu koristite za promjenu postavki pristupa za korisnika ili grupu.
7. Kliknite **OK** dvaput da zatvorite dijalog **Svojstva**.

Pogledajte "iSeries Navigator sigurnost" na stranici 136 za još informacija o sigurnosnim pitanjima iSeries Navigatora.

Ako ste pisac aplikacija, možete koristiti API-je ograničenja pristupa funkcijama programa da učinite sljedeće:

- Registrirate funkciju
- Dohvatite informacije o funkciji
- Definirate tko može ili ne može koristiti funkciju
- Provjerite da vidite da li je korisniku dozvoljena upotreba funkcije

Bilješka: Ova je podrška **nije** zamjena za sigurnost resursa. Ograničenje pristupa funkcijama programa ne spriječava korisniku pristup do resursa (kao što je datoteka ili sučelje) iz drugog sučelja.

Za upotrebu ove podrške unutar aplikacije, dobavljač aplikacije mora registrirati funkcije kad je aplikacija instalirana. Registrirana funkcija se podudara s blokom koda za specifične funkcije u aplikaciji. Kad se aplikacija izvodi od korisnika, aplikacija poziva API prije nego aplikacija pozove blok koda. API poziva API provjere upotrebe da vidi da li je korisniku dozvoljena upotreba funkcije. Ako je korisniku dozvoljena upotreba registrirane funkcije, blok koda se izvodi. Ako je korisniku nije dozvoljena upotreba funkcije, korisniku je spriječeno izvođenje bloka koda.

Bilješka: API je uključio registriranje 30 znakovnog funkcijskog ID-ja u bazi podataka registracije (WRKREGINF). Iako ne postoje izlazne točke koje se odnose na funkcijske ID-e korištene od ograničenog pristupa funkcijskim API-jima, potrebno je imati izlazne točke. Za registriranje bilo čega u registru, **morate** dobaviti ime formata izlazne točke. Da to učini API registriranja funkcije kreira prividno ime formata i koristi ovo prividno ime formata za sve funkcije koje su registrirane. Zbog toga što je ovo prividno ime formata, nikakav program izlazne točke nije nikad pozvan.

Administrator sistema specificira kome je dozvoljen ili zabranjen pristup funkciji. Administrator može ili koristiti API za upravljanje pristupom do funkcije programa ili koristiti iSeries Navigator GUI Administracije aplikacija. Knjiga *iSeries poslužitelj API Upute* daje informacije o API-jima ograničenja pristupa funkcijama programa. Za dodatne informacije o kontroliranju pristupa funkcijama, pogledajte "iSeries Navigator sigurnost" na stranici 136.

Revizije sigurnosti

Ljudi revidiraju svoju sistemsku sigurnost iz nekoliko razloga:

- Da procijene da li je sigurnosni plan potpun.
- Da se osiguraju da su planirane sigurnosne kontrole na mjestu i da rade. Ovaj tip revizije uobičajeno obavlja službenik sigurnosti kao dio dnevne administracije sigurnosti. Također se obavlja, katkada mnogo detaljnije, kao dio periodičkog pregleda sigurnosti od internih ili vanjskih nadzornika.
- Da se osigura da sistemska sigurnost drži takt s promjenama u sistemskom okruženju. Neki primjeri promjena koje utječu na sigurnost su:
  - Novi objekti kreirani od sistemskih korisnika

- Novi korisnici prihvaćeni u sistem
- Promjena vlasništva objekta (autorizacija nije prilagođena)
- Promjena odgovornosti (promijenjena grupa korisnika)
- Privremeno ovlaštenje (nije vremenski opozvano)
- Novoinstalirani proizvodi

• Da se pripremite za budući događaj, kao što je instaliranje nove aplikacije, prelazak na višu sigurnosnu razinu ili uspostava komunikacijske mreže.

Ovdje opisane tehnike prikladne su za sve ove situacije. Što revidirate i kako često ovisi o veličini i sigurnosnim potrebama vaše organizacije.

Revizija sigurnosti uključuje upotrebu naredbi na vašem sistemu i pristup informacijama zapisa i dnevnika. Možete kreirati poseban profil koji će koristiti onaj tko bude obavljao reviziju sigurnosti vašeg sistema. Profil revizora treba *AUDIT posebno ovlaštenje za promjenu osobina revizije sistema. Neki od zadataka revizije predloženih u ovom poglavlju trebaju korisnički profil s *ALLOBJ i *SECADM posebnim ovlaštenjem. Postavite lozinku za profil revizora na *NONE kad se završi razdoblje revizije.

Za više detalja o reviziji sigurnosti pogledajte Poglavlje 9, knjige *Upute za sigurnost*.

Primjer: Izvještaj o sistemskim sigurnosnim atributima

Slika 1pokazuje primjer izlaza naredbe Ispis sistemskih sigurnosnih atributa (PRTSYSSECA). Ovaj izvještaj pokazuje postavke za sistemske vrijednosti vezane uz sigurnost i mrežne atribute koje se preporučuju za sisteme s normalnim sigurnosnim zahtjevima. Također pokazuje trenutne postavke na vašem sistemu.

Bilješka: Stupac *Trenutna vrijednost* na izvještaju prikazuje trenutnu postavku na vašem sistemu. Usporedite ove vrijednosti s preporučenim da vidite gdje možete imati sigurnosna izlaganja.

```
Sistemski sigurnosni atributi

Sistemska vrijednost
Ime             Trenutna vrijednost    Preporučena vrijednost
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
```

Slika 1. Izvještaj o Sistemskim sigurnosnim atributima-Primjer (Dio 1 od 4)

```
QAUTOCFG         0                    0
QAUTORMT         1                    0
QAUTOVRT         9999                 0
QCMNRCYLMT       0 0                  0 0
QCRTAUT          *CHANGE              Kontrola na razini knjižnice
QCRTOBJAUD       *NONE                kontrola na razini knjižnice
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
```

Slika 1. Izvještaj o Sistemskim sigurnosnim atributima-Primjer (Dio 2 od 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
```

Slika 1. Izvještaj o Sistemskim sigurnosnim atributima-Primjer (Dio 3 od 4)

```
Sistemski sigurnosni atributi

Mrežni atributi
Ime              Trenutna vrijednost    Preporučena vrijednost
DDMACC           *OBJAUT                *REJECT
JOBACN           *FILE                  *REJECT
PCSACC           *OBJAUT                *REJECT
```

Slika 1. Izvještaj o Sistemskim sigurnosnim atributima-Primjer (Dio 4 od 4)

Poglavlje 2. iSeries čarobnjak sigurnosti i eServer planer sigurnosti

Alati Čarobnjaka sigurnosti iSeries poslužitelja i eServer planera sigurnosti vam mogu pomoći da odredite koje sigurnosne vrijednosti trebaju postati učinkovite u vašem iSeries poslužitelju. Korištenjem Čarobnjaka sigurnosti iSeries poslužitelja u iSeries Navigatoru ćete dobiti izvještaje koji reflektiraju vaše sigurnosne potrebe na temelju vaših izabranih odgovora. Potom to možete koristiti da konfigurirate sigurnost vašeg sistema.

Koristite iSeries čarobnjaka sigurnosti ili eServer planera sigurnosti kako bi lakše planirali i implementirali osnovnu sigurnosnu politiku za vaše iSeries poslužitelje. Cilj je oba alata da vam pojednostavi implementaciju i upravljanje sigurnosti na vašim sistemima. Čarobnjak, koji je dostupan kao dio OS/400, vam postavlja nekoliko pitanja visoke razine o okruženju vašeg poslužitelja i na osnovi odgovora, daje vam skup preporuka koje čarobnjak može odmah primijeniti na vaš sistem.

eServer planer sigurnosti je online verzija Čarobnjaka sigurnosti. On vam omogućava da izaberete svoje izbore na temelju svojih sigurnosnih potreba i onda vam daje izvještaj koji vam predlaže koja su svojstva potrebna kako bi osigurali svoju stranicu.

eServer planer sigurnosti je Web-zasnovana verzija čarobnjaka. Ona daje preporuke za implementiranje sigurnosti na vašem sistemu, kao što čini i čarobnjak. Međutim, savjetnik ne može primijeniti preporuke. On radije izdaje listu sistemskih sigurnosnih vrijednosti i drugih atributa koje trebate primijeniti na vašem sistemu, osnovanu na vašim odgovorima na pitanja savjetnika.

Čarobnjak sigurnosti

Odlučivanje koje iSeries sigurnosne sistemske vrijednosti trebate koristiti za vaš posao može biti zapleteno. Ako ste novi u implementaciji sigurnosti na iSeries poslužiteljima ili se okolina u kojoj radi vaš iSeries poslužitelj nedavno promijenila, Čarobnjak sigurnosti vam može pomoći s odlukama.

Što je čarobnjak?

- Čarobnjak je alat oblikovan za korištenje od korisnika početnika za instaliranje ili konfiguriranje nečega na sistemu.
- Čarobnjak daje prompt korisniku za informacije postavljanjem pitanja. Odgovor na svako pitanje određuje što će se dalje pitati.
- Kad čarobnjak postavi sva pitanja, korisniku se prezentira završni dijalog. Korisnik tad treba pritisnuti gumb **Završetak** da instalira i konfigurira stavku.

Ciljevi Čarobnjaka sigurnosti

Cilj Čarobnjaka sigurnosti je da konfigurira sljedeće, na osnovu korisnikovih odgovora:

- Sistemske vrijednosti koje se odnose na sigurnost i atribute mreže.
- Izvještavanje i nadgledanje koje se odnosi na sigurnost
- Za generiranje Izvještaja informacija administratora i Izvještaja informacija korisnika:
  - Izvještaj informacija administratora sadržava preporučene postavke sigurnosti i bilo kakve procedure koje treba slijediti prije stavljanja preporuka u djelovanje.
  - Izvještaj informacija korisnika sadržava informacije koje se mogu koristiti za politiku sigurnosti posla. Na primjer, pravila sastavljanja lozinke su uključena u ovom izvještaju.

© Autorska prava IBM Corp. 1996, 2004

- Za omogućavanje preporučenih postavki za raznolike sigurnosno usmjerene stavke na sistemu.

Objektivi Čarobnjaka sigurnosti

- Objektivi Čarobnjaka sigurnosti su:
  - Da odredi što trebaju biti postavke sigurnosti sistema, na osnovi odgovora korisnika na pitanja čarobnjaka i potom implementira postavke kad bude prikladno.
  - Čarobnjak proizvodi detaljne informacijske izvještaje koji uključuju sljedeće:
    - Izvještaj koji objašnjava čarobnjakove preporuke.
    - Izvještaj koji detaljizira procedure koje treba slijediti prije implementacije.
    - Izvještaj koji ispisuje relevantne informacije koje se trebaju razdijeliti korisnicima sistema.
- Ove stavke postavljaju osnovnu politiku sigurnosti aktivnom na vašem sistemu.
- Čarobnjak preporuča izvještaje dnevnika revizije koje trebate rasporediti za periodičko izvođenje. Kad se rasporede, ovi izvještaji pomažu:
  - Osigurati da se slijede sigurnosne politike.
  - Osigurati da se sigurnosne politike mijenjaju samo uz vaše slaganje.
  - Rasporede izvještaje za nadgledanje događaja koji se odnose na sigurnost na vašem sistemu.
- Čarobnjak vam omogućava da spremite preporuke ili da primijenite neke ili sve preporuke na vaš sistem.

Bilješka: Čarobnjak se sigurnosti može koristiti više od jedanput na istom sistemu da dozvoli korisnicima koji možda imaju stariju instalaciju ponovno pregledavanje njihove trenutne sigurnosti. Čarobnjak se sigurnosti može koristiti od V3R7 sistema (kad je iSeries Navigator predstavljen) prema gore.

Za korištenje iSeries Navigatora, morate imati IBM iSeries Access za Windows instaliran na vašem Windows 95/NT PC-u i imati vezu iSeries poslužitelja s tog PC-a. Korisnik čarobnjaka mora biti povezan na iSeries poslužitelj. Korisnik mora imati korisnički ID koji ima *ALLOBJ, *SECADM, *AUDIT i *IOSYSCFG posebna ovlaštenja. Za pomoć pri povezivanju vašeg Windows 95/NT PC-a na vaš iSeries sistem, pogledajte poglavlje IBM iSeries Access za Windows u Informacijskom Centru (pogledajte “Preduvjeti i povezane informacije” na stranici xii za detalje).

Za pristup Čarobnjaku sigurnosti napravite sljedeće:

1. U iSeries Navigatoru, proširite vašeg poslužitelja.
2. Desno kliknite **Sigurnost** i izaberite **Konfiguriranja**.
   - Kad korisnik pokrene opciju **Sigurnost** iSeries Navigatora zahtjev je poslan iSeries poslužitelju za provjeru posebnog ovlaštenja korisnika.
   - Ako korisnik ne bude imao sva potrebna posebna ovlaštenja (*ALLOBJ, *AUDIT, *IOSYSCFG, *SECADM) tada neće vidjeti opciju **Konfiguriranje** i neće moći pristupiti Čarobnjaku sigurnosti.
3. Pretpostavimo da korisnik ima potrebno ovlaštenje:
   - Dohvaćeni su prethodni odgovori čarobnjaka.
   - Dohvaćene su trenutne postavke sigurnosti.

Čarobnjak sigurnosti će vam predstaviti jedan od ekrana dobrodošlice. Koji ekran vidite ovisi o tome koji od sljedećih uvjeta postoji:

- Čarobnjak nikad nije izvođen za ciljni iSeries poslužitelj.
- Čarobnjak je prethodno izvođen, a sigurnosne promjene su odgođene.
- Čarobnjak je prethodno izvođen, a sigurnosne promjene su učinjene aktivnima.

Ako ne koristite iSeries Navigator, još uvijek možete dobiti pomoć za planiranje vaših sigurnosnih potreba. eServer planer sigurnosti je online verzija Čarobnjaka sigurnosti, s jednom razlikom. Savjetnik neće automatski konfigurirati vaš sistem. On će ipak, generirati izvještaj preporučenih sigurnosnih opcija zasnovan na vašim odgovorima. Kako bi pristupili eServer planeru sigurnosti, idite na eServer Informacijski Centar

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

Planer eServer sigurnosti

Planer eServer sigurnosti je online verzija Čarobnjaka sigurnosti. On pita ista pitanja kao i Čarobnjak sigurnosti i na osnovu vaših odgovora, generira iste preporuke. Glavna razlika između ta dva alata je da:

- Planer eServer sigurnosti **ne**—
  - Proizvodi izvještaje.
  - Uspoređuje trenutne postavke s preporučenim postavkama.
  - Postavlja nikakvu sistemsku vrijednost automatski.
- Ne možete primijeniti preporuke planera eServer sigurnosti.

Planer eServer sigurnosti generira CL program koji možete odrezati i zalijepiti i uređivati za vlastito korištenje kako bi automatizirali konfiguraciju sigurnosti. Isto tako, možete se povezati izravno na iSeries dokumentaciju poslužitelja iz planera eServer sigurnosti. To omogućuje informacije o sistemskoj vrijednosti ili izvještaj koji vam može pomoći pri određivanju da li je ovo postavljanje prikladno za vaše okruženje.

Za pristup planeru eServer sigurnosti, usmjerite Internet pretražitelj na sljedeći URL:

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

Poglavlje 3. Kontrola interaktivne prijave

Kad razmišljate o ograničavanju ulaza u vaš sistem, počnite s očitim, ekran Prijave. Slijede opcije koje možete koristiti da nekome otežate prijavu na vaš sistem upotrebom ekrana Prijave.

Postavljanje pravila lozinke

Da osigurate prijavu na vaš sistem, učinite sljedeće:
- Postavite politiku koja traži da lozinke ne smiju biti trivijalne i ne smiju se dijeliti.
- Postavite sistemsku vrijednost koja vam pomaže u forsiranju. Tablica 1 pokazuje preporučene postavke sistemske vrijednosti.

Kombinacija vrijednosti u Tablica 1 je prilično ograničavajuća i namijenjena je značajnom smanjenju vjerojatnosti trivijalnih lozinki. Međutim, vašim se korisnicima izbor lozinke koja zadovoljava ova ograničenja može učiniti teškim i frustrirajućim.

Razmotrite nuđenje korisnicima sljedećeg:
1. Liste kriterija za lozinke.
2. Primjere lozinki koje jesu i koje nisu važeće.
3. Prijedloge za smišljanje dobre lozinke.

Izvedite naredbu Konfiguriranje sigurnosti sistema (CFGSYSSEC) da postavite ove vrijednosti. Koristite naredbu Ispis sigurnosnih atributa sistema (PRTSYSSECA) za ispis vaših trenutnih postavki za ove sistemske vrijednosti.

Poglavlje 3 knjige *Uputa iSeries sigurnosti* "Vrijednosti postavljene naredbom Konfiguriranje sistemske sigurnosti" na stranici 33 daje još informacija o CFGSYSSEC naredbi.

Tablica 1. Sistemske vrijednosti za lozinke

Ime sistemske vrijednosti	Opis	Preporučena vrijednost
QPWDEXPITV	Koliko često korisnici sistema moraju mijenjati svoje lozinke. Možete specificirati različitu vrijednost za pojedinačne korisnike u korisničkom profilu.	60 (dana)
QPWDLMTAJC	Da li sistem spriječava iste susjedne znakove.	1 (da)
QPWDLMTCHR	Koji se znakovi ne mogu koristiti u lozinkama.[2]	AEIOU#$@
QPWDLMTREP	Da li sistem spriječava da se isti znak u lozinci pojavi više od jedanput .	2 (nije dozvoljeno uzastopno)
QPWDLVL	Da li su lozinke korisničkog profila ograničene na 10 znakova ili maksimum od 128.	0[3]
QPWDMAXLEN	Maksimalni broj znakova u lozinci.	8
QPWDMINLEN	Minimalni broj znakova u lozinci.	6
QPWDPOSDIF	Da li svaki znak lozinke mora biti različit od znaka na istom položaju u prethodnoj lozinci.	1 (da)
QPWDRQDDGT	Da li lozinka mora imati bar jedan numerički znak.	1 (da)
QPWDRQDDIF	Koliko dugo korisnik mora čekati prije ponovne upotrebe iste lozinke.[2]	5 ili manje (intervala isteka)[1]
QPWDVLDPGM	Koji se izlazni program poziva za provjeru valjanosti novo dodijeljene lozinke.	*NONE

© Autorska prava IBM Corp. 1996, 2004

Tablica 1. Sistemske vrijednosti za lozinke (nastavak)

Ime sistemske vrijednosti	Opis	Preporučena vrijednost

Bilješke:

1. QPWDEXPITV sistemska vrijednost specificira koliko često morate mijenjati vašu lozinku, kao što je svakih 60 dana. Ovo je **interval isteka**. QPWDRQDDIF sistemska vrijednost specificira koliko mnogo intervala isteka mora proteći prije no što možete ponovo koristiti istu lozinku. Poglavlje 3 *Uputa iSeries sigurnosti* knjige daje još informacija o načinu zajedničkog rada ovih sistemskih vrijednosti.
2. QPWDLMTCHR nije obavezan na razinama lozinki 2 ili 3. Pogledajte "Razine lozinke" za detalje.
3. Pogledajte "Planiranje promjena razine lozinke" da odredite razinu lozinke koja je prava za vaše potrebe.

Razine lozinke

Počevši od V5R1 operativnog sistema, QPWDLVL sistemska vrijednost nudi povećanu sigurnost lozinke. U prethodnim izdanjima, korisnici su bili ograničeni na lozinke koje nisu bile duže od 10 znakova, iz ograničenog raspona znakova. Sad, korisnici mogu izabrati lozinku (ili izraz za prolaz) i sa 128 znakova, ovisno o razini lozinke na koju je njihov sistem postavljen. Razine lozinke su:

- **Razina 0:** Sistemi se otpremaju s ovom razinom. Na razini 0, lozinke nisu duže od 10 znakova, a sadržavaju samo A-Z, 0–9, #, @, $ i _ znakove. Lozinke su na razini 0 manje sigurne od onih na višim razinama lozinki.
- **Razina 1:** Neka pravila kao kod razine lozinke 0, ali lozinke za iSeries Podršku za Windows Network Neighborhood (ovdje se kasnije naziva iSeries NetServer) nisu spremljene.
- **Razina 2:** Lozinke su sigurne na ovoj razini. Ova se razina može koristiti u svrhe testiranja. Lozinke su spremljene za korisnike na razini 0 ili 1 ako su 10 znakova li manje i koriste skup znakova za lozinke razine 0 ili 1. Lozinke (ili izrazi za prolaz) na ovoj razini imaju sljedeće osobine:
  - i do 128 znakova u dužini.
  - sadržavaju sve dostupne znakove tipkovnice.
  - ne mogu se u potpunosti sastojati od praznina; praznine se uklanjaju s kraja lozinke.
  - osjetljive su na velika i mala slova.
- **Razina 3:** Lozinke su na ovoj razini najsigurnije i iskorištavaju najnaprednije dostupne algoritme šifriranja. Lozinke na ovoj razini imaju iste osobine kao na razini 2. Lozinke za iSeries NetServer nisu spremljene na ovoj razini.

Trebate koristiti samo razine lozinki 2 i 3 ako svaki sistem u vašoj mreži odgovara ovom kriteriju:

- Operativni sistem je V5R1 ili kasniji
- Razina lozinke je postavljena na 2 ili 3

Slično, svi se korisnici moraju prijaviti upotrebom iste razine lozinke. Razine lozinki su globalne; korisnici ne mogu izabrati razinu na kojoj žele da se osiguraju njihove lozinke.

Planiranje promjena razine lozinke

Promjenu razina lozinki treba pažljivo planirati. Operacije s drugim sistemima mogu ne uspjeti ili se korisnici možda neće moći prijaviti na sistem, ako niste planirali prikladnu promjenu razine lozinke. Prije promjene QPWDLVL sistemske vrijednosti, osigurajte da ste spremili vaše sigurnosne podatke upotrebom SAVSECDTA ili SAVSYS naredbe. Ako imate trenutnu sigurnosnu kopiju, moće ćete ponovno postaviti lozinke za sve korisničke profile ako se trebate vratiti na nižu razinu lozinki.

Proizvodi koje koristite na sistemu i na klijentima s kojima sistem međudjeluje, mogu imati probleme kad je sistemska vrijednost razine lozinke (QPWDLVL) postavljena na 2 ili 3. Svaki proizvod ili klijent koji sistemu šalju lozinke u šifriranom obliku, umjesto da ih u čistom tekstu korisnik unosi na ekran prijave, mora biti nadograđen za rad s novim pravilima šifriranja lozinke za QPWDLVL 2 ili 3. Slanje šifrirane lozinke poznato je kao **zamjena lozinke**.

Zamjena lozinke se koristi za spriječavanje hvatanja lozinke za vrijeme prijenosa preko mreže. Zamjene lozinke generirane od starih klijenata koji ne podržavaju nove algoritme za QPWDLVL 2 ili 3, čak i ako su specifični znakovi ispravni, neće biti prihvaćene. Ovo se također odnosi na bilo kakav iSeries na iSeries ravnopravan pristup koji koristi šifrirane vrijednosti za provjeru ovlaštenja iz jednog sistema na drugi.

Problem je složen činjenicom da neki utjecajni proizvodi (kao što je Java Toolbox) su dani kao srednji sloj. Proizvodi treće osobe koji pripajaju prethodnu verziju jednog od ovih proizvoda neće ispravno raditi dok nisu iznova izgrađeni upotrebom ažurirane verzije srednjeg sloja.

Davanjem ovih i drugih scenarija, lako je vidjeti zašto je potrebno pažljivo planiranje prije mijenjanja QPWDLVL sistemske vrijednosti.

Razmatranja za promjenu QPWDLVL iz 0 na 1

Razina lozinke 1 omogućuje sistemu, koji nema potrebu za komunikacijom s Windows 95/98/ME AS/400 Podrškom klijenta za Windows Network Neighborhood (iSeries NetServer) proizvodom, da posjeduje iSeries NetServer lozinke eliminirane iz sistema. Eliminiranje nepotrebno šifriranih lozinki iz sistema povećava ukupnu sigurnost sistema.

Na QPWDLVL 1, sve će trenutne, prije-V5R1 zamjene lozinke i mehanizmi provjere autentičnosti lozinki nastaviti raditi. Mala je mogućnost prekida osim za funkcije i usluge koje trebaju iSeries NetServer lozinku.

Razmatranja za promjenu QPWDLVL iz 0 ili 1 na 2

Razina lozinke 2 uvodi upotrebu lozinki osjetljivih na velika i mala slova do 128 znakova dužine (također zvanih izraza za prolaz) i daje maksimalnu sposobnost vraćanja natrag na QPWDLVL 0 ili 1.

Bez obzira na razinu lozinke sistema, lozinke razina lozinke 2 i 3 su kreirane kad god se lozinka promijeni ili se korisnik prijavi na sistem. Posjedovanje lozinki razine 2 i 3 kreiranih dok je sistem još uvijek na razini lozinki 0 ili 1 pomaže u pripremi za promjenu na razinu lozinke 2 ili 3.

Prije mijenjanja QPWDLVL u 2, trebate koristiti DSPAUTUSR ili PRTUSRPRF TYPE(*PWDINFO) naredbe da locirate sve korisničke profile koji nemaju lozinku koja je upotrebljiva na razini lozinke 2. Ovisno o profilima koje ove naredbe lociraju, možda ćete željeti koristiti jedan od sljedećih mehanizama da dodate profilima lozinku razine lozinke 2 i 3.

- Promijenite lozinku za korisnički profil upotrebom CHGUSRPRF ili CHGPWD CL naredbe ili QSYCHGPW API-ja. Ovo će uzrokovati da sistem promijeni lozinku koja je upotrebljiva na razini lozinki 0 i 1; a sistem također kreira dvije ekvivalentne lozinke osjetljive na velika i mala slova koje su upotrebljive na razinama lozinki 2 i 3. Sva velika slova i sva mala slova verzija lozinke je kreirana za upotrebu na razini lozinke 2 ili 3.

  Na primjer, promjena lozinke u C4D2RB4Y rezultira u sistemskom generiranju lozinki C4D2RB4Y i c4d2rb4y razine lozinke 2.
- Prijavite se na sistem kroz mehanizam koji prezentira lozinku u čistom tekstu (ne koristi zamjenu lozinke). Ako je lozinka važeća i korisnički profil nema lozinku koja je

upotrebljiva na razinama lozinki 2 i 3, sistem kreira dvije jednakovrijedne lozinke osjetljive na velika i mala slova koje su upotrebljive na razinama lozinki 2 i 3. Sva velika slova i sva mala slova verzija lozinke je kreirana za upotrebu na razini lozinke 2 ili 3.

Odsustvo lozinke koja je upotrebljiva na razinama lozinki 2 i 3 može biti problem kad god i korisnički profil nema lozinku koja je upotrebljiva na razinama lozinki 0 i 1 ili kad korisnik pokuša prijavu kroz proizvod koji koristi zamjenu lozinke. U ovim slučajevima, korisnik će neće moći prijaviti kad se razina lozinke promijeni na 2.

Ako korisnički profil nema lozinku koja je upotrebljiva na razinama lozinki 2 i 3, korisnički profil ima lozinku koja je upotrebljiva na razinama lozinki 0 i 1, te se korisnik prijavljuje kroz proizvod koji šalje lozinke u čistom tekstu, tad sistem provjeriti valjanost korisnika na razini lozinke 0 i kreira dvije lozinke razine lozinke 2 (kako je gore opisano) za korisnički profil. Valjanosti će narednih prijava biti provjerene na osnovi lozinki razine lozinke 2.

Svaki klijent/usluga koja koristi zamjenu lozinki neće ispravno raditi na QPWDLVL 2 ako klijent/usluga nije ažurirana da koristi novu shemu zamjene lozinke (izraza za prolaz) . Administrator treba provjeriti da li je klijent/usluga koji nije ažuriran na novu shemu zamjene lozinki potreban.

Klijenti/usluge koji koriste zamjenu lozinke uključuju:

- TELNET
- iSeries Access
- iSeries Host poslužitelji
- QFileSrv.400
- iSeries NetServer podrška ispisa
- DDM
- DRDA
- SNA LU6.2

Preporuča se da se sigurnosni podaci spreme prije promjene na QPWDLVL 2. Ovo može učiniti ponovni prijelaz na QPWDLVL 0 ili 1 lakšim, ako on postane potreban.

Preporuča se da se druge sistemske vrijednosti lozinki, kao što je QPWDMINLEN i QPWDMAXLEN ne mijenjaju dok se ne testira QPWDLVL 2. Ovo će prijelaz natrag na QPWDLVL 1 ili 0, ako je potreban, učiniti lakšim. Međutim, QPWDVLDPGM sistemska vrijednost mora specificirati ili *REGFAC ili *NONE prije no sistem dozvoli promjenu QPWDLVL-a na 2. Stoga, ako koristite program provjere valjanosti lozinke, možda ćete željeti pisati novi koji se može registrirati za QIBM_QSY_VLD_PASSWRD izlaznu točku upotrebom ADDEXITPGM naredbe.

iSeries NetServer lozinke su još uvijek podržane na QPWDLVL 2, tako da bi bilo koja funkcija/usluga koja traži iSeries NetServer lozinku svejedno trebala ispravno funkcionirati.

Jednom kad administrator postane sigurniji u izvođenju sistema na QPWDLVL 2, mogu početi mijenjanja sistemske vrijednosti lozinki na iskorištavanje dužih lozinki. Međutim, administrator treba biti svjestan da će duže lozinke imati ove učinke:

- Ako je specificirana lozinka veća od 10 znakova, lozinka je razine lozinke 0 i 1 obrisana. Ovaj se korisnički profil neće moći prijaviti ako se sistem vrati na razinu lozinki 0 ili 1.
- Ako lozinke sadržavaju posebne znakove ili ne slijede pravila sastavljanja za jednostavna imena objekata (isključujući osjetljive na velika i mala slova), lozinka je razine lozinke 0 i 1 obrisana.

- Ako je specificirana lozinka veća od 14 znakova, iSeries NetServer lozinka za korisnički profil je obrisana.
- Sistemske se vrijednosti lozinki jedino odnose na novu vrijednost razine lozinke 2 i ne odnose se na sistemski generiranu lozinku razine lozinke 0 i 1 ili iSeries NetServer vrijednosti lozinke (ako su generirane).

Razmatranja za promjenu QPWDLVL iz 2 na 3

Nakon izvođenja sistema na QPWDLVL 2 jedan period vremena, administrator može razmotriti prelazak na QPWDLVL 3 da maksimizira svoju zaštitu sigurnosti lozinkama.

Kod QPWDLVL 3, sve iSeries NetServer lozinke su obrisane tako da sistem ne treba pomaknuti na QPWDLVL 3 dok ne bude potrebno koristiti iSeries NetServer lozinke.

Kod QPWDLVL 3, sve su lozinke razine lozinki 0 i 1 obrisane. Administrator može koristiti DSPAUTUSR ili PRTUSRPRF naredbe da locira korisnički profil koji nema lozinke razine lozinki 2 ili 3 pridružene njemu.

Promjena na nižu razinu lozinki

Vraćanje na nižu QPWDLVL vrijednost, dok je moguće, nije potpuno bezbolna operacija. Općenito, treba razmišljati da je ovo jednosmjeran put iz nižih QPWDLVL vrijednosti na više QPWDLVL vrijednosti. Međutim, može biti slučaja kad se mora ponovo postaviti niža QPWDLVL vrijednost.

Svaka od sljedećih sekcija raspravlja o radu potrebnom za vraćanje na nižu razinu lozinki.

Razmatranja za promjenu iz QPWDLVL 3 na 2: Ova je promjena relativno laka. Jednom kad se QPWDLVL postavi na 2, administrator treba odrediti da li bilo koji korisnički profil treba sadržavati iSeries NetServer lozinke ili lozinke razine lozinki 0 ili 1 i ako je tako, promijeniti lozinku korisničkog profila na dopustivu vrijednost.

Dodatno, vrijednosti sistema lozinki se mogu vratiti na vrijednosti kompatibilne s lozinkama iSeries NetServera i razinom lozinki 0 ili 1, ako su te lozinke potrebne.

Razmatranja za promjenu iz QPWDLVL 3 na 1 ili 0: Zbog velike mogućnosti uzrokovanja problema za sistem (kao kad se nitko ne može prijaviti zato što su sve lozinke razine lozinki 0 i 1 obrisane), ova promjena nije izravno podržana. Da promijenite iz QPWDLVL 3 na QPWDLVL 1 ili 0, sistem prvo mora napraviti prijelaznu promjenu na QPWDLVL 2.

Razmatranja za promjenu iz QPWDLVL 2 na 1: Prije promjene QPWDLVL na 1, administrator treba koristiti DSPAUTUSR ili PRTUSRPRF TYPE(*PWDINFO) naredbe da locira sve korisničke profile koji nemaju lozinke razine lozinki 0 ili 1. Ako će korisnički profil trebati lozinku nakon promjene QPWDLVL-a, administrator treba osigurati kreiranje lozinke razine lozinke 0 i 1 za profil upotrebom jednog od sljedećih mehanizama:

- Promijenite lozinku za korisnički profil upotrebom CHGUSRPRF ili CHGPWD CL naredbe ili QSYCHGPW API-ja. Ovo će uzrokovati da sistem promijeni lozinku koja je upotrebljiva na razinama lozinki 2 i 3; te sistem također kreira ekvivalentnu lozinku s velikim slovima koja je upotrebljiva na razinama lozinki 0 i 1. Sistem lozinku razine lozinki 0 i 1, jedino može kreirati ako su zadovoljeni sljedeći uvjeti:
  - Lozinka je duga 10 znakova ili manje.
  - Lozinka se može pretvoriti u velika slova EBCDIC znakove A-Z, 0-9, @, #, $ i _.
  - Lozinka ne počinje s numeričkim znakom ili znakom podcrtavanja.

Na primjer, promjena lozinke u vrijednost RainyDay će rezultirati u sistemskom generiranju lozinke RAINYDAY razine lozinke 0 i 1. Ali promjena vrijednosti lozinke u Rainy Days In April, uzrokovati će da sistem obriše lozinku razine lozinke 0 i 1 (jer je lozinka predugačka i sadržava praznine).

Ne proizvodi se nikakva poruka ili znak ako se ne može kreirati lozinka razine lozinki 0 i 1.

- Prijavite se na sistem kroz mehanizam koji prezentira lozinku u čistom tekstu (ne koristi zamjenu lozinke). Ako je lozinka važeća i korisnički profil nema lozinku koja je upotrebljiva na razinama lozinki 0 i 1, sistem kreira jednakovrijednu lozinku koja je upotrebljiva na razinama lozinki 0 i 1. Sistem lozinku razine lozinki 0 i 1, jedino može kreirati ako su zadovoljeni gore navedeni uvjeti.

Administrator tad može promijeniti QPWDLVL na 1. Sve su iSeries NetServer lozinke obrisane kad promjena na QPWDLVL 1 počne djelovati (sljedeći IPL).

Razmatranja za promjenu iz QPWDLVL 2 na 0: Razmatranja su ista kao za promjenu iz QPWDLVL 2 na 1 osim da su sve iSeries NetServer lozinke zadržane kad promjena počne djelovati.

Razmatranja za promjenu iz QPWDLVL 1 na 0: Nakon promjene QPWDLVL na 0, administrator treba koristiti naredbe DSPAUTUSR ili PRTUSRPRF da locira svaki korisnički profil koji nema iSeries NetServer lozinku. Ako korisnički profil treba iSeries NetServer lozinku, ona se može kreirati promjenom lozinke korisnika ili prijavom kroz mehanizam koji prikazuje lozinku u čistom tekstu.

Administrator potom može promijeniti QPWDLVL na 0.

Promjena poznatih lozinki

Učinite sljedeće da zatvorite neke dobro poznate ulaze u iSeries poslužitelj koji možda postoje na vašem sistemu.

__ Korak 1. Osigurajte da nikakav korisnički profil više nema defaultne lozinke (jednake imenu korisničkog profila). Možete koristiti naredbu Analize defaultnih lozinki (ANZDFTPWD). (Pogledajte “Izbjegavanje defaultnih lozinki” na stranici 23.)

__ Korak 2. Pokušajte prijavu na vaš sistem s kombinacijama korisničkih profila i lozinki koje su pokazane u Tablica 2 na stranici 19. Ova lozinke su izdane i one su prvi izbor za bilo koga tko pokušava prodrijeti u vaš sistem. Ako se možete prijaviti, upotrijebite naredbu Promjena korisničkog profila (CHGUSRPRF) da promijenite lozinku na preporučenu vrijednost.

__ Korak 3. Pokrenite Namjenske servisne alate (DST) i pokušajte prijavu s lozinkama koje su pokazane u Tablica 2 na stranici 19. Pogledajte iSeries Informacijski Centar—>Sigurnost—>Servisni alati. Pogledajte “Preduvjeti i povezane informacije” na stranici xii za informacije o pristupu iSeries Informacijskom Centru.

__ Korak 4. Ako se možete prijaviti na DST s bilo kojom od ovih lozinki, trebate promijeniti lozinke. iSeries Informacijski Centar—>Sigurnost—>Servisni alati daju detaljne instrukcije o načinu mijenjanja korisničkih ID-a i lozinki servisnih alata. Pogledajte “Preduvjeti i povezane informacije” na stranici xii za informacije o pristupu iSeries Informacijskom Centru.

__ Korak 5. Konačno, osigurajte da se ne može prijaviti samo s pritiskanjem tipke Enter na ekranu Prijave bez unosa ID-ja korisnika i lozinke. Iskušajte nekoliko različitih ekrana. Ako se možete prijaviti bez upisivanja informacija u ekran Prijave, učinite nešto od sljedećeg:

- Promijenite na razinu sigurnosti 40 ili 50 (QSECURITY sistemska vrijednost).

Bilješka: Vaše se aplikacije mogu različito izvoditi kad povećate vašu razinu sigurnosti na 40 ili 50.

- Promijenite sve ulaze u radnu stanicu za interaktivne podsisteme da ukazuju na opise poslova koje specificira USER(*RQD).

Tablica 2. Lozinke za IBM dobavljeni profil

Korisnički ID	Lozinka	Preporučena vrijednost
QSECOFR	QSECOFR[1]	Netrivijalna vrijednost poznata samo administratoru sigurnosti. **Upišite lozinku koju ste izabrali i pohranite ju na sigurno mjesto.**
QSYSOPR	QSYSOPR	*NONE[2]
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2, 3]
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

Bilješke:

1. Sistem dolazi s *Postavi lozinke na istekle* vrijednosti za QSECOFR postavljeno na *YES. Prvi put kad se prijavite na novi sistem, morate promijeniti QSECOFR lozinku.
2. Sistem treba ove korisničke profile za sistemske funkcije, ali vi ne trebate dozvoliti korisnicima prijavu s ovim profilima. Za nove sisteme instalirane s V3R1 ili kasnijim izdanjima, ova je lozinka otpremljena kao *NONE.

   Kad izvodite naredbu CFGSYSSEC, sistem postavlja ove lozinke na *NONE.
3. Za izvođenje iSeries Accessa za Windows upotrebom TCP/IP, QUSER korisnički profil mora biti omogućen.

Tablica 3. Lozinke za namjenske servisne alate

DST Razina	Korisnički ID[1]	Lozinka	Preporučena vrijednost
Osnovna sposobnost	11111111	11111111	Netrivijalna vrijednost poznata samo administratoru sigurnosti.[2]
Potpuna sposobnost	22222222	22222222[3]	Netrivijalna vrijednost poznata samo administratoru sigurnosti.[2]
Sigurnosna sposobnost	QSECOFR	QSECOFR[3]	Netrivijalna vrijednost poznata samo administratoru sigurnosti.[2]
Sposobnost usluge	QSRV	QSRV[3]	Netrivijalna vrijednost poznata samo administratoru sigurnosti.[2]

Bilješke:

1. Korisnički ID je jedino potreban za PowerPC AS (RISC) izdanja operativnog sistema.
2. Ako se vaš predstavnik hardverskog servisa treba prijaviti s ovim korisničkim ID-om i lozinkom, promijenite lozinku na novu vrijednost nakon što predstavnik hardverskog servisa ode.
3. Korisnički profil servisnih alata će isteći nakon što bude prvi put korišten.

Bilješka: DST lozinke se jedino mogu promijeniti od ovlaštenog uređaja. Ovo je također istinito za sve lozinke i odgovarajuće korisničke ID-e koji su jednaki. Za više informacija o ovlaštenim uređajima, pogledajte informacije postava Operacijske konzole u iSeries Informacijskom Centru.

Postavljanje vrijednosti prijave

Tablica 4 pokazuje nekoliko vrijednosti koje možete postaviti da prijavu neovlaštene osobe učinite još težom. Ako izvodite naredba CFGSYSSEC, on postavlja ove sistemske vrijednosti na preporučene postavke. O ovim sistemskim vrijednostima možete pročitati više u Poglavlju 3 knjige *Uputa iSeries sigurnosti*.

Tablica 4. Sistemske vrijednosti prijave

Ime sistemske vrijednosti	Opis	Preporučeno postavljanje
QAUTOCFG	Da li sistem automatski konfigurira nove uređaje.	0 (Ne)
QAUTOVRT	Broj opisa virtualnih uređaja koji će sistem automatski kreirati ako nikakav uređaj nije dostupan za upotrebu.	0
QDEVRCYACN	Što sistem radi kad se uređaj nakon greške ponovo spaja.[1]	*DSCMSG
QDSCJOBITV	Koliko dugo sistem čeka prije završavanja prekinutog posla.	120
QDSPSGNINF	Da li sistem prikazuje informacije o prethodnoj aktivnosti prijave kad se korisnik prijavljuje.	1 (Da)
QINACTITV	Koliko dugo sistem čeka prije poduzimanja akcije kad je interaktivan posao neaktivan.	60
QINACTMSGQ	Što sistem čini kad je dosegnut QINACTITV vremenski period.	*ENDJOB
QLMTDEVSSN	Da li sistem spriječava prijavljivanje korisnika na više radnih stanica istovremeno.	1 (Da)
QLMTSECOFR	Da li se korisnici s *ALLOBJ ili *SERVICE posebnim ovlaštenjem mogu prijaviti samo na određenim radnim stanicama.	1 (Da)[2]
QMAXSIGN	Maksimum uzastopnih, netočnih pokušaja prijave (pogrešan korisnički profil ili lozinka).	3
QMAXSGNACN	Što sistem čini kad je dosegnuta QMAXSIGN granica.	3 (Onemogućava i korisnički profil i uređaj)

Bilješke:

1. Sistem može odspojiti i ponovo spojiti TELNET sesije kad je opis uređaja za sesiju izričito dodijeljen.
2. Ako postavite sistemsku vrijednost na 1 (Da), trebati ćete izričito ovlastiti korisnike s *ALLOBJ ili *SERVICE posebnim ovlaštenjem za uređaje. Najjednostavniji način za to je davanje QSECOFR korisničkom profilu *CHANGE ovlaštenje za specifične uređaje.

Promjena poruka grešaka kod prijave

Hakeri vole znati kad napreduju pri provaljivanju u vaš sistem. Kad poruka greške na ekranu Prijave kaže Lozinka nije ispravna, haker može pretpostaviti da korisnički ID jeste ispravan. Možete frustrirati hakera upotrebom naredbe Promjena opisa poruke (CHGMSGD) da promijenite tekst za poruke greški kod prijave. Tablica 5 pokazuje preporučeni tekst.

Tablica 5. Poruke greški kod prijave

ID poruke	Otpremljeni tekst	Preporučeni tekst
CPF1107	CPF1107 – Lozinka nije ispravna za korisnički profil.	Informacija prijave nije ispravna **Bilješka:** Ne uključujte ID poruke u tekstu poruke.

Tablica 5. Poruke greški kod prijave (nastavak)

ID poruke	Otpremljeni tekst	Preporučeni tekst
CPF1120	CPF1120 – Korisnik XXXXX ne postoji.	Informacija prijave nije ispravna. **Bilješka:** Ne uključujte ID poruke u tekstu poruke.

Dostupnost rasporeda korisničkih profila

Možda želite da neki korisnički profili budu dostupni za prijavu samo u određenim dijelovima dana ili određenim danima tjedna. Na primjer, ako imate profil postavljen za nadzornika sigurnosti, možda želite omogućiti taj korisnički profil samo za sate kad je nadzornik raspoređen za rad. Možda također želite onemogućiti korisničke profile s *ALLOBJ posebnim ovlaštenjem (uključujući QSECOFR korisnički profil) za vrijeme neradnih sati.

Možete koristiti naredbu Promjena unosa rasporeda aktiviranja (CHGACTSCDE) za postavljanje korisničkih profila koji će biti omogućeni i automatski onemogućeni. Za svaki korisnički profil koji želite rasporediti, kreirate ulaz koji definira raspored korisničkog profila.

Na primjer, ako želite da QSECOFR profil bude dostupan jedino između 7 u jutro i 10 na večer, upisali bi sljedeće u CHGACTSCDE ekran:

```
              Promjena ulaza rasp. aktiviranja (CHGACTSCDE)

Upišite izbore, pritisnite Enter.

Korisnički profil  . . . . . > QSECOFR       Ime
Vrijeme omogućenja . . . . . > '7:00'        Vrijeme, *NONE
Vrijeme onemogućenja . . . . . > '22:00'     Vrijeme, *NONE
Dani . . . . . > *MON        *ALL, *MON, *TUE, *WED...
                               > *TUE
                               > *WED
                               > *THU
              + za više vrijednosti > *FRI
```

Slika 2. Ekran rasporeda aktiviranja profila–Primjer

Zapravo, možda želite imati QSECOFR profil dostupan samo za vrlo ograničen broj sati svakog dana. Možete koristiti drugi korisnički profil sa *SECOFR klasom da obavite većinu sistemskih funkcija. Ovako, ćete izbjeći izlaganje dobro poznatih korisničkih profila od pokušaja hakera.

Povremeno možete koristiti naredbu Prikaz ulaza u dnevnik revizije (DSPAUDJRNE) za ispis CP-a (Promjena profila) unos u dnevnik revizije. Koristite ove unose da provjerite da sistem omogućava i onemogućava korisničke profile na osnovi vašeg planiranog rasporeda.

Drugi način provjeravanja za osiguravanje da se korisnički profili onemogućavaju po vašem planiranom rasporedu je upotreba naredbe Ispisa korisničkog profila (PRTUSRPRF). Kad specificirate *PWDINFO za tip izvještaja , izvještaj uključuje stanje svakog izabranog korisničkog profila. Ako, na primjer, regularno onemogućite sve korisničke profile s *ALLOBJ posebnim ovlaštenjem, sljedeću naredbu možete rasporediti za izvođenje odmah nakon što su profili onemogućeni:

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

Uklanjanje neaktivnih korisničkih profila

Vaš sistem treba sadržavati samo potrebne korisničke profile. Ako više ne trebate korisnički profil zato što je korisnik ili napustio posao ili preuzeo različit posao unutar organizacije, uklonite korisnički profil. Ako je netko odsutan iz organizacije duži period, onemogućite (deaktivirajte) taj korisnički profil. Nepotreban korisnički profil može omogućiti neovlašten ulaz u vaš sistem.

Automatsko onemogućavanje korisničkih profila

Možete koristiti naredbu Analiza aktivnosti profila (ANZPRFACT) da redovito onemogućavate korisničke profile koji su bili neaktivni navedeni broj dana. Kad koristite naredbu ANZPRFACT, specificirate broj neaktivnih dana koji sistem traži. Sistem gleda dan zadnjeg korištenja, dan vraćanja i dan kreiranja za korisnički profil.

Jednom kad specificirate vrijednost za ANZPRFACT naredbu, sistem raspoređuje na tjedno izvođenje u 1 poslije ponoći (počevši s danom kad ste prvi put specificirali vrijednost). Posao ispituje sve profile i onemogućava neaktivne profile. Ne trebate ponovno koristiti naredbu ANZPRFACT, osim ako ne želite promijeniti broj neaktivnih dana.

Možete koristiti naredbu Promjena liste aktivnih profila (CHGACTPRFL) da neke profile učinite izuzetim od ANZPRFACT obrađivanja. CHGACTPRFL naredba kreira listu korisničkih profila koje ANZPRFACT naredba neće onemogućiti, bez obzira koliko dugo ti profili bili neaktivni.

Kad sistem izvodi ANZPRFACT naredbu, on piše CP unos u dnevnik revizije za svaki korisnički profil koji je onemogućen. Za ispis korisničkih profila koji su novo onemogućeni možete koristiti naredbu DSPAUDJRNE.

Bilješka: Sistem piše unose revizije samo ako QAUDCTL vrijednost specificira *AUDLVL, a QAUDLVL sistemska vrijednost specificira *SECURITY.

Drugi način provjeravanja za osiguravanje da se korisnički profili onemogućavaju po vašem planiranom rasporedu je upotreba naredbe Ispisa korisničkog profila (PRTUSRPRF). Kad specificirate *PWDINFO za tip izvještaja, izvještaj uključuje stanje svakog izabranog korisničkog profila.

Automatsko uklanjanje korisničkih profila

Možete koristiti naredbu Promjena unosa rasporeda isteka (CHGEXPSCDE) za upravljanje uklanjanja ili onemogućavanja korisničkih profila. Ako znate da korisnik odlazi na duži period, možete rasporediti korisnički profil da bude uklonjen ili onemogućen.

Kad prvi put koristite naredbu CHGEXPSCDE, ona kreira unos rasporeda posla koji se izvodi svaki dan 1 minutu nakon ponoći. Posao gleda u QASECEXP datoteke da odredi da li su ikakvi korisnički profili raspoređeni za uklanjanje na taj dan.

Sa naredbom CHGEXPSCDE, vi ili onemogućavate ili brišete korisnički profil. Ako izaberete brisanje korisničkog profila, morate specificirati što će sistem učiniti s objektima koje korisnik posjeduje. Prije no što rasporedite korisnički profil na brisanje, trebate istražiti koje objekte korisnik posjeduje. Na primjer, ako korisnik posjeduje programe koji prihvaćaju ovlaštenje, da li želite da ti programi prihvate vlasništvo novog vlasnika? Ili, da li novi vlasnik ima više ovlaštenja nego što je potrebno (npr. posebno ovlaštenje)? Možda trebate kreirati novi korisnički profil sa specifičnim ovlaštenjima koji će posjedovati programe koji trebaju prihvatiti ovlaštenje.

Također trebate istražiti da li će se desiti ikakvi aplikacijski problemi ako obrišete korisnički profil. Na primjer, da li ikakvi opisi poslova specificiraju korisnički profil kao defaultnog korisnika?

Možete koristiti naredbu Prikaz rasporeda isteka (DSPEXPSCD) za prikaz liste profila koji su raspoređeni da budu onemogućeni ili uklonjeni.

Možete koristiti naredbu Prikaz ovlaštenih korisnika (DSPAUTUSR) za ispis svih korisničkih profila na vašem sistemu. Koristite naredbu Brisanje korisničkog profila (DLTUSRPRF) za brisanje profila koji su vremenski istekli.

Sigurnosna napomena:: Korisnički profil onemogućujete postavljanjem njegovog statusa na *DISABLED. Kad onemogućite korisnički profil, činite ga neraspoloživim za interaktivnu upotrebu. Ne možete se prijaviti ili promijeniti vaš posao na onemogućenom korisničkom profilu. Paketni se poslovi mogu izvoditi pod korisničkim profilom koji je onemogućen.

Izbjegavanje defaultnih lozinki

Kad kreirate novi korisnički profil, default je učiniti lozinku istom kao ime korisničkog profila. Ovo nekome daje priliku da prodre u vaš sistem, ako netko zna vašu politiku dodjeljivanja imena profila i zna da se nova osoba pridružuje vašoj organizaciji.

Kad kreirate nove korisničke profile, uzmite u obzir dodjeljivanje jedinstvene, netrivijalne lozinke umjesto upotrebe defaultne lozinke. Lozinku povjerljivo recite novom korisniku, kao na primjer u pismu “Dobro došli u sistem” koje daje obris vaših politika sigurnosti. Zatražite od korisnika da promijeni lozinku kad se prvi put prijavi postavljanjem korisničkog profila na PWDEXP(*YES).

Možete koristiti naredbu Analiza defaultnih lozinki (ANZDFTPWD) da provjerite upotreba za sve korisničke profile na vašem sistemu. Kad ispisujete izvještaj, imate opciju specificiranja da sistem treba poduzeti akciju (kao što je onemogućavanje korisničkog profila) ako je lozinka ista kao ime korisničkog profila. ANZDFTPWD naredba ispisuje listu profila koje je našla i bilo koju akciju koju je poduzela.

Bilješka: Lozinke su na vašem sistemu pohranjene u jednosmjerno šifriranom obliku. One se ne mogu dešifrirati. Sistem šifrira navedenu lozinku i uspoređuje ju s pohranjenom lozinkom kao što bi provjerio lozinku kad se prijavljujete na sistem. Ako revidirate greške ovlaštenja (*AUTFAIL), sistem će pisati PW unos dnevnika revizije za svaki korisnički profil koji *ne* posjeduje defaultnu lozinku (za sisteme koji izvode V4R1 ili ranija izdanja). Počevši s V4R2, sistem ne piše PW unose dnevnika revizije kad izvedete naredbu ANZDFTPWD.

Nadgledanje prijave i aktivnosti lozinke

Ako ste zabrinuti zbog neovlaštenih pokušaja prodora u vaš sistem, možete koristiti naredbu PRTUSRPRF kao pomoć za nadgledanje prijave i aktivnosti lozinke.

Slijedi nekoliko prijedloga za korištenje ovog izvještaja:

- Odredite da li je interval isteka lozinke za neke korisničke profile duži od sistemske vrijednosti i da li je duži interval isteka opravdan. Na primjer, u izvještaju, USERY ima interval isteka lozinke od 120 dana.
- Redovito izvodite ovaj izvještaj za nadgledanje neuspješnih pokušaja prijave. Netko tko pokušava prodrijeti u vaš sistem, može biti svjestan da vaš sistem poduzima akciju nakon

određenog broja neuspješnih pokušaja. Svaku noć, mogući uljez može pokušati više puta, ali manje od vaše QMAXSIGN vrijednosti da izbjegne da budete obaviješteni o pokušajima. Međutim, ako izvodite ovaj izvještaj rano svako jutro i primijetite da određeni profili često imaju neuspješne pokušaje prijave, možete sumnjati da imate problem.

- Identificirajte korisničke profile koji nisu bili korišteni duže vrijeme ili čije lozinke nisu bile promijenjene duže vrijeme.

Informacije o pohrani lozinke

Da podrže neke mrežne funkcije i komunikacijske zahtjeve, iSeries poslužitelji pružaju sigurne metode za spremanje lozinki koje mogu biti dešifrirane. Vaš sistem koristi ove lozinke, na primjer, za uspostavu SLIP veze s drugim sistemom. (“Sigurnost i sesije biranja van” na stranici 111 opisuje ovu upotrebu spremljenih lozinki.)

iSeries poslužitelji spremaju ove posebne lozinke u sigurno područje koje nije dostupno niti jednom korisničkom programu ili sučelju. Samo izričito ovlaštene sistemske funkcije mogu postaviti ove lozinke i dohvatiti ih.

Na primjer, kada koristite spremljenu lozinku za SLIP povezivanje s biranjem van, postavljate lozinku sistemskom naredbom koja kreira konfiguracijski profil (WRKTCPPTP). Morate imati *IOSYSCFG za upotrebu naredbe. Posebno kodirana skripta povezivanja dohvaća lozinku i dešifrira je za vrijeme postupka biranja van. Dešifrirana lozinka nije vidljiva korisniku ili bilo kojem dnevniku posla.

Kao sistemski administrator, morate odlučiti da li ćete dozvoliti da lozinke koje mogu biti dešifrirane budu spremljene na vašem sistemu. Koristite sistemsku vrijednost Zadrži sigurnosne podatke poslužitelja (QRETSVRSEC) da ovo specificirate. Defaultno je 0 (NE). Stoga, vaš sistem neće pohranjivati lozinke koje mogu biti dešifrirane osim ako izričito ne postavite ovu sistemsku vrijednost.

Ako imate mrežne ili komunikacijske zahtjeve za spremljenim lozinkama, trebate postaviti odgovarajuće politike i razumjeti politike i praksu vaših komunikacijskih partnera. Na primjer, kada koristite SLIP da komunicirate s drugim iSeries poslužiteljem, oba sistema trebaju razmotriti postavljanje posebnih korisničkih profila za uspostavljanje sesija. Posebni profili trebaju imati ograničeno ovlaštenje na sistemu. Ovo ograničava utjecaj na vaš sistem ako je spremljena lozinka dovedena u pitanje na partnerovom sistemu.

Poglavlje 4. Konfiguriranje iSeriesa za upotrebu Alata za sigurnost

Ove informacije opisuju postavljanje vašeg sistema za upotrebu Alata za sigurnost koji su dio OS/400. Kad instalirate OS/400, alati za sigurnost su spremni za korištenje. Poglavlja koja slijede daju prijedloge za operacijske procedure s alatima za sigurnost.

Siguran rad s Alatima za sigurnost

Kad instalirate OS/400, objekti koji su pridruženi alatima za sigurnost su sigurni. Da alati za sigurnost rade sigurno, izbjegnite promjenu ovlaštenja za bilo koje objekte alata za sigurnost.

Slijede sigurnosne postavke i zahtjevi za objekte alata za sigurnost:

- Programi i naredbe alata za sigurnost se nalaze u knjižnici QSYS proizvoda. Naredbe i programi se otpremaju s javnim ovlaštenjem *EXCLUDE. Mnoge od naredbi alata za sigurnost kreiraju datoteke u QUSRSYS knjižnici. Kad sistem kreira ove datoteke, javno ovlaštenje za ove datoteke je *EXCLUDE.

  Datoteke koje sadržavaju informacije za proizvođenje promijenjenih izvještaja imaju imena koja počinju s QSEC. Datoteke koje sadržavaju informacije za upravljanje korisničkim profilima imaju imena koja počinju s QASEC. Ove datoteke sadržavaju povjerljive informacije o sistemu. Stoga, ne trebate mijenjati javno ovlaštenje za datoteke.
- alati za sigurnost koriste vaš normalni sistemski postav za usmjeravanje ispisanog izlaza. Ovi izvještaji sadržavaju povjerljive informacije o sistemu. Da usmjerite izlaz da štiti izlazni red, napravite prikladne promjene na korisničkom profilu ili opisu posla za korisnike koji će koristiti alate za sigurnost.
- Zbog njihovih funkcija sigurnosti i zato što oni pristupaju mnogim objektima na sistemu, naredbe alata za sigurnost trebaju *ALLOBJ posebno ovlaštenje. Neke od naredbi također trebaju *SECADM, *AUDIT ili *IOSYSCFG posebno ovlaštenje. Da osigurate da se naredbe uspješno izvode, trebate se prijaviti kao službenik sigurnosti kad koristite alate za sigurnost. Stoga, ne trebate dodijeliti privatno ovlaštenje bilo kojoj naredbi alata za sigurnost.

Izbjegavanje sukoba datoteka

Mnoge od naredbi izvještaja alata za sigurnost kreiraju datoteku baze podataka koju možete koristiti za ispis promijenjene verzije izvještaja. “Naredbe i izbornici za sigurnosne naredbe” na stranici 26 daje ime datoteke za svaku naredbu. Istovremeno možete izvoditi naredbu samo iz jednog posla. Većina naredbi sad ima provjere koje to forsiraju. Ako izvodite naredbu dok drugi posao još nije završio njeno izvođenje, primit ćete poruku o greški.

Mnogi poslovi ispisa su dugo izvodeći poslovi. Trebate biti pažljivi da izbjegnete sukobe datoteka kad submitirate izvještaje u batch ili ih dodajete u raspoređivač posla. Na primjer, možda želite ispisati dvije verzije PRTUSRPRF izvještaja s različitim izbornim kriterijem. Ako šaljete izvještaje na izvođenje u batch, trebate koristiti red posla koji izvodi samo jedan posao u trenutku da osigurate da se poslovi izvještaja izvode sekvencijalno.

Ako koristite raspoređivač posla, trebate rasporediti dva posla dovoljno razdvojena tako da se prva verzija dovrši prije nego što se drugi posao pokrene.

© Autorska prava IBM Corp. 1996, 2004

Spremanje Alata za sigurnost

Programe alata za sigurnost spremate kad god izvodite naredbu Spremanje sistema (SAVSYS) ili opciju iz izbornika Spremanje koja izvodi SAVSYS naredbu.

Datoteke alata za sigurnost su u QUSRSYS knjižnici. Ovu knjižnicu bi već trebali redovito spremati, kao dio vaših normalnih radnih procedura. QUSRSYS knjižnica sadržava podatke za mnoge licencne programe na vašem sistemu. Pogledajte Informacijski Centar za još informacija o naredbama i opcijama koje spremaju QUSRSYS knjižnicu.

Naredbe i izbornici za sigurnosne naredbe

Ovaj odlomak opisuje naredbe i izbornike za sigurnosne alate. Primjeri kako koristiti naredbe, uključeni su skroz ove informacije.

Za sigurnosne alate dostupna su dva izbornika:

- SECTOOLS (Sigurnosni alati) izbornik za interaktivno izvođenje naredbi.
- SECBATCH (Submitiraj ili rasporedi sigurnosne izvještaje u batch) izbornik za izvođenje naredbi izvještaja u batch. SECBATCH izbornik ima dva dijela. Prvi dio ovog izbornika koristi naredbu Submitiranje posla (SBMJOB) za slanje izvještaja na neposrednu obradu u batch.

  Drugi dio izbornika koristi naredbu Dodavanje unosa u raspored posla (ADDJOBSCDE). Koristite je za raspoređivanje izvještaja sigurnosti na redovito izvođenje na specificirani dan i vrijeme.

Opcije izbornika Alata za sigurnost

Tablica 6 opisuje ove opcije izbornika i pridružene naredbe:

Tablica 6. Naredbe alata za korisničke profile

Izbornik[1] opcija	Ime naredbe	Opis	Korištena datoteka baze podataka
1	ANZDFTPWD	Koristite naredbu Analiza defaultnih lozinki da prijavite i poduzmete akciju nad korisničkim profilima koji imaju lozinku jednaku imenu profila.	QASECPWD[2]
2	DSPACTPRFL	Koristite naredbu Prikaz liste aktivnih profila za prikaz ili ispis liste korisničkih profila koji su izuzeti od ANZPRFACT obrade.	QASECIDL[2]
3	CHGACTPRFL	Koristite naredbu Promjena liste aktivnih profila da dodate i uklonite korisničke profile iz liste izuzetaka za ANZPRFACT naredbu. Korisnički profil koji je na listi aktivnih profila, trajno je aktivan (dok ne uklonite profil s liste). ANZPRFACT naredba ne onemogućava profil koji je na listi aktivnih profila, bez obzira koliko je dugo profil bio neaktivan.	QASECIDL[2]
4	ANZPRFACT	Koristite naredbu Analiza aktivnosti profila da onemogućite korisničke profile koji nisu bili korišteni specificirani broj dana. Nakon što upotrijebite ANZPRFACT naredbu da specificirate broj dana, sistem izvodi ANZPRFACT posao svaku noć. Možete koristiti CHGACTPRFL naredbu da izuzmete korisničke profile od onemogućavanja.	QASECIDL[2]

Tablica 6. Naredbe alata za korisničke profile (nastavak)

Izbornik[1] opcija	Ime naredbe	Opis	Korištena datoteka baze podataka
5	DSPACTSCD	Koristite naredbu Prikaz rasporeda aktiviranja profila da prikažete ili ispišete informacije o rasporedu omogućavanja i onemogućavanja određenih korisničkih profila. Raspored kreirate s CHGACTSCDE naredbom.	QASECACT[2]
6	CHGACTSCDE	Koristite naredbu Promjena unosa rasporeda aktiviranja da omogućite korisničkom profilu prijavu samo u određena vremena dana ili tjedna. Za svaki korisnički profil koji raspoređujete, sistem kreira unose rasporeda posla za vremena omogućavanja i onemogućavanja.	QASECACT[2]
7	DSPEXPSCD	Koristite naredbu Prikaz rasporeda isteka za prikaz ili ispis liste korisničkih profila koji su raspoređeni da budu onemogućeni ili uklonjeni iz sistema u budućnosti. Koristite CHGEXPSCDE naredbu da postavite korisničke profile na istek.	QASECEXP[2]
8	CHGEXPSCDE	Koristite naredbu Promjena unosa raspored isteka da rasporedite korisnički profil na uklanjanje. Možete ga privremeno ukloniti (onemogućavanjem) ili ga možete obrisati iz sistema. Ova naredba koristi unos rasporeda posla koji se izvodi svaki dan u 00:01 (1 minuta nakon ponoći). Posao gleda u QASECEXP datoteku da odredi da li su ikakvi korisnički profili postavljeni na isticanje na taj dan. Koristite DSPEXPSCD naredbu za prikaz korisničkih profila koji su raspoređeni na isticanje.	QASECEXP[2]
9	PRTPRFINT	Koristite naredbu Ispis unutrašnjosti profila za ispis izvještaja koji sadržava informacije o broju unosa sadržanih u korisničkom profilu. Broj unosa određuje veličinu korisničkog profila.	

Bilješke:

1. Opcije su iz SECTOOLS izbornika.
2. Ova je datoteka u QUSRSYS knjižnici.

Možete otići stranicu dolje na izborniku da vidite dodatne opcije. Tablica 7 na stranici 28 opisuje opcije izbornika i pridružene naredbe za reviziju sigurnosti:

Tablica 7. Naredbe alata za reviziju sigurnosti

Izbornik[1] opcija	Ime naredbe	Opis	Korištena datoteka baze podataka
10	CHGSECAUD	Koristite naredbu Promjena revizije sigurnosti da postavite reviziju sigurnosti i promijenite sistemske vrijednosti koje kontroliraju reviziju sigurnosti. Kad izvodite naredbu CHGSECAUD, sistem kreira dnevnik revizije sigurnosti (QAUDJRN) ako već ne postoji. CHGSECAUD naredba omogućuje opcije koje pojednostavljuju postavljanje sistemske vrijednosti QAUDLVL (razina revizije). Možete specificirati *ALL da aktivirate sve moguće postavke razine revizije. Ili, možete specificirati *DFTSET da aktivirate najuobičajenije korištene postavke (*AUTFAIL, *CREATE, *DELETE, *SECURITY i *SAVRST). **Bilješka:** Ako koristite alate sigurnosti za postavljanje revizije, ne zaboravite planirati upravljanje vaših primalaca dnevnika revizije. Inače, možete brzo naići na probleme s iskoristivosti diska.	
11	DSPSECAUD	Koristite naredbu Prikaz revizije sigurnosti da prikažete informacije o dnevniku revizije sigurnosti i sistemskim vrijednostima koje kontroliraju reviziju sigurnosti.	

Bilješke:

1. Opcije su iz SECTOOLS izbornika.

Upotreba izbornika Sigurnosni batch

Slijedi prvi dio SECBATCH izbornika:

```
SECBATCH         Submitira ili raspoređuje sigurnosne izvještaje u batch
                                                                  Sistem:
Izaberite jedno od sljedećeg:

  Submit izvještaja u batch
     1. Usvajajući objekti
     2. Unosi u dnevnik revizije
     3. Ovlaštenja autorizacijske liste
     4. Ovlaštenje naredbe
     5. Privatna ovlaštenja naredbe
     6. Sigurnost komunikacija
     7. Ovlaštenje direktorija
     8. Privatno ovlaštenje direktorija
     9. Ovlaštenje dokumenta
    10. Privatno ovlaštenje dokumenta
    11. Ovlaštenje datoteke
    12. Privatno ovlaštenje datoteke
    13. Ovlaštenje foldera
```

Kad izaberete opciju iz ovog izbornika, prikazat će se ekran Submit posla (SBMJOB). Ako želite promijeniti defaultne opcije naredbe, možete pritisnuti F4 (Prompt) na redu *Naredba za izvođenje*.

Da vidite Izvještaje batcha rasporeda, idite stranicu dolje na SECBATCH izborniku. Upotrebom opcija na ovom dijelu izbornika, možete, na primjer, postaviti vas sistem da

redovito izvodi promijenjene verzije izvještaja. Možete otići stranicu dolje za dodatne opcije izbornika. Kad izaberete opciju iz ovog izbornika, prikazuje se ekran Dodavanje unosa rasporeda posla (ADDJOBSCDE).

Možete postaviti kursor na red *Naredba za izvođenje* i pritisnuti F4 (Prompt) da izaberete različite postavke za izvještaj. Trebate dodijeliti znakovito ime posla tako da možete prepoznati unos kad prikazujete unose rasporeda posla.

Opcije izbornika Sigurnosni batch

Tablica 8 opisuje opcije izbornika i pridružene naredbe za izvještaje sigurnosti.

Kad izvodite sigurnosne izvještaje, sistem ispisuje samo informacije koje zadovoljavaju i kriterij izbora koji ste specificirali i kriterij izbora za alat. Na primjer, opisi poslova koji specificiraju ime korisničkog profila su sigurnosno relevantni. Zbog toga izvještaj opisa posla (PRTJOBDAUT) ispisuje opise poslova samo za navedenu knjižnicu, ako javno ovlaštenje za opis posla nije *EXCLUDE *i* ako opis posla specificira ime korisničkog profila u USER parametru.

Slično, kad ispisujete informacije podsistema (PRTSBSDAUT naredba), sistem ispisuje informacije o podsistemu samo kad opis podsistema ima komunikacijski ulaz koji specificira korisnički profil.

Ako određeni izvještaj ispisuje manje informacija nego što očekujete, pogledajte online informacije za pomoć da saznate kriterij izbora za izvještaj.

Tablica 8. Naredbe za sigurnosne izvještaje

Izbornik[1] opcija	**Ime naredbe**	**Opis**	**Korištena datoteka baze podataka**
1, 40	PRTADPOBJ	Koristite naredbu Ispis objekata usvajanja za ispis liste objekata koji usvajaju ovlaštenje specificiranog korisničkog profila. Možete specificirati jednostruki profil, ime generičkog profila (npr. svi profili koji počinju s Q) ili sve korisničke profile na sistemu. Ovaj izvještaj ima dvije verzije. Potpuni izvještaj ispisuje sve usvojene objekte koji zadovoljavaju kriterij izbora. Promijenjeni izvještaj ispisuje razlike između usvojenih objekata koji su trenutno na sistemu i usvojenih objekata koji su bili na sistemu kad ste zadnji put izvodili izvještaj.	QSECADPOLD[2]
2, 41	DSPAUDJRNE	Koristite naredbu Prikaz unosa dnevnika revizije za prikaz ili ispis informacija o ulazima u sigurnosni dnevnik revizije. Možete izabrati određeni tip unosa, određenog korisnika i vremenski period.	QASYxxJ4[3]

Tablica 8. Naredbe za sigurnosne izvještaje (nastavak)

Izbornik[1] opcija	**Ime naredbe**	**Opis**	**Korištena datoteka baze podataka**
3, 42	PRTPVTAUT *AUTL	Kad koristite naredbu Ispis privatnih ovlaštenja za *AUTL objekte, primate listu svih autorizacijskih lista na sistemu. Izvještaj uključuje korisnike koji su ovlašteni za svaku listu i koje ovlaštenje korisnici imaju za listu. Ove informacije koristite kao pomoć pri analizi izvora objektnih ovlaštenja na vašem sistemu. Ovaj izvještaj ima tri verzije. Potpuni izvještaj ispisuje sve autorizacijske liste na sistemu. Promijenjeni izvještaj ispisuje dodatke i promjene autorizacije od vašeg zadnjeg izvođenja izvještaja. Izvještaj brisanja ispisuje čija su ovlaštenja na autorizacijskoj listi obrisana od vašeg zadnjeg izvođenja izvještaja. Kad ispisujete potpuni izvještaj, imate opciju ispisa liste objekata koje svaka autorizacijska lista osigurava. Sistem će kreirati odijeljen izvještaj za svaku autorizacijsku listu.	QSECATLOLD[2]
6, 45	PRTCMNSEC	Koristite naredbu Ispis sigurnosti komunikacije za ispis sigurnosno relevantnih postavki za objekte koji utječu na komunikacije na vašem sistemu. Ove postavke utječu na to kako korisnici ili poslovi mogu ući u vaš sistem. Ova naredba proizvodi dva izvještaja: izvještaj koji prikazuje postavke za konfiguracijske liste na sistemu i izvještaj koji ispisuje sigurnosno relevantne parametre za opise linija, kontrolera i opise uređaja. Svaki od ovih izvještaja ima potpunu verziju i verziju promjena.	QSECCMNOLD[2]
15, 54	PRTJOBDAUT	Koristite naredbu Ispis ovlaštenja opisa posla za ispis liste opisa posla koja specificira korisnički profil i ima javno ovlaštenje koje nije *EXCLUDE. Izvještaj pokazuje posebna ovlaštenja za korisnički profil koji je naveden u opisu posla. Ovaj izvještaj ima dvije verzije. Potpuni izvještaj ispisuje sve objekte opisa posla koji zadovoljavaju kriterij izbora. Promijenjeni izvještaj ispisuje razlike između objekata opisa posla koji su trenutno na sistemu i objekata opisa posla koji su bili na sistemu kad ste zadnji put izvodili izvještaj.	QSECJBDOLD[2]
Pogledajte opasku 4.	PRTPUBAUT	Koristite naredbu Ispis javno ovlaštenih objekata za ispis liste objekata čije javno ovlaštenje nije *EXCLUDE. Kad izvodite naredbu, specificirate tip objekta i knjižnicu ili knjižnice za izvještaj. Koristite naredbu PRTPUBAUT za ispis informacija o objektima kojima može pristupiti svaki korisnik na sistemu. Ovaj izvještaj ima dvije verzije. Potpuni izvještaj ispisuje sve objekte koji zadovoljavaju kriterij izbora. Promijenjeni izvještaj ispisuje razlike između specificiranih objekata koji su trenutno na sistemu i objekata (istog tipa u istoj knjižnici) koji su bili na sistemu kad ste zadnji put izvodili izvještaj.	QPBxxxxxx[5]

Tablica 8. Naredbe za sigurnosne izvještaje (nastavak)

Izbornik[1] opcija	Ime naredbe	Opis	Korištena datoteka baze podataka
Pogledajte opasku 5.	PRTPVTAUT	Koristite naredbu Ispis privatnih ovlaštenja za ispis liste privatnih ovlaštenja na objekte specificiranog tipa u specificiranoj knjižnici. Koristite ovaj izvještaj kao pomoć pri određivanju izvora ovlaštenja za objekte. Ovaj izvještaj ima tri verzije. Potpuni izvještaj ispisuje sve objekte koji zadovoljavaju kriterij izbora. Promijenjeni izvještaj ispisuje razlike između specificiranih objekata koji su trenutno na sistemu i objekata (istog tipa u istoj knjižnici) koji su bili na sistemu kad ste zadnji put izvodili izvještaj. Izvještaj brisanja ispisuje listu korisnika čija su ovlaštenja na objekt obrisana od kad ste zadnji put ispisivali izvještaj.	QPVxxxxxx[5]
24, 63	PRTQAUT	Koristite Ispis ovlaštenja reda za ispis sigurnosnih postavki ili izlaznih redova i redova posla na vašem sistemu. Ove postavke kontroliraju tko može gledati i promijeniti unose u izlazni red ili red posla. Ovaj izvještaj ima dvije verzije. Potpuni izvještaj ispisuje sve objekte izlaznog reda i reda posla koji zadovoljavaju kriterij izbora. Promijenjeni izvještaj ispisuje razlike između objekata izlaznog reda i reda posla koji su trenutno na sistemu i objekata izlaznog reda i reda posla koji su bili na sistemu kad ste zadnji put izvodili izvještaj.	QSECQOLD[2]
25, 64	PRTSBSDAUT	Koristite naredbu Ispis opisa podsistema za ispis sigurnosno relevantnih komunikacijskih unosa za opise podsistema na vašem sistemu. Ove postavke kontroliraju kako posao može ući u vaš sistem i kako se izvode poslovi. Izvještaj ispisuje opis podsistema samo ako on ima komunikacijske unose koji specificiraju ime korisničkog profila. Ovaj izvještaj ima dvije verzije. Potpuni izvještaj ispisuje sve objekte opisa podsistema koji zadovoljavaju kriterij izbora. Promijenjeni izvještaj ispisuje razlike između objekata opisa podsistema koji su trenutno na sistemu i objekata opisa podsistema koji su bili na sistemu kad ste zadnji put izvodili izvještaj.	QSECSBDOLD[2]
26, 65	PRTSYSSECA	Koristite naredbu Ispis sigurnosnih atributa sistema za ispis liste sigurnosno relevantnih sistemskih vrijednosti i mrežnih atributa. Izvještaj pokazuje trenutnu vrijednost i preporučenu vrijednost.	
27, 66	PRTTRGPGM	Koristite naredbu Ispis programa okidača za ispis liste programa okidača koji su pridruženi s datotekama baza podataka na vašem sistemu. Ovaj izvještaj ima dvije verzije. Potpuni izvještaj ispisuje svaki program okidač koji je dodijeljen i zadovoljava vaš kriterij izbora. Promijenjeni izvještaj ispisuje programe okidače koji su bili dodijeljeni od kad ste zadnji put izvodili izvještaj.	QSECTRGOLD[2]

Tablica 8. Naredbe za sigurnosne izvještaje (nastavak)

Izbornik[1] opcija	Ime naredbe	Opis	Korištena datoteka baze podataka
28, 67	PRTUSROBJ	Koristite naredbu Ispis korisničkih objekata za ispis liste korisničkih objekata (objekata koji nisu dobavljeni od IBM-a), a koji su u knjižnici. Možete koristiti ovaj izvještaj za ispis liste korisničkih objekata koji su u knjižnici (npr. QSYS) koja je u sistemskom dijelu liste knjižnice. Ovaj izvještaj ima dvije verzije. Potpuni izvještaj ispisuje sve korisničke objekte koji zadovoljavaju kriterij izbora. Promijenjeni izvještaj ispisuje razlike između korisničkih objekata koji su trenutno na sistemu i korisničkih objekata koji su bili na sistemu kad ste zadnji put izvodili izvještaj.	QSECPUOLD[2]
29, 68	PRTUSRPRF	Koristite naredbu Ispis korisničkog profila za analizu korisničkih profila koji zadovoljavaju specificirani kriterij. Možete izabrati korisničke profile na osnovi posebnih ovlaštenja, korisničke klase ili nepodudarnosti između posebnih ovlaštenja i korisničke klase. Možete ispisati informacije ovlaštenja, informacije okoline, informacije lozinke ili informacije razine lozinke.	
30, 69	PRTPRFINT	Koristite naredbu Ispis unutrašnjosti profila za ispis izvještaja internih informacija o broju unosa.	
31, 70	CHKOBJITG	Koristite naredbu Provjera integriteta objekta da odredite da li su operativni objekti (kao što su programi) promijenjeni bez upotrebe prevodioca. Ova vam naredba može pomoći otkriti pokušaje unosa programa virusa u vaš sistem ili mijenjanja programa da izvodi neovlaštene instrukcije. *Uputa iSeries sigurnosti* knjiga daje još informacija o CHKOBJITG naredbi.	

Bilješke:

1. Opcije su iz SECBATCH izbornika.
2. Ova je datoteka u QUSRSYS knjižnici.
3. xx je dvo-znakovni tip unosa u dnevnik. Na primjer, izlazna datoteka modela za unos AE dnevnika je QSYS/QASYAEJ4. Izlazne su datoteke modela opisane u Dodatku F *Uputa iSeries sigurnosti* knjige.
4. SECBATCH izbornik sadržava opcije za tipove objekata koji se tipično tiču administratore sigurnosti. Na primjer, upotreba opcija 11 ili 50 za izvođenje PRTPUBAUT naredbe za *FILE objekte. Koristite općenite opcije (18 i 57) da specificirate tip objekta.
5. SECBATCH izbornik sadržava opcije za tipove objekata koji se tipično tiču administratore sigurnosti. Na primjer, opcije 12 ili 51 izvode PRTPVTAUT naredbu za *FILE objekte. Koristite općenite opcije (19 i 58) da specificirate tip objekta.
6. xxxxxx u imenu datoteke je tip objekta. Na primjer, datoteka se za objekte programa naziva QPBPGM za javna ovlaštenja i QPVPGM za privatna ovlaštenja. Datoteke su u QUSRSYS knjižnici.

   Datoteka sadržava člana za svaku knjižnicu za koju ste ispisali izvještaj. Ime člana je isto kao ime knjižnice.

Naredbe za prilagodbu sigurnosti

Tablica 9 na stranici 33 opisuje naredbe koje možete koristiti za prilagodbu sigurnosti na vašem sistemu. Ove su naredbe na SECTOOLS izborniku.

Tablica 9. Naredbe za prilagodbu vašeg sistema

Izbornik[1] opcija	Ime naredbe	Opis	Korištena datoteka baze podataka
60	CFGSYSSEC	Koristite naredbu Konfiguriranje sigurnosti sistema da postavite sigurnosno relevantne sistemske vrijednosti na njihove preporučene postavke. Naredba također postavlja reviziju sigurnosti na vašem sistemu. "Vrijednosti postavljene naredbom Konfiguriranje sistemske sigurnosti" opisuje što radi naredba. **Bilješka:** Da postignete sigurnosne preporuke prilagođene vašoj situaciji, izvodite iSeries Čarobnjaka sigurnosti ili iSeries Savjetnika sigurnosti umjesto izvođenja ove naredbe. Pogledajte Poglavlje 2, "iSeries čarobnjak sigurnosti i eServer planer sigurnosti", na stranici 9 za informacije o ovim alatima.	
61	RVKPUBAUT	Koristite naredbu Opoziv javnog ovlaštenja da postavite javno ovlaštenje na *EXCLUDE za skup sigurnosno osjetljivih naredbi na vašem sistemu. "Funkcije naredbe Opoziv javnog ovlaštenja" na stranici 35 ispisuje akcije koje obavlja naredba RVKPUBAUT.	

Bilješke:

1. Opcije su iz SECTOOLS izbornika.

Vrijednosti postavljene naredbom Konfiguriranje sistemske sigurnosti

Tablica 10 ispisuje sistemske vrijednosti koje su postavljene kada izvodite naredbu CFGSYSSEC. Naredba CFGSYSSEC izvodi program koji se zove QSYS/QSECCFGS.

Tablica 10. Vrijednosti postavljene naredbom CFGSYSSEC

Ime sistemske vrijednosti	Postavljanje	Opis sistemske vrijednosti
QALWOBJRST	*NONE	Da li sistemski programi stanja i programi koji usvajaju ovlaštenje mogu biti vraćeni.
QAUTOCFG	0 (Ne)	Automatska konfiguracija novih uređaja
QAUTOVRT	0	Broj opisa virtualnih uređaja koje će sistem automatski kreirati ako uređaj nije dostupan za upotrebu.
QDEVRCYACN	*DSCMSG (Odspajanje s porukom)	Sistemska akcija kada je komunikacija ponovo uspostavljena
QDSCJOBITV	120	Vremenski period prije nego sistem poduzme akcije za odspajanje posla
QDSPSGNINF	1 (Da)	Da li korisnici vide prikaz informacija prijave
QINACTITV	60	Vremenski period prije nego sistem poduzme akcije za neaktivan interaktivan posao
QINACTMSGQ	*ENDJOB	Akcije koje sistem poduzme za neaktivan posao
QLMTDEVSSN	1 (Da)	Da li su korisnici ograničeni na prijavljivanje na jedan uređaj u istom vremenu
QLMTSECOFR	1 (Da)	Da li su *ALLOBJ i *SERVICE korisnici ograničeni na specifične uređaje
QMAXSIGN	3	Koliko je uzastopnih, neuspješnih pokušaja prijave dozvoljeno
QMAXSGNACN	3 (Oboje)	Da li sistem onemogućava radnu stanicu ili korisnički profil kada je dosegnuta QMAXSIGN granica.

Tablica 10. Vrijednosti postavljene naredbom CFGSYSSEC (nastavak)

Ime sistemske vrijednosti	Postavljanje	Opis sistemske vrijednosti
QRMTSIGN	*FRCSIGNON	Kako sistem obrađuje udaljeni (prolaz-kroz ili TELNET) pokušaj prijave.
QRMTSVRATR	0 (Isključen)	Dozvoljava li sistem da bude udaljeno analiziran.
QSECURITY [1]	50	Razina sigurnosti koja se forsira
QVFYOBJRST	3 (Provjera potpisa kod vraćanja)	Provjera objekta kod vraćanja
QPWDEXPITV	60	Kako često korisnici moraju mijenjati svoje lozinke
QPWDMINLEN	6	Minimalna dužina lozinke
QPWDMAXLEN	8	Maksimalna dužina lozinke
QPWDPOSDIF	1 (Da)	Da li se svaka pozicija u novoj lozinki mora razlikovati od iste pozicije u zadnjoj lozinki
QPWDLMTCHR	Pogledajte opasku2	Znakovi koji nisu dozvoljeni u lozinci
QPWDLMTAJC	1 (Da)	Da li su susjedni brojevi zabranjeni u lozinci
QPWDLMTREP	2 (Ne može se ponavljati uzastopno)	Da li su ponavljajući znakovi u lozinci zabranjeni znakovi
QPWDRQDDGT	1 (Da)	Da li lozinke moraju imati najmanje jedan broj
QPWDRQDDIF	1 (32 jedinstvene lozinke)	Koliko jedinstvenih lozinki je potrebno prije nego što se lozinka može ponoviti
QPWDVLDPGM	*NONE	Korisnik izlazi iz programa koji sistem poziva da provjeri valjanost lozinki

Bilješke:

1. Ako trenutno radite s QSECURITY vrijednosti 40 ili niže, ponovo pregledajte informacije u Poglavlju 2 knjige *Uputa iSeries sigurnosti* prije nego pređete na višu razinu sigurnosti.
2. Ograničeni znakovi su spremljeni u poruci ID CPXB302 u datoteci poruka QSYS/QCPFMSG. Otpremaju se kao AEIOU@$#. Možete koristiti naredbu Promjena opisa poruke (CHGMSGD) da promijenite ograničene znakove. Sistemska vrijednost QPWDLMTCHR se ne primjenjuje na razinama sigurnosti 2 ili 3.

Naredba CFGSYSSEC također postavlja lozinku na *NONE za sljedeće IBM-dobavljene korisničke profile:

QSYSOPR
QPGMR
QUSER
QSRV
QSRVBAS

Konačno, naredba CFGSYSSEC postavlja reviziju sigurnosti koristeći naredbu Revizija sigurnosti (CHGSECAUD). Naredba CFGSYSSEC uključuje reviziju akcije i objekta i također, specificira defaultni skup akcija koje treba revidirati naredbom CHGSECAUD.

Prilagodba programa

Ako neke od ovih postavki nisu prikladne za vašu instalaciju, možete kreirati vašu vlastitu verziju programa koja obrađuje naredbu. Učinite sljedeće:

__ Korak 1. Koristite naredbu Dohvat CL izvora (RTVCLSRC) da kopirate izvor za program koji se izvodi kada koristite naredbu CFGSYSSEC. Program za učitavanje je QSYS/QSECCFGS. Kada ga učitate, dajte mu *različito ime* .

__ Korak 2. Napravite vaše promjene u programu. Tada ga prevedite. Kada ga prevodite, uvjerite se da *ne* zamijenite IBM dobavljen QSYS/QSECCFGS program. Vaš program treba imati različito ime.

__ Korak 3. Koristite naredbu Promjena naredbe (CHGCMD) da promijenite parametar programa za obradu naredbe (PGM) za naredbu CFGSYSSEC. Postavite PGM vrijednost na ime vašeg programa. Na primjer, za kreiranje programa u QGPL knjižnici koja se zove MYSECCFG, upisujete sljedeće:

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

Bilješka: Ako promijenite QSYS/QSECCFGS program, IBM ne može jamčiti ili potvrditi pouzdanost, upotrebljivost, izvedbu ili funkcije programa. Posredna jamstva za prođu na tržištu i sposobnosti za određenu svrhu se izričito poriču.

Funkcije naredbe Opoziv javnog ovlaštenja

Možete koristiti naredbu Opoziv javnog ovlaštenja (RVKPUBAUT) da postavite javno ovlaštenje na *EXCLUDE za skup naredbi i programa. Naredba RVKPUBAUT izvodi program koji se zove QSYS/QSECRVKP. Program se dostavlja tako da opoziva javno ovlaštenje (postavljajući javno ovlaštenje na *EXCLUDE) za naredbe koje su popisane u Tablica 11 i sučelja aplikativnog programiranja (API-je) koji su popisani u Tablica 12. Kada vaš sistem dođe, ove naredbe i API-ji imaju njihovo javno ovlaštenje postavljeno na *USE.

Naredbe koje su popisane uTablica 11 i API-ji koji su popisani u Tablica 12 svi izvode funkcije na vašem sistemu koje mogu pružiti priliku za zlonamjerne akcije. Kao sigurnosni administrator, trebate izričito ovlastiti korisnike da izvode ove naredbe i programe, a ne da budu dostupni svim sistemskim korisnicima.

Kada izvodite naredbu RVKPUBAUT, specificirate knjižnicu koja sadrži naredbe. Default je QSYS knjižnica. Ako imate više od jednog nacionalnog jezika na vašem sistemu, trebate izvesti naredbu za svaku QSYSxxx knjižnicu.

Tablica 11. Naredbe čije javno ovlaštenje je postavljeno naredbom 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-ji u Tablica 12 su svi u QSYS knjižnici:

Tablica 12. Programi čije javno ovlaštenje je postavljeno naredbom RVKPUBAUT

QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

Kada izvodite naredbu RVKPUBAUT, sistem postavlja javno ovlaštenje za osnovni direktorij na *USE (osim ako već nije *USE ili manje)

Prilagodba programa

Ako neke od ovih postavki nisu prikladne za vašu instalaciju, možete kreirati vašu vlastitu verziju programa koja obrađuje naredbu. Napravite sljedeće:

__ Korak 1. Koristite naredbu Dohvat CL izvora (RTVCLSRC) da kopirate izvor za program koji se izvodi kada koristite naredbu RVKPUBAUT. Program koji treba učitati je QSYS/QSECRVKP. Kada ga učitate, dajte mu *različito ime* .

__ Korak 2. Napravite vaše promjene u programu. Tada ga prevedite. Kada ga prevodite, uvjerite se da *ne* zamijenite IBM dobavljen QSYS/QSECRVKP program. Vaš program treba imati različito ime.

__ Korak 3. Koristite naredbu Promjena naredbe (CHGCMD) da promijenite parametar programa za obradu naredbe (PGM) za naredbu RVKPUBAUT. Postavite PGM vrijednost na ime vašeg programa. Na primjer, za kreiranje programa u QGPL knjižnici koja se zove MYRVKPGM, upisujete sljedeće:

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

Bilješka: Ako promijenite QSYS/QSECRVKP program, IBM ne može jamčiti ili potvrditi pouzdanost, upotrebljivost, izvedbu ili funkcije programa. Posredna jamstva za prođu na tržištu i sposobnosti za određenu svrhu se izričito poriču.

Dio 2. Napredna iSeries sigurnost

© Autorska prava IBM Corp. 1996, 2004

Poglavlje 5. Zaštita informacijskih sredstava s objektnim ovlaštenjem

Izazov vas kao administratora sigurnosti je zaštita informacijskih sredstava vaše organizacije, bez ometanja korisnika na vašem sistemu. Trebate osigurati da korisnici imaju dovoljno ovlaštenja za obavljanje svojih poslova, a da im ne dozvolite pregledavanje cijelog sistema i obavljanje neovlaštenih promjena.

Sigurnosni savjet

Premalo ovlaštenje može biti dvosjekli mač. Korisnici katkada na ograničenja ovlaštenja reagiraju međusobnim dijeljenjem lozinki.

OS/400 operativni sistem omogućuje integriranu objektnu sigurnost. Korisnici moraju koristiti sučelja koja sistem omogućuje za pristup objektima. Na primjer, ako želite pristupiti datoteci baze podataka, morate koristiti naredbe ili programe koji namijenjeni pristupu datotekama baza podataka. Ne možete koristiti naredbu koja je namijenjena pristupu reda poruka ili dnevniku posla.

Kad god koristite sučelje sistema za pristup objektu, sistem provjerava da li imate ovlaštenje za objekt koje je traženo od tog sučelja. Objektno ovlaštenje je moćan i fleksibilan alat za zaštitu sredstava na vašem sistemu. Vaš izazov kao administratora sigurnosti je postavljanje učinkovite sheme objektne sigurnosti s kojom možete upravljati i održavati ju.

Forsiranje objektnog ovlaštenja

Kad god pokušate pristupiti objektu, operativni sistem provjerava vaše ovlaštenje za taj objekt. Međutim, ako je razina sigurnosti na vašem sistemu (QSECURITY sistemska vrijednost) postavljena na 10 ili 20, svaki korisnik automatski ima ovlaštenje pristupa svakom objektu, jer svaki korisnički profil ima *ALLOBJ posebno ovlaštenje.

Savjet za objektno ovlaštenje: Ako niste sigurni da li koristite objektnu sigurnost, provjerite sistemsku vrijednost QSECURITY (razina sigurnosti). Ako je QSECURITY 10 ili 20, vi ne koristite objektnu sigurnost.

Morate planirati i pripremiti razinu sigurnosti 30 ili višu. Inače, vaši korisnici neće moći pristupati potrebnim informacijama.

Osnovna sigurnost sistema i planiranje poglavlje u Informacijski Centar omogućuje metode za analiziranje vaših aplikacija i odlučivanje kako postaviti objektnu sigurnost. Ako još ne koristite objektnu sigurnost ili ako je vaša shema objektne sigurnost zastarjela ili kompliciranа, pročitajte ovo poglavlje kao početnu pomoć.

Sigurnost izbornika

iSeries poslužitelj je originalno oblikovan kao proizvod koji nasljeđuje S/36 i S/38. Mnoge instalacije iSeries poslužitelja, u to vrijeme, bile su S/36 ili S/38 instalacije. Za kontrolu što su korisnici mogli raditi, administratori sigurnosti na tim ranijim sistemima su često koristili tehniku koja se naziva **sigurnost izbornika** ili **kontrola pristupa izborniku**.

© Autorska prava IBM Corp. 1996, 2004

Kontrola pristupa izborniku znači da kad se korisnik prijavljuje, korisnik vidi izbornik. Korisnik može izvoditi samo funkcije koje su na tom izborniku. Korisnik ne može doći do reda za naredbe na sistemu da obavlja ikakve funkcije koje nisu na izborniku. Teoretski, administrator se sigurnosti ne mora brinuti o ovlaštenjima za objekte jer izbornici i programi kontroliraju što korisnici mogu raditi.

iSeries poslužitelj omogućuje nekoliko opcija korisničkog profila za pomoć pri kontroli pristupa izborniku:
- **Početni izbornik** (INLMNU) parametar za kontrolu koji izbornik korisnik vidi prvi nakon prijave.
- **Početni program** (INLPGM) parametar za izvođenje programa postavljanja prije no što korisnik vidi izbornik. Ili, možete koristiti INLPGM parametar da ograničite korisnika na izvođenje pojedinačnog programa.
- **Ograničene sposobnosti** (LMTCPB) parametar za ograničavanje korisnika na ograničen skup naredbi. On također spriječava korisniku specificiranje drugog početnog programa ili izbornika na ekranu Prijave. (LMTCPB parametar samo ograničava naredbe koje su upisane iz reda za naredbe.)

Ograničenja kontrole pristupa izborniku

Računalni korisnici su se prilično promijenili u nekoliko zadnjih godina. Dostupni su mnogi alati, kao što su programi za upite i tablični kalkulatori, tako da korisnici mogu obaviti nešto vlastitog programiranja i rasteretiti IS odjele. Neki alati, kao što su SQL ili ODBC, omogućavaju sposobnost gledanja informacija i promjene informacija. Omogućavanje ovih alata unutar strukture izbornika vrlo je teško.

Radne stanice s fiksnim funkcijama ("zeleni ekran") rapidno se zamjenjuju osobnim računalima i mrežama računalo-računalo. Ako vaš sistem sudjeluje u mreži, korisnici mogu prodrijeti u vaš sistem bez da ikad vide ekran ili izbornik prijave.

Kao administrator sigurnosti koji pokušava forsirati kontrolu pristupa izbornika, imate dva osnovna problema:
- Ako ste uspješni u ograničavanju korisnika na izbornike, vaši korisnici će vjerojatno biti nezadovoljni, jer će im mogućnost upotrebe modernih alata biti ograničena.
- Ako niste uspješni, možete ugroziti kritične, povjerljive informacije koje kontrola pristupa izborniku treba zaštititi. Kad vaš sistem sudjeluje u mreži, vaša sposobnost forsiranja kontrole pristupa izborniku se smanjuje. Na primjer, LMTCPB parametar se primjenjuje samo na naredbe koje su upisane iz reda za naredbe u interaktivnoj sesiji. LMTCPB parametar nema utjecaja na zahtjeve od komunikacijskih sesija, kao što je PC prijenos datoteka, FTP ili udaljene naredbe.

Poboljšanje kontrole pristupa izborniku s objektnom sigurnosti

S mnogim novim opcijama koje su dostupne za povezivanje na sisteme, upotrebljiva shema sigurnosti iSeries poslužitelja, u budućnosti se ne može pouzdati samo na kontrolu pristupa izborniku. Ovo poglavlje daje prijedloge za prelazak na okruženje objektne sigurnosti za dopunu vašoj kontroli pristupa izborniku.

Poglavlje *Osnovna sigurnost sistema i planiranje* u Informacijskom Centru opisuje tehnike za analizu ovlaštenja koja korisnici moraju imati za objekte da bi izvodili vaše trenutne aplikacije. Trebate dodijeliti korisnike grupama i dati grupama prikladno ovlaštenje. Ovaj je pristup prihvatljiv i logičan. Međutim, ako vaš sistem radi već mnogo godina i ima mnogo aplikacija, zadatak analize aplikacija i uspostavljanja objektnog ovlaštenja se vjerojatno čini preteškim.

Savjet za objektno ovlaštenje: Vaši trenutni izbornici kombinirani s programima koji prihvaćaju ovlaštenja vlasnika programa može omogućiti prijelaz iznad kontrole pristupa izbornika. Osigurajte zaštitu i programa koji prihvaćaju ovlaštenje i korisničkih profila koji ih posjeduju.

Možete koristiti trenutne izbornike za pomoć pri postavljanju prijelazne okoline dok vi postupno analizirate vaše aplikacije i objekte. Slijedi primjer koji koristi izbornik Unos poretka (OEMENU) i pridružene datoteke i programe.

Primjer: Uspostavljanje prijelazne okoline

Ovaj primjer počinje sa sljedećim pretpostavkama i zahtjevima:

- Sve datoteke su u knjižnici ORDERLIB.
- Vi ne znate imena svih datoteka. Vi također ne znate koja su ovlaštenja potrebna opcijama izbornika za različite datoteke.
- Izbornik i svi programi koje on poziva nalaze se u knjižnici ORDERPGM.
- Želite da svatko tko se može prijaviti na vaš sistem može gledati informacije u svim datotekama narudžbi, datotekama korisnika i datotekama stavki (s upitima ili tabličnim kalkulatorima, na primjer).
- Samo korisnici čiji trenutni izbornik za prijavu je OEMENU trebaju imati mogućnost mijenjanja datoteka. Oni moraju koristiti programe u izborniku da to izvedu.
- Korisnici sistema, osim administratora sigurnosti, nemaju *ALLOBJ ili *SECADM posebno ovlaštenje.

Izvedite sljedeće korake da promijenite ovo okruženje kontrole pristupa izborniku, da zadovoljite potrebe za upite:

__ Korak 1. Napravite listu korisnika čiji je početni izbornik OEMENU.

Možete koristiti naredbu Ispis korisničkog profila (PRTUSRPRF *ENVINFO) za ispis okruženja za svaki korisnički profil na vašem sistemu. Izvještaj uključuje početni izbornik, početni program i trenutnu knjižnicu. Slika 7 na stranici 55 pokazuje primjer izvještaja.

__ Korak 2. Osigurajte da je OEMENU objekt (to može biti *PGM objekt ili *MENU objekt) posjedovan od korisničkog profila koji nije korišten za prijavu. Korisnički profil treba biti onemogućen ili imati lozinku *NONE. Za ovaj primjer, pretpostavimo da OEOWNER posjeduje OEMENU programski objekt.

__ Korak 3. Osigurajte da korisnički profil koji posjeduje OEMENU programski objekt nije profil grupe. Možete koristiti sljedeću naredbu:

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

__ Korak 4. Promijenite OEMENU program tako da prihvaća ovlaštenje OEOWNER korisničkog profila. (Koristite CHGPGM naredbu da promijenite USRPRF parametar na *OWNER.)

Bilješka: *MENU objekti ne mogu prihvatiti ovlaštenje. Ako je OEMENU *MENU objekt, možete prilagoditi ovaj primjer radeći nešto od sljedećeg:

- Kreirajte program za prikaz izbornika.
- Koristite usvojeno ovlaštenje za programe koji se izvode kad korisnik bira opcije iz OEMENU izbornika.

__ Korak 5. Postavite javno ovlaštenje za sve datoteke u ORDERLIB na *USE upisivanjem sljedeće dvije naredbe:

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

Zapamtite da ukoliko izaberete *USE ovlaštenje, korisnici mogu kopirati datoteku upotrebom PC prijenosa datoteke ili FTP-a.

__ Korak 6. Dajte profilu koji posjeduje program izbornika *ALL ovlaštenje za datoteke upisivanjem sljedećeg:

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

Za većinu aplikacija, dovoljno je *CHANGE ovlaštenje za datoteke. Međutim, vaše aplikacije mogu obavljati funkcije, kao što je brisanje fizičkih članova datoteka, koje trebaju ovlaštenje veće od *CHANGE. Konačno, trebate analizirati vaše aplikacije i dati samo minimum ovlaštenja koja su potrebna za aplikaciju. Međutim, za vrijeme prijelaznog razdoblja, prihvaćanjem *ALL ovlaštenja, izbjegavate aplikacijske greške koje mogu biti uzrokovane nedovoljnim ovlaštenjem.

__ Korak 7. Ograničite ovlaštenje za programe u knjižnici poretka upisivanjem sljedećeg:

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

__ Korak 8. Dajte OEOWNER profilu ovlaštenje za programe u knjižnici upisivanjem sljedećeg:

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

__ Korak 9. Dajte korisnicima koje ste identificirali u koraku 1 ovlaštenje za program izbornika upisivanjem sljedećeg za svakog korisnika:

```
GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM)
     USER(user-profile-name) AUT(*USE)
```

Kad ste dovršili ove korake, svi sistemski korisnici koji nisu izričito isključeni će moći pristupiti (ali ne mijenjati) datotekama u ORDERLIB knjižnici. Korisnici koji imaju ovlaštenje za OEMENU program će moći koristiti programe koji su na izborniku, da ažuriraju datoteke u ORDERLIB knjižnici. Samo korisnici koji imaju ovlaštenje za OEMENU program će sad moći mijenjati datoteke u ovoj knjižnici. Kombinacija objektne sigurnosti i kontrole pristupa izborniku štiti datoteke.

Kad dovršite slične korake za sve knjižnice koje sadržavaju korisničke podatke, kreirali ste jednostavnu shemu za kontrolu ažuriranja baza podataka. Ova metoda spriječava korisnike sistema da ažuriraju datoteke baze podatke osim kad koriste dozvoljene izbornike i programe. Istovremeno, napravili ste datoteke baze podataka dostupnim za gledanje, analizu i kopiranje za korisnike s alatima podrške-odluke ili s vezama iz drugog sistema ili iz PC-a.

Savjet za objektno ovlaštenje: Kad vaš sistem sudjeluje u mreži, *USE ovlaštenje može omogućiti više ovlaštenja nego što očekujete. Na primjer, s FTP-om, možete napraviti kopiju datoteke na drugom sistemu (uključujući PC) ako imate *USE ovlaštenje za datoteku.

Upotreba sigurnosti knjižnice za nadopunu sigurnosti izbornika

Za pristup objektu u knjižnici, morate imati ovlaštenje i za objekt i za knjižnicu. Većina operacija treba ili *EXECUTE ovlaštenje ili *USE ovlaštenje za knjižnicu.

Ovisno o situaciji, možete koristiti ovlaštenje knjižnice kao jednostavan način osiguravanja objekata. Na primjer, pretpostavimo da za primjer izbornika Unosa-narudžbe, svatko tko ima ovlaštenje za izbornik Unosa narudžbe može koristiti sve programe u ORDERPGM knjižnici.

Umjesto da osiguravate pojedinačne programe, možete postaviti javno ovlaštenje za ORDERPGM knjižnicu na *EXCLUDE. Tad možete dodijeliti *USE ovlaštenje za knjižnicu određenim korisničkim profilima, što će im dozvoliti upotrebu programa u knjižnici. (Ovo pretpostavlja da je javno ovlaštenje za programe *USE ili veće.)

Ovlaštenje za knjižnicu može biti jednostavan, djelotvoran način administriranja objektnog ovlaštenja. Međutim, morate osigurati da ste upoznati sa sadržajima knjižnica koje osiguravate tako da ne dajete nenamjeravan pristup objektima.

Konfiguriranje vlasništva objekta

Vlasništvo objekata na vašem sistemu važan je dio vaše sheme objektnog ovlaštenja. Po defaultu, vlasnik objekta ima *ALL ovlaštenje za objekt. Poglavlje 5 u *Uputa iSeries sigurnosti* knjizi daje preporuke i primjere za planiranje objektnog vlasništva. Slijedi nekoliko savjeta:

- Općenito, grupni profili ne trebaju posjedovati objekte. Ako grupni profil posjeduje objekt, svi članovi grupe imaju *ALL ovlaštenje za objekte osim ako član grupe nije izričito isključen.
- Ako koristite usvojeno ovlaštenje, razmotrite da li korisnički profili koji posjeduju programe također trebaju posjedovati aplikacijske objekte, kao što su datoteke. Možda ne želite da korisnici koji izvode programe koji usvajaju ovlaštenje imaju *ALL ovlaštenje za datoteke.

Ako koristite iSeries Navigator, ovo se može postići dovršenjem promjena upotrebom funkcije sigurnosnih **politika**. Za još informacija, pogledajte iSeries Informacijski Centar (pogledajte “Preduvjeti i povezane informacije” na stranici xii za detalje).

Objektno ovlaštenje za sistemske naredbe i programe

Slijedi nekoliko prijedloga kad ograničavate ovlaštenje za IBM dobavljene objekte:

- Kad na vašem sistemu imate više od jednog nacionalnog jezika, vaš sistem ima više od jedne sistemske (QSYS) knjižnice. Vaš sistem ima QSYSxxxx knjižnicu za svaki nacionalni jezik na vašem sistemu. Ako koristite objektno ovlaštenje za kontrolu pristupa sistemskim naredbama, imajte na umu osiguravanja naredbe u QSYS knjižnici i svakoj QSYSxxx knjižnici na vašem sistemu.
- System/38 knjižnica katkada omogućuje naredbu s funkcijom koja je ekvivalentna naredbama koje želite ograničiti. Osigurajte da ste ograničili ekvivalentnu naredbu u QSYS38 knjižnici.
- Ako imate System/36 okruženje, možda trebate ograničiti dodatne programe. Na primjer, QY2FTML program omogućuje System/36 prijenos datoteke.

Funkcije revizije sigurnosti

Ovo poglavlje opisuje tehnike za reviziju učinkovitosti sigurnosti na vašem sistemu. Ljudi revidiraju svoju sistemsku sigurnost iz nekoliko razloga:

- Da procijene da li je sigurnosni plan potpun.
- Da se osiguraju da su planirane sigurnosne kontrole na mjestu i da rade. Ovaj tip revizije uobičajeno obavlja službenik sigurnosti kao dio dnevne administracije sigurnosti. Također se obavlja, katkada mnogo detaljnije, kao dio periodičkog pregleda sigurnosti od internih ili vanjskih nadzornika.
- Da se osigura da sistemska sigurnost drži takt s promjenama u sistemskom okruženju. Neki primjeri promjena koje utječu na sigurnost su:
  - Novi objekti kreirani od sistemskih korisnika

- Novi korisnici prihvaćeni u sistem
- Promjena vlasništva objekta (autorizacija nije prilagođena)
- Promjena odgovornosti (promijenjena grupa korisnika)
- Privremeno ovlaštenje (nije vremenski opozvano)
- Novoinstalirani proizvodi

• Da se pripremite za budući događaj, kao što je instaliranje nove aplikacije, prelazak na višu sigurnosnu razinu ili uspostava komunikacijske mreže.

Tehnike opisane u ovom poglavlju prikladne su za sve ove situacije. Što revidirate i kako često ovisi o veličini i sigurnosnim potrebama vaše organizacije. Svrha ovog poglavlja je da raspravlja koje informacije su dostupne, kako ih dobiti i zašto su potrebne, a ne davanje uputa za učestalost revizija.

Ove informacije imaju tri dijela:

• Kontrolna lista sigurnosnih stavki koje se mogu planirati i revidirati.
• Informacije o postavljanju i upotrebi dnevnika revizije danog od sistema.
• Druge dostupne tehnike za skupljanje sigurnosnih informacija o sistemu.

Revizija sigurnosti uključuje upotrebu naredbi na iSeries sistemu i pristup informacijama zapisa i dnevnika na sistemu. Možete kreirati poseban profil koji će koristiti netko tko će obavljati reviziju sigurnosti vašeg sistema. Profil revizora će trebati *AUDIT posebno ovlaštenje da bi mogao mijenjati osobine revizije vašeg sistema. Neki od zadataka revizije predloženih u ovom poglavlju trebaju korisnički profil s *ALLOBJ i *SECADM posebnim ovlaštenjem. Osigurajte da ste postavili lozinku za profil revizora na *NONE kad završi razdoblje revizije.

Za više detalja o reviziji sigurnosti pogledajte Poglavlje 9, knjige *Upute za sigurnost*.

Analiza korisničkih profila

Možete prikazati ili ispisati potpunu listu svih korisnika na vašem sistemu s naredbom Prikaz ovlaštenih korisnika (DSPAUTUSR). Redoslijed liste može biti po imenu profila ili imenu profila grupe. Slijedi primjer redoslijeda po profilu grupe:

```
                          Prikaz ovlaštenih korisnika

                       Lozinka
Grupni      Korisnički Zadnje    Nema
Profil      Profil     Promij.   Lozinke  Tekst
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       Prodaja i marketing
            DPTWH      08/13/0x    X       Skladište
            RICHARDS   09/05/0x            Janet Richards
            SMITHJ     09/18/0x            John Smith
```

Ispis izabranih korisničkih profila

Možete koristiti naredbu Prikaz korisničkog profila (DSPUSRPRF) da kreirate izlaznu datoteku, koju možete obrađivati upotrebom alata za upite.

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

Možete koristiti alat za upite da kreirate raznolike izvještaje analiza vaše izlazne datoteke, kao što su:

- Popis svih korisnika koji imaju i *ALLOBJ i *SPLCTL posebna ovlaštenja.
- Popis svih korisnika uređen po polju korisničkog profila, kao što je početni program ili korisnička klasa.

Možete kreirati programe za upite da proizvedete različite izvještaje iz vaše izlazne datoteke. Na primjer:

- Ispišite sve korisničke profile koji imaju bilo kakvo posebno ovlaštenje izabiranjem slogova u kojima polje UPSPAU nije jednako *NONE.
- Ispišite sve korisnike koji mogu upisivati naredbe izborom slogova u kojima je polje *Ograničenje mogućnosti* (koje se zove UPLTCP u izlaznoj datoteci modela baze podataka) jednako *NO ili *PARTIAL.
- Ispišite sve korisnike koji imaju određeni početni izbornik ili početni program.
- Ispišite neaktivne korisnike gledanjem u polje datuma zadnje prijave.

Ispitivanje velikih korisničkih profila

Korisnički profili s velikim brojem ovlaštenja, koji izgledaju kao da su bez pravila raspršeni preko najvećeg dijela sistema, mogu odražavati nedostatak planiranja sigurnosti. Slijedi jedan način lociranja velikih korisničkih profila i njihove procijene:

1. Koristite naredbu Prikaz opisa objekta (DSPOBJD) za kreiranje izlazne datoteke koja sadržava informacije o svim korisničkim profilima u sistemu:

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

2. Kreirajte program za upite da ispišete ime i veličinu svakog korisničkog profila, u silaznom redoslijedu po veličini.
3. Ispišite detaljne informacije o najvećem korisničkom profilu i procijenite ovlaštenja i objekte koje posjeduje da provjerite njihovu prikladnost:

   ```
   DSPUSRPRF USRPRF(korisnik-profil-ime) +
             TYPE(*OBJAUT) OUTPUT(*PRINT)
   DSPUSRPRF USRPRF(korisnik-profil-ime) +
             TYPE(*OBJOWN) OUTPUT(*PRINT)
   ```

   Neki IBM dobavljeni korisnički profili su vrlo veliki zbog broja objekata koje posjeduju. Njihovo listanje i analiza obično nisu potrebni. Međutim, trebali bi provjeriti programe koji usvajaju ovlaštenje od IBM dobavljenih korisničkih profila koji imaju *ALLOBJ posebno ovlaštenje, kao što su QSECOFR i QSYS.

Za više detalja o reviziji sigurnosti pogledajte Poglavlje 9, knjige *Upute za sigurnost*.

Analiza objektnih ovlaštenja

Možete koristiti sljedeću metodu da odredite tko ima ovlaštenje za knjižnice u sistemu:

1. Koristite naredbu DSPOBJD za ispis svih knjižnica u sistemu:

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

   Bilješka: Knjižnice u nezavisnim pomoćnim spremištima memorije koji nisu u stanju AVAILABLE neće biti prikazani ovom naredbom.

2. Koristite naredbu Prikaz objektnog ovlaštenja (DSPOBJAUT)za ispis ovlaštenja za određenu knjižnicu:

   ```
   DSPOBJAUT OBJ(QSYS/ime-knjižnice) OBJTYPE(*LIB) +
             ASPDEV(asp-ime-uređaja) OUTPUT(*PRINT)
   ```

3. Koristite naredbu Prikaz knjižnice (DSPLIB) za ispis objekata u knjižnici:

   ```
   DSPLIB LIB(QSYS/ime-knjižnice) ASPDEV(asp-ime-uređaja) OUTPUT(*PRINT)
   ```

Upotrebom ovih izvještaja, možete odrediti što se nalazi u knjižnici i tko ima pristup knjižnici. Ako je potrebno, također možete koristiti naredbu DSPOBJAUT da vidite ovlaštenja za izabrane objekte u knjižnici.

Provjera promijenjenih objekata

Možete koristiti naredbu Provjera integriteta objekta (CHKOBJITG) da bi pronašli objekte koji su mijenjani. Mijenjani objekt je obično znak da netko pokušava raditi neovlaštene promjene na vašem sistemu. Možda bi trebali izvesti ovu naredbu nakon što je netko:

- Vratio programe na vaš sistem
- Koristio Namjenske servisne alate (DST)

Kad izvedete naredbu, sistem kreira datoteku baze podataka koja sadržava informacije o bilo kakvim potencijalnim problemima integriteta. Možete provjeriti objekte koje posjeduje jedan profil, nekoliko različitih profila ili svi profili. Možete vidjeti kojim objektima je mijenjana domena. Također možete ponovo izračunati vrijednosti provjere valjanosti programa da nađete objekte tipa *PGM, *SRVPGM, *MODULE i *SQLPKG koji su mijenjani.

Izvođenje programa CHKOBJITG zahtijeva posebno ovlaštenje *AUDIT. Izvođenje naredbe može trajati dugo zbog pretraživanja i računanja koje obavlja. Trebali bi je izvoditi u vrijeme kad vaš sistem nije zauzet.

Bilješka: Profili koji posjeduju puno objekata s mnoštvom privatnih ovlaštenja mogu postati vrlo veliki. Veličina profila vlasnika utječe na performanse kod prikaza i rada s ovlaštenjima s posjedovanim objektima i kod spremanja ili vraćanja profila. Također se može utjecati na operacije sistema. Da spriječite utjecaj ili na performanse ili sistemske operacije, distribuirajte vlasništvo nad objektima na više profila. **Nemojte dodijeliti sve (ili skoro sve) objekte samo jednom vlasničkom profilu.**

Analiza programa koji usvajaju ovlaštenje

Programi koji usvajaju ovlaštenje korisnika s posebnim ovlaštenjem *ALLOBJ predstavljaju sigurnosno izlaganje. Za pronalazak i ispitivanje tih programa može se koristiti sljedeća metoda:

1. Za svakog korisnika s posebnim ovlaštenjem *ALLOBJ, koristite naredbu Prikaz programa koji usvajaju (DSPPGMADP) za ispis programa koji usvajaju korisničko ovlaštenje:

   ```
   DSPPGMADP USRPRF(ime-korisničkog-profila) +
             OUTPUT(*PRINT)
   ```

   Bilješka: Poglavlje “Ispis izabranih korisničkih profila” na stranici 45 pokazuje kako ispisati korisnike s *ALLOBJ ovlaštenjem.

2. Koristite naredbu DSPOBJAUT da odredite tko je ovlašten koristiti svaki program za usvajanje i koje je javno ovlaštenje za program:

   ```
   DSPOBJAUT OBJ(ime-knjižnice/ime-programa) +
             OBJTYPE(*PGM) ASPDEV(ime-knjižnice/ime-programa) +
             OUTPUT(*PRINT)
   ```

3. Pretražite izvorni kod i opis programa da procijenite:
   - Da li je korisnik programa spriječen u upotrebi nekih funkcija, kao što su upotreba reda za naredbe, dok se izvodi pod usvojenim profilom.
   - Da li program prihvaća minimalni razinu ovlaštenja potrebnu za namjeravanu funkciju. Aplikacije koje koriste grešku programa mogu biti oblikovane upotrebom istog vlasničkog profila za objekte i programe. Kad je ovlaštenje vlasnika programa usvojeno, korisnik ima *ALL ovlaštenje za aplikacijske objekte. U mnogim slučajevima, vlasnički profil ne treba nikakva posebna ovlaštenja.
4. Provjerite kad je program zadnji put promijenjen, upotrebom DSPOBJD naredbe:

```
DSPOBJD OBJ(ime-knjižnice/ime-programa) +
        OBJTYPE(*PGM) ASPDEV(ime-knjižnice/ime-programa) +
        DETAIL(*FULL)
```

Upravljanje dnevnikom revizija i primateljima dnevnika

Dnevnik revizije, QSYS/QAUDJRN, je namijenjen isključivo za reviziju sigurnosti. Objekte ne treba zapisivati u dnevnik revizije. Kontrola predavanja ne treba koristiti dnevnik revizije. Unose korisnika ne treba slati u ovaj dnevnik upotrebom naredbe Slanje unosa u dnevnik (SNDJRNE) ili API-ja Slanje unosa u dnevnik (QJOSJRNE).

Posebna zaštita zaključavanja se koristi za osiguravanje da sistem može pisati unose revizije u dnevnik revizije. Kad je revizija aktivna (QAUDCTL sistemska vrijednost nije *NONE), posao sistemskog arbitra (QSYSARB) zaključava QSYS/QAUDJRN dnevnik. Dok je revizija aktivna, ne možete obavljati određene operacije na dnevniku revizije, kao što su:

- DLTJRN naredba
- ENDJRNxxx naredba
- APYJRNCHG naredba
- RMVJRNCHG naredba
- DMPOBJ ili DMPSYSOBJ naredba
- Premještanje dnevnika
- Vraćanje dnevnika
- Operacije koje rade s ovlaštenjima, kao što je naredba GRTOBJAUT
- WRKJRN naredba

Informacije zapisane u unosima dnevnika sigurnosti, opisane su u knjizi *Upute za sigurnost*. Svi sigurnosni unosi u dnevnik revizije imaju kod dnevnika T. Dodatno sigurnosnim unosima, sistemski unosi se također pojavljuju u dnevniku QAUDJRN. To su unosi s kodom dnevnika J, koji se odnose na punjenje početnog programa (IPL) i općenite operacije obavljene na primateljima dnevnika (npr. spremanje primatelja).

Ako se desi oštećenje dnevnika ili njegovog trenutnog primatelja, tako da se unosi revizije ne mogu zapisati u dnevnik, sistemska vrijednost QAUDENDACN određuje koju će akciju poduzeti sistem. Obnavljanje od oštećenja dnevnika ili primatelja dnevnika je isto kao i za sve druge dnevnike.

Možete željeti da sistem upravlja promjenom primalaca dnevnika. Specificirajte MNGRCV(*SYSTEM) kad kreirate dnevnik QAUDJRN ili promijenite dnevnik na tu vrijednost. Ako specificirate MNGRCV(*SYSTEM), sistem automatski odspaja primaoca kad dosegne svoju veličinu praga i kreira i dodaje novog primaoca dnevnika. To se zove **Sistemsko upravljanje promjene-dnevnika**. Pogledajte iSeries Informacijski Centar—>Upravljanje sistemom–> Upravljanje dnevnikom–>Lokalno upravljanje dnevnikom–>Upravljanje dnevnikom za više informacija. Pogledajte “Preduvjeti i povezane informacije” na stranici xii za informacije o pristupu iSeries Informacijskom Centru.

Poglavlje 6. Upravljanje ovlaštenjima

Dostupan je skup sigurnosnih izvještaja koji vam može pomoći u čuvanju traga o tome kako su ovlaštenja postavljena na vašem sistemu. Kada na početku pokrećete ove izvještaje, možete ispisati sve (ovlaštenje za sve datoteke ili za sve programa, na primjer).

Nakon što uspostavite vašu bazu informacija, možete redovito izvoditi promijenjene verzije izvještaja. Promijenjena verzija vam pomaže identificirati promjene važne za sigurnost na vašem sistemu koje trebaju vašu pažnju. Na primjer, možete izvoditi izvještaj koji svaki tjedan pokazuje javno ovlaštenje za datoteke. Možete zatražiti samo promijenjenu verziju izvještaja. Pokazat će vam i nove datoteke na sistemu koje su dostupne svima i postojeće datoteke čije je javno ovlaštenje promijenjeno od zadnjeg izvještaja.

Dostupna su dva izbornika za izvođenje sigurnosnih alata.

- Koristite SECTOOLS izbornik za interaktivno izvođenje programa.
- Koristite SECBATCH izbornik za batch izvođenje programa. SECBATCH izbornik ima dva dijela: jadan za submitiranje poslova odmah u red poslova i drugi za smještanje poslova u raspoređivač poslova.

Ako koristite iSeries Navigator, slijedite ove korake da izvedete sigurnosne alate.

1. U iSeries Navigatoru proširite vaš poslužitelj—>**Sigurnost**.
2. Desno kliknite **Politike** i izaberite **Istraživanje** da prikažete popis politika koje možete kreirati i kojima možete upravljati.

Nadgledanje javnog ovlaštenja objekata

Zbog jednostavnosti i performansi, većina sistema je tako postavljena da je većina objekata dostupna većini korisnika. Korisnicima se izričito zabranjuje pristup određenim povjerljivim, sigurnosno osjetljivim objektima, umjesto da moraju izričito biti ovlašteni za korištenje svakog objekta. Nekoliko sistema s visokim sigurnosnim zahtjevima koriste suprotan pristup i ovlašćuju objekte na osnovama koje je potrebno znati. U ovakvim sistemima, većina objekata se kreira s javnim ovlaštenjem postavljenim na *EXCLUDE.

iSeries je objektno baziran sistem s mnogo različitih tipova objekata. Većina tipova objekata ne sadrži osjetljive informacije ili ne izvodi funkcije važne za sigurnost. Kao sigurnosni administrator na iSeries sistemima s tipičnim sigurnosnim potrebama, vi vjerojatno želite fokusirati vašu pažnju na objekte koji zahtijevaju zaštitu, kao što su datoteke i programi baze podataka. Za ostale tipove podataka, možete samo postaviti ovlaštenje koje je dovoljno za vaše aplikacije, što je za većinu tipova objekata *USE ovlaštenje.

Možete koristiti naredbu Javno ovlaštenje (PRTPUBAUT) da ispišete informacije o objektima kojima javni korisnici mogu pristupiti. (**javni korisnik** je svatko s ovlaštenjem za prijavu tko nema izričito ovlaštenje za objekt.) Kada koristite naredbu PRTPUBAUT, možete specificirati tipove objekta i knjižnice i direktorije koje želite ispitati. Opcije su dostupne na izbornicima SECBATCH i SECTOOLS za ispis Izvještaja o javno ovlaštenim objektima za tipove objekata koji obično imaju sigurnosne implikacije. Možete redovito ispisati promijenjenu verziju ovog izvještaja da vidite koji objekti mogu zahtjevati vašu pažnju.

© Autorska prava IBM Corp. 1996, 2004

Upravljanje ovlaštenjem za nove objekte

OS/400 osigurava funkcije koje vam pomažu u upravljanju ovlaštenjima i vlasništvima za nove objekte na vašem sistemu. Kada korisnik kreira novi objekt, sistem određuje sljedeće:

- Tko će posjedovati objekt
- Koje je javno ovlaštenje za objekt
- Da li objekt ima bilo kakva privatna ovlaštenja
- Gdje staviti objekt (koja knjižnica ili direktorij)
- Da li će pristup objektu biti revidiran

Sistem koristi sistemske vrijednosti, parametre knjižnice i parametre korisničkog profila da donese ove odluke. “Dodjela ovlaštenja i vlasništva novim objektima ” u poglavlju 5 knjige *Uputa iSeries sigurnosti* osigurava nekoliko primjera o dostupnim opcijama.

Možete koristiti naredbu PRTUSRPRF da ispišete parametre korisničkog profila koji utječu na vlasništvo i ovlaštenje za nove objekte. Slika 5 na stranici 54 pokazuje primjer ovog izvještaja.

Nadgledanje autorizacijskih listi

Možete grupirati objekte sa sličnim sigurnosnim zahtjevima koristeći autorizacijsku listu. Konceptualno, autorizacijska lista sadrži listu korisnika i ovlaštenje koje korisnici imaju za objekte koje osigurava lista. Autorizacijske liste osiguravaju efikasan način upravljanja sličnim objektima u sistemu. Međutim, u nekim slučajevima otežavaju čuvanje traga ovlaštenja nad objektima.

Možete koristiti naredbu Privatno ovlaštenje (PRTPVTAUT) da ispišete informacije o ovlaštenjima autorizacijske liste. Slika 3 pokazuje primjer izvještaja.

```
                          Privatna ovlaštenja (Potpun izvještaj)
SYSTEM4
Autorizacija            Primaran                              Lista  ----------Objekt---------- ------------Podaci------------
Lista         Vlasnik   Grupa      Korisnik    Ovlaštenje     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
```

Slika 3. Izvještaj o privatnim ovlaštenjima za autorizacijske liste

Ovaj izvještaj pokazuje iste informacije koje vidite na ekranu Uređivanje autorizacijske liste (EDTAUTL). Prednost izvještaja je da omogućuje informacije o svim autorizacijskim listama na jednom mjestu. Ako postavljate sigurnost za novu grupu objekata, na primjer, možete brzo pretražiti izvještaj da vidite da li postojeća autorizacijska lista zadovoljava vaše potrebe za ove objekte.

Možete ispisati promijenjenu verziju izvještaja da vidite nove autorizacijske liste ili autorizacijske liste s promjenama ovlaštenja od zadnjeg ispisa izvještaja. Također imate mogućnost ispisa liste objekata koji su osigurani sa svakom autorizacijskom listom. Slika 4 na stranici 51 pokazuje primjer izvještaja za jednu autorizacijsku listu:

```
                    Prikaz objekata autorizacijske liste
Autorizacijska lista . . . . . :   CUSTAUTL
Knjižnica  . . . . . . . . . . :     QSYS
Vlasnik. . . . . . . . . . . . :   AROWNER
Primarna grupa . . . . . . . . :   *NONE

                                                        Primaran
Objekt         Knjižnica      Tip          Vlasnik      grupa          Tekst
CUSTMAS        CUSTLIB        *FILE        AROWNER      *NONE
CUSTORD        CUSTORD        *FILE        OEOWNER      *NONE
```

Slika 4. Prikaz izvještaja o objektima autorizacijske liste

Možete koristiti ovaj izvještaj, na primjer, da razumijete učinak dodavanja novog korisnika na autorizacijsku listu (koja ovlaštenja će dobiti taj korisnik).

Upotreba autorizacijskih listi

iSeries Navigator omogućava svojstva sigurnosti oblikovana da vam pomognu u razvoju sigurnosnog plana i politike i konfigurira vaš sistem da zadovolji potrebe vašeg poduzeća. Jedna od dostupnih funkcija je upotreba autorizacijskih listi.

Autorizacijske liste imaju sljedeća svojstva.
- Autorizacijska lista grupira objekte sa sličnim sigurnosnim zahtjevima.
- Autorizacijska lista konceptualno sadrži listu korisnika i grupa i ovlaštenje koje svaki ima za objekte koje osigurava lista.
- Svaki korisnik i grupa može imati različito ovlaštenje za skup objekata koje lista osigurava.
- Ovlaštenje može biti dano putem liste, umjesto pojedinačnim korisnicima i grupama.

Zadaci koji mogu biti napravljeni korištenjem autorizacijskih listi uključuju sljedeće.
- Kreiranje autorizacijske liste
- Promjena autorizacijske liste
- Dodavanje korisnika i grupa.
- Promjena dozvola korisnika.
- Prikaz osiguranih objekata.

Za upotrebu ovih funkcija, izvedite sljedeće korake:
1. Iz iSeries Navigatora, proširite vaš poslužitelj—>Sigurnost. Vidjet ćete **Autorizacijske liste** i **Politike**.
2. Desno kliknite **Autorizacijske liste** i izaberite **Nova autorizacijska lista**. **Nova autorizacijska lista** vam dozvoljava da napravite sljedeće.
   - **Upotreba:** Dozvoljava pristup atributima objekta i upotrebu objekta. Javnost može gledati, ali ne promijeniti objekte.
   - **Promjena:** Dozvoljava da sadržaji objekta (s nekim iznimkama) mogu biti promijenjeni.
   - **Sve:** Dozvoljava sve operacije na objektu, osim onih koje su ograničene na vlasnika. Korisnik ili grupa može kontrolirati postojanje objekta, specificirati sigurnost za objekta, promijeniti objekt i izvoditi osnovne funkcije na objektu. Korisnik ili grupa može također promijeniti vlasništvo objekta.
   - **Isključeno:** Sve operacije na objektu su zabranjene. Pristup ili operacije nisu dozvoljene na objektima za korisnike i grupe koje imaju ovu dozvolu. Specificira da javnosti nije dozvoljeno korištenje objekta.

Dok radite s autorizacijskim listama trebat ćete dodijeliti dozvole i za objekte i za podatke. Slijedi popis dozvola za objekte koje možete izabrati.

- **Operativna:** Osigurava dozvolu za gledanje opisa objekta i korištenje objekta kako je određeno podatkovnom dozvolom koju korisnik ili grupa ima za objekt.
- **Upravljanje:** Osigurava dozvolu za specifikaciju sigurnosti za objekt, premještanje ili preimenovanje objekta i dodaje članove datotekama baze podataka.
- **Postojanje:** Osigurava dozvolu za kontrolu postojanja i vlasništva objekta. Korisnik ili grupa može obrisati objekt, osloboditi memoriju objekta, izvoditi operacije spremanja i vraćanja za objekt i prenijeti vlasništvo objekta. Ako korisnik ili grupa ima posebnu dozvolu za spremanje, korisnik ili grupa ne treba dozvolu za postojanje objekta.
- **Promjena** (koristi se samo za datoteke baze podataka i SQL pakete): Osigurava dozvolu potrebnu za promjenu atributa objekta. Ako korisnik ili grupa ima ovu dozvolu za datoteku baze podataka, korisnik ili grupa može dodati ili ukloniti okidače, dodati ili ukloniti referentna ili jednoznačna ograničenja i promijeniti atribute datoteke baze podataka. Ako korisnik ili grupa ima ovu dozvolu za SQL paket, korisnik ili grupa može promijeniti atribute SQL paketa. Ova dozvola se trenutno koristi samo za datoteke baze podataka i SQL pakete.
- **Referenca** (koristi se samo za datoteke baze podataka i SQL pakete): Osigurava dozvolu potrebnu za referenciranje objekta iz drugog objekta takvo da operacije na tom objektu može ograničiti drugi objekt. Ako korisnik ili grupa ima ovu dozvolu za fizičku datoteku, korisnik ili grupa može dodati referentna ograničenja u kojima je fizička datoteka nadređena. Ova dozvola se trenutno koristi samo za datoteke baze podataka.

Slijedi popis dozvola za podatke koje možete izabrati.
- **Čitanje:** Osigurava dozvolu potrebnu za dobivanje i prikaz sadržaja objekta, kao što je gledanje zapisa u datoteci.
- **Dodavanje:** Osigurava dozvolu za dodavanje unosa objektu, kao što je dodavanje poruka u red poruka ili dodavanje zapisa u datoteku.
- **Ažuriranje:** Osigurava dozvolu za promjenu unosa u objektu, kao što je promjena zapisa u datoteci.
- **Brisanje:** Osigurava dozvolu za uklanjanje unosa iz objekta, kao što je uklanjanje poruka iz reda poruka ili brisanje zapisa iz datoteke.
- **Izvedba:** Osigurava dozvolu potrebnu za izvođenje programa, posluživanje programa ili SQL paketa. Korisnik može također locirati objekt u knjižnici ili direktoriju.

Za više informacija o svakom procesu u kreiranju ili uređivanju vaših autorizacijskih listi, koristite online pomoć dostupnu u iSeries Navigatoru.

Pristup politikama u iSeries Navigatoru

Možete koristiti iSeries Navigator za gledanje i upravljanje politikama za vaš iSeries poslužitelj. iSeries Navigator ima pet područja politika:

- **Revizijska politika**
  Ovo vam dozvoljava postavljenje nadgledanja za specifične akcije i pristup specifičnim resursima na vašem sistemu.
- **Sigurnosna politika**
  Ovo vam dozvoljava da specificirate razine sigurnosti i dodatne opcije koje se odnose na sistemsku sigurnost.
- **Politika lozinke**
  Ovo vam dozvoljava da specificirate razine lozinke za sistem.
- **Politika vraćanja**
  Ovo vam dozvoljava da specificirate kako su određeni objekti vraćeni u sistem.
- **Politika prijave**
  Ovo vam dozvoljava da specificirate kako se korisnik može prijaviti u sistem.

Da gledate ili promijenite politike s iSeries Navigatorom, slijedite ove korake:

1. Iz iSeries Navigatora, proširite vaš poslužitelj—>**Sigurnost.**.

2. Desno kliknite **Politike** i izaberite **Istraživanje** da prikažete popis politika koje možete kreirati i kojima možete upravljati. Pogledajte iSeries Navigator pomoć za specifičnosti ovih politika.

Nadgledanje privatnog ovlaštenja objekata

Opcije izbornika SECBATCH:
12 *za submit odmah* **41** *za korištenje raspoređivača poslova*

Možete koristiti naredbu Ispis privatnog ovlaštenja (PRTPVTAUT) da ispišete popis svih privatnih ovlaštenja za objekte specificiranog tipa u specificiranoj knjižnici.

Možete koristiti ovaj izvještaj kao pomoć u otkrivanju novih ovlaštenja za objekte. Može vam također pomoći da spriječite da vaša shema privatnih ovlaštenja postane komplicirana i neupotrebljiva.

Nadgledanje pristupa izlaznim redovima i redovima poslova

Ponekad administrator sigurnosti jako dobro zaštiti pristup datotekama, ali zaboravi što se dešava kada se ispisuje sadržaj datoteke. iSeries poslužitelji osiguravaju funkcije pomoću kojih možete zaštititi osjetljive izlazne redove i redove poslova. Trebate zaštititi izlazni red tako da neovlašteni korisnici ne mogu, na primjer, vidjeti ili kopirati povjerljive spool datoteke koje čekaju ispis. Trebate zaštititi i redove poslova tako da neovlašteni korisnik ne može niti preusmjeriti povjerljivi posao u nepovjerljivi izlazni red, niti potpuno opozvati posao.

Opcije izbornika SECBATCH:
24 za submit odmah 63 *za korištenje raspoređivača poslova*

Knjige *Osnovna sistemska sigurnost i planiranje* u Informacijskom Centru i *Uputa iSeries sigurnosti* opisuju kako da zaštitite vaše izlazne redove i redove poslova.

Možete koristiti naredbu Ispis ovlaštenja reda (PRTQAUT) da ispišete sigurnosne postavke za redove poslova i izlazne redove u vašem sistemu. Tada možete procijeniti poslove ispisa koji ispisuju povjerljive informacije i osigurati da idu u izlazne redove i redove poslova koji su zaštićeni.

Za izlazne redove i redove poslova koje smatrate sigurnosno osjetljivim, možete usporediti vaše sigurnosne postavke s informacijama u dodatku D knjige *Uputa iSeries sigurnosti*. Tablice u dodatku D pokazuju koje su postavke potrebne za izvođenje različitih funkcija izlaznog reda i reda poslova.

Nadgledanje posebnog ovlaštenja

Kada korisnik na vašem sistemu ima nepotrebna posebna ovlaštenja, vaša nastojanja da razvijete dobru shemu ovlaštenja objekata mogu biti izgubljena. Ovlaštenje objekta je bez značenja kada korisnički profil ima posebno ovlaštenje *ALLOBJ. Korisnik s posebnim ovlaštenjem *SPLCTL može vidjeti bilo koju spool datoteku u sistemu, bez obzira na trud koji uložite da osigurate vaše izlazne redove. Korisnik s posebnim ovlaštenjem *JOBCTL

može utjecati na sistemske operacije i preusmjeriti poslove. Korisnik s posebnim ovlaštenjem *SERVICE može koristiti servisne alate da pristupi podacima bez prolaska kroz operacijski sistem.

Opcije izbornika SECBATCH:
29 za submit odmah 68 *za korištenje raspoređivača poslova*

Možete koristiti naredbu Ispis korisničkog profila (PRTUSRPRF) da ispišete informacije o posebnim ovlaštenjima i korisničkim klasama za korisničke profile u vašem sistemu. Kada izvodite izvještaj, imate nekoliko opcija:
- Svi korisnički profili
- Korisnički profili sa specifičnim posebnim ovlaštenjima
- Korisnički profili koji imaju specifične korisničke klase
- Korisnički profili s nepodudarnostima između korisničke klase i posebnih ovlaštenja.

Slika 5 pokazuje primjer izvještaja koji pokazuje posebna ovlaštenja za sve korisničke profile:

```
                                    Informacije korisničkog profila
  Tip izvještaja . . . . . :   *AUTINFO
  Izabran od . . . . . :   *SPCAUT
  Posebna ovlaštenja  . . . . . :   *ALL
                   ------------Posebna ovlaštenja-------------
                               *IO                                                    Grupa
Korisnik  Grupa     *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  Korisnik            Grupa      Ovlaštenje  Ograničeno
Profil    Profili    OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  Klasa      Vlasnik  Ovlaštenje  Tip         Sposobnost
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
```

Slika 5. Izvještaj korisničke informacije: Primjer1

Kao dodatak posebnim ovlaštenjima, izvještaj pokazuje sljedeće:
- Da li korisnički profil ima ograničene sposobnosti.
- Da li korisnik ili grupa korisnika posjeduje objekte koje korisnik kreira.
- Koje ovlaštenje grupa korisnika automatski prima za nove objekte koje korisnik kreira.

Slika 6 pokazuje primjer izvještaja za nepodudarnosti posebnih ovlaštenja i korisničkih klasa:

```
Informacije korisničkog profila
Tip izvještaja . . . . . :   *AUTINFO
Izabran od . . . . . :   *MISMATCH
-------------------------------Posebna ovlaštenja-------------
                               *IO                                                    Grupa
Korisnik  Grupa     *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  Korisnik            Grupa      Ovlaštenje Ograničeno
Profil    Profili    OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  Klasa      Vlasnik  Ovlaštenje  Tip         Sposobnost
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
```

Slika 6. Izvještaj korisničke informacije: Primjer 2

Na Slika 6, obratite pažnju na sljedeće:
- USERX ima korisničku klasu (*SYSOPR) sistemskog operatera, ali ima posebna ovlaštenja *ALLOBJ i *SPLCTL.
- USERY ima korisničku klasu (*USER) korisnika, ali ima posebno ovlaštenje *SECADM.

- USERZ također ima korisničku klasu (*USER) i posebno ovlaštenje *SECADM. Možete također vidjeti da je USERZ član grupe QPGMR, koja ima posebna ovlaštenja *JOBCTL i *SAVSYS.

Možete redovito izvoditi ove izvještaje kao pomoć u nadgledanju administracije korisničkih profila.

Nadgledanje korisničkih okolina

Jedna od uloga korisničkog profila je definiranje okoline za korisnika, uključujući izlazni red, početni izbornik i opis posla. Okolina korisnika utječe kako korisnik vidi sistem i, do nekog stupnja, što korisnik smije raditi. Korisnik mora imati ovlaštenje za objekte koji su specificirani u korisničkom profilu. Međutim, ako je vaša shema ovlaštenja još uvijek u napredovanju ili nije jako ograničavajuća, korisnička okolina koja je definirana u korisničkom profilu može proizvesti rezultate koje niste htjeli. Slijedi nekoliko primjera:

Opcije izbornika SECBATCH:

29 *za submit odmah* **68** *za korištenje raspoređivača poslova*

- Opis posla korisnika može specificirati korisnički profil koji ima više ovlaštenja nego korisnik.
- Korisnik može imati početni izbornik koji nema red za naredbe. Međutim, korisnički program rukovanja tipkom Attention može omogućiti red za naredbe.
- Korisnik može biti ovlašten za izvođenje povjerljivih izvještaja. Međutim, korisnički izlaz može biti usmjeren na izlazni red koji je dostupan korisnicima koji ne trebaju vidjeti izvještaje.

Možete koristiti opciju *ENVINFO naredbe Ispis korisničkog profila (PRTUSRPRF) da vam pomogne nadgledati okoline koje su definirali sistemski korisnici. Slika 7 pokazuje primjer izvještaja:

```
                                    Informacije korisničkog profila
  Tip izvještaja . . . . . :   *ENVINFO
  Izabran od . . . . . :   *USRCLS
                          Početan        Početan          Posao        Poruka        Izlaz          Pažnja
Korisnik       Trenutan     Izbornik/        Program/       Opis/         Red/   Red/          Program/
Profil         Knjižnica      Knjižnica      Knjižnica      Knjižnica      Knjižnica      Knjižnica      Knjižnica
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
```

Slika 7. Primjer ispisa okoline-korisnika profila-korisnika

Upravljanje servisnim alatima

Servisni alati se koriste za konfiguriranje, upravljanje i servisiranje vaših poslužitelja. Servisnim alatima se može pristupiti iz Namjenskih servisnih alata (DST) ili Sistemskih servisnih alata (SST). Korisnički ID-ovi servisnih alata su potrebni za pristup DST-u, SST-u i za korištenje funkcija iSeries Navigatora za upravljanje logičkim particijama (LPAR) i upravljanje diskovnom jedinicom.

DST je dostupan kada je pokrenut Licencni interni kod, čak i ako OS/400 još nije učitan. SST je dostupan iz OS/400. Sljedeća tablica pokazuje osnovne razlike između DST-a i SST-a.

Osobine	DST	SST
Kako pristupiti	Fizički pristup kroz konzolu za vrijeme ručnog IPL-a ili selektirajući opciju 21 u kontrolnom panelu.	Pristup kroz interaktivan posao sa sposobnosti za prijavu s QSRV-om ili sljedećim ovlaštenjima: • Ovlašten za CL naredbu STRSST (Pokretanje SST-a). • Posebno ovlaštenja servisa (*SERVICE) ili posebno ovlaštenje svih objekata (*ALLOBJ). • Funkcionalna povlastica za korištenje SST-a.
Kad je dostupan	Dostupan čak i kad poslužitelj ima ograničene sposobnosti. OS/400 nije potreban za pristup DST-u.	Dostupan kad je OS/400 pokrenut. OS/400 je potreban za pristup SST-u.
Kako provjeriti autentičnost	Treba korisnički ID i lozinku servisnih alata.	Treba korisnički ID i lozinku servisnih alata.

Pogledajte iSeries Informacijski Centar —>Sigurnost—>Servisni alati za informacije o korištenju Servisnih alata da izvedete sljedeće zadatke:

- Pristup servisnim alatima s DST-om
- Pristup servisnim alatima sa SST-om
- Pristup servisnim alatima s iSeries Navigatorom
- Kreiranje korisničkog ID-a servisnih alata
- Promjena funkcionalnih povlastica za korisnički ID servisnih alata
- Promjena opisa za korisnički ID servisnih alata
- Prikaz korisničkog ID-a servisnih alata
- Omogućavanje i onemogućavanje korisničkog ID-a servisnih alata
- Brisanje korisničkog ID-a servisnih alata
- Promjena korisničkih ID-a servisnih alata i lozinki pomoću SST ili DST
- Promjena lozinke korisničkog ID-a vaših servisnih alata pomoću STRSST
- Promjena korisničkih ID-a i lozinki servisnih alata pomoću
- API Promjena korisničkog ID-a servisnih alata (QSYCHGDS)
- Ponovo postavljanje QSECOFR OS/400 lozinke korisničkog profila
- Ponovo postavljanje QSECOFR korisničkog ID-a i lozinke servisnih alata
- Spremanje sigurnosnih podataka servisnih alata Vraćanje sigurnosnih podataka servisnih alata
- Kreiranje vaše vlastite verzije QSECOFR korisničkog ID-a servisnih alata
- Konfiguriranje poslužitelja servisnih alata za DST
- Konfiguriranje poslužitelja servisnih alata za OS/400
- Nadgledanje upotrebe servisnih funkcija pomoću DST-a
- Nadgledanje upotrebe servisnih alata pomoću OS/400 sigurnosnog dnevnika revizije

Pogledajte “Preduvjeti i povezane informacije” na stranici xii za informacije o pristupu iSeries Informacijskom Centru.

Poglavlje 7. Upotreba sigurnosti logičkih particija (LPAR)

Posjedovanje višestrukih logičkih particija na jednom iSeries poslužitelju može se pokazati korisnim u sljedećim scenarijima.

- **Održavanje nezavisnih sistema**: Namjenom dijela resursa (jedinica disk memorije, procesora, memorije i I/O uređaja) za particiju postiže se logička izolacija softvera. Logičke particije, ako su ispravno konfigurirane također posjeduju određenu hardversku toleranciju grešaka. Interaktivna i paketna radna opterećenja, koja se možda ne izvode dobro na jednom stroju, mogu biti izolirana i djelotvorno se izvoditi na odijeljenim particijama.
- **Konsolidiranje** : Logički particioniran sistem može smanjiti broj iSeries poslužiteljskih sistema koji su potrebni u poduzeću. Možete konsolidirati nekoliko sistema u jedan logički particionirani sistem. To eliminira potrebu i trošak za dodatnu opremu. Po potrebi možete seliti resurse iz jedne logičke particije na drugu.
- **Kreiranje miješane okoline za proizvodnju i testiranje:** Možete kreirati kombiniranu okolinu za proizvodnju i za testiranje. Možete kreirati pojedinačnu particiju za proizvodnju u primarnoj particiji. Za višestruke particije za proizvodnju, pogledajte dolje *Kreiranje okruženja višestrukih particija za proizvodnju*.

  Logička particija je ili testna ili proizvodna particija. Particija za proizvodnju izvodi vaše glavne poslovne aplikacije. Greška u particiji za proizvodnju može značajno kočiti poslovne operacije i koštati vas vremena i novaca. Testna particija provjerava softver. Greška u testnoj particiji, koja nije nužno planirana, neće ometati normalne poslovne operacije.
- **Kreiranje okruženja višestruke particije za proizvodnju:** Višestruke particije za proizvodnju bi trebali kreirati samo u vašim sekundarnim particijama. U toj situaciji, primarnoj particiji namjenjujete upravljanje particijama.
- **Vruća sigurnosna kopija:** Kad se sekundarna particija replicira u drugu logičku particiju u istom sistemu, prebacivanje na sigurnosnu kopiju za vrijeme kvara particije bi uzrokovalo minimalne smetnje. Ova konfiguracija također smanjuje učinak dugog prozora za spremanje. Možete staviti rezervnu particiju u offline i spremiti je, dok druga logička particija nastavlja izvoditi proizvodni posao. Trebati ćete poseban softver da bi koristili ovu strategiju vrućeg sigurnosnog kopiranja.
- **Integrirani klaster:** Uz upotrebu OptiConnect/400 i aplikacijskog softvera visoke dostupnosti, vaš particionirani sistem može raditi kao integrirani klaster. Možete koristiti integrirani klaster da zaštitite vaš sistem od većine neraspoređenih grešaka unutar sekundarne particije.

Bilješka: Pri postavljanju sekundarne particije, treba se dodatno razmotriti smještaj kartica. Ukoliko Ulazno/Izlazni procesor (IOP) koji ste izabrali za konzolu također ima LAN karticu, a LAN kartica se ne može koristiti s Operacijskom konzolom, konzola će ga aktivirati za upotrebu, a vi ga nećete moći koristiti za namjeravanu svrhu. Za više informacija o radu s Operacijskom konzolom, pogledajte Poglavlje 8, “iSeries Operacijska konzola”, na stranici 59.

Pogledajte ″Logičke particije″ u Informacijskom Centru za detaljnije informacije o ovom poglavlju.

© Autorska prava IBM Corp. 1996, 2004

Upravljanje sigurnošću za logičke particije

Zadaci, koji se odnose na sigurnost, koje izvodite na particioniranim sistemima su isti kao na sistemu bez logičkih particija. Međutim, kad kreirate logičke particije, radite s više nezavisnih sistema. Stoga ćete iste zadatke morati obavljati na svakoj logičkoj particiji za razliku od samo jedanput na sistemu bez logičkih particija.

Evo nekoliko osnovnih pravila koje treba zapamtiti kad se bavite sigurnošću na logičkim particijama:

- Korisnike dodajete sistemu samo jednoj particiji u jednom trenutku. Trebate dodati korisnike svakoj logičkoj particiji kojoj želite da oni pristupaju.
- Ograničite broj ljudi koji imaju ovlaštenje pristupa Namjenskim servisnim alatima (DST) i Sistemskim servisnim alatima (SST) u primarnoj particiji. Pogledajte poglavlje ″Upravljanje logičkim particijama korištenjem iSeries Navigatora, DST i SST″ u iSeries Informacijski Centar kako bi dobili više informacija o DST i SST. Pogledajte “Upravljanje servisnim alatima” na stranici 55 za informacije o upotrebi korisničkih profila servisnih alata za kontrolu pristupa aktivnostima particije.

  Bilješka: Morate incijalizirati poslužitelj Servisnih alata (STS) prije korištenja iSeries Navigatora za pristup LPAR funkcijama. PogledajteiSeries Informacijski Centar—>Sigurnost—>Servisni alati za odgovarajuće informacije. Pogledajte “Preduvjeti i povezane informacije” na stranici xii za informacije o pristupu iSeries Informacijskom Centru.
- Sekundarne particije ne mogu vidjeti ili koristiti glavnu memoriju i disk jedinice druge logičke particije.
- Sekundarne particije jedino mogu vidjeti svoje vlastite resurse hardvera.
- Primarna particija može vidjeti sve sistemske resurse hardvera u ekranima Rad sa sistemskim particijama DST-a i SST-a.
- Primarna particija operacijskog sistema ipak vidi samo svoje dostupne resurse.
- Kontrolni panel sistema kontrolira primarnu particiju. Kad postavite način na panelu na Siguran, nikakve akcije se ne mogu izvesti u ekranu Rad sa stanjem particije iz SST-a. Da forsirate DST iz sistemskog kontrolnog panela, morate promijeniti način u Ručno.
- Kad postavite operacijski način sekundarne particije na Siguran, ograničavate upotrebu Rada sa stanjem particije na sljedeći način:
  - Možete koristiti samo DST na sekundarnoj particiji za promjenu stanja particije; ne možete koristiti SST za promjenu stanja particije.
  - DST na sekundarnoj particiji možete forsirati samo iz ekrana primarne particije Rad sa stanjem particije upotrebom ili DST-a ili SST-a.
  - DST možete koristiti na primarnoj particiji samo za promjenu načina sekundarne particije iz sigurnog na bilo koju drugu vrijednost.

Kad način sekundarne particije više nije Siguran, možete koristiti i DST i SST na sekundarnoj particiji za promjenu stanja particije.

Za više informacija o sigurnosti na vašem iSeries poslužitelju, pogledajte knjigu Upute za sigurnost, Osnovna sistemska sigurnost i stranice za planiranje od iSeries Informacijski Centar.

Poglavlje 8. iSeries Operacijska konzola

Operacijska konzola dozvoljava vam da koristite vaš PC za pristup i kontrolu vašeg iSeries poslužitelja. Operacijska konzola uključuje podršku za pozivanje iSeries poslužitelja s udaljenog PC-a, bez uređaja konzole, dozvoljavajući udaljenim PC-ima da postanu konzole. Kad koristite Operacijsku konzolu imajte na umu sljedeće:

- Možete obaviti bilo koji zadatak koji ste mogli i iz tradicionalne konzole s Operacijskom konzolom. Na primjer, korisnički profili koji imaju *SERVICE ili *ALLOBJ posebno ovlaštenje mogu se prijaviti na sesiju Operacijske konzole, čak i ako su onemogućeni.
- Operacijska konzola koristi Korisničke profile i lozinke servisnih alata da omogući povezivanje na iSeries poslužitelj. Ovo čini naročito važnim promjenu vaših Korisničkih profila i lozinki servisnih alata. Hakeri su vjerojatno upoznati s defaultnim korisničkim ID-ovima i lozinkama Korisničkih profila servisnih alata i mogli bi ih koristiti za pokušaj udaljene sesije konzole na vašem iSeries poslužitelju. Pogledajte “Promjena poznatih lozinki” na stranici 18 i “Izbjegavanje defaultnih lozinki” na stranici 23 za savjete za lozinke.
- Da zaštitite vaše informacije kad koristite Udaljenu konzolu, koristite opciju poziva natrag od Windows Dial-Up networkinga.
- Pri postavljanju sekundarne particije, treba se dodatno razmotriti smještaj kartica. Ako Ulazno/Izlazni procesor (IOP) koji ste izabrali za konzolu također ima LAN karticu, a LAN kartica se ne može koristiti s Operacijskom konzolom, konzola će ga aktivirati za upotrebu, a vi ga nećete moći koristiti za namjeravane svrhe.

U V5R1, Operacijska konzola je poboljšana da omogući da se aktivnosti konzole izvode preko Mreže lokalnog područja (LAN). Poboljšana provjera autentičnosti i šifriranje podataka daje mrežnu sigurnost za procedure konzole. Za upotrebu Operacijske konzole s LAN povezanosti preporuča se da instalirate sljedeće proizvode:

- Dobavljač kriptografičkog pristupa, 5722–AC2 ili 5722–AC3 na vaš iSeries poslužitelj
- Šifriranje klijenta, 5722–CE2 ili 5722–CE3 na vaš PC Operacijske konzole

Da bi podaci konzole bili šifrirani, iSeries poslužitelj mora imati instaliran jedan od proizvoda Dobavljača kriptografičkog pristupa **i** PC mora imati instaliran jedan od proizvoda Šifriranja klijenta.

Bilješka: Ako nikakvi kriptografski proizvodi nisu instalirani, neće biti nikakvog šifriranja podataka.

Sljedeća tablica sumira rezultate šifriranja dostupnih proizvoda:

Tablica 13. Rezultati šifriranja

Dobavljač kriptografskog pristupa na vašem iSeries poslužitelju	**Šifriranje klijenta na vašem Operacijska konzola PC-ju**	**Rezultirajuće šifriranje podataka**
Ništa	Ništa	Ništa
5722–AC2	5722–CE2	56 bit
5722–AC2	5722–CE3	56 bit
5722–AC3	5722–CE2	56 bit
5722–AC3	5722–CE3	128 bit

© Autorska prava IBM Corp. 1996, 2004

Za dodatne informacije o postavljanju i administriranju iSeries Operacijske konzole pogledajte iSeries Informacijski Centar.

Pregled sigurnosti Operacijske konzole

Sigurnost Operacijske konzole se sastoji od:

- provjere autentičnosti uređaja konzole
- provjere autentičnosti korisnika
- privatnosti podataka
- integriteta podataka

Operacijska konzola s izravnom povezanosti ima uključenu provjeru autentičnosti uređaja, privatnosti podataka i integriteta podataka zbog svog point-to-point povezivanja. Sigurnost provjere autentičnosti korisnika je potrebna za prijavu na ekran konzole.

Provjera autentičnosti uređaja konzole

Provjera autentičnosti uređaja konzole osigurava koji fizički uređaj je konzola. Operacijska konzola s izravnom povezanosti koristi fizičko povezivanje slično twinax konzoli. Operacijska konzola koja koristi izravno povezivanje može biti fizički osigurana slično kao i twinax povezivanje za kontrolu pristupa na fizički uređaj konzole.

Operacijska konzola s LAN povezanosti koristi verziju sloja sigurnih utičnica (SSL) koji podržava provjeru autentičnosti uređaja i korisnika, ali bez upotrebe certifikata. Za ovaj oblik povezivanja, provjera autentičnosti uređaja je bazirana na profilu uređaja servisnih alata. Pogledajte 61 za još detalja.

Provjera autentičnosti korisnika

Provjera autentičnosti korisnika daje osiguranje o onome tko koristi uređaj konzole. Sva pitanja koja se odnose na provjeru autentičnosti korisnika ista su bez obzira na tip konzole.

Privatnost podataka

Privatnost podataka daje osiguranje da podatke konzole može čitati samo namjeravani primalac. Operacijska konzola s izravnom povezanosti koristi fizičko povezivanje slično twinax konzoli ili sigurno mrežno povezivanje za LAN povezivanje za zaštitu podataka konzole. Operacijska konzola koja koristi izravno povezivanje ima istu privatnost podataka kao i twinax veza. Ako je fizička veza sigurna, podaci konzole ostaju zaštićeni.

Operacijska konzola s LAN povezanosti koristi povezivanje sigurne mreže ako su instalirani prikladni kriptografski proizvodi (ACx i CEx). Sesija konzole koristi najjače moguće šifriranje ovisno o kriptografskim proizvodima instaliranim na iSeries poslužitelju i PC-ju koji izvodi Operacijsku konzolu.

Bilješka: Ako nikakvi kriptografski proizvodi nisu instalirani, neće biti nikakvog šifriranja podataka.

Integritet podataka

Integritet podataka daje sigurnost da podaci konzole nisu promijenjeni na putu do primatelja. Operacijska konzola s izravnom povezanosti koristi fizičko povezivanje slično twinax konzoli ili povezivanje sigurne mreže za LAN povezivanje za zaštitu podataka konzole. Operacijska konzola koja koristi izravnu vezu ima isti integritet podataka kao i twinax veza. Ako je fizička veza sigurna, podaci konzole ostaju zaštićeni.

Operacijska konzola s LAN povezanosti koristi povezivanje sigurne mreže ako su instalirani prikladni kriptografski proizvodi (ACx i CEx). Sesija konzole koristi najjače moguće šifriranje ovisno o kriptografičkim proizvodima instaliranim na iSeries poslužitelju i PC-u koji izvodi Operacijsku konzolu.

Bilješka: Ako nikakvi kriptografički proizvodi nisu instalirani, neće biti nikakvog šifriranja podataka.

Upotreba Operacijske konzole s LAN povezanosti

Bilješka: Bilo koji uređaj Operacijske konzole može biti konzola, ali samo LAN-bazirane konfiguracije koriste korisnički profil servisnih alata.

iSeries poslužitelj se otprema s defaultnim profilom uređaja servisnih alata QCONSOLE, s defaultnom lozinkom QCONSOLE. Operacijska konzola s LAN povezanosti će promijeniti lozinku za vrijeme svakog uspješnog povezivanja. Pogledajte "Upotreba čarobnjaka postavljanja Operacijske konzole" za još informacija.

Za dodatne informacije o iSeries Operacijskoj konzoli s LAN povezanosti, pogledajte poglavlje, Konfiguriranje Operacijske konzole s LAN povezanosti, u Informacijskom Centru.

Zaštita Operacijske konzole s LAN povezanosti

Kod upotrebe Operacijske konzole s LAN povezanosti, preporučuju se donje stavke:

- Kreirajte drugi profil uređaja servisnih alata s atributima konzole i pohranite informacije o profilu na sigurno mjesto.
- Instalirajte Dobavljača kriptografičkog pristupa, 5722–AC2 ili 5722–AC3 na vaš iSeries poslužitelj i Šifriranje klijenta, 5722–CE2 ili 5722–CE3 na vaš PC Operacijske konzole.
- Izaberite ne-trivijalnu lozinku informacija uređaja posluživanja.
- Zaštitite PC Operacijske konzole na isti način na koji bi zaštitili twinax konzolu ili Operacijsku konzolu s izravnom povezanosti.

Upotreba čarobnjaka postavljanja Operacijske konzole

Čarobnjak postavljanja će dodati potrebne informacije na PC kad koristite Operacijsku konzolu s LAN povezanosti. Čarobnjak postavljanja pita za profil uređaja servisnih alata, lozinku profila uređaja servisnih alata i lozinku za zaštitu informacija profila uređaja servisnih alata.

Bilješka: Lozinka informacija profila uređaja servisnih alata se koristi za zaključavanje i otključavanje informacija profila uređaja servisnih alata (profil uređaja servisnih alata i lozinka) na PC-u.

Kad uspostavljate mrežnu vezu, čarobnjak postavljanja Operacijske konzole će vam dati prompt za lozinku informacija servisnih uređaja za pristup šifriranom profilu uređaja servisnih alata i lozinci. Također ćete dobiti prompt za važeću korisničku identifikaciju i lozinku servisnih alata.

Poglavlje 9. Otkrivanje sumnjivih programa

Novi trendovi u upotrebi računala su povećali vjerojatnost da vaš sistem ima programe od nepovjerljivih izvora ili programe koji izvode nepoznate funkcije. Sljedeće su primjeri:

- Korisnik osobnog računala ponekad dobiva programe od drugih PC korisnika. Ako je PC pripojen vašem iSeries sistemu, taj program može utjecati na vaš iSeries poslužitelj.
- Korisnici koji se povezuju na mreže mogu također dobiti programe, na primjer iz oglasnih ploča.
- Hakeri su postali aktivniji i slavni. Oni često objavljuju svoje metode i rezultate. Ovo može dovesti do toga da ih i programeri koji poštuju zakon počnu imitirati.

Ovi trendovi su doveli do problema u računalnoj sigurnosti poznatog kao **računalni virus**. Virus je program koji može promijeniti druge programe tako da uključi svoju kopiju. Za druge programe se tad kaže da su zaraženi virusom. Dodatno, virus može izvoditi druge operacije koje mogu preuzeti resurse sistema ili uništiti podatke.

Arhitektura iSeries poslužitelja osigurava određenu zaštitu od zaraznih osobina računalnih virusa. “Zaštita od računalnih virusa” to opisuje. Administrator sigurnosti iSeries poslužitelja se treba više brinuti o programima koji izvode neovlaštene funkcije. Preostale teme u ovom poglavlju opisuju načine na koje netko s lošim namjerama može postaviti štetne programe da se izvode na vašem sistemu. Teme pružaju savjete za spriječavanje programa od izvođenja neovlaštenih funkcija.

Sigurnosni savjet

Ovlaštenje objekta je uvijek prva linija obrane. Ako nemate dobar plan za zaštitu vaših objekata, vaš sistem nije sposoban za obranu. Ove informacije raspravljaju načine koje ovlašteni korisnik može isprobati kako bi iskoristio rupe u zakonu u vašoj shemi za ovlaštenje objekta.

Zaštita od računalnih virusa

Računalo koje je zaraženo virusom ima program koji može promijeniti drugi program. Objektno bazirana arhitektura iSeriesa više otežava zlonamjernim osobama proizvodnju i širenje ovog tipa virusa, nego što je to slučaj kod nekih drugih računalnih arhitektura. Na iSeries poslužitelju, koristite specifične naredbe i upute za rad na svakom tipu objekta. Ne možete koristiti upute za datoteku da promijenite operabilni programski objekt (to je ono što većina kreatora virusa radi). Također, ne možete lako kreirati program koji mijenja drugi programski objekt. Da to napravite potrebno je znatno vrijeme, napor i stručnost i zahtijeva pristup alatima i dokumentaciji koji nisi općenito dostupni.

Međutim, kada nove funkcije iSeries poslužitelja postanu dostupne za sudjelovanje u okolinama otvorenih sistema, neke od objektno baziranih funkcija zaštite iSeries poslužitelja se ne mogu više primijeniti. Na primjer, s integriranim sistemom datoteka (IFS), korisnici mogu direktno rukovati nekim objektima u direktorijima, kao što su datoteke toka.

Također, iako arhitektura iSeries poslužitelja otežava virusima širenje kroz programe iSeries poslužitelja, njegova arhitektura ne spriječava iSeries poslužitelj da bude nosilac virusa. Kao poslužitelj datoteka, iSeries poslužitelj može spremiti programe koje mnogi PC korisnici

© Autorska prava IBM Corp. 1996, 2004

dijele. Bilo koji od ovih virusa može sadržavati virus koji iSeries poslužitelj ne otkriva. Da se spriječi da ovaj tip virusa zarazi PC-ove koji su pripojeni na vaš iSeries poslužitelj, morate koristiti softver za traženje virusa na PC-u.

Nekoliko funkcija postoji na iSeries poslužitelju za zaštitu od korištenja jezika niske razine koji mogu upotrebom pointera promijeniti operabilni objektni program:

- Ako vaš sistem radi na sigurnosnoj razini 40 ili višoj, zaštita integriteta uključuje zaštitu od promjene objekata programa. Na primjer, ne možete uspješno izvoditi program koji sadrži blokirane (zaštićene) instrukcije stroja.
- Vrijednost provjere valjanosti programa je također namijenjena za zaštitu kod vraćanja programa koji je spremljen (i možda promijenjen) na drugom sistemu. Poglavlje 2 u knjizi *Uputa iSeries sigurnosti* opisuje funkcije zaštite integriteta za sigurnosnu razinu 40 i više, uključujući vrijednosti provjere valjanosti programa.

  Bilješka: Vrijednost provjere valjanosti programa nije potpuni dokaz i nije zamjena za opreznost kod procjenjivanja programa koji su vraćeni na vaš sistem.

Dostupno je također nekoliko alata koji vam mogu pomoći otkriti uvođenje promijenjenih programa u vaš sistem:

- Možete koristiti naredbu Provjera integriteta objekta (CHKOBJITG) da pretražite objekte (operabilne objekte) koji zadovoljavaju vaše vrijednosti traženja radi osiguranja da ti objekti nisu mijenjani. Ovo je slično funkciji za traženje virusa.
- Možete koristiti revizijsku funkciju sigurnosti da nadgledate programe koji su promijenjeni ili vraćeni. Vrijednosti *PGMFAIL, *SAVRST i *SECURITY za sistemsku vrijednost razine ovlaštenja osiguravaju zapise revizije koji vam mogu pomoći da otkrijete pokušaje uvođenja programa tipa virus u vaš sistem. Poglavlje 9 i dodatak F u knjizi *Uputa iSeries sigurnosti* pružaju više informacija o vrijednostima revizije i unosima dnevnika revizije.
- Možete koristiti parametar forsiranja kreiranja (FRCCRT) u naredbi Promjena programa (CHGPGM) da ponovno kreirate bilo koji program koji je vraćen na vaš sistem. Sistem koristi predložak programa da ponovo kreira program. Ako je programski objekt promijenjen nakon što je preveden, sistem ponovo kreira promijenjeni program i zamjenjuje ga. Ako programski predložak sadrži blokirane (zaštićene) upute, sistem neće ponovo uspješno kreirati program.
- Možete koristiti sistemsku vrijednost QFRCCVNRST (forsiranje konverzije kod vraćanja) da ponovno kreirate bilo koji program vraćen na vaš sistem. Sistem koristi programski predložak da ponovo kreira program. Ova sistemska vrijednost omogućuje nekoliko izbora na kojim programima se treba ponovno kreirati.
- Možete koristiti sistemsku vrijednost QVFYOBJRST (provjera objekata kod vraćanja) da spriječite vraćanje programa koji nemaju digitalni potpis ili nemaju važeći digitalni potpis. Kada digitalni potpis nije važeći, to znači da je program mijenjan od kad ga je potpisao njegov razvijač. Postoje API-ji koji vam dozvoljavaju da potpišete vaše vlastite programe, spremite datoteke i datoteke toka.

Za više informacija o potpisivanju i kako se to može koristiti za zaštitu vašeg sistema od napada, pogledajte “Potpisivanje objekata” na stranici 74.

Nadgledanje upotrebe usvojenog ovlaštenja

Na iSeries poslužitelju možete kreirati program koji usvaja ovlaštenje vlasnika programa. Ovo znači da bilo koji korisnik koji izvodi program ima ista ovlaštenja (privatna ovlaštenja i posebna ovlaštenja) kao i korisnički profil koji posjeduje program.

Usvojeno ovlaštenje je vrijedan sigurnosni alat kada se koristi ispravno. “Poboljšanje kontrole pristupa izborniku s objektnom sigurnosti” na stranici 40, na primjer, opisuje kako

kombinirati usvojeno ovlaštenje i izbornike da vam pomognu proširiti se iza kontrole pristupa izbornika. Možete koristiti usvojeno ovlaštenje da zaštitite vaše važne datoteke od promjene izvan odobrenih dopuštenih aplikacijskih programa dok još uvijek dozvoljavate redove za datoteke.

Kao sigurnosni administrator, morate se uvjeriti da se usvojeno ovlaštenje koristi ispravno:

- Programi trebaju usvojiti ovlaštenje korisničkog profila koji ima jedino dovoljno ovlaštenja za potrebne funkcije, a ne pretjerano ovlaštenje. Trebate biti posebno oprezni s programima koji usvajaju ovlaštenje korisničkog profila koji ili ima posebno ovlaštenje *ALLOBJ ili posjeduje važne objekte.
- Programi koji usvajaju ovlaštenje trebaju imati specifične, ograničene funkcije i ne trebaju imati sposobnost unosa naredbe.
- Programi koji usvajaju ovlaštenje trebaju biti ispravno osigurani.
- Pretjerana upotreba usvojenog ovlaštenja može imati negativan utjecaj na vaše sistemske performanse. Za pomoć u izbjegavanju problema s performansama, pregledajte dijagrame toka o provjeri ovlaštenja i prijedloge za korištenje usvojenih ovlaštenja u poglavlju 5 knjige *Uputa iSeries sigurnosti*.

Opcije izbornika SECBATCH:
1 *za submit odmah* **40 za korištenje raspoređivača poslova**

Možete koristiti naredbu Ispis usvajajućih objekata (PRTADPOBJ) (opcija 21 u izborniku SECTOOLS) da vam pomogne nadgledati upotrebu usvojenih ovlaštenja na vašem sistemu.

Izvještaj prikazuje posebna ovlaštenja specificiranog korisničkog profila, programe koji usvajaju ovlaštenja korisničkih profila, kao i ASP uređaji koji koriste ovlaštenja profila. Nakon što ste uspostavili bazu informacija, možete redovito ispisivati promijenjene verzije izvještaja usvojenih objekata. Ispisuje nove programe koji usvajaju ovlaštenje i programe koji su promijenjeni da usvoje ovlaštenje od onda kad ste zadnji put izvodili izvještaj.

Ako sumnjate da se usvojeno ovlaštenje pogrešno koristi na vašem sistemu, možete postaviti sistemsku vrijednost QAUDLVL da uključuje *PGMADP. Kada je aktivna ova vrijednost, sistem kreira unos dnevnika revizije kad god netko pokreće ili završava program koji usvaja ovlaštenje. Unos uključuje ime korisnika koji je pokrenuo program i ime programa.

Ograničavanje upotrebe usvojenog ovlaštenja

Kada se iSeries program izvodi, program može koristiti usvojeno ovlaštenje kako bi dobio pristup objektima na dva različita načina:

- Sam program može usvojiti ovlaštenje njegovog vlasnika. Ovo se specificira u parametru korisničkog profila (USRPRF) programa ili servisnog programa.
- Program može koristiti (naslijediti) usvojeno ovlaštenje od prethodnog programa koji je još na stogu poziva poslova. Program može naslijediti programe usvojenog ovlaštenja od prethodnih programa čak i ako sam program ne usvaja ovlaštenje. Upotreba usvojenog ovlaštenja (USEADPAUT) parametar programa ili servisnog programa kontrolira da li program nasljeđuje usvojeno ovlaštenje od prethodnih programa na stogu programa.

Sljedeće je primjer kako koristiti usvojeno ovlaštenje od rada prethodnih programa.

Pretpostavite da ICOWNER korisnički profil ima *CHANGE ovlaštenje za ITEM datoteku i da je javno ovlaštenje za ITEM datoteku *USE. Niti jedan drugi korisnički profil nema

izričito definirano ovlaštenje za ITEM datoteku. Tablica 14 pokazuje atribute za tri programa koji koriste ITEM datoteku:

Tablica 14. Primjer Upotrebe usvojenog ovlaštenja (USEADPAUT)

Programsko ime	Programski vlasnik	USRPRF vrijednost	USEADPAUT vrijednost
PGMA	ICOWNER	*OWNER	*YES
PGMB	ICOWNER	*USER	*YES
PGMC	ICOWNER	*USER	*NO

Primjer 1–Usvajanje ovlaštenja
1. USERA izvodi PGMA program.
2. PGMA program pokušava otvoriti ITEM datoteku sa sposobnošću ažuriranja.

Rezultat: Pokušaj je uspješan. USERA ima *CHANGE pristup ITEM datoteci, jer PGMA usvaja ICOWNER ovlaštenje.

Primjer 2–Upotreba usvojenog ovlaštenja
1. USERA izvodi PGMA program.
2. PGMA program poziva PGMB program.
3. PGMB program pokušava otvoriti ITEM datoteku sa sposobnošću ažuriranja.

Rezultat: Pokušaj je uspješan. Iako PGMB program ne usvaja ovlaštenje (*USRPRF je *USER), on dozvoljava upotrebu prethodno usvojenog ovlaštenja (*USEADPAUT je *YES). PGMA program je još na stogu programa. Stoga, USERA dobiva *CHANGE pristup ITEM datoteci, jer PGMA usvaja ICOWNER ovlaštenje.

Primjer 3–Ne korištenje usvojenog ovlaštenja
1. USERA izvodi PGMA program.
2. PGMA program poziva PGMC program.
3. PGMC program pokušava otvoriti ITEM datoteku sa sposobnošću ažuriranja.

Rezultat: Greška ovlaštenja. PGMC program ne usvaja ovlaštenje. PGMC program također ne dozvoljava usvojeno ovlaštenje iz prethodnog programa. Iako je PGMA još na stogu poziva, njegovo usvojeno ovlaštenje nije korišteno.

Spriječavanje novih programa da koriste usvojeno ovlaštenje

Predavanje usvojenog ovlaštenja kasnijim programima na stogu omogućava priliku dobrom programeru da kreira program Trojanskog konja. Program Trojanski konj može se osloniti na prethodne programe u stogu za dobivanje ovlaštenja koje je potrebno za izvođenje zlog djela. Da spriječite ovo, možete ograničite kojim korisnicima je dozvoljeno kreiranje programa koji koriste usvojeno ovlaštenje iz prethodnih programa.

Kada kreirate novi program, sistem automatski postavlja parametar USEADPAUT na *YES. Ako ne želite da program naslijedi usvojeno ovlaštenje, morate koristiti naredbu Promjena programa (CHGPGM) ili Promjena servisnog programa (CHGSRVPGM) da postavite parametar USEADPAUT na *NO.

Možete koristiti autorizacijsku listu i sistemsku vrijednost usvojenog ovlaštenja (QUSEADPAUT) da kontrolirate tko može kreirati programe koji nasljeđuju usvojeno ovlaštenje. Kada specificirate ime autorizacijske liste u sistemskoj vrijednosti QUSEADPAUT, sistem koristi ovu autorizacijsku listu za određivanje kako kreirati nove programe.

Kada korisnik kreira program ili servisni program, sistem provjerava ovlaštenje korisnika na autorizacijskoj listi. Ako korisnik uma *USE ovlaštenje, parametar USEADPAUT za novi program je postavljen na *YES. Ako korisnik nema *USE ovlaštenje, parametar USEADPAUT je postavljen na *NO. Ovlaštenje korisnika na autorizacijskoj listi ne može doći od usvojenog ovlaštenja.

Autorizacijska lista koji specificirate u sistemskoj vrijednosti QUSEADPAUT također kontrolira da li korisnik koristi naredbu CHGxxx da postavi vrijednost USEADPAUT za program ili servisni program.

Bilješke:

1. Ne trebate pozivati vašu autorizacijsku listu QUESADPAUT. Možete kreirati listu ovlaštenja s različitim imenom. Tada specificirati tu autorizacijsku listu za sistemsku vrijednost QUSEADPAUT. U naredbama u ovom primjeru, zamijenite ime vaše autorizacijske liste.
2. Sistemska vrijednost QUSEADPAUT ne utječe na postojeće programe na vašem sistemu. Upotrebite naredbu CGHPGM ili CHGSRVPGM da postavite USEADPAUT parametar za postojeće programe.

Više ograničavajuća okolina: Ako želite da većina korisnika kreira nove programe s parametrom USEADPAUT postavljenim na *NO, učinite sljedeće:

1. Da postavite javno ovlaštenje za autorizacijsku listu na *EXCLUDE, upišite sljedeće:

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

2. Da postavite da specifični korisnici kreiraju programe koji koriste usvojeno ovlaštenje prethodnih programa, upišite sljedeće:

   ```
   ADDAUTLE AUTL(QUSEADPAUT) USER(korisničko-ime)
      AUT(*USE)
   ```

Manje ograničavajuća okolina: Ako želite da većina korisnika kreira nove programe s parametrom USEADPAUT postavljenim na *YES, učinite sljedeće:

1. Ostavite javno ovlaštenje za autorizacijsku listu postavljeno na *USE.
2. Da spriječite da specifični korisnici kreiraju programe koji koriste usvojeno ovlaštenje prethodnih programa, upišite sljedeće:

   ```
   ADDAUTLE AUTL(QUSEADPAUT)
      USER(korisničko-ime) AUT(*EXCLUDE)
   ```

Nadgledanje upotrebe programa okidača

DB2 UDB ima sposobnost pridruživanja programa okidača s datotekama baze podataka. Svojstvo programa okidača je zajedničko u industriji za visoko funkcionalne upravitelje baza podataka.

Kada pridružujete program okidača s datotekom baze podataka, specificirate kada se izvodi program okidača. Na primjer, možete postaviti datoteku narudžbi kupaca da izvodi program okidača kad god se novi slog doda u datoteku. Kad saldo korisnika premaši kreditni limit, program okidača može ispisati pismo upozorenja korisniku i poslati poruku nadležnom upravitelju.

Programi okidača su produktivan način i za omogućavanje aplikacijskih funkcija i za upravljanje informacijama. Programi okidača također omogućuju da netko s lošim namjerama kreira “Trojanskog konja” na vašem sistemu. Destruktivan program može sjediti i čekati da se izvede kad se određeni događaj dogodi u datoteci baze podataka na vašem sistemu.

Bilješka: U povijesti, Trojanski konj je bio veliki šuplji drveni konj koji je bio ispunjen s grčkim vojnicima. Nakon što je konj uveden unutar zidova Troje, vojnici su izašli iz konja i borili se s Trojancima. U računalnom svijetu, program koji sakriva destruktivne funkcije često se naziva Trojanskim konjem.

Opcije izbornika SECBATCH:
27 *za submit odmah* **66** *za korištenje raspoređivača poslova*

Kada se vaš sistem isporuči, sposobnost dodavanja programa okidača u datoteku baze podataka je ograničena. Ako pažljivo upravljate ovlaštenjem objekta, tipičan korisnik neće imati dovoljno ovlaštenje da doda program okidača u datoteku baze podataka. (Dodatak D u knjizi *Uputa iSeries sigurnosti* govori o ovlaštenjima koja su potrebna ili svim naredbama, uključujući naredbu Dodaj okidač fizičkoj datoteci (ADDPFTRG).

Možete koristiti naredbu Ispis programa okidača (PRTTRGPGM) da ispišete popis svih programa okidača u određenoj knjižnici ili u svim knjižnicama.

Možete koristiti početni izvještaj kao bazu za procjenjivanje bilo kojih programa okidača koji već postoje na vašem sistemu. Tada možete redovito ispisati promijenjeni izvještaj da vidite da li su novi programi okidača dodani na vaš sistem.

Kada procjenjujete programe okidača, razmotrite sljedeće:

- Tko je kreirao program okidača? Možete koristiti naredbu Prikaz opisa objekta (DSPOBJD) da odredite ovo.
- Što radi program? Morati ćete pogledati u izvorni program ili razgovarati s kreatorom programa da to odredite. Na primjer, da li program okidača provjerava da vidi tko je korisnik? Možda program okidača čeka određenog korisnika (QSECOFR) kako bi dobio pristup sistemskim resursima.

Nakon što ste uspostavili bazu informacija, možete redovito ispisivati promijenjeni izvještaj kako bi nadgledali nove programe okidača koji su dodani vašem sistemu.

Provjera skrivenih programa

Programi okidača nisu jedini moguć način za uvođenje Trojanskog konja u vaš sistem. Programi okidača su primjer **izlaznih programa**. Kada se određeni događaj desi, kao što je ažuriranje datoteke u slučaju programa okidača, sistem izvodi izlazni program koji je povezan s događajem.

Tablica 15 opisuje druge primjere izlaznih programa koji mogu biti u vašem sistem. Trebate koristiti iste metode za procjenjivanje upotrebe i sadržaja ovih izlaznih programa koje koristite za programe okidače.

Bilješka: Tablica 15 nije potpuna lista mogućih izlaznih programa.

.

Tablica 15. Sistemski-dobavljeni izlazni programi

Ime programa	Kada se program izvodi
Korisnički-specificirano ime na DDMACC mrežnim atributima.	Kada korisnik pokuša otvoriti DDM datoteku na vašem sistemu ili napravi DRDA povezivanje.
Korisnički-specificirano ime na PCSACC mrežnim atributima.	Kada pokuša koristiti funkcije Client Access koristeći originalne klijente za pristup objektima na vašem sistemu.

Tablica 15. Sistemski-dobavljeni izlazni programi (nastavak)

Ime programa	Kada se program izvodi
Korisnički-specificirano ime na QPWDVLDPGM sistemskoj vrijednosti	Kada korisnik izvodi funkciju Promijeni lozinku
Korisnički-specificirano ime na QRMTSIGN sistemskoj vrijednosti.	Kada se korisnik pokuša prijaviti interaktivno iz udaljenog sistema.
QSYS/QEZUSRCLNP	Kada se izvodi funkcija automatskog čišćenja.
Korisnički-specificirano ime na parametru EXITPGM naredbe CHGBCKUP.	Kada koristite backup funkcije Pomoćnika za operacije.
Korisnički-specificirana imena na naredbi CRTPRDLOD.	Prije i poslije nego što spremite, vratite ili brišete proizvod koji je kreiran naredbom.
Korisnički specificirano ime na parametru DFTPGM naredbe CHGMSGD.	Ako je specificiran defaultni program za poruku, sistem izvodi program kada je poruka izdana. Zbog velikog broja opisa poruka na tipičnom sistemu, upotreba defaultnih programa je teška za nadgledati. Da spriječite javne korisnike od dodavanja defaultnih programa za poruke, razmotrite postavljanje javnog ovlaštenja za datoteke poruka (*MSGF objekti) na *USE.
Korisnički specificirano ime na parametru FKEYPGM naredbe STREML3270.	Kada korisnik pritisne funkcijsku tipku za vrijeme 3270 sesije emulacije uređaja. Sistem vraća kontrolu na 3270 sesiju emulacije uređaja kada izlazni program završava.
Korisnički-specificirano ime na parametru EXITPGM naredbe Monitora performansi.	Za obradu podataka koji su skupljeni sljedećim naredbama: STRPFRMON, ENDPFRMON, ADDPFRCOL i CHGPFRCOL. Program se izvodi kada završi skupljanje podataka.
Korisnički-specificirano ime na parametru EXITPGM naredbe RCVJRNE.	Za svaki unos dnevnika ili grupu unosa dnevnika koju čita iz specificiranog dnevnika ili primalaca dnevnika.
Korisnički specificirano ime na QTNADDCR API.	Za vrijeme operacije COMMIT ili ROLLBACK.
Korisnički specificirana imena na QHFRGFS API.	Za izvođenje funkcija sistema datoteka.
Korisnički specificirano ime na parametru SEPPGM opisa uređaja pisača.	Za određivanje što ispisati na stranici odjelitelja prije ili poslije spool datoteke ili ispisa posla.
QGPL/QUSCLSXT	Kada je datoteka baze podataka zatvorena da dozvoli hvatanje informacija o upotrebi datoteke.
Korisnički specificirano ime na parametru FMTSLR logičke datoteke.	Kada je zapis napisan u datoteku baze podataka i ime formata zapisa nije uključeno u programski jezik visoke razine. Selektor programa prima zapis kao ulaz, određuje korišteni format zapisa i vraća ga bazi podataka.
_Korisnički specificirano ime koje je specificirano u sistemskoj vrijednosti QATNPGM, parametru ATNPGM u korisničkom profilu ili parametru PGM naredbe SETATNPGM.	Kada korisnik pritisne tipku attention.
Korisnički-specificirano ime na parametru EXITPGM naredbe TRCJOB.	Prije pokretanja procedure Praćenje posla.

Za naredbe koje vam dozvoljavaju specificiranje izlaznog programa, trebate osigurati da default naredbe nije promijenjen za specificiranje izlaznog programa. Također trebate osigurati da javno ovlaštenje za ove naredbe nije dovoljno za promjenu defaulta naredbe. Naredba CHGCMDDFT treba ovlaštenje *OBJMGT za naredbu. Vi ne trebate ovlaštenje *OBJMGT da izvedete naredbu.

Procjena registriranih izlaznih programa

Možete koristiti sistemsku registracijsku funkciju za registriranje izlaznih programa koji se trebaju izvoditi kada se dogodi određeni događaj. Da ispišete registracijske informacije na vašem sistemu, upišite WRKREGINF OUTPUT(*PRINT). Slika 8 pokazuje primjer izvještaja:

```
              Rad s informacijama registracije
Izlazna točka. . . . . . . . . . . . . :   QIBM_QGW_NJEOUTBOUND
Format izlazne točke . . . . . . . . . :   NJEO0100
Registrirana izlazna točka . . . . . . :   *YES
Dozvoli deregistraciju . . . . . . . . :   *YES
Maksimalan broj izlaznih programa. . . :   *NOMAX
Trenutni broj izlaznih programa. . . . :   0
Predobrađivanje za dodavanje . . . . . :   *NONE
  Knjižnica. . . . . . . . . . . . . . :
  Format . . . . . . . . . . . . . . . :
Predobrađivanje za uklanjanje. . . . . :   *NONE
  Knjižnica. . . . . . . . . . . . . . :
  Format . . . . . . . . . . . . . . . :
Predobrađivanje za dohvaćanje. . . . . :   *NONE
  Knjižnica. . . . . . . . . . . . . . :
```

Slika 8. Rad s informacijama registracije-Primjer

Za svaku točku u sistemu, izvještaj pokazuje da li su bilo koji izlazni programi trenutno registrirani. Kada izlazna točka ima programe koji su trenutno registrirani, možete izabrati opciju 8 (Prikaz programa) s verzije prikaza WRKREGINF da prikažete informacije o programima:

```
                     Rad s informacijama registracije

Upišite opcije, pritisnite Enter.
5=Prikaz točke izlaza  8=Rad s izlaznim programima

                          Izlaz
     Izlaz                Točka
Opt  Točka                Format    Registriran Tekst
     QIBM_QGW_NJEOUTBOUND NJEO0100     *YES     Unos mrežnog posla nadmašen skokom ex
8    QIBM_QHQ_DTAQ        DTAQ0100     *YES     Poslužitelj originalnog reda podataka
     QIBM_QLZP_LICENSE    LICM0100     *YES     Originalni licencni Mgmt poslužitelj
     QIBM_QMF_MESSAGE     MESS0100     *YES     Originalni poslužitelj poruka
     QIBM_QNPS_ENTRY      ENTR0100     *YES     Poslužitelj mrežnog ispisa - unos
     QIBM_QNPS_SPLF       SPLF0100     *YES     Poslužitelj mrežnog ispisa - spool
     QIBM_QNS_CRADDACT    ADDA0100     *YES     Dodaj CRQ aktivnost opisa
     QIBM_QNS_CRCHGACT    CHGA0100     *YES     Promijeni CRQ aktivnost opisa
```

Koristite istu metodu za procjenu izlaznih programa koju koristite za druge izlazne programe i programe okidača.

Provjera raspoređenih programa

iSeries pruža nekoliko metoda za raspoređivanje poslova da se izvode kasnije, uključujući raspoređivača poslova. Normalno, ove metode ne predstavljaju sigurnosno izlaganje, jer korisnik koji raspoređuje posao mora imati isto ovlaštenje koje je potrebno za slanje na izvođenje posla u batch.

Međutim, trebate povremeno provjeriti raspoređene poslove u budućnosti. Nezadovoljni korisnik koji više nije u organizaciji može koristiti ovu metodu da rasporedi katastrofu.

Sposobnost ograničavanja spremanja i vraćanja

Većina korisnika ne treba spremiti i vratiti objekte na vaš sistem. Naredba spremanja ima mogućnost kopiranja važnih sredstava vaše organizacije na medij ili na drugi sistem. Većina naredbi spremanja podržava datoteke za spremanje koje mogu biti poslane drugom sistemu (koristeći naredbu SNDNETF datoteka) bez da imaju pristup mediju ili spremi/vrati uređaju.

Naredbe vraćanja pružaju priliku za vraćanje neovlaštenih objekata, kao što su programi, naredbe i datoteke, vašem sistemu. Možete također vratiti informacije bez pristupa mediju ili spremi/vrati uređaju koristeći datoteke spremanja. Datoteke spremanja mogu biti poslane iz drugog sistema koristeći naredbu SNDNETF ili koristeći FTP funkcija.

Sljedeće su prijedlozi za ograničavanje operacija spremanja i vraćanja na vašem sistemu:

- Kontrolirajte koji korisnici imaju *SAVSYS posebno ovlaštenje. *SAVSYS posebno ovlaštenje dozvoljava korisniku spremanje i vraćanje objekata čak i kad korisnik nema potrebno ovlaštenje za objekte.
- Kontroliranje fizičkog pristupa za uređaje spremanja i vraćanja
- Ograničite pristup naredbama spremanja i vraćanja. Kada instalirate OS/400 licencne programe, javno ovlaštenje za naredbe RSTxxx je *EXCLUDE. Javno ovlaštenje za naredbe SAVxxx je *USE. Razmotrite promjenu javnog ovlaštenja za naredbe SAVxxx u *EXCLUDE. Pažljivo ograničite korisnike koje ovlašćujete za naredbe RSTxxx.
- Koristite sistemsku vrijednost QALWOBJRST da ograničite vraćanje programa sistemskog stanja, programa koji usvajaju ovlaštenje i objekata koji imaju greške provjere valjanosti.
- Koristite QVFYOBJRST sistemsku vrijednost za kontrolu vraćanja potpisanih objekata na vaš sistem .
- Upotrebite QFRCCVNRST sistemsku vrijednost za kontrolu ponovnog kreiranja određenih objekata koji se vraćaju na vaš sistem.
- Koristite reviziju sigurnosti za nadgledanje operacija vraćanja. Uključite *SAVRST u sistemskoj vrijednosti QAUDLVL i povremeno ispisujte zapise revizije koji su kreirani operacijama vraćanja. (Poglavlje 9 i Dodatak F knjige *Uputa iSeries sigurnosti* pružaju više informacija o operacijama unosa revizije.)

Provjera korisničkih objekata u zaštićenim knjižnicama

Svaki posao iSeries poslužitelja ima popis knjižnica. Popis knjižnica određuje redoslijed po kojem sistem traži objekte ako ime knjižnice nije specificirano s imenom objekta. Na primjer, kada pozivate program bez da specificirate gdje je program, sistem pretražuje vaš popis knjižnica po redu i izvodi prvu kopiju programa koju nađe.

Knjiga *Uputa iSeries sigurnosti* pruža više informacija o sigurnosnim izlaganjima popisa knjižnice i pozivanja programa bez imena knjižnice (nazvano **nekvalificiran poziv**). Također pruža prijedloge za kontroliranje sadržaja knjižnice i sposobnost promjene popisa sistemske knjižnice.

Da se vaš sistem izvodi ispravno, određene sistemske knjižnice, kao QSYS i QGPL, moraju biti na popisu knjižnica za svaki posao. Trebate koristiti ovlaštenje objekta za kontrolu tko može dodati programe ovim knjižnicama. Ovo pomaže spriječiti nekoga od smještanja varajućih programa u jednu od ovih knjižnica s istim imenom kao i program koji se kasnije pojavljuje na popisu knjižnice.

Također trebate procijeniti tko ima ovlaštenje za naredbu CHGSYSLIBL i nadgledanje SV zapisa u dnevniku sigurnosne revizije. Zlonamjerni korisnik može smjestiti knjižnicu ispred QSYS u popisu knjižnica i uzrokovati da drugi korisnici izvode neovlaštene naredbe s istim imenima kao i IBM-dobavljene naredbe.

Opcije izbornika SECBATCH:
28 *za submit odmah* **67** *za korištenje raspoređivača poslova*

Možete koristiti naredbu Ispis korisničkih objekata (PRTUSROBJ) da ispišete popis korisničkih objekata (objekte nije kreirao IBM) koji su u specificiranoj knjižnici. Tada možete procijeniti programe na popisu da odredite tko ih je kreirao i koje funkcije izvode.

Korisnički objekti koji nisu programi mogu također predstavljati sigurnosno izlaganje kada su u sistemskim knjižnicama. Na primjer, ako program piše povjerljive podatke u datoteku čije ime nije kvalificirano, taj program može otvoriti krivu verziju programa u sistemskoj knjižnici.

Poglavlje 10. Spriječavanje i otkrivanje hakerskih pokušaja

Ove su informacije zbirka mješovitih savjeta za pomoć pri otkrivanju mogućih ekspozicija sigurnosti i onih koji čine nepodopštine.

Fizička sigurnost

Jedinica vašeg sistema predstavlja važno poslovno sredstvo i potencijalna vrata u vaš sistem. Neke sistemske komponente unutar sistema su malene, ali vrijedne. Trebate smjestiti sistemsku jedinicu u kontroliranu lokaciju da spriječite nekoga da ukloni vrijedne sistemske komponente.

Sistemska jedinica ima kontrolni panel koji omogućuje obavljanje osnovnih funkcija bez radne stanice. Na primjer, kontrolni panel možete koristiti za:

- Zaustavljanje sistema.
- Pokretanje sistema.
- Učitavanje operativnog sistema.
- Pokretanje funkcija servisa.

Sve ove aktivnosti mogu zasmetati rad korisnika vašeg sistema. One također predstavljaju potencijalno izlaganje sigurnosti vašeg sistema. Možete koristiti blokiranje ključa koje dolazi s vašim sistemom za kontrolu kad su ove aktivnosti dozvoljene. Da spriječite upotrebu kontrolnog panela, postavite blokiranje ključa u položaj Siguran, uklonite ključ i spremite ga na sigurno mjesto.

Bilješke:

1. Ako trebate izvoditi udaljene IPL-ove da bi obavili udaljeno dijagnosticiranje na vašem sistemu, možda ćete trebati izabrati drugačije postavljanje ključa. Poglavlje Kako započeti u Informacijskom Centru daje više informacija o postavkama blokiranja ključa (pogledajte “Preduvjeti i povezane informacije” na stranici xii za detalje).
2. Ne dolaze svi sistemski modeli s blokiranjem ključa kao standardnim svojstvom.

Nadgledanje aktivnosti korisničkog profila

Korisnički profili omogućuju ulaz u vaš sistem. Parametri u korisničkom profilu određuju okruženje korisnika i sigurnosne osobine korisnika. Kao administrator sigurnosti, trebate kontrolirati i revidirati promjene koje se dešavaju korisničkim profilima na vašem sistemu.

Reviziju sigurnosti možete postaviti tako da vaš sistem piše zapis o promjenama na korisničkom profilu. Za ispis izvještaja o ovim promjenama možete koristiti naredbu DSPAUDJRNE.

Možete kreirati izlazne programe za procjenjivanje zahtijevanih akcija na korisničkom profilu. Tablica 16 pokazuje izlazne točke koje su dostupne za naredbe korisničkog profila.

Tablica 16. Izlazne točke za aktivnost korisničkog profila

Naredba korisničkog profila	Ime izlazne točke
Kreiranje korisničkog profila (CRTUSRPRF)	QIBM_QSY_CRT_PROFILE
Promjena korisničkog profila (CHGUSRPRF)	QIBM_QSY_CHG_PROFILE
Brisanje korisničkog profila (DLTUSRPRF)	QIBM_QSY_DLT_PROFILE
Vraćanje korisničkog profila (RSTUSRPRF)	QIBM_QSY_RST_PROFILE

© Autorska prava IBM Corp. 1996, 2004

Vaš izlazni program može, na primjer, tražiti promjene koje su možda uzrokovale da korisnik izvodi neovlaštenu verziju programa. Ove promjene možda dodjeljuju ili različit opis posla ili novu trenutnu knjižnicu. Vaš izlazni program može ili obavijestiti red poruka ili poduzeti neku akciju (kao što je promjena ili onemogućavanje korisničkog profila) osnovanu na informacijama koje izlazni program dobiva.

Knjiga *Uputa iSeries sigurnosti* daje još informacija o izlaznim programima za akcije korisničkih profila.

Potpisivanje objekata

Sve su sigurnosne predostrožnosti koje poduzmete besmislene ako ih netko može premostiti unošenjem patvorenih podataka u vaš sistem. iSeries poslužitelj ima mnoštvo ugrađenih funkcija koje možete koristiti za spriječavanje učitavanja patvorenog softvera u vaš sistem i za otkrivanje ikakvog takvog softvera koji je već tu. Jedna je od tehnika dodanih u V5R1 potpisivanje objekata.

Potpisivanje objekata je iSeries poslužiteljska implementacija kriptografičkog koncepta poznatog kao ″digitali potpisi.″ Ideja je relativno jednostavna: jednom kad je proizvođač softvera spreman otpremiti softver korisniku, proizvođač ″potpisuje″ softver. Ovaj potpis nije jamstvo da softver obavlja bilo kakvu određenu funkciju. Međutim, on nudi način za dokaz da je softver dopremljen od proizvođača koji ga je potpisao i da softver nije promijenjen od kad je proizveden i potpisan. Ovo je osobito važno ukoliko je softver prenijet preko Interneta ili pohranjen na mediju za koji mislite da je mogao biti modificiran.

Upotreba digitalnih potpisa, daje vam veću kontrolu preko koje se softver može učitati na vaš sistem i daje vam veću moć za otkrivanje promjena kad se jednom učita. Nova sistemska vrijednost Provjera vraćanja objekta (QVFYOBJRST) nudi mehanizam za postavljanje ograničavajuće politike koja zahtijeva da sav softver učitan u sistem bude potpisan od poznatog izvora softvera. Također možete izabrati otvoreniju politiku i jednostavno provjeravati potpise ukoliko su prisutni.

Sav je OS/400 softver, kao i softver za opcije i iSeries poslužitelj licencne programe, potpisan od izvora kojem sistem vjeruje. Ovi potpisi pomažu sistemu da zaštititi svoj integritet i oni se provjeravaju kad se primjenjuju popravke na sistemu, da se osigura da je popravka stigla od izvora kojem sistem vjeruje i da nije mijenjana u transportu. Ovi se potpisi također mogu provjeriti i kad je softver već na sistemu. Naredba CHKOBJITG (Provjera integriteta objekta), je proširena tako da provjerava potpise dodatno drugim funkcijama integriteta objekata na vašem sistemu. Dodatno, Upravitelj digitalnih certifikata ima panele koje možete koristiti za provjeru potpisa objekata, uključujući objekata u operativnom sistemu.

Kao što je potpisan operativni sistem, možete koristiti digitalne potpise da zaštitite integritet softvera koji je kritičan za posao. Možete kupiti softver koji je potpisan od dobavljača softvera ili možete potpisati softver koji ste kupili ili napisali. Dio vaše sigurnosne politike, tad, može biti periodička upotreba CHKOBJITG ili Upravitelja digitalnih certifikata, za provjeru da su potpisi softvera još važeći— da objekti nisu promijenjeni od kad su potpisani. Nadalje možete tražiti da sav softver koji biva vraćen na vaš sistem bude potpisan od vas ili poznatog izvora. Međutim, budući da većina iSeries poslužiteljskog softvera koja nije proizvedena od IBM-a trenutno nije potpisana, ovo može biti previše ograničavajuće za vaš sistem. Nova vam podrška digitalnih potpisa daje fleksibilnost u odlučivanju što je najbolje za zaštitu integriteta vašeg softvera.

Digitali su potpisi koji zaštićuju softver samo jedan način upotrebe digitalnih certifikata. Dodatne informacije o upravljanju digitalnim certifikatima mogu se naći u poglavlju

Upravljanje digitalnim certifikatima u Informacijski Centar (pogledajte “Preduvjeti i povezane informacije” na stranici xii za detalje).

Nadgledanje opisa podsistema

Kada pokrenete podsistem na iSeries poslužitelju, sistem kreira okolinu za rad da se upiše sistem i izvodi. Opis podsistema definira kako izgleda okolina. Opisi podsistema, stoga, mogu pružiti priliku nepoštenim korisnicima. Netko tko želi nanijeti zlo može koristiti opis podsistema da pokrene program automatski ili da napravi mogućim prijavu bez korisničkog profila.

Kada izvodite naredbu Opozovi javno ovlaštenje naredba (RVKPUBAUT), sistem postavlja javno ovlaštenje opisu podsistema naredbom *EXCLUDE. Ovo spriječava korisnike koji nisu posebno ovlašteni (i koji nemaju *ALLOBJ posebno ovlaštenje) da promijene ili kreiraju opise podsistema.

Poglavlja koja slijede pružaju prijedloge za pregled opisa podsistema koji trenutno postoje na vašem sistemu. Možete koristiti naredbu Rad s opisima podsistema (WRKSBSD) da kreirate popis svih opisa podsistema. Kada izaberete 5 (Prikaz) s popisa, izbornik prikazuje za opis sistema koji ste izabrali. Pokazuje listu dijelova okoline podsistema.

Izabirete opcije da vidite detalje o dijelovima. Koristite naredbu Promjena opisa podsistema (CHGSBSD) da promijenite prve dvije stavke na izborniku. Da promijenite druge stavke, koristite prikladne naredbe za dodavanje, uklanjanje ili promjenu za tip unosa. Na primjer, da promijenite unos radne stanice, koristite naredbu Promjena unosa radne stanice (CHGWSE).

Knjiga *Upravljanje poslom* pruža više informacija o radu s opisima podsistema. Također ispisuje otpremljene vrijednosti za IBM dobavljene opise podsistema.

Unosi autostart poslova

Unos autostart posla sadrži ime opisa posla. Opis posla može sadržavati podatke zahtjeva (RQSDTA) koji uzrokuju da se program ili naredba izvodi. Na primjer, RQSDTA može biti CALL LIB1/PROGRAM1. Svaki put kada se podsistem pokreće, sistem će izvoditi program PROGRAM1 u knjižnici LIB1.

Pogledajte u unose autostart poslova i pridružene opise poslova. Osigurajte da razumijete funkciju svakog programa koji se izvodi automatski kada se podsistem pokreće.

Imena radnih stanica i tipovi radnih stanica

Kada se podsistem pokreće, dodjeljuje sve nedodijeljene radne stanice koje su popisane (specifično ili općenito) u njegovim unosima za imena radne stanice i tipove radne stanice. Kada se korisnik prijavljuje, korisnik se prijavljuje podsistemu koji je dodijelio radnu stanicu.

Unos radne stanice govori koji će opis posla biti korišten kada se posao pokreće u radnoj stanici. Opis posla može sadržavati podatke zahtjeva koji uzrokuju da se program ili naredba izvodi. Na primjer, parametar RQSDTA može biti CALL LIB1/PROGRAM1. Svaki put kada se korisnik prijavljuje na radnu stanicu u tom podsistemu, sistem će izvoditi PROGRAM1 u LIB1.

Pogledajte unose vaše radne stanice i pridružene opise poslova. Osigurajte da nitko nije dodao ili ažurirao bilo koji unos da izvodi programe kojih niste svjesni.

Unos radne stanice može također specificirati defaultni korisnički profil. Za određene konfiguracije podsistema, ovo dozvoljava nekome da se prijavi jednostavno pritišćući tipku

Enter. Ako je razina sigurnosti (QSECURITY sistemska vrijednost) na vašem sistemu manja od 40, trebate pregledati unose vaše radne stanice za defaultne korisnike.

Unosi reda poslova

Kada se podsistem pokreće, dodjeljuje bilo koje nedodijeljene redove poslova koje su popisani u opisu podsistema. Unosi reda poslova ne pružaju nikakvo direktno sigurnosno izlaganje. Međutim, oni pružaju mogućnost za nekoga da pokvari sistemsku izvedbu uzrokujući da se poslovi izvode u nenamjeravanim okolinama.

Trebate povremeno pregledati unose reda poslova u vašim opisima podsistema da osigurate da se batch poslovi izvode gdje očekujete da se izvode.

Unosi usmjeravanja

Unos usmjeravanja definira što čini posao jednom kad se unese u podsistem. Podsistem koristi unose usmjeravanja za sve tipove poslova: batch, interaktivni i komunikacijski poslovi. Unos usmjeravanja specificira sljedeće:

- Klasu za posao. Kao i unosi reda poslova, klasa koja je pridružena s poslom može utjecati na njegovu izvedbu ali ne predstavlja sigurnosno izlaganje.
- Program koji se izvodi kada se pokreće posao. Pogledajte u unose usmjeravanja i osigurajte da nitko nije dodao ili ažurirao bilo koje unose da izvodi programe kojih niste svjesni.

Komunikacijski unosi i imena udaljenih lokacija

Kada se komunikacijski posao upisuje u vaš sistem, sistem koristi komunikacijske unose i unose imena udaljene lokacije u aktivnom podsistemu da odredi kako će se izvoditi komunikacijski poslovi. Pogledajte sljedeće za ove unose:

- Svi podsistemi mogu izvoditi komunikacijske poslove. Ako podsistem koji ste namjeravali za komunikaciju nije aktivan, posao koji pokušava upisat se u vaš sistem može naći unos u opis drugog podsistema koju susreće njegove potrebe. Trebate pogledati unose u svim opisima podsistema.
- Komunikacijski unos sadrži opis posla. Opis posla može sadržavati podatke zahtjeva koji izvode naredbu ili program. Pogledajte vaše komunikacijske unose i njihove pridružene opise poslova da osigurate da razumijete kako će se poslovi pokrenuti.
- Komunikacijski unos također specificira defaultni korisnički profil koji sistem koristi u nekim situacijama. Budite sigurni da razumijete ulogu defaultnih profila. Ako vaš sistem sadrži defaultne profile, trebate osigurati da su to profili s minimalnim ovlaštenjem. Pogledajte Poglavlje 12, “Sigurne APPC komunikacije” za više informacija o defaultnim korisničkim profilima.

  Možete koristiti naredbu Ispiši opis podsistema (PRTSBSDAUT) da identificirate komunikacijske unose koji specificiraju ime korisničkog profila.

Unosi predpokrenutog posla

Možete koristiti unose posla da učinite podsistem spremnim za određene vrste poslova tako da se poslovi brže pokrenu. Predpokrenuti poslovi se mogu pokrenuti kada se podsistem pokreće ili kada su potrebni. Unos predpokrenutog posla specificira sljedeće:

- Program za izvođenje

  Defaultni korisnički profil

  Opis posla

Sve od ovog predstavlja moguće sigurnosno izlaganje. Trebate se uvjeriti da predpokrenuti poslovi izvode samo ovlaštene, namjeravane funkcije.

Poslovi i opisi poslova

Opisi posla sadržavaju podatke zahtjeva i podatke usmjeravanja koji mogu uzrokovati da se izvodi specifični program kada je korišten taj opis posla. Kada opis posla specificira program u parametru podataka zahtjeva, sistem izvodi program. Kada opis posla specificira podatke usmjeravanja, sistem izvodi program koji je specificiran u unosu usmjeravanja koji se podudara s podacima usmjeravanja.

Sistem koristi opise posla i za interaktivne i za batch poslove. Za interaktivne poslove, unos radne stanice specificira opis posla. Tipično, vrijednost unosa radne stanice je *USRPRF, tako sistem koristi opis posla koji je specificiran u korisničkom profilu. Za batch poslove, specificirate opis posla kada šaljete posao na izvođenje.

Povremeno trebate pregledati opise poslova da se uvjerite da ne izvode nenamjeravane programe. Trebate također koristiti ovlaštenje objekta da spriječite promjene opisa posla. *USE ovlaštenje je dovoljno za izvođenje posla s opisom posla. Tipični korisnik ne treba *CHANGE ovlaštenje za opise poslova.

Opcije izbornika SECBATCH:
15 *za submit odmah* **54** *za korištenje raspoređivača poslova*

Opisi poslova mogu također specificirati pod kojim korisničkim profilom se trebaju izvoditi poslovi. S razinom sigurnosti 40 ili više, morate imati *USE ovlaštenje za opis posla i korisnički profil koji je specificiran u opisu posla. S razinama sigurnosti nižim od 40, trebate *USE ovlaštenje samo za opis posla.

Možete koristiti naredbu Ispis ovlaštenja opisa posla (PRTJOBDAUT) da ispišete listu opisa poslova koji specificiraju korisničke profile i imaju javno ovlaštenje *USE.

Izvještaj pokazuje posebna ovlaštenja korisničkog profila koji je specificiran u opisu posla. Izvještaj uključuje posebna ovlaštenja bilo kojih profila grupe koje ima korisnički profil. Možete koristiti sljedeću naredbu da prikažete privatna ovlaštenja korisničkih profila:

```
DSPUSRPRF USRPRF(ime profila) TYPE(*OBJAUT)
```

Opis posla specificira popis knjižnica koje posao koristi kada se izvodi. Ako netko može promijeniti korisnički popis knjižnica, taj korisnik može izvoditi nenamjeravanu verziju programa u različitoj knjižnici. Trebate povremeno pregledati popise knjižnica koje su specificirane u opisima poslova u vašem sistemu.

Konačno, trebate osigurati da defaultne vrijednosti za naredbu Pošalji posao na izvođenje (SBMJOB) i naredbu Kreiraj korisnički profil (CRTUSRPRF) nisu promijenjene da pokazuju na nenamjeravane opise poslova.

Imena arhitekturnih transakcijskih programa

Neki komunikacijski zahtjevi šalju specifičan tip signala vašem sistemu. Ovaj zahtjev se zove **ime arhitekturnog transakcijskog programa (TPN)**, jer je ime transakcijskog programa dio APPC arhitekture za sistem. Zahtjev za prolaz-kroz ekranske stanice je primjer arhitekturnog TPN-a. Arhitekturni TPN-ovi su normalan način funkcioniranja komunikacija i ne predstavljaju nužno sigurnosno izlaganje. Međutim, arhitekturni TPN-ovi mogu pružiti neočekivani ulaz u vaš sistem.

Neki TPN-ovi ne predaju profil na zahtjev. Ako zahtjev postane pridružen s komunikacijskim unosom čiji defaultni korisnik je *SYS, zahtjev može biti pokrenut na vašem sistemu. Međutim, *SYS profil može izvoditi samo sistemske funkcije, a ne korisničke aplikacije.

Ako ne želite da se arhitekturni TPN-ovi izvode s defaultnim profilom, može promijeniti defaultnog korisnika sa *SYS na *NONE u komunikacijskim unosima. “Zahtjevi arhitekturnih TPN-ova” ispisuje arhitekturne TPN-ove i pridružene korisničke profile.

Ako ne želite da se specifični TPN uopće izvodi na vašem sistemu, napravite sljedeće:

1. Kreirajte CL program koji prihvaća nekoliko parametara. Program ne treba izvoditi funkcije. Treba jednostavno imati Declare (DCL) izraze za parametre i tada završiti.
2. Dodajte unos usmjeravanja za TPN za svaki podsistem koji ima komunikacijske unose ili unose imena udaljene lokacije. Unos usmjeravanja treba specificirati sljedeće:
   - *Vrijednost usporedbe* (CMPVAL) vrijednost jednaku imenu programa za TPN (pogledajte Zahtjevi arhitekturnih TPN-ova) s početnom pozicijom 37.
   - *Program za poziv* (PGM) vrijednost jednaku imenu programa koji ste kreirali u koraku 1. Ovo spriječava TPN od lociranja drugog unosa usmjeravanja, kao što je *ANY.

Nekoliko TPN-a već ima svoj vlastiti unos usmjeravanja u QCMN podsistemu. Ovo je dodano zbog razloga performansi.

Zahtjevi arhitekturnih TPN-ova

Tablica 17. Programi i korisnici za TPN zahtjeve

TPN zahtjev	Program	Korisnički profil	Opis
X'30F0F8F1'	AMQCRC6A	*NONE	stavljanje u red poruka
X'06F3F0F1'	QACSOTP	QUSER	APPC transakcijski program za prijavu
X'30F0F2D1'	QANRTP	QADSM	ADSM/400 APPC konfiguracija
X'30F0F1F9'	QCNPCSUP	*NONE	Podijeljeni folderi
X'07F0F0F1'	QCNTEDDM	QUSER	DDM
X'07F6C4C2'	QCNTEDDM	QUSER	Udaljeni SQL–DRDA1
X'30F0F7F7'	QCQNRBAS	QSVCCS	SNA CC_Server
X'30F0F1F4'	QDXPRCV	QUSER	DSNX–PC primalac
X'30F0F1F3'	QDXPSEND	QUSER	DSNX–PC odašiljač
X'30F0F2C4'	QEVYMAIN	QUSER	ENVY**/400 Poslužitelj
X'30F0F6F0'	QHQTRGT	*NONE	PC red podataka
X'30F0F8F0'	QLZPSERV	*NONE	Client Access upravitelj licence
X'30F0F1F7'	QMFRCVR	*NONE	PC primalac poruke
X'30F0F1F8'	QMFSNDR	*NONE	PC odašiljač poruke
X'30F0F6F6'	QND5MAIN	QUSER	APPN 5394 kontroler radne stanice
DB2DRDA	QCNTEDDDM	QUSER	DB2DRDA
APINGD	QNMAPINGD	QUSER	APINGD
X'30F0F5F4'	QNMEVK	QUSER	Pomoćni programi sistemskog upravljanja
X'30F0F2C1'	QNPSERVR	*NONE	PWS-I poslužitelj mrežnog ispisa
X'30F0F7F9'	QOCEVOKE	*NONE	Kalendar na više-sistema
X'30F0F6F1'	QOKCSUP	QDOC	Zasjenjivanje direktorija

Tablica 17. Programi i korisnici za TPN zahtjeve (nastavak)

TPN zahtjev	Program	Korisnički profil	Opis
X'20F0F0F7'	QOQSESRV	QUSER	DIA Verzija 2
X'20F0F0F8'	QOQSESRV	QUSER	DIA Verzija 2
X'30F0F5F1'	QOQSESRV	QUSER	DIA Verzija 2
X'20F0F0F0'	QOSAPPC	QUSER	DIA Verzija 1
X'30F0F0F5'	QPAPAST2	QUSER	S/36—S/38 prolaz-kroz
X'30F0F0F9'	QPAPAST2	QUSER	Pisač prolaz-kroz
X'30F0F4F6'	QPWFSTP0	*NONE	Podijeljeni folderi Tip 2
X'30F0F2C8'	QPWFSTP1	*NONE	Client Access poslužitelj datoteka
X'30F0F2C9'	QPWFSTP2	*NONE	Windows** Client Access poslužitelj datoteka
X'30F0F6F9'	QRQSRVX	*NONE	Udaljeni SQL–konvergentan poslužitelj
X'30F0F6F5'	QRQSRV0	*NONE	Udaljeni SQL bez predavanja
X'30F0F6F4'	QRQSRV1	*NONE	Udaljeni SQL bez predavanja
X'30F0F2D2'	QSVRCI	QUSER	SOC/CT
X'21F0F0F8'	QS2RCVR	QGATE	SNADS FS2 primalac
X'21F0F0F7'	QS2STSND	QGATE	SNADS FS2 odašiljač
X'30F0F1F6'	QTFDWNLD	*NONE	PC funkcija prijenosa
X'30F0F2F4'	QTIHNPCS	QUSER	TIE funkcija
X'30F0F1F5'	QVPPRINT	*NONE	PC virtualan ispis
X'30F0F2D3'	QWGMTP	QWGM	Ultimedia Mail/400 Poslužitelj
X'30F0F8F3'	QZDAINIT	QUSER	PWS-I poslužitelj pristupa podacima
X'21F0F0F2'	QZDRCVR	QSNADS	SNADS primalac
X'21F0F0F1'	QZDSTSND	QSNADS	SNADS odašiljač
X'30F0F2C5'	QZHQTRG	*NONE	PWS-I poslužitelj reda podataka
X'30F0F2C6'	QZRCSRVR	*NONE	PWS-I poslužitelj udaljene naredbe
X'30F0F2C7'	QZSCSRVR	*NONE	PWS-I centralni poslužitelj

Metode za nadgledanje sigurnosnih događaja

Postavljanje sigurnosti nije povremeno nastojanje. Trebate konstantno procjenjivati i promjene na vašem sistemu i vaše sigurnosne greške. Tada napravite prilagodbu vaše sigurnosne okoline tako da odgovara onom što ste otkrili.

Izvještaji sigurnosti pomažu vam u nadgledanju promjena relevantnih za sigurnost koje se dešavaju u vašem sistemu. Slijede ostale sistemske funkcije koje možete koristiti kao pomoć u otkrivanju sigurnosnih greški ili izlaganja:

- Revizija sigurnosti je moćan alat koji možete koristiti za promatranje mnogih različitih tipova događaja relevantnih za sigurnost koji se dešavaju u vašem sistemu. Na primjer, možete postaviti sistem da piše zapis revizije svaki put kada korisnik otvori određenu datoteku baze podataka za ažuriranje. Možete napraviti reviziju svih promjena na sistemske vrijednosti. Možete napraviti reviziju akcija koje se dešavaju kad korisnici vraćaju objekte.

  Poglavlje 9 u knjizi *Uputa iSeries sigurnosti* pruža potpune informacije o funkciji revizije sigurnosti. Možete koristiti naredbu Promjena revizije sigurnosti (CHGSECAUD) da

postavite reviziju sigurnosti na vašem sistemu. Možete također koristiti naredbu Prikaz unosa dnevnika revizije (DSPAUDJRNE) da ispišete izabrane informacije iz dnevnika revizije sigurnosti

- Možete kreirati QSYSMSG red poruka za hvatanje kritičnih poruka sistemskog operatera. QSYSOPR red poruka prima puno poruka promjenjive važnosti kroz tipični poslovni dan. Kritične poruke relevantne za sigurnost mogu se predvidjeti zbog velikog volumena poruka u QSYSOPR redu poruka.

  Ako kreirate QSYSMSG red poruka u QSYS knjižnici u vašem sistemu, sistem automatski usmjerava određene kritične poruke u QSYSMSG red poruka umjesto u QSYSOPR red poruka.

  Možete kreirati program za nadgledanje QSYSMSG reda poruka ili ga možete dodijeliti u načinu prekida sebi ili drugom povjerljivom korisniku.

Dio 3. Aplikacije i mrežne komunikacije

© Autorska prava IBM Corp. 1996, 2004

Poglavlje 11. Upotreba Integriranog sistema datoteka za osiguravanje datoteka

Integrirani sistem datoteka vam nudi razne načine za pohranjivanje i pregled informacija na iSeries poslužitelju. Integrirani sistem datoteka je dio OS/400 operativnog sistema koji podržava operacije protočnog ulaza i izlaza. On daje metode upravljanja memorijom koje su slične (i kompatibilne s) operativnim sistemima osobnog računala i UNIX operativnim sistemima.

S integriranim sistemom datoteka, svi objekti na sistemu se mogu gledati iz perspektive hijerarhijske strukture direktorija. Međutim, u većini slučaja, korisnici gledaju objekte na način koji je najčešći za određeni sistem datoteka. Na primjer, ″tradicionalni″ iSeries objekti su u QSYS.LIB sistemu datoteka. Tipično, korisnici vide ove objekte iz perspektive knjižnica. Korisnici tipično vide objekte u QDLS sistemu datoteka iz perspektive dokumenata unutar foldera. Korijenski (/), QOpenSys i korisnički-definirani sistemi datoteka predstavljaju strukturu hijerarhijskih (ugniježđenih) direktorija.

Kao administrator sigurnosti, trebate razumjeti sljedeće:

- Koji sistemi datoteka se koriste na vašem sistemu
- Jedinstvene osobine sigurnosti svakog sistema datoteka

Poglavlja koja slijede daju neka općenita razmatranja sigurnosti Integriranog sistema datoteka.

Pristup Integriranog sistema datoteka sigurnosti

Sistem datoteka s ishodištem djeluje kao kišobran (ili temelj) za sve druge sisteme datoteka na iSeries poslužiteljima. Na visokoj razini, on daje integriran pogled na sve objekte u sistemu. Drugi sistemi datoteka koji mogu postojati na iSeries poslužiteljima daju raznolike pristupe upravljanju objekata i integraciji, ovisno o naglašenoj svrsi svakog sistema datoteka. QOPT (optički) sistem datoteka, na primjer, omogućuje iSeries aplikacijama i poslužiteljima (uključujući iSeries Access za Windows poslužitelj datoteka) pristup do CD-ROM-a na iSeries poslužitelju. Slično, QFileSvr.400 sistem datoteka omogućuje aplikacijama pristup do podataka integriranog sistema datoteka na udaljenim iSeries poslužiteljima. QLANSrv poslužitelj datoteka omogućuje pristup datotekama pohranjenim na Integrirani xSeries poslužitelj za iSeries ili drugim povezanim poslužiteljima u mreži.

Pristup sigurnosti za svaki sistem datoteka ovisi o podacima koje sistem datoteka čini dostupnim. QOPT sistem datoteka, na primjer, ne nudi sigurnost objektne razine jer ne postoji tehnologija za pisanje informacija ovlaštenja na CD-ROM. Za QFileSvr.400 sistem datoteka, kontrola se pristupa nalazi na udaljenom sistemu (gdje su datoteke fizički pohranjene i upravljane). Za sisteme datoteka kao što je QLANSrv, Integrirani xSeries poslužitelj za iSeries nudi kontrolu pristupa. Unatoč različitim modelima sigurnosti, mnogi sistemi datoteka podržavaju konzistentno upravljanje kontrole pristupa kroz naredbe integriranog sistema, kao što je Promjena ovlaštenja (CHGAUT) i Promjena vlasnika (CHGOWN).

Slijede neka upozorenje za skrovišta i pukotine sigurnosti integriranog sistema datoteka. Integrirani je sistem datoteka oblikovan da što vjernije slijedi POSIX standarde. To vodi do nekih interesantnih ponašanja gdje su iSeries ovlaštenja poslužitelja i POSIX dozvole ″izmiješani″:

1. Ne uklanjajte privatno ovlaštenje korisnika za direktorij koji taj korisnik posjeduje, čak i kad je taj korisnik ovlašten kroz javno ovlaštenje, grupu ili autorizacijsku listu. Kad radite

© Autorska prava IBM Corp. 1996, 2004

s knjižnicama ili folderima u standardnom modelu sigurnosti iSeries poslužitelja, uklanjanje bi vlasnikovog privatnog ovlaštenja smanjilo količinu informacija ovlaštenja pohranjenih za korisnički profil i ne bi utjecalo na druge operacije. Ali, zbog načina na koji POSIX standard definira nasljednost dozvola za direktorije, vlasnik će novostvorenog direktorija imati ista objektna ovlaštenja nad tim direktorijom kao što vlasnik nadređenog ima nad nadređenim, čak i ako vlasnik novostvorenog direktorija ima druga privatna ovlaštenja nad nadređenim. To može biti teško razumjeti, stoga evo primjera: KORISNIK A posjeduje direktorij /DIRA, ali su privatna ovlaštenja KORISNIKA A uklonjena. KORISNIK B ima privatno ovlaštenje za /DIRA. KORISNIK B kreira direktorij /DIRA/DIRB. Zbog toga što KORISNIK A nema objektnih ovlaštenja za /DIRA, KORISNIK B nema objektnih ovlaštenja za /DIRA/DIRB. KORISNIK B neće moći preimenovati ili brisati /DIRA/DIRB bez dodatne akcije promjene objektnih ovlaštenja KORISNIKA A. To također dolazi do izražaja kod kreiranja datoteka s open() API-jem pomoću O_INHERITMODE oznake. Ako je KORISNIK B kreirao datoteku /DIRA/FILEB, KORISNIK B neće imati niti objektna ovlaštenja niti podatkovna ovlaštenja za njih. KORISNIK B ne može pisati u tu novu datoteku.

2. Usvojeno ovlaštenje nije poštovano od većine fizičkih sistema datoteka. To uključuje korijenski (/), QOpenSys i korisnički-definirane sisteme datoteka.
3. Svaki objekt posjeduje korisnički profil koji je kreirao taj objekti i ako je polje OWNER korisničkog profila postavljeno na *GRPPRF.
4. Mnoge operacije sistema datoteka trebaju *RX podatkovno ovlaštenje za svaku komponentu staza, uključujući korijenski (/) direktorij. Kad se suočite s problemima s ovlaštenjem, obavezno provjerite korisničko ovlaštenje za sam korijen.
5. Prikaz ili dohvat trenutnog radnog direktorija (DSPCURDIR, getcwd(),itd.) zahtijeva *RX podatkovno ovlaštenje za svaku komponentu staze. Međutim, promjena trenutnog radnog direktorija (CD, chdir(), itd.) zahtijeva samo *X podatkovno ovlaštenje za svaku komponentu. Stoga, korisnik može promijeniti trenutni radni direktorij na određenu stazu i tad biti nesposoban prikazati tu stazu.
6. Namjera je naredbe COPY dupliciranje objekta. Postavke će ovlaštenja na novoj datoteci biti iste kao na originalu osim za vlasnika. Namjera je naredbe CPYTOSTMF, jednostavno da duplicira podatke. Postavke ovlaštenja na novoj datoteci vlasnik ne može kontrolirati. Kreator/vlasnik će imati *RWX podatkovno ovlaštenje, ali će grupno i javno ovlaštenje biti *EXCLUDE. Korisnik mora koristiti druga značenja (CHGAUT, chmod(), itd.) za dodjeljivanje željenih ovlaštenja.
7. Korisnik mora biti vlasnik ili imati *OBJMGT objektno ovlaštenje nad objektom da dohvati informacije ovlaštenja o objektu. Ovo se dešava na nekim neočekivanim mjestima, kao COPY, koji mora dohvatiti informacije ovlaštenje nad izvornim objektom da postavi ekvivalentno ovlaštenje na ciljnom objektu.
8. Kad mijenjate vlasnika ili grupu objekta, korisnik ne samo da mora imati prikladno ovlaštenje za objekt, nego mora imati *ADD podatkovno ovlaštenje za novog vlasnika/grupu korisničkog profila i *DELETE podatkovno ovlaštenje za stari vlasnički/grupni profil. Ova se podatkovna ovlaštenja ne odnose na podatkovna ovlaštenja sistema datoteka. Ova se podatkovna ovlaštenja mogu prikazati upotrebom DSPOBJAUT naredbe i promijeniti upotrebom EDTOBJAUT naredbe. Ovo se također neočekivano pojavljuje kod COPY kad ona pokuša postaviti ID grupe za novi objekt.
9. MOV naredba je sklona stvaranju grešaka ovlaštenja, posebno pri premještanju iz jednog fizičkog sistema datoteka na drugi ili pri konverziji podataka. U ovim slučajevima, premještanje postaje operacija kopiranja i brisanja. Stoga, na naredbu MOV mogu utjecati sva ista razmatranja o ovlaštenjima kao kod COPY naredbe (pogledajte 7 i 8 iznad) i naredbe RMVLNK, dodatno s drugim specifičnim MOV razmatranjima.

Sljedeći odjeljci daju neka razmatranja za nekoliko reprezentativnih sistema datoteka. Za više informacija o specifičnom sistemu datoteka na vašem iSeries poslužitelju, trebate pogledati dokumentaciju za licencni program koji koristi sistem datoteka.

Korijenski (/), QOpenSys i korisnički-definirani sistemi datoteka

Slijede sigurnosna razmatranja za korijenski (/), QOpenSys i korisnički-definirane sisteme datoteka.

Kako rade ovlaštenja

Korijenski (/), QOpenSys i korisnički-definirani sistemi datoteka daju mješavinu iSeries poslužitelj, PC i UNIX** sposobnosti i za upravljanje objektima i za sigurnost. Kad koristite naredbe integriranog sistema datoteka iz neke sesije iSeries poslužitelja (WRKAUT i CHGAUT), možete postaviti sva normalna objektna ovlaštenja iSeries poslužitelja. Ovo uključuje *R, *W i *X ovlaštenja koja su kompatibilna sa Spec 1170 (operativnim sistemima UNIX-tipa).

Bilješka: Korijenski (/), QOpenSys i korisnički-definirani sistemi datoteka su funkcionalno ekvivalentni. QOpenSys sistem datoteka je osjetljiv na velika i mala slova. Korijenski sistem datoteka nije. Korisnički-definirani sistemi datoteka mogu biti definirani kao osjetljivi na velika i mala slova. Zbog toga što ovi sistemi datoteka imaju iste osobine sigurnosti, možete pretpostaviti da su njihova imena, u poglavljima koja slijede, korištena zamjenjivo.

Korijenskom sistemu datoteka možete pristupiti kao administrator iz PC sesije, možete postaviti objektne atribute koje PC koristi da ograničite određene tipove pristupa:
- Sistem
- Skriven
- Arhiva
- Samo za čitanje

Ovi PC atributi su dodaci, a ne zamjena za, vrijednosti ovlaštenja objekta iSeries poslužitelja.

Kad korisnik pokušava pristupiti objektu u korijenskom sistemu datoteka, OS/400 pretražuje sve vrijednosti objektnih ovlaštenja i atribute za objekt, bez obzira da li su ta ovlaštenja ″vidljiva″ iz korisničkog sučelja. Na primjer, pretpostavimo da je atribut samo-za-čitanje za objekt uključen. PC korisnik ne može obrisati objekt preko iSeries Access sučelja. Korisnik iSeries poslužitelja s radnom stanicom fiksne funkcije, također ne može obrisati objekt, iako korisnik iSeries poslužitelja ima *ALLOBJ posebno ovlaštenje. Prije nego se objekt može obrisati, ovlašteni korisnik mora koristiti PC funkciju za ponovo postavljanje vrijednosti samo-za-čitanje na off. Slično, PC korisnik možda nema dovoljno OS/400 ovlaštenje da promijeni PC-relevantne sigurnosne atribute objekta.

Aplikacije UNIX-tipa koje se izvode na iSeries poslužiteljima koriste UNIX-srodna sučelja aplikativnog programiranja (API-i) za pristup podacima u korijenskom sistemu datoteka. Sa UNIX-srodnim API-ima, aplikacije mogu prepoznati i održavati sljedeće sigurnosne informacije:
- Vlasnik objekta
- Vlasnik grupe (primarno grupno ovlaštenje iSeries poslužitelja)
- Čitanje (datoteka)
- Pisanje (promjena sadržaja)
- Izvođenje (izvodi programe ili traži direktorije)

Sistem mapira ova podatkovna ovlaštenja na postojeći objekt iSeries poslužitelja i podatkovna ovlaštenja:
- Čitanje (*R) = *OBJOPR i *READ
- Pisanje (*W) = *OBJOPR, *ADD, *UPD, *DLT
- Izvođenje (*X) = *OBJOPR i *EXECUTE

Koncepti za druga objektna ovlaštenja (*OBJMGT, *OBJEXIST, *OBJALTER, i *OBJREF) ne postoje u okruženjima UNIX-tipa.

Međutim, ova objektna ovlaštenja postoje za sve objekte u korijenskom sistemu datoteka. Kad kreirate objekt upotrebom UNIX-srodnog API-ja, taj objekt nasljeđuje ta ovlaštenja iz nadređenog direktorija, što rezultira sljedećim:

- Novi vlasnik objekta ima ista objektna ovlaštenja kao i vlasnik nadređenog direktorija.
- Nova primarna grupa objekta ima ista objektna ovlaštenja kao i primarna grupa nadređenog direktorija.
- Nova javnost objekta ima ista objektna ovlaštenja kao i javnost nadređenog direktorija.

Nova su objektna podatkovna ovlaštenja za vlasnika, primarnu grupu i javnost specificirana u API-ju s parametrom načina. Kad su sva objektna ovlaštenja postavljena 'on', dobivate ponašanje ovlaštenja koje očekujete u okruženjima UNIX-tipa. Najbolje ih je ostaviti postavljene na 'on', osim ako ne želite POSIX-srodno ponašanje.

Kad izvodite aplikacije koje koriste UNIX-srodne API-je, sistem pretražuje sva objektna ovlaštenja, bez obzira da li su ″vidljiva″ aplikacijama UNIX-tipa. Na primjer, sistem će tražiti ovlaštenje autorizacijske liste iako koncept autorizacijskih lista ne postoji u operativnim sistemima UNIX-tipa.

Kad imate okruženje miješanih-aplikacija, trebate osigurati da ne radite promjene ovlaštenja u jednom okruženju koje će prekinuti aplikacije u drugom okruženju.

Rad sa sigurnošću za Korijenske (/), QOpenSys i korisnički-definirane sisteme datoteka

Uvođenjem integriranog sistema datoteka, iSeries poslužitelji daju novi skup naredbi za rad s objektima u višestrukim sistemima datoteka. Ovaj skup naredbi uključuje naredbe za rad sa sigurnošću:

- Promjena revizije (CHGAUD)
- Promjena ovlaštenja (CHGAUT)
- Promjena vlasnika (CHGOWN)
- Promjena primarne grupe (CHGPGP)
- Prikaz ovlaštenja (DSPAUT)
- Rad s ovlaštenjima (WRKAUT)

Ove naredbe grupiraju označene podatke i objektna ovlaštenja u UNIX-srodne podskupove ovlaštenja:

***RWX** Čitanje/pisanje/izvođenje
***RW** Čitanje/pisanje
***R** Čitanje
***WX** Pisanje/izvođenje
***W** Pisanje
***X** Izvođenje

Dodatno, dostupni su UNIX-srodni API-ji za rad sa sigurnošću.

Opće ovlaštenje za osnovni direktorij

Prilikom isporuke vašeg sistema, opće je ovlaštenje za osnovni direktorij *ALL (sva objektna ovlaštenja i sva podatkovna ovlaštenja). Ovo postavljanje daje fleksibilnost i kompatibilnost i s tim što UNIX-srodne aplikacije očekuju i što očekuju tipični korisnici iSeries poslužitelja. Korisnik iSeries poslužitelja iz reda za naredbe može jednostavno kreirati novu knjižnicu u QSYS.LIB sistemu datoteka upotrebom CRTLIB naredbe. Normalno, ovo dozvoljava ovlaštenje na tipičnom iSeries poslužitelju. Slično, s dostavljenom postavkom za korijenski sistem datoteka, tipičan korisnik može kreirati novi direktorij u korijenskom sistemu datoteka (kao što vi možete kreirati novi direktorij na vašem PC-u).

Kao sigurnosni administrator, morate učiti svoje korisnike o prikladnoj zaštititi objekata koje kreiraju. Kad korisnik kreira knjižnicu, javno ovlaštenje za knjižnicu vjerojatno ne bi trebao biti *CHANGE (default). Korisnik treba postaviti javno ovlaštenje na ili *USE ili *EXCLUDE, ovisno o sadržajima knjižnice.

Ako korisnici žele kreirati nove direktorije u korijenskom (/), QOpenSys ili korisnički-definiranom sistemu datoteka, vi imate nekoliko sigurnosnih opcija:

- Možete naučiti svoje korisnike kako da pregaze defaultno ovlaštenje kad kreiraju nove direktorije. Default je nasljeđivanje ovlaštenja od neposrednog nadređenog direktorija. U slučaju novo kreiranog direktorija u osnovnom direktoriju, po defaultu javno će ovlaštenje biti *ALL.
- Možete kreirati ″glavni″ poddirektorij ispod osnovnog direktorija. Postavite javno ovlaštenje na tom glavnom direktoriju na prikladno postavljanje za vašu organizaciju. Zatim uputite korisnike da kreiraju nove osobne direktorije u ovom glavnom poddirektoriju. Njihovi će novi direktoriji naslijediti njegovo ovlaštenje.
- Možete uzeti u obzir promjenu javnog ovlaštenja za osnovni direktorij da spriječite korisnike da kreiraju objekte u tom direktoriju. (Uklonite *W, *OBJEXIST, *OBJALTER, *OBJREF i *OBJMGT ovlaštenja.) Međutim, morate procijeniti da li će ova promjena uzrokovati probleme za bilo koju od vaših aplikacija. Možete, na primjer, posjedovati UNIX-srodne aplikacije koje očekuju da mogu brisati objekte iz osnovnog direktorija.

Naredba Ispis objekata s privatnim ovlaštenjima (PRTPVTAUT)

Naredba Ispis objekata s privatnim ovlaštenjima (PRTPVTAUT) vam dozvoljava ispis izvještaja o svim privatnim ovlaštenjima za objekte specificiranog tipa u specificiranu knjižnicu, folder ili direktorij. Izvještaj ispisuje sve objekte specificiranog tipa i korisnike koji imaju ovlaštenja na taj objekt. Ovo je način provjere različitih izvora ovlaštenja na objekte.

Ova naredba ispisuje tri izvještaja za izabrane objekte. Prvi izvještaj (Potpuni izvještaj) sadržava sva privatna ovlaštenja za svaki od izabranih objekata. Drugi izvještaj (Izvještaj promjena) sadržava dodatke i promjene privatnih ovlaštenja za izabrane objekte, ako je naredba PRTPVTAUT prethodno izvođena za specificirane objekte u specificiranoj knjižnici, folderu ili direktoriju. Svi su novi objekti izabranog tipa, nova ovlaštenja za postojeće objekte ili promjene postojećih ovlaštenja na postojećim objektima ispisani u ’Izvještaju promjena’. Ako naredba PRTPVTAUT nije prethodno izvođena za specificirane objekte u specificiranoj knjižnici, folderu ili direktoriju, neće biti ’Izvještaja promjena’. Ako je naredba prethodno izvođena ali nikakve promjene nisu načinjene na ovlaštenjima nad objektima, tad je ’Izvještaj promjena’ ispisan, ali nema ispisanih objekata.

Treći izvještaj (Izvještaj brisanja) sadržava bilo kakva brisanja privatno ovlaštenih korisnika sa specificiranih objekata od kad se zadnji put izvodila naredba PRTPVTAUT. Svi su objekti koji su obrisani ili svi korisnici koji su uklonjeni kao privatno ovlašteni korisnici, ispisani su u ’Izvještaju brisanja’. Ako naredba PRTPVTAUT nije prethodno izvođena, neće biti ’Izvještaja brisanja’. Ako je naredba prethodno izvođena, ali nisu napravljene nikakve operacije brisanja nad objektima, tad je ’Izvještaj brisanja’ ispisan ali nema ispisanih objekata.

Ograničenje: Morate imati *ALLOBJ posebno ovlaštenje za korištenje ove naredbe.

Primjeri:

Ova naredba kreira potpuni izvještaj i izvještaje promjena i brisanja za sve objekte datoteka u PAYROLLLIB:

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

Ova naredba kreira potpuni izvještaj i izvještaje promjena i brisanja za sve objekte datoteka protoka u direktoriju GARRY:

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

Ova naredba kreira potpuni izvještaj i izvještaje promjena i brisanja za sve objekte datoteka protoka u strukturi poddirektorija koja počinje u direktoriju GARRY:

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

Naredba Ispis javno ovlaštenih objekata (PRTPUBAUT)

Naredba Ispis javno ovlaštenih objekata (PRTPUBAUT) vam dozvoljava ispis izvještaja specificiranih objekata koji nemaju javno ovlaštenje *EXCLUDE. Za *PGM objekte, samo programi koji nemaju javno ovlaštenje *EXCLUDE, koje korisnici mogu pozvati (program je ili korisničke domene ili je sigurnosna razina sistema (QSECURITY sistemska vrijednost) 30 ili ispod) biti će uključeni u izvještaj. Ovo je način provjere objekata kojima je svaki korisnik na sistemu ovlašten pristupati.

Ova će naredba ispisati dva izvještaja. Prvi izvještaj (Potpuni izvještaj) sadržava sve specificirane objekte koji nemaju javno ovlaštenje *EXCLUDE. Drugi izvještaj (Izvještaj promjena) sadržava objekte koji sad više nemaju javno ovlaštenje *EXCLUDE, a koji su imali javno ovlaštenje *EXCLUDE ili nisu postojali kad se prethodno izvodila naredba PRTPUBAUT. Ako naredba PRTPUBAUT nije prethodno izvođena za specificirane objekte i knjižnicu, folder ili direktorij, neće biti 'Izvještaja promjena'. Ako je naredba prethodno izvođena ali nikakvi dodatni objekti nemaju javna ovlaštenja *EXCLUDE, tad će se 'Izvještaj promjena' ispisati ali neće biti ispisanih objekata.

Ograničenje: Morate imati *ALLOBJ posebno ovlaštenje za korištenje ove naredbe.

Primjeri:

Ova naredba kreira potpuni izvještaj i izvještaj promjena za sve objekte datoteka u knjižnici GARRY koji nemaju javno ovlaštenje *EXCLUDE:

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

Ova naredba kreira potpuni izvještaj i izvještaj promjena za sve objekte datoteka protoka u strukturi poddirektorija koja počinje u direktoriju GARRY koji nemaju javno ovlaštenje *EXCLUDE:

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

Ograničavanje pristupa QSYS.LIB sistemu datoteka

Zbog toga što je ishodišna sistemska datoteka gornja sistemska datoteka, QSYS.LIB sistem datoteka se čini kao poddirektorij unutar osnovnog direktorija. Stoga, svaki PC korisnik s pristupom na vaš iSeries poslužitelj može rukovati objektima pohranjenim u knjižnicama iSeries poslužitelja (QSYS.LIB sistem datoteka) s normalnim PC naredbama i akcijama. PC korisnik može, na primjer, dovući QSYS.LIB objekt (kao što je knjižnica s datotekama vaših kritičnih podataka) u poništavač.

Kako ste naučili u "Korijenski (/), QOpenSys i korisnički-definirani sistemi datoteka" na stranici 85, sistem traži sva objektna ovlaštenja bez obzira da li su ona vidljiva sučelju. Stoga, korisnik ne može rascijepati (brisati) objekt osim ako korisnik nema *OBJEXIST ovlaštenje za objekt. Međutim, ako vaš iSeries ovisi o sigurnosti pristupa izborniku umjesto sigurnosti objekta, PC korisnik može vrlo dobro otkriti objekte u QSYS.LIB sistemu datoteka koji su dostupni za uništavanje.

Kako proširujete upotrebljivost vašeg sistema i različite metode pristupa koje nudite, uskoro ćete otkriti da sigurnost pristupa izborniku nije dovoljna. Poglavlje 5, “Zaštita informacijskih sredstava s objektnim ovlaštenjem”, na stranici 39 raspravlja o vašim strategijama za nadopunu kontrole pristupa izborniku s objektnom sigurnosti. Međutim, iSeries poslužitelji također daju jednostavan način na koji možete spriječiti pristup QSYS.LIB sistemu datoteka kroz strukturu korijenskog sistema direktorija. Možete koristiti QPWFSERVER autorizacijsku listu za kontrolu korisnika koji mogu pristupati QSYS.LIB sistemu datoteka kroz osnovni direktorij.

Kad je korisničko ovlaštenje za QPWFSERVER autorizacijsku listu *EXCLUDE, korisnik ne može ući u QSYS.LIB direktorij iz strukture osnovnog direktorija. Kad je korisničko ovlaštenje *USE, korisnik može ući u direktorij. Jednom kad korisnik dobije ovlaštenje za ulaz u direktorij, primjenjuje se ovlaštenje normalnog objekta za svaku akciju koju korisnik pokuša obaviti na objektu unutar QSYS.LIB sistemu datoteka. Drugim riječima, ovlaštenje za QPWFSERVER autorizacijsku listu djeluje kao vrata za cijeli QSYS.LIB sistem datoteka. Za korisnika s ovlaštenjem *EXCLUDE, vrata su zaključana. Za korisnika s ovlaštenjem *USE (ili bilo kojim većim ovlaštenjem), vrata su otvorena.

U većini situacija, korisnici ne trebaju koristiti sučelje direktorija za pristup objektima u QSYS.LIB sistemu datoteka. Vjerojatno ćete željeti postaviti javno ovlaštenje na QPWFSERVER autorizacijskoj listi na *EXCLUDE. Zapamtite, da ovlaštenje za autorizacijsku listu otvara ili zatvara vrata za sve knjižnice unutar QSYS.LIB sistema datoteka, uključujući knjižnice korisnika. Ako naiđete na korisnike koji su objekt ovog isključenja, možete procijeniti njihove zahtjeve na pojedinačnim osnovama. Ako je prikladno, možete izričito ovlastiti pojedinačnog korisnika za autorizacijsku listu. Međutim, morate osigurati da korisnik ima prikladno ovlaštenje za objekte unutar QSYS.LIB sistema datoteka. Inače, korisnik može slučajno obrisati objekte ili cijele knjižnice.

Bilješke:

1. Kad vaš sistem otprema, opće je ovlaštenje za QPWFSERVER autorizacijsku listu *USE
2. Ako izričito ovlastite pojedinačnog korisnika, autorizacijska lista kontrolira pristup samo s iSeries Access posluživanjem datoteka, NetServer posluživanjem datoteka i posluživanjem datoteka između iSeries poslužitelja. Ovo ne spriječava pristup istim direktorijima putem FTP, ODBC i drugih mreža.

Sigurni direktoriji

Za pristup objektu unutar korijenskog sistema datoteka, čitate kroz cijelu stazu do tog objekta. Da bi tražili direktorij, morate imati *X (*OBJOPR i *EXECUTE) ovlaštenje za taj direktorij. Pretpostavimo, na primjer, da želite pristupiti sljedećem objektu:

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

Morate imati *X ovlaštenje za companya direktorij i customers direktorij.

S korijenskim sistemom datoteka, možete kreirati simboličku vezu na objekt. Konceptualno, simbolička veza je zamjensko ime za ime staze. Uobičajeno je to kraće i lakše za zapamtiti nego ime pune staze. Simbolička veza ipak ne kreira različitu fizičku stazu do objekta. Korisnik još uvijek treba *X ovlaštenje za svaki direktorij i poddirektorij u fizičkoj stazi do objekta.

Za objekte u korijenskom sistemu datoteka, sigurnost direktorija možete koristiti jednako kao što koristite sigurnost knjižnica u QSYS.LIB sistemu datoteka. Možete, na primjer, postaviti javno ovlaštenje direktorija na *EXCLUDE da spriječite pristup javnih korisnika bilo kojem objektu u stablu.

Sigurnost za nove objekte

Možete kreirati novi objekt u korijenskom sistemu datoteka, sučelje koje koristite za kreiranje određuje njegova ovlaštenja. Na primjer, ako koristite CRTDIR naredbu i njene defaulte, novi direktorij nasljeđuje sve osobine ovlaštenja svog nadređenog direktorija, uključujući privatna ovlaštenja, ovlaštenje primarne grupe i udruženje autorizacijske liste. Sljedeći odlomci opisuju kako su određena ovlaštenja za svaki tip sučelja.

Ovlaštenje dolazi od neposrednog nadređenog direktorija, ne od direktorija koji se nalaze više uz stablo. Stoga, kao administrator sigurnosti, trebate vidjeti ovlaštenje koje dodjeljujete direktorijima u hijerarhiji iz dvije perspektive:

- Kako ovlaštenje utječe na objekte u stablu (kao ovlaštenje knjižnice).
- Kako ovlaštenje utječe na novo kreirane objekte (kao vrijednost CRTAUT za knjižnice).

Preporuka: Možda bi trebali dati korisnicima koji rade u integriranom sistemu datoteka home direktorij (na primjer, /home/usrxxx) i potom postaviti odgovarajuću sigurnost (kao što je PUBLIC *EXCLUDE). Svi će direktoriji koji korisnik kreira pod svojim home direktorijom tad naslijediti ovlaštenja.

Slijede opisi nasljeđivanja ovlaštenja za različita sučelja:

Upotreba naredbe Kreiranje direktorija

Kad kreirate novi poddirektorij upotrebom CRTDIR naredbe, imate dvije opcije za specificiranje ovlaštenja:

- Možete specificirati javno ovlaštenje (ovlaštenje podataka, ovlaštenje objekta ili oba).
- Možete specificirati *INDIR za podatkovno ovlaštenje, objektno ovlaštenje ili oba. Kad specificirate *INDIR i za ovlaštenje podataka i za objektno ovlaštenje, sistem radi točnu kopiju svih informacija ovlaštenja iz nadređenog direktorija na novi objekt, uključujući autorizacijsku listu, primarnu grupu, javno ovlaštenje i javna ovlaštenja. (Sistem ne kopira privatno ovlaštenje koje QSYS profil ili QSECOFR profil ima nad objektom.)

Kreiranje direktorija s API-jem

Kad kreirate direktorij upotrebom mkdir() API-a, specificirate podatkovna ovlaštenja za vlasnika, primarnu grupu i javnost (upotrebom mapiranja ovlaštenja *R, *W i *X). Sistem koristi informacije u nadređenom direktoriju za postavljanje objektnih ovlaštenja za vlasnika, primarnu grupu i javnost.

Zbog toga što operativni sistemi UNIX-tipa nemaju koncept objektnih ovlaštenja, mkdir() API ne podržava specificiranje objektnih ovlaštenja. Ako želite različita objektna ovlaštenja, možete koristiti naredbu iSeries poslužitelja (CHGAUT). Međutim, kad uklonite neka objektna ovlaštenja, UNIX-srodne aplikacije mogu ne raditi kao što se od njih očekuje.

Kreiranje datoteke protoka s open() ili creat() API-jem

Kad koristite creat() API za kreiranje datoteke protoka, možete specificirati podatkovna ovlaštenja za vlasnika, primarnu grupu i javnost (upotrebom UNIX-srodnih ovlaštenja *R, *W i *X). Sistem koristi informacije u nadređenom direktoriju za postavljanje objektnih ovlaštenja za vlasnika, primarnu grupu i javnost.

Također možete specificirati ova ovlaštenja pri korištenju open() API-ja za kreiranje datoteke protoka. Alternativno, kad koristite open() API možete specificirati da objekt treba naslijediti sva ovlaštenja od nadređenog direktorija. To se zove nasljedni način. Kad specificirate

nasljedni način, sistem radi potpuno uparivanje za nadređene direktorije, uključujući autorizacijsku listu, primarnu grupu, javno ovlaštenje i javna ovlaštenja. Ova opcija radi kao i specificiranje *INDIR u naredbi CRTDIR.

Kreiranje objekta upotrebom PC sučelja

Kad koristite PC aplikaciju za kreiranje objekta u korijenskom sistemu datoteka, sistem automatski nasljeđuje sva ovlaštenja od nadređenog direktorija. To uključuje autorizacijsku listu, primarnu grupu, javno ovlaštenje i javna ovlaštenja. PC aplikacije nemaju ekvivalent za specificiranje ovlaštenja kad kreirate objekt.

QFileSvr.400 sistem datoteka

S QFileSvr.400 sistemom datoteka, korisnik (USERX) na jednom iSeries sistemu (SYSTEMA) može pristupati podacima na drugom povezanom iSeries sistemu (SYSTEMB). USERX ima sučelje koje je isto kao i Client Access sučelje. Udaljeni iSeries poslužitelj (SYSTEMB) izgleda kao direktorij sa svim svojim sistemima datoteka i poddirektorijima.

Kad USERX pokuša pristup na SYSTEMB s ovim sučeljem, SYSTEMA šalje ime profila USERX-a i šifriranu lozinku na SYSTEMB. Isti korisnički profil i lozinka moraju postojati na SYSTEMB, inače SYSTEMB odbija zahtjev.

Ako SYSTEMB prihvati zahtjev, USERX izgleda za SYSTEMB kao bilo koji Client Access korisnik. Ista se pravila provjere ovlaštenja primjenjuju na sve akcije koje USERX pokuša.

Kao administrator sigurnosti, trebate znati da QFileSvr.400 sistem datoteka predstavlja druga moguća vrata u vaš sistem. Ne možete pretpostaviti da ograničavate vaše udaljene korisnike na interaktivnu prijavu s prolaskom kroz ekran stanice. Ako vam se izvodi QSERVER podsistem, a vaš je sistem povezan na drugi iSeries sistem, udaljeni korisnici mogu pristupati vašem sistemu kao da se nalaze na lokalnom PC koji izvodi Client Access. Najvjerojatnije će vaš sistem imati vezu koja zahtijeva izvođenje QSERVER podsistema. Ovo je još jedan razlog potrebe za dobrom shemom ovlaštenja objekta.

Mrežni sistem datoteka

Mrežni sistem datoteka (NFS) omogućuje pristup na i iz sistema koji imaju NFS implementacije. NFS je industrijski standardan način dijeljenja informacija među korisnicima umreženih sistema. Većina glavnih operativnih sistema (uključujući PC operativne sisteme) omogućuje NFS. Za UNIX sisteme, NFS je primaran način pristupa podacima. iSeries poslužitelji mogu djelovati i na NFS klijentu i na NFS poslužitelju.

Kad ste administrator sigurnosti iSeries sistema koji se ponaša kao NFS poslužitelj, morate razumjeti i upravljati sigurnosnim aspektima NFS-a. Slijede prijedlozi i razmatranja:

- Morate izričito startati funkciju NFS poslužitelja upotrebom STRNFSSVR naredbe. Kontrolirajte tko ima ovlaštenje upotrebe ove naredbe.
- direktorij ili objekt činite dostupnim NFS klijentu eksportiranjem istog. Stoga, imate vrlo specifičnu kontrolu, preko kojih ćete dijelova vašeg sistema postati dostupan NFS klijentima na vašoj mreži.
- Kad eksportirate, možete specificirati klijente koji imaju pristup objektu. Klijenta identificirate sistemskim imenom ili IP adresom. Klijent može biti pojedinačan PC ili cijeli iSeries poslužitelj ili UNIX sistem. U NFS terminologiji, klijent (IP adresa) se naziva stroj.
- Kad eksportirate, možete specificirati pristup samo za čitanje ili pristup piši/čitaj za svaki stroj koji ima pristup eksportiranom direktoriju ili objektu. U većini ćete slučajeva, vjerojatno željeti omogućiti pristup samo za čitanje.

- NFS ne daje zaštitu lozinkama. On je oblikovan i namjeravan za dijeljenje podataka između zajednice sistema kojima se vjeruje. Kad korisnik zahtijeva pristup, poslužitelj prima korisnički uid. Slijede neka uid razmatranja:
  - iSeries poslužitelj pokušava pronaći korisnički profil s istim uid. Ako pronađe podudarajući uid, koristi vjerodajnice korisničkog profila. Vjerodajnice su NFS termin za opis upotrebu ovlaštenja korisnika. To je slično razmjeni profila u drugim aplikacijama iSeries poslužitelja.
  - Kad eksportirate direktorij ili objekt, možete specificirati da li ćete dozvoliti pristup profila s ovlaštenjem korijena. NFS poslužitelj na iSeries poslužiteljima izjednačava korijensko ovlaštenje s *ALLOBJ posebnim ovlaštenjem. Ako specificirate da nećete dozvoliti korijensko ovlaštenje, NFS korisnik s uid-jem koje mapira na korisnički profil s *ALLOBJ posebnim ovlaštenjem neće moći pristupiti objektima pod tim profilom. Umjesto toga, ako je dozvoljen anoniman pristup, zahtjevatelj će biti mapiran anonimnim profilom.
  - Kad eksportirate direktorij ili objekt, možete specificirati da li ćete dozvoliti anonimne zahtjeve. Anoniman zahtjev je zahtjev s uid-jem koji se ne podudara ni s jednim uid-jem na vašem sistemu. Ako izaberete dozvoljavanje anonimnih zahtjeva, sistem mapira anonimnog korisnika na IBM dobavljeni QNFSANON korisnički profil. Ovaj korisnički profil nema nikakva posebna ovlaštenja ili izričita ovlaštenja. (Pri eksportu, ako želite, možete specificirati neki drugi korisnički profil za anonimne zahtjeve.)
- Kad vaš iSeries poslužitelj sudjeluje u NFS mreži (ili bilo kojoj mreži s UNIX sistemima koji ovise o uid-jima), vjerojatno trebate upravljati vašim vlastitim uid-jima umjesto dozvoljavanja da im sistem automatski dodjeljuje. Trebati ćete uskladiti uid-jeve s drugim sistemima u vašoj mreži.

  Možda otkrijete da trebate promijeniti uid-jeve (ili za IBM dobavljene korisničke profile) da bi imali kompatibilnost s drugim sistemima u vašoj mreži. Program može pojednostaviti promjenu uid-ja za korisnički profil. Kad promijenite uid za korisnički profil, također trebate promijeniti uid za sve objekte koje profil posjeduje ili u osnovnom direktoriju ili u QOpenSrv direktoriju.) QSYCHGID program automatski mijenja uid i u korisničkom profilu i u svim posjedovanim objektima. Za informacije o načinu korištenja ovog programa, pogledajte knjigu *iSeries Sistemski API Upute*.

Poglavlje 12. Sigurne APPC komunikacije

Kad vaš sistem sudjeluje u mreži s drugim sistemima, postaje dostupan novi skup vrata i prozora u vaš sistem. Kao administrator sigurnosti, trebate biti svjesni opcije koje možete koristiti za kontrolu ulaza u vaš sistem u APPC okruženju.

Napredne program-program komunikacije (APPC) je način na koji računala, uključujući osobna računala, međusobno komuniciraju. Prikaz prolaza-kroz za stanicu, distribuirano upravljanje podacima i iSeries Access za Windows mogu svi koristiti APPC komunikacije.

Poglavlja koja slijede daju neke osnovne informacije o načinu rada APPC komunikacija i načinu postavljanja prikladne sigurnosti. Ova se poglavlja primarno odnose na sigurnosno-relevantne elemente APPC konfiguracije. Da prilagodite ovaj primjer vašoj situaciji, trebati ćete raditi s ljudima koji upravljaju vašom komunikacijskom mrežom i možda dobavljačima vaših aplikacija. Ove informacija koristite kao osnovu koja će vam pomoći razumjeti sigurnosna pitanja i opcije dostupne za APPC.

Sigurnost nije nikad “slobodna”. Neki prijedlozi koji čine mrežnu sigurnost lakšom, čine mrežnu administraciju još težom. Na primjer, ove informacija ne naglašavaju APPN (Napredni ravnopravni mrežni rad), jer je sigurnost lakše razumjeti i upravljati bez APPN-a. Međutim, bez APPN-a, mrežni administrator mora ručno kreirati konfiguracijske informacije koje APPN kreira automatski.

PC-ovi također koriste komunikacije

Mnoge metode za povezivanje vaših PC-ova na vaše iSeries poslužitelje ovise o komunikacijama, kao što su APPC ili TCP/IP. Dok čitate poglavlja koja slijede, uzmite u obzir sigurnosna pitanja za povezivanje i na druge sisteme i na PC-ove. Kad planirate vašu mrežnu zaštitu, osigurajte se da nećete nepovoljno utjecati na PC-ove koji su spojeni na vaš sistem.

APPC terminologija

APPC omogućuje korisnicima jednog sistema da obavljaju rad na drugom sistemu. Sistem na kojem je zahtjev pokrenut, zove se na jedan od sljedećih načina:

- **Izvorni sistem**
- **Lokalni sistem**
- **Klijent**

Sistem koji prima zahtjev, zove se na jedan od sljedećih načina:

- **Ciljni sistem**
- **Udaljeni sistem**
- **Poslužitelj**

Osnovni elementi APPC komunikacija

Iz perspektive administratora sigurnosti, mora se dogoditi sljedeće prije nego korisnik na jednom sistemu (SYSTEMA) može obaviti značajan rad na drugom sistemu (SYSTEMB):

- Izvorni sistem (SYSTEMA) mora dati stazu do ciljnog sistema (SYSTEMB). Ova se staza zove **APPC sesija**.

© Autorska prava IBM Corp. 1996, 2004

- Ciljni sistem mora identificirati korisnika i pridružiti mu korisnički profil. Ciljni sistem mora podržavati algoritam šifriranja izvornog sistema (pogledajte “Razine lozinke” na stranici 14 za više informacija).
- Ciljni sistem mora startati posao za korisnika s prikladnim okruženjem (vrijednosti upravljanja poslom).

Poglavlja koja slijede raspravljaju o ovim elementima i njihovom odnosu sa sigurnošću. Administrator sigurnosti na ciljnom sistemu ima primarnu odgovornost osiguravanja da APPC korisnici ne krše sigurnost. No , kad administratori sigurnosti na oba sistema rade zajedno, posao je upravljanja APPC sigurnosti mnogo lakši.

Primjer: Osnovna APPC sesija

U APPC okruženju, kad korisnik ili aplikacija na jednom sistemu zahtijevaju pristup drugom sistemu, dva sistema uspostavljaju sesiju. Za uspostavljanje sesije, sistemi moraju povezati dva podudarajuća opisa APPC uređaja. Parametar Imena udaljene lokacije (RMTLOCNAME) u opisu uređaja SYSTEMA, mora se podudarati s parametrom Imena lokalne lokacije (LCLLOCNAME) u opisu uređaja SYSTEMB i obratno.

Da dva sistema uspostave APPC sesiju, lozinke lokacija u opisima APPC uređaja na SYSTEMA i SYSTEMB moraju biti iste. Oba moraju specificirati *NONE ili oba moraju specificirati istu vrijednost.

Ako su lozinke vrijednosti različite od *NONE, one su pohranjene i šalju se u šifriranom formatu. Ako se lozinke podudaraju, sistemi uspostavljaju sesiju. Ako se lozinke ne podudaraju, zahtjev korisnika se odbacuje. Kad sistemi specificiraju lozinke lokacija za uspostavu sesije, to se naziva **sigurno vezanje**.

Bilješka: Ne pružaju svi računalni sistemi podršku za funkciju sigurnog vezanja.

Ograničenja APPC sesija

Kao administrator sigurnosti na vašem izvornom sistemu, možete koristiti objektno ovlaštenje za kontrolu tko može pokušavati pristup drugim sistemima. Postavite javno ovlaštenje za opise APPC uređaja na *EXCLUDE i dajte *CHANGE ovlaštenje određenim korisnicima. Koristite QLMTSECOFR sistemsku vrijednost za spriječavanje korisnika s *ALLOBJ posebnim ovlaštenjem, od upotrebe APPC komunikacija.

Kao administrator sigurnosti na ciljnom sistemu, možete također koristiti ovlaštenje za APPC uređaje da spriječite korisnicima pokretanje APPC. sesije na vašem sistemu. Međutim, trebate razumjeti što će korisnički ID pokušati za pristup opisu APPC uređaja. “Pristup APPC korisnika ciljnom sistemu” na stranici 95 opisuje kako iSeries poslužitelji pridružuju korisnički ID sa zahtjevom za APPC sesiju.

Bilješka: Možete koristiti naredbu Ispis javno ovlaštenih objekata (PRTPUBAUT *DEVD) i Ispis privatnih ovlaštenja (PRTPVTAUT *DEVD) naredbu da saznate tko ima ovlaštenja za opise uređaja na vašem sistemu.

Kad vaš sistem koristi APPN, on automatski kreira novi APPC uređaj kad nikakav postojeći uređaj nije dostupan za smjer koji je sistem izabrao. Jedna je metoda ograničavanja pristupa APPC uređajima na sistemu koju koristi APPN kreiranje autorizacijske liste. Autorizacijska lista sadržava popis korisnika koje treba ovlastiti za APPC uređaje. Potom koristite naredbu Promjena defaulta naredbe(CHGCMDDFT) da promijenite CRTDEVAPPC naredbu. Za parametar ovlaštenja (AUT) u CRTDEVAPPC naredbi, postavite defaultnu vrijednost na autorizacijsku listu koju ste kreirali.

Bilješka: Ako vaš sistem na jeziku različitom od engleskog, trebate promijeniti default naredbe u QSYSxxxx knjižnici za svaki nacionalni jezik koji je na vašem sistemu.

Koristite parametar lozinke lokacije (LOCPWD) u opisu APPC uređaja za provjeru valjanosti identiteta drugog sistema koji zahtjeva sesiju s vašim sistemom (u ime korisnika ili aplikacije). Lokacijska vam lozinka može pomoći u otkrivanju varalačkog sistema.

Pri upotrebi lokacijskih lozinki, morate koordinirati rad s administratorima sigurnosti za druge sisteme u mreži. Također morate kontrolirati tko može kreirati promjene opisa APPC uređaja i konfiguracijskih listi. Sistem treba *IOSYSCFG posebno ovlaštenje za upotrebu naredbi koje rade s APPC uređajima i konfiguracijskim listama.

Bilješka: Kad koristite APPN, lokacijske su lozinke pohranjene u QAPPNRMT konfiguracijskoj listi umjesto u opisima uređaja.

Pristup APPC korisnika ciljnom sistemu

Kad sistemi uspostave APPC sesiju, kreiraju stazu za zahtijevanje korisnika da dohvati vrata ciljnog sistema. Nekoliko drugih elemenata određuje što korisnik mora da bi dobio ulaz u drugi sistem.

Poglavlja koja slijede opisuju elemente koji određuju kako APPC korisnik dobiva ulazak u ciljni sistem.

Sistemske metode slanja informacija o korisniku

APPC arhitektura omogućuje tri metode slanja sigurnosnih informacija o korisniku iz izvornog sistema na ciljni sistem. Ove se metode nazivaju **arhitekturne sigurnosne vrijednosti**. Tablica 18 pokazuje ove metode:

Bilješka: *APPC programiranje* knjiga daje još informacija o arhitekturnim sigurnosnim vrijednostima.

Tablica 18. Sigurnosne vrijednosti u APPC arhitekturi

arhitekturna sigurnosna vrijednost	Korisnički ID poslan ciljnom sistemu	Lozinka poslana ciljnom sistemu
Ništa	Ne	Ne
Isto	Da[1]	Pogledajte opasku 2.
Program	Da	Da[3]

Bilješke:

1. Izvorni sistem šalje ID korisnika ako ciljni sistem specificira SECURELOC(*YES) ili SECURELOC(*VFYENCPWD).
2. Korisnik ne unosi lozinku na zahtjev jer je lozinka već verificirana na izvornom sistemu. Za SECURELOC(*YES) i SECURELOC(*NO), izvorni sistem ne šalje lozinku. Za SECURELOC(*VFYENCPWD), izvorni sistem dohvaća pohranjenu, šifriranu lozinku te je šalje (u šifriranom obliku).
3. Sistem šalje lozinku u šifriranom obliku ako i izvorni i ciljni sistemi podržavaju šifriranje lozinke. Inače, lozinka nije šifrirana.

Aplikacija koju korisnik zahtijeva određuje arhitekturnu sigurnosnu vrijednost. Na primjer, SNADS uvijek koristi SECURITY(NONE). DDM koristi SECURITY(SAME). Sa prolaskom kroz ekran stanice, korisnik specificira sigurnosnu vrijednost upotrebom parametara u STRPASTHR naredbi.

U svim slučajevima, ciljni sistem bira da li će prihvatiti zahtjev sa sigurnosnom vrijednosti koja je specificirana u izvornom sistemu. U nekim situacijama, ciljni sistem može potpuno odbaciti zahtjev. U drugim situacijama, ciljni sistem može forsirati drugu sigurnosnu vrijednost. Na primjer, kad korisnik specificira i ID korisnika i lozinku u STRPASTHR naredbi, zahtjev koristi SECURITY(PGM). Međutim, ako je na ciljnom sistemu QRMTSIGN sistemska vrijednost *FRCSIGNON, korisnik još uvijek vidi ekran prijave. S postavkom *FRCSIGNON, sistemi uvijek koriste SECURITY(NONE), što je ekvivalent korisničkom ne upisivanju korisničkog ID-ja i lozinke u STRPASTHR naredbi.

Bilješke:

1. Izvorni i ciljni sistemi dogovaraju sigurnosnu vrijednost prije slanja podataka. U situaciji u kojoj ciljni sistem specificira SECURELOC(*NO) a zahtjev je SECURITY(SAME), na primjer, ciljni sistem govori izvornom sistemu da koristi SECURITY(NONE). Izvorni sistem ne šalje ID korisnika.
2. Ciljni sistem odbacuje zahtjev za sesijom kad istekne korisnička lozinka na ciljnom sistemu. Ovo se odnosi samo na zahtjeve za povezivanjem koji šalju lozinku, uključujući sljedeće:
   - Zahtjev za sesijom tipa SECURITY(PROGRAM).
   - Zahtjev za sesijom tipa SECURITY(SAME) kad je SECURELOC vrijednost *VFYENCPWD.

Opcije za podjelu odgovornosti mrežne sigurnosti

Kad vaš sistem sudjeluje na mreži, morate odlučiti da li ćete vjerovati provjeri valjanosti identiteta korisnika koji pokušava ući u vaš sistem, na drugom sistemu. Da li ćete vjerovati SYSTEMA da osigurate da je USERA stvarno USERA (ili da je QSECOFR stvarno QSECOFR)? Ili ćete tražiti da korisnik ponovo da ID korisnika i lozinku?

Parametar sigurne lokacije (SECURELOC) na opisu APPC uređaja na ciljnom sistemu specificira da li je izvorni sistem sigurna (pouzdana) lokacija.

Kad oba sistema izvode izdanje koje podržava *VFYENCPWD, SECURELOC(*VFYENCPWD) omogućuje dodatnu zaštitu kad aplikacije koriste SECURITY(SAME). Iako zahtjevatelj ne upisuje lozinku na zahtjev, izvorni sistem dohvaća lozinku korisnika i šalje je sa zahtjevom. Da bi zahtjev bio uspješan, korisnik mora imati isti korisnički ID i lozinku na oba sistema.

Kad ciljni sistem specificira SECURELOC(*VFYENCPWD) a izvorni sistem ne podržava ovu vrijednost, ciljni sistem rukuje zahtjevom kao SECURITY(NONE).

Tablica 19 pokazuje kako arhitekturna sigurnosna vrijednost i SECURELOC vrijednost funkcioniraju zajedno:

Tablica 19. Kako APPC sigurnosna vrijednost i SECURELOC vrijednost funkcioniraju zajedno

Izvorni sistem	**Ciljni sistem**	
arhitekturna sigurnosna vrijednost	**SECURELOC vrijednost**	**Korisnički profil za posao**
Ništa	Bilo koji	Defaultni korisnik[1]

Tablica 19. Kako APPC sigurnosna vrijednost i SECURELOC vrijednost funkcioniraju zajedno (nastavak)

Izvorni sistem	Ciljni sistem	
arhitekturna sigurnosna vrijednost	**SECURELOC vrijednost**	**Korisnički profil za posao**
Isto	*NO	Defaultni korisnik[1]
	*YES	Isto ime korisničkog profila kao zahtjevatelj iz izvornog sistema
	*VFYENCPWD	Isto ime korisničkog profila kao zahtjevatelj iz izvornog sistema. Korisnik mora imati istu lozinku na oba sistema.
Program	Bilo koji	Korisnički profil specificiran na zahtjev izvornog sistema.

Bilješke:

1. Defaultni je korisnik određen komunikacijskim unosom u opisu podsistema. “Dodjela korisničkih profila za poslove na ciljnom sistemu” opisuje ovo.

Dodjela korisničkih profila za poslove na ciljnom sistemu

Kad korisnik zahtijeva APPC posao na drugom sistemu, zahtjevu je pridruženo ime načina. Ime načina može doći od korisničkog zahtjeva ili može biti defaultna vrijednost od mrežnih atributa izvornog sistema.

Ciljni sistem koristi ime načina i ime uređaja APPC za određivanje kako će se posao izvoditi. Ciljni sistem pretražuje aktivne podsisteme za komunikacijski unos koji se najbolje podudara s imenom APPC uređaja i imena načina.

Komunikacijski unos specificira koje će korisničke profile sistem koristiti za SECURITY(NONE) zahtjeve. Slijedi primjer komunikacijskog unosa u opis podsistema:

```
                      Prikaz komunikacijskih Unosa

Opis podsistema:      QCMN          Status:   ACTIVE

                       Posao                      Default        Max
Uređaj       Način     Opis          Knjižnica    Korisnik     Aktivnost
*ALL         *ANY      *USRPRF                    *SYS         *NOMAX
*ALL         QPCSUPP   *USRPRF                    *NONE        *NOMAX
```

Tablica 20 pokazuje moguće vrijednosti za defaultne korisničke parametre u komunikacijskom unosu:

Tablica 20. Moguće vrijednosti za defaultni korisnički parametar

Vrijednost	Rezultat
***NONE**	Nikakav defaultni korisnik nije dostupan. Ako izvorni sistem ne dobavi ID korisnika na zahtjev, posao se neće izvoditi.
***SYS**	Samo će se IBM dobavljeni programi (sistemski poslovi) izvoditi. Nikakva se korisnička aplikacija neće izvoditi.
ime-korisnika	Ako izvorni sistem ne šalje ID korisnika, posao se izvodi pod ovim korisničkim profilom.

Možete koristiti naredbu Ispis opisa podsistema (PRTSBSDAUT) za ispis liste svih podsistema koji imaju komunikacijske ulaze s defaultnim korisničkim profilom.

Opcije prolaza-kroz ekranske stanice

Prolaz-kroz ekranske stanice je primjer aplikacije koja koristi APPC komunikacije. Možete koristiti prolaz-kroz ekranske stanice za prijavu na drugi sistem koji je povezan na vaš sistem kroz mrežu.

Tablica 21 pokazuje primjere zahtjeva za prolaz-kroz (STRPASTHR naredba) i kako ciljni sistem rukuje istima. Za prolaz-kroz ekranske stanice, sistem koristi osnovne elemente APPC komunikacija i sistemsku vrijednost udaljene prijave (QRMTSIGN).

Bilješka: Zahtjevi za prolaz-kroz ekranske stanice se više ne usmjeravaju kroz QCMN ili QBASE podsisteme. Počevši od V4R1, oni se usmjeravaju kroz QSYSWRK podsistem. Prije V4R1 mogli ste pretpostaviti da bez pokretanja QCMD ili QBASE podsistema, Prolaz-kroz ekransku stanicu ne bi radio. To više nije istina. Možete forsirati Prolaz-kroz ekransku stanicu da ide kroz QCMN (ili QBASE ako je aktivan) promjenom QPASTHRSVR sistemske vrijednosti na 0.

Tablica 21. Uzorak zahtjeva za prijavu za prolaz-kroz

Vrijednosti u STRPASTHR naredbi		**Ciljni sistem**		
Korisnički ID	**Lozinka**	**SECURELOC vrijednost**	**QRMTSIGN vrijednost**	**rezultat**
*NONE	*NONE	Bilo koji	Bilo koji	Korisnik se mora prijaviti u ciljni sistem.
Ime korisničkog profila	Nije upisano	Bilo koji	Bilo koji	Zahtjev ne uspijeva.
*CURRENT	Nije upisano	*NO	Bilo koji	Zahtjev ne uspijeva
		*YES	*SAMEPRF	Interaktivan posao počinje s istim imenom korisničkog profila kao i korisnički profil u izvorišnom sistemu. Nijedna lozinka se ne propušta na udaljeni sistem. Ime korisničkog profila mora postojati u ciljnom sistemu.
			*VERIFY	
			*FRCSIGNON	Korisnik se mora prijaviti u ciljni sistem.
		*VFYENCPWD	*SAMEPRF	Interaktivan posao počinje s istim imenom korisničkog profila kao i korisnički profil u izvorišnom sistemu. Izvorišni sistem dohvaća korisničku lozinku i šalje ju udaljenom sistemu. Ime korisničkog profila mora postojati u ciljnom sistemu.
			*VERIFY	
			*FRCSIGNON	Korisnik se mora prijaviti u ciljni sistem.

Tablica 21. Uzorak zahtjeva za prijavu za prolaz-kroz (nastavak)

Vrijednosti u STRPASTHR naredbi		Ciljni sistem		
Korisnički ID	**Lozinka**	**SECURELOC vrijednost**	**QRMTSIGN vrijednost**	**rezultat**
*CURRENT (ili ime trenutnog korisničkog profila za posao)	Upisano	Bilo koji	*SAMEPRF	Interaktivan posao počinje s istim imenom korisničkog profila kao i korisnički profil u izvorišnom sistemu. Lozinka *je* poslana na udaljeni sistem. Ime korisničkog profila mora postojati u ciljnom sistemu.
			*VERIFY	
			*FRCSIGNON	Korisnik se mora prijaviti u ciljni sistem.
Ime korisničkog profila (ime različito od trenutnog korisničkog profila za posao)	Upisano	Bilo koji	*SAMEPRF	Zahtjev ne uspijeva.
			*VERIFY	Interaktivan posao počinje s istim imenom korisničkog profila kao i korisnički profil u izvorišnom sistemu. Lozinka *je* poslana na udaljeni sistem. Ime korisničkog profila mora postojati u ciljnom sistemu.
			*FRCSIGNON	Interaktivan posao počinje sa specificiranim imenom korisničkog profila. Lozinka se šalje na ciljni sistem. Ime korisničkog profila mora postojati na ciljnom sistemu.

Izbjegavanje neočekivanih dodjela uređaja

Kad se desi greška na aktivnom uređaju, sistem se pokušava obnoviti. U nekim okolnostima, kad je veza prekinuta, drugi korisnik može nenamjerno ponovo uspostaviti sesiju koja je imala grešku. Na primjer, pretpostavimo da je USERA isključio radnu stanicu bez odjavljivanja. USERB bi mogao uključiti radnu stanicu i ponovo početi sesiju USERA bez prijavljivanja.

Da spriječite ovu mogućnost, postavite sistemsku vrijednost Akcije greške I/O uređaja (QDEVRCYACN) na *DSCMSG. Kad uređaj ne uspije, sistem će završiti posao korisnika.

Kontrola udaljenih naredbi i paketnih poslova

Dostupno je nekoliko opcija za pomoć u kontroli onog što udaljene naredbe i poslovi mogu izvoditi na vašem sistemu, uključujući sljedeće:

- Ako vaš sistem koristi DDM, možete ograničiti pristup na DDM datoteke da spriječite da korisnici koriste naredbu Submit udaljene naredbe (SBMRMTCMD) iz drugog sistema. Za korištenje SBMRMTCMD, korisnik mora moći otvoriti DDM datoteku. Također trebate ograničiti sposobnost kreiranja DDM datoteka.
- Možete specificirati izlazni program za sistemsku vrijednost pristupa DDM zahtjeva (DDMACC). U izlaznom programu, možete procijeniti sve DDM zahtjeve prije dozvoljavanja istih.
- Možete koristiti mrežni atribut akcije mrežnog posla (JOBACN) da spriječite da se mrežni poslovi šalju na izvođenje ili da spriječite njihovo automatsko izvođenje.

- Možete izričito specificirati koji programski zahtjevi se mogu izvoditi u komunikacijskom okruženju uklanjanjem PGMEVOKE usmjeravanja unosa iz opisa podsistema. PGMEVOKE unos za usmjeravanje omogućuje zahtjevatelju specificiranje programa koji se izvodi. Kad uklonite ovaj unos iz opisa podsistema, kao što je opis QCMN podsistema, morate dodati unose usmjeravanja za komunikacijske zahtjeve koji se trebaju uspješno izvesti.

  "Zahtjevi arhitekturnih TPN-ova" na stranici 78 ispisuje imena programa za komunikacijske zahtjeve s IBM dobavljenim aplikacijama. Za svaki zahtjev koji želite dozvoliti, možete dodati unos za usmjeravanje s vrijednosti usporedbe i imenom programa koji su oba jednaka imenu programa.

  Kad koristite ovu metodu, trebate razumjeti okruženje upravljanja poslom na vašem sistemu i tipove komunikacijskih zahtjeva koji se mogu desiti na vašem sistemu. Ako je moguće, trebali bi provjeriti sve tipove komunikacijskih zahtjeva da osigurate da ispravno rade nakon što ste promijenili unose za usmjeravanje. Kad komunikacijski zahtjev ne nađe dostupan unos za usmjeravanje, vi primite CPF1269 poruku. Druga je alternativa (manja sklonost greškama ali možda neznatno manja učinkovitost) je postavljanje javnog ovlaštenja na *EXCLUDE za transakcijske programe koje ne želite da se izvode na vašem sistemu.

  Bilješka: Knjiga *Upravljanje poslom* daje još informacija o unosima usmjeravanja i kako sistem rukuje zahtjevima za pokretanje programa.

Procjena vaše APPC konfiguracije

Možete koristiti naredbu Ispis komunikacijske sigurnosti (PRTCMNSEC) opcije izbornika da ispišete vrijednosti relevantne za sigurnost u vašoj APPC konfiguraciji. Poglavlja koja slijede opisuju informacije o izvještajima.

Relevantni parametri za APPC uređaje

Slika 9 pokazuje primjer Izvještaja komunikacijskih informacija za opise uređaja. Slika 10 na stranici 101 pokazuje primjer izvještaja za konfiguracijske liste. Iza izvještaja slijede objašnjenja polja u izvještaju.

```
                          Komunikacijske Informacije (Potpun izvještaj)
                                                                                SYSTEM4
Tip objekta  . . . . . . . . . :   *DEVD
                                                                                    Pre           SNUF
Objekt         Objekt        Uređaj          Siguran     Lokacija      APPN       Jednostruk  Postav        Program
Ime            Tip           Kategorija      Lokacija    Lozinka       Sposoban   Sesija       Sesija        Start

CDMDEV1        *DEVD         *APPC             *NO         *NO          *NO         *YES         *NO
CDMDEV2        *DEVD         *APPC             *NO         *NO          *NO         *YES         *NO
```

Slika 9. Opisi-primjer izvještaja APPC uređaja

```
                  Prikaz Konfiguracijske liste                    Stranica 1
                            SYSTEM4  12/17/95  07:24:36
Konfiguracijska lista. . . . . . . :   QAPPNRMT
Tip konfiguracijske liste. . . . . :   *APPNRMT
Tekst. . . . . . . . . . . . . . . :
-----------------APPN udaljene lokacije-----------------
          ID                  Udaljena  ID mreže
Udaljena  udaljene  Lokalna   kontrol.  kontrol.  Sigurna
lokacija  mreže     lokacija  točka     točke     lokac.
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 udaljene lokacije-----------------
          ID                                        Lokalna      Pred-
Udaljena  udaljene  Lokalna   Jednostruka     Broj   kontrol.  uspostavljena
lokacija  mreže     lokacija   sesija      razgovora  točka       sesija
SYSTEM36  APPN      SYSTEM4    *NO             10      *NO        *NO
SYSTEM32  APPN      SYSTEM4    *NO             10      *NO        *NO
```

Slika 10. Izvještaj-primjer Konfiguracijska lista

Polje sigurne lokacije

Polje sigurne lokacije (SECURELOC) specificira da li lokalni sistem vjeruje udaljenom sistemu tako da radi provjeru lozinke u ime lokalnog sistema. SECURELOC polje primjenjuje se samo na aplikacije koje koriste vrijednost SECURITY(SAME), kao što je DDM i aplikacije koje koriste CPI-komunikacijski API.

SECURELOC(*YES) čini lokalni sistem ranjivim na moguće slabosti u udaljenom sistemu. Bilo koji korisnik koji postoji na oba sistema može pozvati programe na lokalnom sistemu. Ovo je osobito opasno zato jer korisnički profil QSECOFR (službenik sigurnosti) postoji na svim iSeries sistemima i ima *ALLOBJ posebno ovlaštenje. Ako sistem u mreži ne radi dobar posao zaštite QSECOFR lozinke, drugi sistemi koji tretiraju taj sistem kao sigurnu lokaciju su na riziku.

Kada koristite SECURELOC(*VFYENCPWD), vaš sistem je manje ranjiv nego drugi sistemi koji ne zaštićuju prikladno lozinke. Korisnik koji zahtijeva aplikaciju koja koristi SECURITY(SAME) mora imati isti korisnički ID i lozinku na oba sistema. SECURELOC(*VFYENCPWD) zahtijeva administracijske politike za lozinku po vašoj mreži tako da korisnici imaju istu lozinku na svim sistemima.

Bilješka: SECURELOC(*VFYENCPWD) je podržan samo između sistema koji izvode V3R2, V3R7 ili V4R1. Ako ciljni sistem specificira SECURELOC(*VFYENCPWD) i izvorišni sistem ne podržava ovu funkciju, zahtjev se tretira kao SECURITY(NONE).

Ako sistem specificira SECURELOC(*NO), aplikacije koje koriste SECURITY(SAME) će trebati defaultnog korisnika da izvedu programe. Defaultni korisnik ovisi i o opisu uređaja i o načinu koji je pridružen zahtjevu. (Pogledajte “Dodjela korisničkih profila za poslove na ciljnom sistemu” na stranici 97.)

Polje lozinke lokacije

Polje lozinke lokacije određuje da li će dva sistema izmijeniti lozinke da provjere da li su sistemi koji zahtijevaju varajući sistemi. “Primjer: Osnovna APPC sesija” na stranici 94 pruža više informacija o lozinkama lokacije.

APPN Sposobno polje

APPN-sposobno (APPN) polje specificira da li udaljeni sistem može podržavati funkcije napredne mreže ili je ograničen na povezivanje s jednim skokom. APPN(*YES) znači sljedeće:

- Ako je udaljeni sistem mrežni čvor, udaljeni sistem može povezati lokalni sistem s drugim sistemima. Ovo se zove **posredno usmjeravanje čvora** . To znači da korisnici na vašem sistemu mogu koristiti udaljeni sistem kao put do veće mreže.
- Ako je lokalni sistem mrežni čvor, udaljeni sistem može koristiti lokalni za povezivanje na druge sisteme. Korisnici na udaljenom sistemu mogu koristiti vaš sistem kao smjer do velikih mreža.

Bilješka: Možete koristiti naredbu DSPNETA da odredite da li je sistem mrežni čvor ili krajnji čvor.

Polje jednostruke sesije

Polje jednostruke sesije (SNGSSN) specificira da li udaljeni sistem može izvoditi više nego jednu sesiju u istom vremenu koristeći isti opis APPC uređaja. SNGSSN(*NO) se obično koristi jer eliminira potrebu za višestrukim opisima uređaja za udaljeni sistem. Na primjer, PC korisnik često želi više od jedne 5250-emulacija sesije i sesija za funkcije Fileservera i Printservera. Sa SNGSSN(*NO), možete pružiti ovu funkciju s jednim opisom uređaja za PC na iSeries sistemu.

SNGSSN(*NO) znači da se morate pouzdati na sigurnosno-svjesne operacijske procedure za PC korisnike i druge APPC korisnike. Vaš sistem je ranjiv za nekog na udaljenom sistemu tko pokreće neovlaštenu sesiju koja koristi neki opis uređaja kao postojeću sesiju. (Na ovu praksu se katkada odnosi kao na **piggy-backing**.)

Polje pred-postavljene sesije

Polje pred-postavljene sesije (PREESTSSN) za uređaj jednostruke sesije kontrolira da li lokalni sistem pokreće sesiju s udaljenim sistemom kada udaljeni sistem prvi kontaktira lokalni sistem. PREESTSSN(*NO) znači da lokalni sistem čeka da pokrene sesiju dok aplikacija zahtijeva sesiju sa sistemom. PREESTSSN(*YES) je koristan za smanjivanje kako dugo treba aplikacijskom programu da dovrši povezivanje.

PREESTSSN(*YES) spriječava sistem od prekidanja komutirane (birane) linije koja se više ne koristi. Aplikacija ili korisnik moraju izričito staviti liniju u stanje vary off. PREESTSSN(*YES) može produžiti vrijeme u kojem je lokalni sistem ranjiv na piggy-backing sesije.

Polje pokretanje SNUF programa

Polje pokretanje SNUF programa specificira da li je udaljenom sistemu dozvoljeno pokretanje programa na lokalnom sistemu. *YES znači shema ovlaštenja objekta na lokalnom sistemu mora biti prikladna da zaštiti objekte kada korisnici na udaljenom sistemu pokreću programe i izvode programe na lokalnom sistemu.

Parametri za APPC kontrolere

Slika 11 na stranici 103 pokazuje primjer Izvještaja komunikacijskih informacija za opise kontrolera. Iza izvještaja naći ćete objašnjenja polja u izvještaju.

```
                          Komunikacijske informacije (Potpuni izvještaj)
                                                                                SYSTEM4
Tip objekta. . . . . . . . . . :   *CTLD

Ime       Tip       Kategorija    Auto    Komutirani     Smjer      APPN        CP      Timer    Brisanje Ime
objekta   objekta   kontrolera    kreir.  kontroler      poziva   sposobno    sesije odspaj.  sekundi uređaja
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
```

Slika 11. Uzorak izvještaja Opisi APPC kontrolera

Polje auto-kreiraj

Na opisu linije, polje auto-kreiraj (AUTOCRTCTL) specificira da li lokalni sistem automatski kreira opis kontrolera kada nadolazeći zahtjev ne može naći opis kontrolera koji se podudara. U opisu kontrolera, polje auto-kreiraj (AUTOCRTDEV) specificira da li lokalni sistem automatski kreira opis uređaja kada dolazeći zahtjev ne može naći podudarajući opis uređaja.

Za kontrolere koji su APPN-sposobni, polje auto-kreiraj nema učinka. Sistem automatski kreira opis uređaja kada je potrebno, bez obzira kako postavite polje auto-kreiraj.

Kada specificirate *YES za opis linije, svatko s pristupom liniji može se povezati na vaš sistem. Ovo uključuje stranice koje su povezane mostovima i usmjerivačima.

Polje sesija kontrolne točke

Za APPN-sposobne kontrolere, polje sesija kontrolne točke (CPSSN) kontrolira da li sistem automatski uspostavlja APPC povezivanje s udaljenim sistemom. Sistem koristi CP sesiju za zamjenu mrežnih informacija i stanja s udaljenim sistemom. Izmjena suvremenih informacija između APPN mrežnih čvorova je osobito važna da vaša mreže može glatko funkcionirati.

Kada specificirate *YES, nezaposlena komutirana linija se ne odspaja automatski. Ovo čini vaš sistem ranjivijim na piggy-back sesije.

Polje timera odspajanja

Za APPC kontrolere, polje timera odspajanja specificira kako dugo kontroler mora biti nekorišten (bez aktivnih sesija) prije nego sistem odspoji liniju do udaljenog sistema. Ovo polje ime dvije vrijednosti. Prva vrijednost specificira kako dugo će kontroler ostati aktivan od vremena kad je početno kontaktiran. Druga vrijednost određuje kako dugo sistem čeka nakon što je zadnja sesija završila prije nego sistem ispusti liniju.

Sistem koristi timer odspajanja samo kada je polje komutirano odspajanje (SWTDSC) *YES.

Ako povećate ovu vrijednost, vaš sistem je ranjiviji na piggy-back sesije

Parametri za opise linije

Slika 12 na stranici 104 pokazuje primjer Izvještaja komunikacijskih informacija za opise linije. Iza izvještaja naći ćete objašnjenja polja u izvještaju.

```
                          Komunikacijske informacije (Potpuni izvještaj)

Tip objekta. . . . . . . . . . :   *LIND
Ime
auto            Tip           Kategorija      Auto      Brisanje     Auto      Auto
objekta         objekta         linije       kreiraj    sekunde     odgovor    biraj
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
```

Slika 12. Uzorak izvještaja Opisi APPC linija

Polje auto odgovora

Polje auto odgovora (AUTOANS) specificira da li će komutirana linija prihvatiti dolazeće pozive bez intervencije operatora.

Kada specificirate *YES, vaš sistem je manje siguran jer mu se može lakše pristupiti. Da smanjite sigurnosno izlaganje kada specificirate *YES, trebate staviti liniju u stanje vary off kada ju trebate.

Polje automatskog biranja

Polje automatskog biranja (AUTODIAL) specificira da li komutirana linija može činiti izlazne pozive bez intervencije operatera. Kada specificirate *YES, dozvoljavate lokalnim korisnicima koji nemaju fizički pristup komunikacijskim linijama i modemima da se povežu na druge sisteme.

Poglavlje 13. Sigurne TCP/IP komunikacije

TCP/IP (Transmission Control Protocol/Internet Protocol) je zajednički način na koji računala svih tipova međusobno komuniciraju. TCP/IP aplikacije su dobro poznate i široko korištene kroz "informacijski put".

Ovo poglavlje daje savjete za sljedeće:

- Spriječavanje da se TCP/IP aplikacije izvode na vašem sistemu.
- Zaštita sistemskih resursa kad dozvolite TCP/IP aplikacijama izvođenje na vašem sistemu.

iSeries Informacijski Centar—>Mrežni rad—>TCP/IP Web stranica je potpun izvor informacija o svim TCP/IP aplikacijama. *SecureWay: iSeries i Internet* (iSeries Informacijski Centar—>Sigurnost—>SecureWay opisuje razmatranja o sigurnosti kad povežete vašeg iSeries poslužitelja ili na Internet (jako velika TCP/IP mreža) ili Intranet. Pogledajte "Preduvjeti i povezane informacije" na stranici xii za informacije o pristupu iSeries Informacijskom Centru.

Zapamtite da iSeries poslužitelji podržavaju mnoge moguće TCP/IP aplikacije. Kad odlučite dozvoliti jednu TCP/IP aplikaciju na vašem sistemu, možda također omogućujete i druge TCP/IP aplikacije. Kao administrator sigurnosti, trebate biti svjesni dosega TCP/IP aplikacija i sigurnosnih implikacija ovih aplikacija.

Spriječavanje TCP/IP obrade

Poslovi TCP/IP poslužitelja se izvode u QSYSWRK podsistemu. Koristite naredbu Pokretanje TCP/IP (STRTCP) za pokretanje TCP/IP-a na vašem sistemu. Ako ne želite da se izvode nikakve TCP/IP obrade ili aplikacije, ne koristite STRTCP naredbu. Vaš sistem se isporučuje s javnim ovlaštenjem za STRTCP naredbu postavljenim na *EXCLUDE.

Ako sumnjate da netko s pristupom naredbi pokreće TCP/IP (za vrijeme neradnih sati, na primjer), možete postaviti reviziju objekta u STRTCP naredbi. Sistemska će napisati unos u dnevnik revizije uvijek kad korisnik izvede naredbu.

Komponente TCP/IP sigurnosti

Možete iskoristiti prednost nekoliko TCP/IP sigurnosnih komponenata koje povećavaju sigurnost i fleksibilnost vaše mreže. Iako se neke od ovih tehnologija također mogu naći u proizvodima vatrenog zida, ove komponente TCP/IP sigurnosti za OS/400 nisu namijenjene da se koriste kao vatreni zid. Međutim, vi možete koristiti neka od ovih svojstava, u nekim instancama da eliminirate potrebu za odijeljenim proizvodima vatrenog zida. Također možete koristiti ova TCP/IP svojstva da omogućite dodatnu sigurnost u okruženjima u kojima već koristite vatreni zid.

Sljedeće komponente se mogu iskoristiti za povećanje TCP/IP sigurnosti:

- Pravila paketa
- HTTP Proxy poslužitelj
- VPN (virtualno privatno umrežavanje)
- SSL (sloj sigurnih utičnica)

© Autorska prava IBM Corp. 1996, 2004

Upotreba pravila paketa za osiguranje TCP/IP prometa

Pravila paketa, što je kombinacija IP filtriranja i prijevoda mrežne adrese (NAT) djeluje kao vatreni zid za zaštitu vaše interne mreže od uljeza. IP filtriranje vam dozvoljava kontrolu IP prometa koji može ulaziti i izlaziti iz vaše mreže. U osnovi, ono zaštićuje vašu mrežu filtriranjem paketa na osnovi pravila koja vi definirate. NAT, međutim, dozvoljava da sakrijete vaše neregistrirane privatne IP adrese iza skupa registriranih IP adresa. Ovo pomaže u zaštiti vaše interne mreže od vanjskih mreža. NAT također pomaže ublažiti problem iscrpljivanja IP adresa, budući da se mnoge privatne adrese mogu predstaviti malim skupom registriranih adresa. Pogledajte iSeries Informacijski Centar za još detalja.

HTTP proxy poslužitelj

HTTP proxy poslužitelj dolazi s IBM HTTP poslužiteljem za iSeries poslužitelj. HTTP poslužitelj je dio OS/400. Proxy poslužitelj prima HTTP zahtjeve od Web pretražitelja i šalje ih ponovo Web poslužiteljima. Web poslužitelji koji prime zahtjeve, svjesni su samo IP adrese proxy poslužitelja i ne mogu odrediti imena ili adrese PC-a koji su izvorni za zahtjeve. Proxy poslužitelj može rukovati URL zahtjevima za HTTP, FTP, Gopher i WAIS.

Proxy poslužitelj stavlja u predmemoriju vraćene Web stranice koje su napravili svi korisnici proxy poslužitelja. Kao posljedica, kada korisnici zahtijevaju stranicu, proxy poslužitelj provjerava da li je stranica u predmemoriji. Ako je, proxy poslužitelj vraća tu uhvaćenu stranicu. Korištenjem stranica stavljenih u predmemoriju, proxy poslužitelj je sposoban poslužiti Web stranice brže, što eliminira potencijalne zahtjeve koji troše vrijeme za Web poslužitelj.

Proxy poslužitelj može također zapisati sve URL zahtjeve u svrhu praćenja. Tada možete pregledati dnevnike radi nadgledanja upotrebe i krive upotrebe mrežnih resursa.

Možete koristiti podršku za HTTP proxy poslužitelj u IBM HTTP poslužitelju da konsolidirate Web pristup. Adrese PC klijenata su skrivene od Web poslužitelja koje posjećuju; samo IP adresa proxy poslužitelja je poznata. Stavljanje u predmemoriju Web stranica također smanjuje zahtjeve za komunikacijskom pojasnom širinom i radno opterećenje vatrenog zida. Pogledajte IBM HTTP poslužitelj za iSeries Početnu stranicu za više informacija: http://www-1.ibm.com/servers/eserver/iseries/software/http/index.html

Virtualno privatno umrežavanje (VPN)

Virtualna privatna mreža (VPN) omogućuje vašem poduzeću sigurno proširivanje svojeg privatnog Intraneta preko postojeće građe javne mreže, kao što je Internet. Sa VPN-om, vaše poduzeće može kontrolirati mrežni promet dok omogućuje važna sigurnosna svojstva kao što je provjera autentičnosti i privatnost podataka.

OS/400 VPN je komponenta koju se ne mora instalirati od iSeries Navigator, grafičkog korisničkog sučelja (GUI) za OS/400. Ona vam omogućava kreiranje sigurne staze s kraja na kraj između bilo koje kombinacije hostova i gatewaya. OS/400 VPN koristi metode provjere autentičnosti, algoritme šifriranja i druge mjere kako bi se osiguralo da podaci poslani između dvije krajnje točke njegove veze ostanu sigurni.

VPN se izvodi na mrežnom sloju modelu stoga TCP/IP slojnih komunikacija. Specifično, VPN koristi IP sigurnosnu arhitekturu (IPSec) otvorene građe. IPSec daje osnovne sigurnosne funkcije za Internet, kao što i osigurava fleksibilne gradbene blokove od kojih možete kreirati robusne, sigurne virtualne privatne mreže.

VPN podržava VPN rješenje Layer 2 Tunnel Protocol (L2TP). L2TP veze, koje se još nazivaju virtualne linije, daju isplativ pristup za udaljene korisnike dozvoljavanjem

korporativnim mrežama upravljanje IP adresama dodijeljenih njegovim udaljenim korisnicima. Dalje, L2TP veze omogućuju siguran pristup vašem sistemu ili mreži kad ih zaštitite s IPSec-om.

Važno je da razumijete utjecaj koji će VPN imati na cijelu vašu mrežu. Prikladno planiranje i implementacija su bitni za vaš uspjeh. Trebali bi ponovo pregledati VPN poglavlje u iSeries Informacijskom Centru da osigurate da znate kao VPN-ovi rade i kako ih možete koristiti. Za još informacija, pogledajte iSeries Informacijski Centar—>Sigurnost—>Virtualno privatno umrežavanje. Pogledajte “Preduvjeti i povezane informacije” na stranici xii za informacije o pristupu iSeries Informacijskom Centru.

Sloj sigurnih utičnica (SSL)

Sloj sigurnih utičnica (SSL) je postao industrijski standard za omogućavanje aplikacija za sigurne komunikacijske sesije preko nezaštićene mreže, kao što je Internet. SSL protokol uspostavlja sigurno povezivanje između aplikacija klijenta i poslužitelja što omogućuje provjeru autentičnosti za jednu ili obje krajnje točke komunikacijske sesije. SSL također daje privatnost i integritet podacima koje aplikacije klijenta i poslužitelja zamjenjuju. Za više informacija, pogledajte iSeries Informacijski Centar–>Sigurnost—>Sloj sigurnih utičnica (SSL). Pogledajte “Preduvjeti i povezane informacije” na stranici xii za informacije o pristupu iSeries Informacijskom Centru.

Osiguravanje vaše TCP/IP okoline

Ovo poglavlje osigurava općenite prijedloge za korake koje možete poduzeti da smanjite sigurnosna izlaganja u TCP/IP okolini na vašem sistemu. Ovi savjeti se primjenjuju na vašu čitavu TCP/IP okolinu prije nego na specifične aplikacije koje su objašnjene u poglavljima koja slijede.

- Kada pišete aplikaciju za TCP/IP port, uvjerite se da je aplikacija ispravno osigurana. Trebate pretpostaviti da netko izvana može pokušati pristupiti toj aplikaciji preko tog porta. Netko izvana s dobrim znanjem može pokušati TELNET tu aplikaciju.
- Nadgledajte upotrebu TCP/IP portova na vašem sistemu. Korisnička aplikacija koja je povezana s TCP/IP portom može osigurati ulaz na “stražnja vrata” u vaš sistem bez korisničkog ID-a ili lozinke. Netko s dovoljnim ovlaštenjem na vašem sistemu može pridružiti aplikaciju bez TCP ili UDP porta.
- Kao sigurnosni administrator, trebate biti svjesni tehnike nazvane *IP obmana* koju koriste hakeri. Svaki sistem u TCP/IP mreži ima IP adresu. Netko tko koristi IP obmanu postavlja sistem (obično PC) da se pretvara da je postojeća IP adresa ili povjerljiva IP adresa. Stoga, varalica može uspostaviti vezu s vašim sistemom pretvarajući se da je sistem s kojim vi inače kontaktirate.

  Ako izvoditi TCP/IP na vašem sistemu i vaš sistem sudjeluje u mreži koja nije fizički zaštićena (sve neuključene linije i predefinirane veze), vi ste osjetljivi na IP obmanu. Da zaštite vaš sistem od štete od “obmane ”, krenite s prijedlozima u ovom poglavlju, kao što je zaštita prijave i sigurnost objekta. Trebate također osigurati da sistem ima prihvatljivo postavljene granice pomoćne memorije. Ovo spriječava prevaranta od preplavljanja vašeg sistema s poštom ili spool datotekama do točke u kojoj vaš sistem postaje nedjelotvoran.

  Dodatno, trebate redovito nadgledati TCP/IP aktivnost na vašem sistemu. Ako otkrijete IP obmanu, možete probati otkriti slabe točke u vašoj TCP/IP postavci i napraviti prilagodbu.
- Za vaš intranet (mreža sistema koja se ne treba povezivati direktno van), koristite IP adrese koje se mogu ponovo koristiti. Adrese koje se mogu ponovo koristiti su namijenjene za korištenje u privatnim mrežama. Internet backbone ne usmjerava pakete koji imaju IP adresu koja se može ponovo koristiti. Stoga, adrese koje se mogu ponovo koristiti osiguravaju dodani sloj zaštite unutar vašeg vatrenog zida.

iSeries Informacijski Centar—>Umrežavanje—>TCP/IP Web stranica osigurava informacije o tome kako su IP adrese dodijeljene i o rasponima IP adresa, kao i sigurnosne informacije o TCP/IP-u.

- Ako razmatrate povezivanje vašeg sistema na Internet ili intranet, pregledajte sigurnosne informacije na *SecureWay: iSeries i Internet* (iSeries Informacijskom Centru—>Sigurnost—>SecureWay). Pogledajte"Preduvjeti i povezane informacije" na stranici xii za informacije o pristupu iSeries Informacijskom Centru.

Kontrola koju TCP/IP poslužitelji pokreću automatski

Kao sigurnosni administrator, trebate kontrolirati koje se TCP/IP aplikacije pokreću automatski kada pokrenete TCP/IP. Dostupne su dvije naredbe za pokretanje TCP/IP-a. Za svaku naredbu, sistem koristi različitu metodu da odredi koje aplikacije (poslužitelji) da pokrene.

Tablica 22 pokazuje dvije naredbe i sigurnosne preporuke za njih. Tablica 23 pokazuje vrijednosti defaultnog autostarta za poslužitelje. Da promijenite autostart vrijednost za poslužitelj, koristite naredbu CHGxxxA (Promijeni xxx atribute) za poslužitelj. server. Na primjer, naredba za TELNET je CHGTELNA.

Tablica 22. Kako TCP/IP naredbe određuju koje poslužitelje pokrenuti

Naredba	Koje poslužitelje pokrenuti	Sigurnosne preporuke
Pokreni TCP/IP (STRTCP)	Sistem pokreće svaki poslužitelj koji specificira AUTOSTART(*YES). Tablica 23 pokazuje otpremljenu vrijednost za svaki TCP/IP poslužitelj.	• Pridružite *IOSYSCFG posebno ovlaštenje pažljivo za kontrolu tko može promijeniti autostart postavke. • Pažljivo kontrolirajte tko ima ovlaštenje za upotrebu naredbe STRTCP. Defaultno javno ovlaštenje za naredbu je *EXCLUDE. • Postavite reviziranje objekta za naredbu Promijeni *ime-poslužitelja* atribute (kao što je CHGTELNA) da nadgledate korisnike koji pokušaju promijeniti AUTOSTART vrijednost za poslužitelj.
Pokreni TCP/IP Poslužitelj (STRTCPSVR)	Koristite parametar da specificirate koje poslužitelje da pokrenete. Defaultno kada se ova naredba otprema je da se pokreću svi poslužitelji.	• Koristite naredbu Promjena default naredbe (CHGCMDDFT) da postavite naredbu STRTCPSVR da pokrenete samo određeni poslužitelj. Ovo ne zaštićuje korisnike od pokretanja drugih poslužitelja. Međutim, promjenom defaulta naredbe, smanjujete mogućnost da će korisnici pokrenuti slučajno sve poslužitelje. Na primjer, koristite sljedeću naredbu da postavite default da pokrenete samo TELNET poslužitelj:CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*TELNET)') **Bilješka:** Kada promijenite defaultnu vrijednost, možete specificirati samo pojedinačni poslužitelj. Izaberite ili poslužitelj koji koristite redovito ili poslužitelj koji ima najmanju vjerojatnost da uzrokuje sigurnosno izlaganje (kao što je TFTP). • Pažljivo kontrolirajte tko ima ovlaštenje za upotrebu naredbe STRTCPSVR. Defaultno javno ovlaštenje za naredbu je *EXCLUDE.

Sljedeća tablica sadrži autostart vrijednosti za TCP/IP poslužitelje. Za više informacija o svakom od ovih poslužitelja, pogledajte iSeries Informacijski Centar (**Umrežavanje—>TCP/IP**). Pogledajte"Preduvjeti i povezane informacije" na stranici xii za detalje o pristupu iSeries Informacijski Centar.

Tablica 23. Autostart vrijednosti za TCP/IP poslužitelj

Poslužitelj	Defaultna vrijednost	Vaša vrijednost
TELNET	AUTOSTART(*YES)	
FTP (file transfer protocol)	AUTOSTART(*YES)	

Tablica 23. Autostart vrijednosti za TCP/IP poslužitelj (nastavak)

Poslužitelj	Defaultna vrijednost	Vaša vrijednost
BOOTP (Protokol za podizanje sistema)	AUTOSTART(*NO)	
TFTP (trivial file transfer protocol)	AUTOSTART(*NO)	
REXEC (Udaljeni EXECution poslužitelj)	AUTOSTART(*NO)	
RouteD (Demon smjera)	AUTOSTART(*NO)	
SMTP (simple mail transfer protocol)	AUTOSTART(*YES)	
POP (Protokol poštanskog ureda)	AUTOSTART(*NO)	
HTTP (Hypertext Transfer Protocol) [1]	AUTOSTART(*NO)	
ICS (Poslužitelj Internet povezivanja)[1]	AUTOSTART(*NO)	
LPD (Demon pisača linije)	AUTOSTART(*YES)	
SNMP (Jednostavni protokol za upravljanje mrežom (SNMP))	AUTOSTART(*YES)	
DNS (Sistem imena domene)	AUTOSTART(*NO)	
DDM	AUTOSTART(*NO)	
DHCP (dynamic host configuration protocol)	AUTOSTART(*NO)	
NSMI	AUTOSTART(*NO)	
INETD	AUTOSTART(*NO)	

Bilješke:

1. S IBM HTTP Poslužiteljem za iSeries poslužitelj, koristite naredbu CHGHTTPA da postavite AUTOSTART vrijednost.

Sigurnosna razmatranja za korištenje SLIP-a

iSeries TCP/IP podrška poslužitelja uključuje Serial Interface Line Protocol (SLIP). SLIP osigurava point-to-point povezanost niskog troška. SLIP korisnik se može povezati na LAN ili WAN uspostavljajući point-to-point vezu sa sistemom koji je dio LAN-a ili WAN-a.

SLIP se izvodi na asinkronoj vezi. Možete koristiti SLIP za telefonsku vezu do i od iSeries poslužitelja. Na primjer, možete koristiti SLIP za biranje od vašeg PC-a do iSeries sistema. Nakon uspostavljanja veze, možete koristiti TELNET aplikaciju na vašem PC-u da se povežete na iSeries TELNET poslužitelj. Ili, možete koristiti FTP aplikaciju za prijenos podataka između dva sistema.

SLIP konfiguracija ne postoji na vašem sistemu kod njegove isporuke. Stoga, ako ne želite SLIP (i TCP/IP na biranje) da se izvodi na vašem sistemu, ne konfigurirajte nikakve konfiguracijske profile za SLIP. Koristite naredbu Rad s TCP/IP Point-to-Point (WRKTCPPTP) da kreirate SLIP konfiguraciju. morate imati *IOSYSCFG posebno ovlaštenje za korištenje naredbe WRKTCPPTP.

Ako želite da se SLIP izvodi na vašem sistemu, kreirate jedan ili više SLIP (point-to-point) konfiguracijskih profila. Možete kreirati konfiguracijske profile sa sljedećim konfiguracijskim načinima:

- Birati u (*ANS)
- Birati iz (*DIAL)

Teme koje slijede raspravljaju kako možete postaviti sigurnost za SLIP konfiguracijske profile.

Bilješka: **korisnički profil** je iSeries poslužiteljski objekt koji dozvoljava prijavu. Svaki iSeries poslužiteljski posao mora imati korisnički profil koji se izvodi. **konfiguracijski profil** sprema informacije koje se koriste za uspostavljanje SLIP veze s iSeries sistemom. Kada pokrećete SLIP vezu s iSeries poslužiteljima, vi jednostavno uspostavljate vezu. Niste se prijavili i pokrenuli iSeries poslužiteljski posao. Stoga, ne trebate nužno korisnički profil da pokrenete SLIP vezu s iSeries poslužiteljima. Međutim, kako ćete vidjeti u raspravi koja slijedi, SLIP konfiguracijski profil mreže trebati korisnički profil da odredi da li da dozvoli vezu.

Kontrola biranih SLIP povezivanja

Prije nego netko može uspostaviti vezu biranja s vašim sistemom sa SLIP-om, morate pokrenuti SLIP *ANS konfiguracijski profil. Da kreirate ili promijeniti SLIP konfiguracijski profil, koristite naredbu Rad s TCP/IP Point-to-Point (WRKTCPPTP). Da pokrenete konfiguracijski profil, koristite ili naredbu Pokreni TCP/IP Point-to-Point (STRTCPPTP) ili opciju iz WRKTCPPTP prikaza. Vaš sistem se isporučuje s javnim ovlaštenjem za naredbe STRTCPPTP i ENDTCPPTP na *EXCLUDE. Opcije za dodavanje, promjenu i brisanje SLIP konfiguracijskih profila su dostupne samo ako imate *IOSYSCFG posebno ovlaštenje. Kao administrator sigurnosti možete koristiti i ovlaštenje naredbe i posebno ovlaštenje da odredite tko može postaviti vaš sistem da dozvoli veze biranja.

Osiguravanje SLIP birane veze

Ako želite provjeriti valjanost sistema koji bira vaš sistem, tada želite da sistem koji šalje zahtjev pošalje korisnički ID i lozinku. Vaš sistem može tada provjeriti korisnički ID i lozinku. Ako korisnički ID i lozinka nisu valjani, vaš sistem može odbiti zahtjev za sesijom.

Da postavite provjeru valjanosti kod biranja, napravite sljedeće:

__ Korak 1. Kreirajte korisnički profil koji sistem koji zahtijeva može koristiti za uspostavljanje veze. Korisnički ID i lozinka koji zahtjevatelj šalje moraju se podudarati s imenom korisničkog profila i lozinkom.

Bilješka: Da sistem izvede provjeru valjanosti lozinke, sistemska vrijednost QSECURITY mora biti postavljena na 20 ili više.

Kao dodatnu zaštitu, vjerojatno želite kreirati korisnički profil specifično za SLIP veze. Korisnički profili trebaju imati ograničeno ovlaštenje na sistemu. Ako ne planirate koristiti profile za neku drugu funkciju osim za uspostavljanje SLIP veza, možete postaviti sljedeće vrijednosti u korisničkom profilu:

- Početni izbornik (INLMNU) *SIGNOFF
- Početni program (INLPGM) *NONE.
- Ograničene sposobnosti (LMTCPB) *YES

Ove vrijednosti spriječavaju bilo koga da se prijavi interaktivno s korisničkim profilom.

__ Korak 2. Kreirajte autorizacijsku listu za sistem da provjerite kada zahtjevatelj pokušava uspostaviti SLIP vezu.

Bilješka: Specificirate ovu autorizacijsku listu u polju *Autorizacijska lista sistemskog pristupa* kada kreirate ili mijenjate SLIP profil. Pogledajte korak 4.)

__ Korak 3. Koristite naredbu Dodavanje autorizacijskog unosa (ADDAUTLE) da dodate korisnički profil koji ste kreirali u koraku 1 u autorizacijsku listu. Možete kreirati jedinstvenu autorizacijsku listu za svaki point-to-point konfiguracijski profil ili možete kreirati autorizacijsku listu koju dijeli nekoliko konfiguracijskih profila.

__ Korak 4. Koristite naredbu WRKTCPPTP da postavite TCP/IP point-to-point *ANS profil koji ima sljedeće osobine:

- Konfiguracijski profil mora koristiti skriptu dijaloga povezivanja koja uključuje funkcije za provjeru valjanosti korisnika. Provjera valjanosti korisnika uključuje prihvaćanje korisničkog ID-a i lozinke od zahtjevatelja i njihovo provjeravanje. Sistem se isporučuje s nekoliko primjera skripti dijaloga koje omogućuju ovu funkciju.
- Konfiguracijski profil mora specificirati ime autorizacijske liste koju ste kreirali u koraku 2. Korisnički ID koji prima skripta dijaloga povezivanja mora biti u autorizacijskoj listi.

Zapamtite da na vrijednost postavljanja sigurnosti biranja utječu sigurnosne prakse i sposobnosti sistema da bira. Ako trebate korisnički ID i lozinku, tada skripta dijaloga veze na sistemu koji zahtijeva mora poslati taj korisnički ID i lozinku. Neki sistemi, kao iSeries poslužitelji, omogućuju sigurne metode za spremanje korisničkih ID-ova i lozinki. ("Sigurnost i sesije biranja van" opisuje metodu.) Drugi sistemi spremaju korisnički ID i lozinku u skriptu koja može biti dostupna bilo kome tko zna kako naći skriptu na sistemu.

Zbog različitih sigurnosnih praksi i sposobnosti vaših komunikacijskih partnera, možete željeti kreirati različite konfiguracijske profile za različite zahtjevateljske okoline. Koristite naredbu STRTCPPTP da postavite vaš sistem da prihvaća sesiju za specifične konfiguracijske profile. Možete pokrenuti sesije za neke konfiguracijske profile samo u određenom vremenu dana, na primjer. Možete koristiti reviziju sigurnosti da zapišete aktivnost za pridruženi korisnički profil.

Spriječavanje korisnika s biranjem u pristupu drugim sistemima

Ovisno o vašem sistemu i mrežnoj konfiguraciji, korisnik koji pokreće SLIP vezu je sposoban pristupiti drugom sistemu u vašoj mreži bez da se prijavi u vaš sistem. Na primjer, korisnik može uspostaviti SLIP vezu s vašim sistemom. Tada korisnik može uspostaviti FTP vezu s drugim sistemom u vašoj mreži koji ne dozvoljava da ga se bira.

Možete spriječiti SLIP korisnike da pristupaju drugim sistemima u vašoj mreži specificirajući N (No) za polje *Dozvoli prosljeđivanje IP datograma* u konfiguracijskom profilu. Ovo spriječava korisnika da pristupi vašoj mreži prije nego se prijavi na vaš sistem. Međutim, nakon što se je korisnik uspješno prijavio na vaš sistem, vrijednost prosljeđivanja datograma nema učinka. To ne ograničava sposobnost korisnika da koristi TCP/IP aplikaciju na vašem iSeries sistemu (kao što je FTP ili TELNET), da uspostavi vezu s drugim sistemom u vašoj mreži.

Kontrola sesija biranja

Prije nego što netko može koristiti SLIP da uspostavi vezu biranja iz vašeg sistema, morate pokrenuti SLIP *DIAL konfiguracijski profil. Da kreirate ili promijenite SLIP konfiguracijski profil, koristite naredbu WRKTCPPTP. Da pokrenete konfiguracijski profil, koristite naredbu Pokreni TCP/IP Point-to-Point (STRTCPPTP) ili opciju iz WRKTCPPTP prikaza. Kada se vaš sistem oprema, javno ovlaštenje za naredbe STRTCPPTP i ENDTCPPTP je *EXCLUDE. Opcije za dodavanje, promjenu i brisanje SLIP konfiguracijskih profila je dostupno samo ako imate *IOSYSCFG posebno ovlaštenje. Kao administrator sigurnosti možete koristiti i ovlaštenje naredbe i posebno ovlaštenje da odredite tko može postaviti vaš sistem da dozvoli veze biranja van.

Sigurnost i sesije biranja van

Korisnici na vašem iSeries sistemu mogu željeti uspostaviti veze biranja van na sisteme koji zahtijevaju provjeru valjanosti korisnika. Skripta dijaloga povezivanja na vašem iSeries

poslužitelju mora poslati korisnički ID i lozinku udaljenom sistemu. iSeries poslužitelji pružaju sigurne metode za spremanje te lozinke. Lozinka ne treba biti spremljena u skriptu dijaloga povezivanja.

Bilješke:

1. Iako vaš sistem sprema lozinku povezivanja u šifriranom obliku, vaš sistem je dešifrira prije slanja. SLIP lozinke, kao i FTP i TELNET lozinke, se šalju dešifrirane ("u očišćenom"). Međutim, za razliku od FTP-a i TELNET-a, SLIP lozinka se šalje prije nego sistemi uspostave TCP/IP način.

   Zato jer SLIP koristi point-to-point vezu u asinkronom načinu, izlaganje sigurnosti kod slanje dešifriranih lozinki je drugačije od izlaganja s FTP i TELNET lozinkama. Dešifrirane FTP i TELNET lozinke mogu biti poslane IP prometom u mreži i stoga su osjetljive na elektroničko njuškanje. Transmisija vaše SLIP lozinke je sigurna kao i telefonska veza između dva sistema.
2. Defaultna datoteka za spremanje SLIP skripte dijaloga veze je QUSRSYS/QATOCPPSCR. Javno ovlaštenje za ovu datoteku je *USE, koji spriječava javne korisnike da mijenjaju defaultne skripte dijaloga veze.

Kada kreirate profil povezivanja za udaljenu sesiju koja treba provjeru valjanosti, učinite sljedeće:

__ Korak 1. Osigurajte da sistem Zadrži sigurnosne podatke poslužitelja (QRETSVRSEC) vrijednost je 1 (Da). Ova sistemska vrijednost određuje da li ćete dozvoliti lozinke koje mogu biti dešifrirane da budu spremljene u zaštićenom području vašeg sistema.

__ Korak 2. Koristite naredbu WRKTCPPTP da kreirate konfiguracijski profil koji ima sljedeće osobine:

- Za način konfiguracijskog profila, specificirajte *DIAL.
- Za *Ime pristupa udaljene usluge*, specificirajte korisnički ID koji udaljeni sistem očekuje. Na primjer, ako se povezujete na drugi iSeries poslužitelj, specificirajte ime korisničkog profila na tom iSeries poslužitelju.
- Za *Lozinka pristupa udaljene usluge*, specificirajte lozinku koji udaljeni sistem očekuje. Na vašem iSeries poslužitelju, ova lozinka je spremljena u zaštićenom području u obliku koji može biti dešifriran. Imena i lozinke koje dodjeljujete korisničkim profilima su pridružene s QTCP korisničkim profilom. Imena i lozinke nisu dostupne s nijednom korisničkom naredbom ili sučeljem. Samo registrirani sistemski programi mogu pristupiti informacijama o ovoj lozinki.

  Bilješka: Zapamtite da lozinke za vaše profile povezivanja nisu spremljene kada spremite TCP/IP konfiguracijske datoteke. Da spremite SLIP lozinke, trebate koristiti naredbu Spremanje sigurnosnih podataka (SAVSECDTA) da spremite QTCP korisnički profil.
- Za skriptu dijaloga povezivanja, specificirajte skriptu koja šalje korisnički ID i lozinku. Sistem se isporučuje s nekoliko primjera skripti dijaloga koje omogućuju ovu funkciju.Kada sistem izvodi skriptu, sistem dohvaća lozinku, dešifrira je i šalje ju udaljenom sistemu.

Sigurnosna razmatranja za point-to-point protokol

Point-to-point protokol (PPP) je dostupan kao dio TCP/IP-a. PPP je industrijski standard za point-to-point povezivanja koji omogućava dodatne funkcije na ono što je dostupno sa SLIP-om.

S PPP-om, vaš iSeries poslužitelj može imati vezu velike brzine direktno s Dobavljačem Internet usluga ili s drugim sistemima i intranetu ili extranetu. Udaljeni LAN-ovi mogu realistično napraviti veze biranja na vaš iSeries poslužitelj.

Zapamtite da PPP, kao SLIP, osigurava mrežno povezivanje na vaš iSeries poslužitelj. PPP veza u osnovi donosi zahtjevatelja na vrata vašeg sistema. Zahtjevatelj još uvijek treba korisnički ID i lozinku da se upiše u vaš sistem i poveže na TCP/IP poslužitelj kao TELNET i FTP. Sljedeće su sigurnosna razmatranja s ovom novom sposobnosti povezivanja:

Bilješka: Vi konfigurirate PPP koristeći iSeries Navigator na IBM iSeries Access za Windows radnu stanicu.

- PPP osigurava sposobnost posjedovanje namjenskih veza (gdje isti korisnik uvijek ima istu IP adresu). S namjenskom adresom, imate potencijal za IP obmanu (nepovjerljivi sistem koji se pretvara da je povjerljiv s poznatom IP adresom). Međutim, povećane sposobnosti provjere autentičnosti koje osigurava PPP pomažu kod zaštite od IP obmane.
- S PPP-om, kao i SLIP-om, vi kreirate profile povezivanja koji imaju korisničko ime i pridruženu lozinku. Međutim, za razliku od SLIP-a, korisnik ne mora imati valjani korisnički profil i lozinku. Korisničko ime i lozinka se ne pridružuju s korisničkim profilom. Umjesto toga, validacijska lista se koristi za PPP provjeru autentičnosti. Dodatno, PPP ne zahtijeva skriptu povezivanja. Provjera autentičnosti (zamjena korisničkog imena i lozinke) je dio PPP arhitekture i dešava se na nižoj razini nego sa SLIP-om.
- S PPP-om, imate opciju korištenja CHAP (protokol provjere autentičnosti rukovanja izazovom). Više se ne trebate brinuti o obmani prisluškivanjem lozinki jer CHAP šifrira korisnička imena i lozinke.

  Vaša PPP veza koristi CHAP jedino ako obje strane podržavaju CHAP. Za vrijeme zamjene signala radi postavljanja komunikacije između dva modema, sistemi se dogovaraju. Na primjer, ako SYSTEMA podržava CHAP, a SYSTEMB ne, SYSTEMA može ili ne prihvatiti sesiju ili se složiti da koristi nešifrirano korisničko ime i lozinku. Slaganje s upotrebom nešifriranog korisničkog imena i lozinke se tretira kao prekid dogovaranja. Odluka o prekidu dogovora je konfiguracijska opcija. U vašem intranetu, na primjer, gdje znate da svi vaši sistemi imaju CHAP sposobnost, trebate konfigurirati vaš korisnički profil tako da neće prekinuti dogovor. Kod javnog povezivanja gdje vaš sistem bira, možete željeti prekinuti dogovor.

  Profil povezivanja za PPP osigurava sposobnost da specificira važeću IP adresu. Možete, na primjer, pokazati da očekujete specifičnu adresu ili raspon adresa za specifičnog korisnika. Ova sposobnost, zajedno sa sposobnošću šifriranja lozinki, osigurava daljnju zaštitu od obmane.

  Kao dodatna zaštita od obmane ili stalnog povratka aktivne sesije, možete konfigurirati PPP da ponovo izazove dodatne intervale. Na primjer, dok je PPP sesija aktivna, vaš iSeries poslužitelj može izazvati drugi sistem za korisničko ime i lozinku. To čini svakih 15 minuta da osigura isti profil povezivanja. (Krajnji korisnik se ne brine o ovoj aktivnosti ponovnog izazivanja. Sistemska imena zamjene i lozinke su ispod razine koju korisnik može vidjeti.)

  S PPP je realno očekivati da udaljeni LAN-ovi mogu uspostaviti vezu biranja na vaš iSeries poslužitelj i vašu proširenu mrežu. U ovoj okolini, vjerojatno je preporuka da je IP prosljeđivanje uključeno. IP prosljeđivanje ima potencijal da dozvoli uljezu da slobodno šeće kroz vašu mrežu. Međutim, PPP ima jaku zaštitu (kao što je šifriranje lozinki i provjera valjanosti IP adresa). Ovo čini manje vjerojatnim da uljez uopće može uspostaviti mrežno povezivanje.

Za više informacija o PPP-u pogledajte iSeries Informacijski Centar.

Sigurnosna razmatranja za upotrebu Protokola za podizanje sistema poslužitelja

Protokol za podizanje sistema (BOOTP) pruža dinamičku metodu za pridruživanje radnih stanica s poslužiteljima i pridruživanje IP adrese radne stanice i izvora punjenja početnog programa (IPL).

BOOTP je TCP/IP protokol koji se koristi da se dozvoli radnoj stanici bez medija (klijent) da zahtijeva datoteku koja sadrži početni kod od poslužitelja u mreži. BOOTP poslužitelj sluša na dobro poznatom portu 67 BOOTP poslužitelja. Kada je klijentov zahtjev primljen, poslužitelj analizira IP adresu definiranu za klijenta i vraća odgovor klijentu s klijentovom IP adresom i imenom učitane datoteke. Klijent tada započinje TFTP zahtjev s poslužiteljem za učitavanjem datoteke. Mapiranje između hardverske adrese klijenta i IP adrese se drži u BOOTP tablici na iSeries poslužitelju.

Spriječavanje BOOTP pristupa

Ako nemate nikakve tanke klijente pripojene na vašu mrežu, ne trebate izvoditi BOOTP poslužitelj na vašem sistemu. Može biti korišten za drugi uređaj, ali preferirano rješenje za ove uređaje je korištenje DHCP-a. Učinite sljedeće za spriječite BOOTP poslužitelj od izvođenja:

__ Korak 1. Da spriječite poslove BOOTP poslužitelja od automatskog pokretanja kada pokrenete TCP/IP, upišite sljedeće:

```
CHGBPA AUTOSTART(*NO)
```

Bilješke:

a. AUTOSTART(*NO) je defaultna vrijednost.

b. “Kontrola koju TCP/IP poslužitelji pokreću automatski” na stranici 108 pruža više informacija o kontroliranju koje TCP/IP poslužitelji pokreću automatski.

__ Korak 2. Da spriječite nekoga od pridruživanja korisničke aplikacije, kao što je aplikacija utičnica, s portom koji sistem normalno koristi BOOTP, učinite sljedeće:

Bilješka: Zato jer DHCP i BOOTP koriste isti broj porta, ovo će također onemogućiti port koji koristi DHCP. Ne ograničavajte port ako želite koristiti DHCP.

__ Korak a. Upišite GO CFGTCP za prikaz izbornika Konfiguriranje TCP/IP-a.

__ Korak b. Izaberite opciju 4 (Rad s ograničenjima TCP/IP porta).

__ Korak c. Na prikazu Rad s ograničenjima TCP/IP porta, specificirajte opciju 1 (Dodavanje).

__ Korak d. Za nižu razinu porta, specificirajte 67.

__ Korak e. Za višu razinu porta, specificirajte *ONLY.

Bilješke:

1) Ograničenja porta imaju učinak sljedeći put kada pokrenete TCP/IP. Ako je TCP/IP aktivan kada postavljate ograničenja porta, trebate zaustaviti TCP/IP i ponovo ga pokrenuti.

2) RFC1700 pruža više informacija o dodjelama broja zajedničkog porta.

__ Korak f. Za protokol, specificirajte *UDP.

__ Korak g. Za polje korisničkog profila, specificirajte ime korisničkog profila koje je zaštićeno u vašem sistemu. (Zaštićeni korisnički

profil je korisnički profil koji ne posjeduje programe koji usvajaju ovlaštenje i nema lozinku koju znaju ostali korisnici.) Ograničavanjem porta na određenog korisnika, automatski isključujete sve druge korisnike.

Sigurni BOOTP poslužitelj

BOOTP poslužitelj ne pruža direktan pristup vašem iSeries sistemu i ovo predstavlja ograničeno sigurnosno izlaganje. Vaša primarna briga kao sigurnosnog administratora je osigurati da je ispravna informacija pridružena s ispravnim tankim klijentom. Drugim riječima, netko tko radi nevolje može promijeniti BOOTP tablicu i uzrokovati da vaši tanki klijenti ne rade ispravno ili da uopće ne rade.

Za administriranje BOOTP poslužitelja i BOOTP tablice, morate imati *IOSYSCFG posebno ovlaštenje. Trebate pažljivo kontrolirati korisničke profile koji imaju *IOSYSCFG posebno ovlaštenje na vašem sistemu.

Sigurnosna razmatranja za upotrebu DHCP poslužitelja

Dynamic host configuration protocol (DHCP) pruža okosnicu za prolazak konfiguracijskih informacija do hosta na TCP/IP mreži. Za radne stanice vašeg klijenta, DHCP može pružiti funkciju sličnu auto konfiguraciji. DHCP-omogućen program na klijentovoj radnoj stanici emitira zahtjev za konfiguracijskim informacijama. Ako se izvodi DHCP poslužitelj na vašem iSeries poslužitelju, poslužitelj odgovara na zahtjev šaljući informacije da klijentova radna stanica treba ispravno konfigurirati TCP/IP.

Možete koristiti DHCP da pojednostavite korisnicima povezivanje na vaš iSeries poslužitelj po prvi put. Ovo je jer korisnik ne treba upisati TCP/IP konfiguracijske informacije. Možete također koristiti DHCP da smanjite broj internih TCP/IP adresa koje trebate u podmreži. DHCP poslužitelj može privremeno dodijeliti IP adrese aktivnim korisnicima (iz njegovog spremišta IP adresa).

Za ove klijente, možete koristiti DHCP umjesto BOOTP-a. DHCP pruža više funkcija od BOOTP i može podržavati dinamičku konfiguraciju i za tanke klijente i PC-ove.

Spriječavanje DHCP pristupa

Ako *ne* želite da bilo tko koristi DHCP poslužitelj za pristup vašem sistemu, napravite sljedeće:

1. Da spriječite poslove DHCP poslužitelja od automatskog pokretanja kada pokrenete TCP/IP, upišite sljedeće:

   ```
   CHGDHCPA AUTOSTART(*NO)
   ```

   Bilješke:

   a. AUTOSTART(*NO) je defaultna vrijednost.
   b. “Kontrola koju TCP/IP poslužitelji pokreću automatski” na stranici 108 pruža više informacija o kontroliranju koje TCP/IP poslužitelji pokreću automatski.

2. Da spriječite nekoga od pridruživanja korisničke aplikacije, kao što je aplikacija utičnica, s portom koji sistem normalno koristi DHCP, učinite sljedeće:
   a. Upišite GO CFGTCP za prikaz izbornika Konfiguriranje TCP/IP-a.
   b. Izaberite opciju 4 (Rad s ograničenjima TCP/IP porta).
   c. Na prikazu Rad s ograničenjima TCP/IP porta, specificirajte opciju 1 (Dodavanje).
   d. Za nižu razinu porta, specificirajte 67.
   e. Za višu razinu porta, specificirajte 68.

Bilješke:

1) Ograničenja porta imaju učinak sljedeći put kada pokrenete TCP/IP. Ako je TCP/IP aktivan kada postavljate ograničenja porta, trebate zaustaviti TCP/IP i ponovo ga pokrenuti.
2) RFC1700 pruža više informacija o dodjelama broja zajedničkog porta.

f. Za protokol, specificirajte *UDP.

g. Za polje korisničkog profila, specificirajte ime korisničkog profila koje je zaštićeno u vašem sistemu. (Zaštićeni korisnički profil je korisnički profil koji ne posjeduje programe koji usvajaju ovlaštenje i nema lozinku koju znaju ostali korisnici.) Ograničavanjem porta na određenog korisnika, automatski isključujete sve druge korisnike.

Sigurni DHCP poslužitelj

Sljedeće su sigurnosna razmatranja ako izaberete izvođenje DHCP-a na vašem iSeries sistemu:

- Smanjite broj korisnika koji imaju ovlaštenje za administriranje DHCP-a. Administriranje DHCP-a treba sljedeće ovlaštenje:
  - *IOSYSCFG posebno ovlaštenje
  - *RW ovlaštenje za sljedeće datoteke:

    ```
    /QIBM/UserData/OS400/DHCP/dhcpsd.cfg
    /QIBM/UserData/OS400/DHCP/dhcprd.cfg
    ```
- Procijenite kako je fizički dohvatljiv vaš LAN. Može li netko izvana lako ušetati na vašu lokaciju s laptopom i fizički se povezati na vaš LAN? Ako je ovo izlaganje, DHCP pruža sposobnost kreiranja popisa klijenata (hardverske adrese) koje će DHCP poslužitelj konfigurirati. Kada koristite ovo svojstvo, uklanjate neke od produktivnih prednosti koje ima DHCP za vaše mrežne administratore. Međutim, vi zaštićujete sistem od konfiguriranja nepoznatih radnih stanica.
- Ako je moguće, koristite spremište IP adresa koje se mogu ponovo koristiti (ne dizajniranih za Internet). Ovo pomaže spriječiti radnu stanicu izvan vaše mreže od dobivanja upotrebljivih konfiguracijskih informacija od poslužitelja.
- Koristite DHCP izlazne točke ako trebate dodatnu sigurnosnu zaštitu. Sljedeće je pregled izlaznih točaka i njihovih mogućnosti. *iSeries Sistemska API referenca* opisuje kako koristiti ove izlazne točke.

  Unos porta
  Sistem poziva vaš izlazni program kada pročita podatkovni paket s porta 67 (DHCP port). Vaš izlazni program prima potpun podatkovni paket. Može odlučiti da li sistem treba obrađivati ili odbaciti paket. Možete koristiti ovu izlaznu točku kada postojeće DHCP ekranske značajke nisu dovoljne za vaše potrebe.

  Dodjela adresa
  Sistem poziva vaš izlazni program svaki put kada DHCP formalno pridružuje adresu klijentu.

  Oslobađanje adresa
  Sistem poziva vaš izlazni program svaki put kada DHCP formalno oslobađa adresu i ponovo je smješta u spremište adresa.

Sigurnosna razmatranja za upotrebu TFTP poslužitelja

Trivial file transfer protocol (TFTP) pruža osnovan prijenos datoteka bez provjere autentičnosti korisnika. TFTP radi s Protokol za podizanje sistema (BOOTP) ili Dynamic Host Configuration Protocol (DHCP).

Klijent se na početku povezuje s BOOTP poslužiteljem ili DHCP poslužiteljem. BOOTP poslužitelj ili DHCP poslužitelj odgovara s IP adresom klijenta i imenom učitane datoteke. Klijent tada započinje TFTP zahtjev s poslužiteljem za učitavanjem datoteke. Kada klijent dovrši spuštanje učitane datoteke, to završava TFTP sesiju.

Spriječavanje TFTP pristupa

Ako nemate nikakve tanke klijente pripojene na vašu mrežu, ne trebate vjerojatno izvoditi TFTP poslužitelj na vašem sistemu. Učinite sljedeće za spriječite TFTP poslužitelj od izvođenja:

__ Korak 1. Da spriječite poslove TFTP poslužitelja od automatskog pokretanja kada pokrenete TCP/IP, upišite sljedeće:

```
CHGTFTPA AUTOSTART(*NO)
```

Bilješke:

a. AUTOSTART(*NO) je defaultna vrijednost.

b. “Kontrola koju TCP/IP poslužitelji pokreću automatski” na stranici 108 pruža više informacija o kontroliranju koje TCP/IP poslužitelji pokreću automatski.

__ Korak 2. Da spriječite nekoga od pridruživanja korisničke aplikacije, kao što je aplikacija utičnica, s portom koji sistem normalno koristi TFTP, učinite sljedeće:

__ Korak a. Upišite GO CFGTCP za prikaz izbornika Konfiguriranje TCP/IP-a.

__ Korak b. Izaberite opciju 4 (Rad s ograničenjima TCP/IP porta).

__ Korak c. Na prikazu Rad s ograničenjima TCP/IP porta, specificirajte opciju 1 (Dodavanje).

__ Korak d. Za nižu razinu porta, specificirajte 69.

__ Korak e. Za višu razinu porta, specificirajte *ONLY.

Bilješke:

1) Ograničenja porta imaju učinak sljedeći put kada pokrenete TCP/IP. Ako je TCP/IP aktivan kada postavljate ograničenja porta, trebate zaustaviti TCP/IP i ponovo ga pokrenuti.

2) RFC1700 pruža više informacija o dodjelama broja zajedničkog porta.

__ Korak f. Za protokol, specificirajte *UDP.

__ Korak g. Za polje korisničkog profila, specificirajte ime korisničkog profila koje je zaštićeno u vašem sistemu. (Zaštićeni korisnički profil je korisnički profil koji ne posjeduje programe koji usvajaju ovlaštenje i nema lozinku koju znaju ostali korisnici.) Ograničavanjem porta na određenog korisnika, automatski isključujete sve druge korisnike.

Sigurni TFTP poslužitelj

Po defaultu, TFTP poslužitelj pruža vrlo ograničen pristup vašem iSeries sistemu. Posebno je konfiguriran za pružanje početnog koda za tanke klijente. Kao sigurnosni administrator, trebate biti svjesni sljedećih karakteristika TFTP poslužitelja:

- TFTP poslužitelj ne treba provjeru autentičnosti (korisnički ID i lozinku). Svi TFTP poslovi se izvode pod QTFTP korisničkim profilom. QTFTP korisnički profil nema lozinku. Stoga, nije dostupan za interaktivnu prijavu. QTFTP korisnički profil nema nikakva posebna ovlaštenja, niti je izričito ovlašten za sistemske resurse. Koristi javno ovlaštenje za pristup resursima koje treba za tanke klijente.

- Kada TFTP poslužitelj dođe, konfiguriran je za pristup direktoriju koji sadrži informacije o tankom klijentu. Morate imati *PUBLIC ili QTFTP ovlaštenje za čitanje ili pisanje u tom direktoriju. Za pisanje u direktorij morate imati *CREATE specificirano u parametru ″Dozvoli pisanje u datoteku″ naredbe CHGTFTPA. Za pisanje u postojeću datoteku morate imati specificiran *REPLACE u parametru ″Dozvoli pisanje u datoteku″ naredbe CHGTFTPA. *CREATE vam dozvoljava da zamijenite postojeće datoteke ili kreirate nove datoteke. *REPLACE jedino vama dozvoljava da zamijenite postojeće datoteke.

  A TFTP klijent ne može pristupiti niti jednom drugom direktoriju osim ako izričito ne definirate direktorij naredbom Promijeni TFTP atribute (CHGTFTPA). Stoga, ako lokalni ili udaljeni korisnik pokuša pokrenuti TFTP sesiju na vašem sistemu, korisnikova mogućnost pristupa informacijama ili njihovog oštećivanja je izričito ograničena.
- Ako izaberete konfiguriranje vašeg TFTP poslužitelja da može pružiti druge usluge kao dodatak na rukovanje tankim klijentima, možete definirati izlazni program da procijenite i ovlastite svaki TFTP zahtjev. TFTP poslužitelj osigurava izlaz provjere valjanosti zahtjeva sličan izlazu koji je dostupan za FTP poslužitelj. Za više informacija, pogledajte iSeries Informacijski Centar—>Umrežavanje—>TCP/IP—>TFTP. Pogledajte“Preduvjeti i povezane informacije” na stranici xii za informacije o pristupu iSeries Informacijskom Centru.

Sigurnosna razmatranja za upotrebu REXEC poslužitelja

Udaljeni EXECution poslužitelj (REXEC) prima i izvodi naredbe iz REXEC klijenta. REXEC klijent je tipično PC ili UNIX aplikacija koja podržava slanje REXEC naredbi. Podrška koju pruža ovaj poslužitelj je slična sposobnosti koja je dostupna kad koristite podnaredbu RCMD (Udaljena naredba) za FTP poslužitelj.

Spriječavanje REXEC pristupa

Ako ne želite da vaš iSeries poslužitelj prihvati naredbe od REXEC klijenta, učinite sljedeće da zaštitite REXEC poslužitelj od izvođenja.

__ Korak 1. Da spriječite poslove REXEC poslužitelja od automatskog pokretanja kada pokrenete TCP/IP, upišite sljedeće:

```
CHGRXCA AUTOSTART(*NO)
```

Bilješke:

a. AUTOSTART(*NO) je defaultna vrijednost.

b. “Kontrola koju TCP/IP poslužitelji pokreću automatski” na stranici 108 pruža više informacija o kontroliranju koje TCP/IP poslužitelji pokreću automatski.

__ Korak 2. Da spriječite nekoga od pridruživanja korisničke aplikacije, kao što je aplikacija utičnica, s portom koji sistem normalno koristi REXEC, učinite sljedeće:

__ Korak a. Upišite GO CFGTCP za prikaz izbornika Konfiguriranje TCP/IP-a.

__ Korak b. Izaberite opciju 4 (Rad s ograničenjima TCP/IP porta).

__ Korak c. Na prikazu Rad s ograničenjima TCP/IP porta, specificirajte opciju 1 (Dodavanje).

__ Korak d. Za nižu razinu porta, specificirajte 512.

__ Korak e. Za višu razinu porta, specificirajte *ONLY.

__ Korak f. Za protokol, specificirajte *TCP.

__ Korak g. Za polje korisničkog profila, specificirajte ime korisničkog profila koje je zaštićeno u vašem sistemu. (Zaštićeni korisnički profil je korisnički profil koji ne posjeduje programe koji

usvajaju ovlaštenje i nema lozinku koju znaju ostali korisnici.) Ograničavanjem porta na određenog korisnika, automatski isključujete sve druge korisnike.

Bilješke:

a. Ograničenja porta imaju učinak sljedeći put kada pokrenete TCP/IP. Ako je TCP/IP aktivan kada postavljate ograničenja porta, trebate zaustaviti TCP/IP i ponovo ga pokrenuti.
b. RFC1700 pruža više informacija o dodjelama broja zajedničkog porta.

Sigurni REXEC poslužitelj

Sljedeće su razmatranja kada izaberete izvođenje Udaljeni EXECution poslužitelj na vašem sistemu:

- REXCD zahtjev uključuje korisnički ID, lozinku i naredbu za izvođenje. Primjenjuje se provjera autentičnosti normalnog iSeries poslužitelja i provjeravanje ovlaštenja:
  - Kombinacija korisničkog profila i lozinke mora biti važeća.
  - Sistem primjenjuje vrijednost *Granične sposobnosti* (LMTCPB) za korisnički profil.
  - Korisnik mora biti ovlašten za naredbu i za sve resurse koje ta naredba koristi.
- REXEC poslužitelj osigurava izlazne točke slične izlaznim točkama koje su dostupne za FTP poslužitelj. Možete koristiti izlaznu točku za provjeru valjanosti da procijenite naredbu i da odlučite da li je dozvoliti. Za više informacija, pogledajte iSeries Informacijski Centar—>Umrežavanje—>TCP/IP—>REXEC. Pogledajte“Preduvjeti i povezane informacije” na stranici xii za informacije o pristupu iSeries Informacijskom Centru.
- Kada izaberete izvođenje REXEC poslužitelja, izvodite ga izvan kontrole pristupa bilo kojeg izbornika koji imate na vašem sistemu. Morate se uvjeriti da je shema ovlaštenja vašeg objekta prikladna za zaštitu vaših resursa.

Sigurnosna razmatranja za upotrebu RouteD

Demon smjera (RouteD) poslužitelj osigurava podršku za Routing Information Protocol (RIP) na iSeries poslužiteljima. RIP je najraširenije korišteni protokol usmjeravanja. Interior Gateway Protocol pomaže TCP/IP-u kod usmjeravanja IP paketa u autonomnim sistemima.

Namjena RouteD je da poveća djelotvornost mrežnog prometa dozvoljavajući sistemima u povjerljivoj mreži da ažuriraju jedan drugog s informacijama trenutnog puta. Kada izvodite RouteD, vaš sistem može primiti ažurirane podatke od drugih sistema koji sudjeluju o tome kako prijenos (paketi) treba biti usmjeren. Stoga, ako je vaš RouteD poslužitelj dostupan hakerima, haker ga može koristiti da ponovo usmjeri vaše pakete kroz sistem koji može njuškati ili modificirati te pakete. Sljedeće su prijedlozi za RouteD sigurnost:

- iSeries poslužitelji koriste RIPv1, koji ne pruža nikakve metode za provjeru autentičnosti usmjerivača. Namijenjen je za korištenje u povjerljivim mrežama. Ako je vaš sistem mreža s drugim sistemima kojima trebate ″vjerovati″, ne trebate izvoditi RouteD poslužitelj. Da se uvjerite da se RouteD poslužitelj ne pokrene automatski, upišite sljedeće:

  ```
  CHGRTDA AUTOSTART(*NO)
  ```

  Bilješke:

  1. AUTOSTART(*NO) je defaultna vrijednost.
  2. “Kontrola koju TCP/IP poslužitelji pokreću automatski” na stranici 108 pruža više informacija o kontroliranju koje TCP/IP poslužitelji pokreću automatski.
- Uvjerite se da kontrolirate tko može promijeniti RouteD konfiguraciju, što zahtijeva *IOSYSCFG posebno ovlaštenje.
- Ako vaš sistem sudjeluje u više od jedne mreže (na primjer, intranet i Internet), možete prihvatiti promjene samo od sigurne mreže.

Sigurnosna razmatranja za upotrebu DNS poslužitelja

Sistem imena domene (DNS) poslužitelj pruža prijevod imena hosta u IP adresu i obrnuto. Na iSeries poslužiteljima, DNS poslužitelj ima namjenu da osigura prijevod adrese za internu, sigurnu mrežu (intranet).

Spriječavanje DNS pristupa

Ako *ne* želite da bilo tko koristi DNS poslužitelj na vašem sistemu, napravite sljedeće:

1. Da spriječite poslove DNS poslužitelja od automatskog pokretanja kada pokrenete TCP/IP, upišite sljedeće:

   ```
   CHGDNSA AUTOSTART(*NO)
   ```

   Bilješke:

   a. AUTOSTART(*NO) je defaultna vrijednost.

   b. “Kontrola koju TCP/IP poslužitelji pokreću automatski” na stranici 108 pruža više informacija o kontroliranju koje TCP/IP poslužitelji pokreću automatski.

2. Da spriječite nekoga od pridruživanja korisničke aplikacije, kao što je aplikacija utičnica, s portom koji sistem normalno koristi DNS, učinite sljedeće:

   a. Upišite GO CFGTCP za prikaz izbornika Konfiguriranje TCP/IP-a.

   b. Izaberite opciju 4 (Rad s ograničenjima TCP/IP porta).

   c. Na prikazu Rad s ograničenjima TCP/IP porta, specificirajte opciju 1 (Dodavanje).

   d. Za nižu razinu porta, specificirajte 53.

   e. Za višu razinu porta, specificirajte *ONLY.

      Bilješke:

      1) Ograničenja porta imaju učinak sljedeći put kada pokrenete TCP/IP. Ako je TCP/IP aktivan kada postavljate ograničenja porta, trebate zaustaviti TCP/IP i ponovo ga pokrenuti.

      2) RFC1700 pruža više informacija o dodjelama broja zajedničkog porta.

   f. Za protokol, specificirajte *TCP.

   g. Za polje korisničkog profila, specificirajte ime korisničkog profila koje je zaštićeno u vašem sistemu. (Zaštićeni korisnički profil je korisnički profil koji ne posjeduje programe koji usvajaju ovlaštenje i nema lozinku koju znaju ostali korisnici.) Ograničavanjem porta na određenog korisnika, automatski isključujete sve druge korisnike.

   h. Ponavljajte korake 2c do 2g za *UDP (korisnički datagram) protokol.

Sigurni DNS poslužitelj

Sljedeće su sigurnosna razmatranja ako izaberete izvođenje DNS-a na vašem iSeries sistemu:

- Funkcija koju pruža DNS poslužitelj je prijevod IP adrese i imena. Ne pruža nikakav pristup objektima na vašem iSeries sistemu. Vaš rizik kada netko izvana pristupa vašem DNS poslužitelju je da poslužitelj pruža lagan način za pregledavanje topologije vaše mreže. Vaš DNS može uštediti hakerima neko nastojanje kod određivanja adresa potencijalnog cilja. Međutim, vaš DNS ne pruža informacije koje će pomoći promijeniti te ciljne sisteme.
- Tipično, koristite iSeries DNS poslužitelj za vaš intranet. Stoga, vjerojatno nemate potrebu da ograničite sposobnost upita DNS-a. Međutim, možete, na primjer, imati nekoliko podmreža u vašem intranetu. Možete ne željeti da korisnici iz različitih podmreža mogu radite upite na DNS na vašem iSeries poslužitelju. Sigurnosna opcija DNS-a dozvoljava vam ograničavanje pristupa primarnoj domeni. Koristite iSeries Navigator da specificirate IP adrese na koje DNS poslužitelj treba odgovoriti.

Druga sigurnosna opcija dozvoljava vam specificiranje sekundarnih poslužitelja koji mogu kopirati informacije iz vašeg primarnog DNS poslužitelja. Kada koristite ovu opciju, vaš poslužitelj će prihvatiti zahtjeve prijenosa zone (zahtjev za kopiranjem informacija) samo od sekundarnih poslužitelja koje izričito navedete.

- Pažljivo ograničite sposobnost promjene konfiguracijske datoteke za vaš DNS poslužitelj. Netko sa zlobnim namjerama može, na primjer, promijeniti vašu DNS datoteku da pokazuje na IP adresu izvan vaše mreže. Mogu simulirati poslužitelj u vašoj mreži i možda, dobiti pristup povjerljivim informacijama od korisnika koji posjećuju poslužitelj.

Sigurnosna razmatranja za korištenje HTTP poslužitelja za iSeries

HTTP poslužitelj osigurava World Wide Web pretražitelja klijentima s pristupom multimedijalnim objektima iSeries poslužitelja, kao npr.HTML (Hypertext Markup Language) dokumenti. Također podržava specifikaciju *Common Gateway Interface (CGI)*. Aplikacijski programeri mogu pisati CGI programe kako bi proširili funkcionalnost poslužitelja.

Administrator može koristiti Poslužitelj Internet povezivanja ili IBM HTTP poslužitelj za iSeries za izvođenje višestrukih poslužitelja istodobno na istom iSeries poslužitelju. Svaki poslužitelj koji se izvodi se naziva **poslužiteljska instanca**. Svaka poslužiteljska instanca ima jednoznačno ime. Administrator kontrolira koje instance su pokrenute i što svaka instanca može napraviti.

Bilješka: Morate imati instancu *ADMIN HTTP poslužitelja koji se izvodi kada koristite Web pretražitelj da konfigurirate ili administrirate bilo što od sljedećeg:

- Vatreni zid za iSeries
- Poslužitelj Internet povezivanja
- Sigurni poslužitelj Internet veze
- IBM HTTP poslužitelj za iSeries

Korisnik (posjetitelj Web stranice) nikad ne vidi iSeries ekran za prijavu poslužitelja. Međutim, administrator iSeries poslužitelja mora izričito ovlastiti sve HTML dokumente i CGI programe definirajući ih u HTTP direktivama. Dodatno, administrator može postaviti i sigurnost resursa i provjeru autentičnosti korisnika (korisnički ID i lozinka) za neke ili sve zahtjeve.

Napad hakera može rezultirati odbijanjem usluga vašem Web poslužitelju. Vaš poslužitelj može otkriti napad odbijanja usluga mjereći timeout određenih klijentovih zahtjeva. Ako poslužitelj ne primi zahtjev od klijenta, tada vaš poslužitelj određuje da napad odbijanja usluga napreduje. Ovo se dešava nakon inicijalnog povezivanja klijenta na vaš poslužitelj. Default poslužitelja je da izvodi otkrivanje napada i kažnjavanje.

Spriječavanje HTTP pristupa

Ako *ne* želite da bilo tko koristi program za pristup vašem sistemu, trebate zaštiti HTTP poslužitelj od izvođenja. Napravite sljedeće:

__ Korak 1. Da spriječite poslove HTTP poslužitelja od automatskog pokretanja kada pokrenete TCP/IP, upišite sljedeće:

```
CHGHTTPA AUTOSTART(*NO)
```

Bilješke:

a. AUTOSTART(*NO) je defaultna vrijednost.

b. “Kontrola koju TCP/IP poslužitelji pokreću automatski” na stranici 108 pruža više informacija o kontroliranju koje TCP/IP poslužitelji pokreću automatski.

__ Korak 2. Po defaultu, posao HTTP poslužitelja koristi QTMHHTTP korisnički profil. Da spriječite HTTP poslužitelj od pokretanja, postavite stanje QTMHHTTP korisničkog profila na *DISABLED.

Kontrola pristupa HTTP poslužitelju

Primarna svrha izvođenja HTTP poslužitelja je omogućavanje pristupa za posjetitelje Web stranice na vašem iSeries sistemu. Možete misliti o nekome tko posjećuje vašu Web stranicu kao što mislite o nekome tko gleda oglas u trgovinskom dnevniku. Posjetitelj se ne brine o hardveru i softveru koji izvodi vašu Web stranicu, kao što je tip poslužitelja koji koristite i gdje je vaš poslužitelj fizički smješten. Obično, ne želite staviti nikakve prepreke (kao što je ekran za prijavu) između potencijalnog posjetitelja i vaše Web stranice. Međutim, možete željeti ograničiti pristup nekim dokumentima ili CGI programima koje osigurava vaša Web stranica.

Također, možete željeti da jednostruki iSeries sistem osigurava višestruke logičke Web stranice. Na primjer, vaš iSeries sistem može podržavati različite grane vašeg posla koji ima različite postavke za korisnika. Za svaku od ovih grana posla, vi želite jedinstvenu Web stranicu koja se pojavljuje potpuno nezavisno posjetitelju. Dodatno, možete željeti osigurati interne Web stranice (intranet) s povjerljivim informacijama o vašem poslu.

Kao administrator sigurnosti, trebate zaštititi sadržaj vaše Web stranice dok, u isto vrijeme, trebate osigurati da vaše sigurnosne prakse ne utječu negativno na vašu Web stranicu. Dodatno, trebate osigurati da HTTP aktivnost ne ugrozi cjelovitost vašeg sistema ili mreže. Poglavlja koja slijede daju sigurnosne prijedloge kada koristite program.

Razmatranja o administraciji

Sljedeće su neka sigurnosna razmatranja za administriranje vašeg Internet poslužitelja.

- Izvodite postav i konfiguracijske funkcije koristeći Web pretražitelj i *ADMIN instancu. Za neke funkcije, kao što je kreiranje dodatnih instanci na poslužitelju, *morate* koristiti *ADMIN poslužitelj.
- Default URL za administrativnu home stranicu (home stranica za *ADMIN poslužitelj) je objavljen u dokumentaciji za proizvode koji osiguravaju administrativne funkcije poslužitelja. Stoga će default URL vjerojatno biti poznat hakerima i biti će objavljen u forumima hakera, kao što su i default lozinke za IBM-dobavljene profile korisnika isto tako poznate i objavljene. Možete se zaštititi od ovog izlaganja na nekoliko načina:
  - *ADMIN instancu HTTP poslužitelja izvodite samo kada trebate izvoditi administrativne funkcije. Ne izvodite *ADMIN instancu čitavo vrijeme.
  - Aktivirajte SSL podršku za *ADMIN instancu (koristeći Upravitelja digitalnih certifikata). *ADMIN instanca koristi HTTP zaštitne direktive za traženje korisničkog ID-a i lozinke. Kada koristite SSL, vaš korisnički ID i lozinka su šifrirani (zajedno sa svim drugim informacijama o vašoj konfiguraciji koje se pojavljuju na administrativnim formama).
  - Koristite vatreni zid i za zaštitu pristupa *ADMIN poslužitelju s Interneta i za skrivanje vašeg sistema i imena domene, koji su dio URL-a.
- Kada izvodite administrativne funkcije, morate se prijaviti s korisničkim profilom koji ima *IOSYSCFG posebna ovlaštenja. Možete također trebati ovlaštenje za specifične objekte na sistemu, kao što su sljedeći:
  - Knjižnice ili direktoriji koji sadrže vaše HTML dokumente i CGI programe.
  - Bilo koji korisnički profili koje planirate razmijeniti s direktivama za poslužitelj.
  - Liste kontrole pristupa (ACL-i) za bilo koje direktorije koje vaši direktivi koriste.
  - Objekt validacijske liste za kreiranje i održavanje korisničkih ID-a i lozinki.

  S *ADMIN poslužiteljem i TELNET-om, imate sposobnost udaljenog izvođenja administrativnih funkcija, možda preko Internet veze. Budite svjesni da ako izvodite

administraciju preko javne veze (Internet), možete se izlagati moćan korisnički ID ili lozinku njuškanju. ″Njuškalo″ može tada koristiti ovaj korisnički ID i lozinku za pokušaj pristupa sistemu koristeći, na primjer, TELNET ili FTP.

Bilješke:

1. S TELNET-om, ekran prijave se tretira kao bilo koji drugi ekran. Iako se lozinka ne prikazuje dok je upisujete, sistem je prenosi bez bilo kakvog šifriranja ili kodiranja.
2. S *ADMIN poslužiteljem, lozinka je kodirana, a ne šifrirana. Shema kodiranja je industrijski standard i stoga je obično poznata unutar hakerske zajednice. Iako kodiranje nije lako razumljivo običnom ″njuškalu″, sofisticirano njuškalo vjerojatno ima alate za dekodiranje lozinke.

Sigurnosni savjet

Ako planirate izvoditi udaljenu administraciju preko Interneta, trebate koristiti *ADMIN instancu sa SSL-om, tako da je vaš prijenos šifriran. Ne koristite nesigurne aplikacije, kao što je prije-V4R4 verzija TELNET-a (TELNET podržava SSL počevši s V4R4). Ako koristite *ADMIN poslužitelj preko intraneta *povjerljivih* korisnika, vjerojatno možete sigurno koristiti ovo za administraciju.

- HTTP direktive osiguravaju fondaciju za sve aktivnosti na vašem poslužitelju. Otpremljena konfiguracija pruža sposobnost posluživanja defaultne pozdravne stranice. Klijent ne može gledati nikakve dokumente osim pozdravne stranice dok poslužiteljski administrator ne definira direktive za poslužitelj. Za definiranje direktiva, koristite Web pretražitelj i *ADMIN poslužitelj ili naredbu Rad s HTTP konfiguracijom (WRKHTTPCFG). Obje metode trebaju *IOSYSCFG posebno ovlaštenje. Kada povežete vaš iSeries poslužitelj na Internet, postaje čak i kritičnije kontrolirati broj korisnika u vašoj organizaciji koji imaju *IOSYSCFG posebno ovlaštenje.

Zaštita resursa

IBM HTTP poslužitelj za iSeries uključuje HTTP direktive koje mogu osigurati detaljnu kontrolu informacijske aktive koju poslužitelj koristi. Možete koristiti direktive za kontrolu iz kojih direktorija Web poslužitelj poslužuje URL-e i za HTML datoteke i za CGI programe, da se prebaci na druge korisničke profile i da traži provjeru autentičnosti za neke resurse.

Bilješka: Dokumentacija pod ″Web posluživanje″ u Informacijski Centar osigurava potpune opise dostupnih HTTP direktiva i kako ih koristiti. Sljedeće su neki prijedlozi i razmatranja za korištenje ove podrške:

- HTTP poslužitelj se pokreće na bazi ″izričitog ovlaštenja.″ Poslužitelj ne prihvaća zahtjev osim ako taj zahtjev nije izričito definiran u direktivama. Drugim riječima, poslužitelj odmah odbija bilo koji zahtjev za URL osim ako taj URL nije definiran u direktivama (ili po imenu ili općenito).
- Možete koristiti zaštitne direktive za traženje za traženje korisničkog ID-a i lozinke prije prihvaćanja zahtjeva za neke ili sve vaše resurse.
  - Kada korisnik (klijent) zahtjeva zaštićeni resurs, poslužitelj upućuje pretražitelja na korisnički ID i lozinku. Pretražitelj traži korisnika da upiše korisnički ID i lozinku i tada šalje informacije poslužitelju. Neki pretražitelji spremaju korisnički ID i lozinku i šalju ih automatski s narednim zahtjevima. Ovo oslobađa korisnika od ponavljajućeg upisa istog korisničkog ID-a i lozinke kod svakog zahtjeva.

    Zato jer neki pretražitelji spremaju korisnički ID i lozinku, vi imate isti korisnički edukacijski zadatak koji imate kada korisnici ulaze u vaš sistem preko ekrana prijave iSeries poslužitelja ili kroz usmjeritelj. Nenadzirana sesija pretražitelja predstavlja potencijalno sigurnosno izlaganje.
  - Imate tri opcije za to kako sistem rukuje korisničkim ID-ima i lozinkama (specificirano u zaštitnim direktivama):

1. Možete koristiti korisnički profil normalnog iSeries poslužitelja i provjeru valjanosti lozinke. Ovo se najčešće koristi za zaštitu resursa u intranetu (sigurna mreža).
2. Možete kreirati ″Internet korisnike″: korisnici kojima se može provjeriti valjanost ali nemaju korisnički profil na iSeries poslužitelju. Internet korisnici se primjenjuju kroz iSeries objekt poslužitelja nazvan ″validacijska lista″. Objekti validacijske liste sadržavaju popis korisnika i lozinki koji su posebno definirani za upotrebu s posebnim aplikacijama.

   Vi odlučujete kako se Internet korisnički ID-i i lozinke dobavljaju (kao što je pomoću aplikacije ili pomoću administratora u odgovoru na zahtjev e-pošte), kao i kako upravljati Internet korisnicima. Koristite sučelje HTTP poslužitelja temeljeno na pretražitelju da ovo postavite.

   Za nesigurne mreže (Internet), koristeći Internet korisnici osiguravaju bolju opću zaštitu nego koristeći normalne korisničke profile i lozinke. Jedinstven skup korisničkih ID-a i lozinki kreira ugrađeno ograničenje na ono što ti korisnici mogu učiniti. Korisnički ID-i i lozinke nisu dostupne za normalne prijave (kao s TELNET-om ili FTP-om). Dodatno, ne izlažete normalne korisničke ID-i i lozinke za njuškanje.
3. Lightweight directory access protocol (LDAP) je uslužni protokol direktorija koji osigurava pristup direktoriju preko Transmission Control Protocol (TCP-a). Dopušta vam spremanje informacija u te usluge direktorija i upite. LDAP je podržan kao izbor za korisničku provjeru autentičnosti.

Bilješke:

1. Kada pretražitelj pošalje korisnički ID i lozinku (bilo za korisnički profil ili Internet korisnika) oni se kodiraju, ali ne šifriraju. Shema kodiranja je industrijski standard i stoga je obično poznata unutar hakerske zajednice. Iako kodiranje nije lako razumljivo običnom ″njuškalu″, sofisticirano njuškalo vjerojatno ima alate da ga dekodira.
2. iSeries poslužitelj sprema objekte provjere valjanosti u zaštićeno sistemsko područje. Možete mu pristupiti samo s definiranim sistemskim sučeljima (API-i) i prikladnom autorizacijom.

– Možete koristiti Upravitelja digitalnih certifikata (DCM) da kreirate vaš vlastiti intranet Izdavač certifikata. Digitalni certifikat automatski pridružuje certifikat s korisničkim profilom vlasnika. Certifikat ima iste autorizacije i dozvole kao pridruženi profil.

- Kada poslužitelj prihvaća zahtjev, preuzima sigurnost resursa normalnog iSeries poslužitelja. Korisnički profil koji zahtjeva resurs mora imati ovlaštenje (kao što je folder ili izvorišna fizička datoteka koja sadrži HTML dokument). Po defaultu, poslovi se izvode pod QTMHHTTP korisničkim profilom. Možete koristiti direktivu za prebacivanje na drugačiji korisnički profil. Sistem tada koristi ovlaštenje tog korisničkog profila za pristup objektima. Sljedeće su neka razmatranja za ovu podršku:
  – Zamjena korisničkih profila može biti posebno korisna kada vaš poslužitelj pruža više od jedne logičke Web stranice. Možete pridružiti različite korisničke profile s direktivama za svaku Web stranicu i ovo koristi sigurnost resursa normalnog iSeries poslužitelja da zaštiti dokumente za svaku stranicu.
  – Možete koristiti sposobnost prebacivanje korisničkih profila u kombinaciji s provjerom valjanosti objekta. Poslužitelj koristi jedinstveni korisnički ID i lozinku (odvojeno od vašeg normalnog korisničkog ID-a i lozinke) da procijeni početni zahtjev. Nakon što je poslužitelj provjerio korisnika, sistem se prebacuje na drugi korisnički profil i tako iskorištava prednost sigurnosti resursa. Korisnik se tako ne mora zabrinjavati oko istinitog imena korisničkog profila i ne može ga pokušati koristiti na druge načine (kao što je FTP).
- Neki zahtjevi HTTP poslužitelja trebaju izvoditi program na HTTP poslužitelju. Na primjer, program može pristupiti podacima na vašem sistemu. Prije nego što se program može izvoditi, poslužiteljski administrator mora mapirati zahtjev (URL) na specifičan,

korisnički definiran, program koji se prilagođava standardima CGI korisničkog sučelja. Sljedeće su neka razmatranja za CGI programe.

- Možete koristiti zaštitne direktive za CGI programe upravo kako radite i za HTML dokumente. Tako da možete trebati korisnički ID i lozinku prije izvođenja programa.
- Po defaultu, CGI programi se izvode pod QTMHHTP1 korisničkim profilom. Možete se prebaciti na drugačiji korisnički profil prije izvođenja programa. Stoga, možete postaviti sigurnost resursa normalnog iSeries poslužitelja za resurse kojima vaši CGI programi pristupaju.
- Kao sigurnosni administrator, trebate izvoditi pregled sigurnosti prije provjere autentičnosti upotrebe bilo kojeg CGI programa na vašem sistemu. Trebate znati od kuda je došao program i koje funkcije izvodi CGI program. Također trebate nadgledati sposobnosti korisničkih profila pod kojima izvodite CGI programe. Također trebate izvoditi provjeravanje s CGI programi da odredite, na primjer, da li možete dobiti pristup redu za naredbe. Tretirajte CGI programe s istom opreznošću s kojom tretirate programe koji usvajaju ovlaštenje.
- Dodatno, procijeniti koji osjetljivi objekti mogu imati neprikladno javno ovlaštenje. Slabo oblikovan CGI program može, u rijetkim slučajevima, dozvoliti zaobilaznom korisniku dobrog znanja da se pokuša slobodno kretati vašim sistemom.
- Koristite specifične korisničke knjižnice, kao što je CGILIB, da možete držati sve vaše CGI programe. Koristite ovlaštenje objekta za kontrolu i tko može smjestiti nove objekte u ovu knjižnicu i tko može izvoditi programe u ovoj knjižnici. Koristite direktive da ograničite HTTP poslužitelj na izvođenje CGI programa koji su u ovoj knjižnici.

Bilješka: Ako vaš poslužitelj osigurava višestruke logičke Web stranice, možete željeti postaviti odvojenu knjižnicu za CGI programe za svaku stranicu.

Ostala sigurnosna razmatranja

Sljedeće su ostala sigurnosna razmatranja:

- HTTP osigurava pristup samo za čitanje za vaš iSeries sistem. Zahtjevi HTTP poslužitelja ne mogu izravno ažurirati ili obrisati podatke na vašem sistemu. Međutim, možete imati CGI programe koji ažuriraju podatke. Dodatno, možete omogućiti Net.Data CGI program za pristup bazi podataka vašeg iSeries poslužitelja. Sistem koristi skriptu (koja je slična izlaznom programu) da procijeni zahtjeve Net.Data programu. Stoga, sistemski administrator može kontrolirati koje akcije Net.Data program može poduzeti.
- HTTP poslužitelj osigurava dnevnik pristupa koji možete koristiti i za pristup i za pokušaje pristupa kroz poslužitelj.

Sigurnosna razmatranja za upotrebu SSL-a s IBM HTTP poslužiteljem za iSeries

IBM HTTP poslužitelj za iSeries može pružiti sigurna Web povezivanja s vašim iSeries poslužiteljem. **Sigurna Web stranica** znači da je prijenos između klijenta i poslužitelja (u oba smjera) šifriran. Ovaj šifrirani prijenos je siguran i od ispitivanja njuškala i od onih koji pokušaju ili uhvatiti ili promijeniti prijenos.

Bilješka: Zapamtite da se Sigurna Web stranica primjenjuje strogo na sigurnost informacija koje prolaze između klijenta i poslužitelja. Namjera ovoga nije smanjiti ranjivost vašeg poslužitelja od hakera. Međutim, to sigurno ograničava informacije koje mogući haker može lako dobiti pomoću njuškanja.

Poglavlja o SSL-u i Posluživanju Weba (HTTP) i Informacijskom Centru pružaju potpune informacije za instalaciju, konfiguriranje i upravljanje šifriranom obradom. Ova poglavlja pružaju i pregled svojstava poslužitelja i neka razmatranja za korištenje poslužitelja.

Poslužitelj Internet povezivanja pruža HTTP i HTTPS podršku kada je instaliran jedan od sljedećih licencnih programa.

- 5722–NC1
- 5722–NCE

Kada su instalirane ove opcije, proizvod se tretira kao Siguran poslužitelj Internet povezivanja.

IBM HTTP Poslužitelj za iSeries (5722–DG1) pruža i http i https podršku. Morate instalirati jedan od sljedećih kriptografičkih proizvoda da omogućite SSL:

- 5722–AC2
- 5722–AC3

Sigurnost koja ovisi o šifriranju ima nekoliko zahtjeva:

- I odašiljač i primalac (poslužitelj i klijent) moraju ″razumjeti″ mehanizme šifriranja i moći izvesti šifriranje i dešifriranje. HTTP poslužitelj treba klijenta s omogućenim SSL-om. (Većina popularnih Web pretražitelja je ima omogućen SSL.) Licencni programi za iSeries šifriranje podržavaju nekoliko metoda za šifriranje s industrijskim standardom. Kada klijent pokuša postaviti sigurnu sesiju, poslužitelj i klijent se dogovaraju da mogu naći najsigurniju metodu šifriranja koju podržavaju i jedan i drugi.
- Prisluškivači ne smiju moći dešifrirati prijenos. Na taj način, metode šifriranja traže da obje strane imaju **privatni ključ** za šifriranje/dešifriranje koji samo one znaju. Ako želite imati sigurnu *vanjsku* Web stranicu, trebali bi koristiti nezavisno ovlaštenje certifikata (CA) kako bi kreirali i izdali digitalne certifikate korisnicima i poslužiteljima. Izdavač certifikata je poznat kao povjerljiva strana.

Šifriranje zaštićuje povjerljivost prenesenih informacija. Međutim, za osjetljive informacije, kao što su financijske informacije, želite cjelovitost i provjeru autentičnosti uz povjerljivost. Drugim riječima, klijenti i (neobavezno) poslužitelj moraju vjerovati strani na drugom kraju (preko neovisne reference) i moraju biti sigurni da prijenos nije mijenjan. Digitalni potpis, koji osigurava Ovlašteni izdavač certifikata (CA), pruža ovo osiguranje autentičnosti i cjelovitosti. SSL protokol osigurava provjeru autentičnosti provjeravajući digitalni potpis poslužiteljskog certifikata (i neobavezno klijentovog certifikata).

Šifriranje i dešifriranje trebaju vrijeme za obradu i utjecat će na performanse vašeg prijenosa. Stoga, iSeries poslužitelji pružaju sposobnost izvođenja programa i za sigurno i za nesigurno posluživanje u isto vrijeme. Možete koristiti nesigurni HTTP poslužitelj za posluživanje dokumenata koji ne trebaju sigurnost, kao što je katalog za vaš proizvod. Ovi dokumenti će imati URL koji počinje s http://. Možete izabrati siguran HTTP poslužitelj za osjetljive informacije kao što je obrazac gdje korisnici upisuju informacije o kreditnoj kartici. Program može posluživati dokumente čiji URL počinje ili s http:// ili s https://.

Podsjetnik

Dobra Internet etika je informiranje vaših klijenata kada je prijenos siguran i kada nije, posebno kada vaša Web stranica koristi sigurni poslužitelj za neke dokumente.

Zapamtite da šifriranje treba i sigurnog klijenta i sigurnog poslužitelja. Sigurni pretražitelji (HTTP klijenti) su postali jako česti.

Razmatranja sigurnosti za LDAP

Lightweight Directory Access Protocol (LDAP) značajke sigurnosti uključuju Sloj sigurnih utičnica (SSL), Liste kontrole pristupa i CRAM-MD5 šifriranje lozinke. U V5R1, dodane su Kerberos veze i podrška revizije sigurnosti za poboljšanje LDAP sigurnosti.

Za više informacija o ovim predmetima, pogledajte iSeries Informacijski Centar—>Mrežni rad–>TCP/IP–>Usluge Direktorija (LDAP). Pogledajte "Preduvjeti i povezane informacije" na stranici xii za informacije o pristupu iSeries Informacijskom Centru.

Sigurnosna razmatranja za LPD

LPD (demon pisača linije) osigurava sposobnost distribuiranja izlaza pisača vašem sistemu. Sistem ne radi nikakvo obrađivanje prijave za LPD.

Spriječavanje LPD pristupa

Ako *ne* želite da bilo tko koristi LPD za pristup vašem sistemu, trebate zaštiti LPD poslužitelj od izvođenja. Napravite sljedeće:

__ Korak 1. Da spriječite poslove LPD poslužitelja od automatskog pokretanja kada pokrenete TCP/IP, upišite sljedeće:

```
CHGLPDA AUTOSTART(*NO)
```

Bilješke:

a. AUTOSTART(*YES) je defaultna vrijednost.

b. "Kontrola koju TCP/IP poslužitelji pokreću automatski" na stranici 108 pruža više informacija o kontroliranju koje TCP/IP poslužitelji pokreću automatski.

__ Korak 2. Da spriječite nekoga od pridruživanja korisničke aplikacije, kao što je aplikacija utičnica, s portom koji sistem normalno koristi LPD, učinite sljedeće:

__ Korak a. Upišite GO CFGTCP za prikaz izbornika Konfiguriranje TCP/IP-a.

__ Korak b. Izaberite opciju 4 (Rad s ograničenjima TCP/IP porta).

__ Korak c. Na prikazu Rad s ograničenjima TCP/IP porta, specificirajte opciju 1 (Dodavanje).

__ Korak d. Za nižu razinu porta, specificirajte 515.

__ Korak e. Za višu razinu porta, specificirajte *ONLY.

Bilješke:

1) Ograničenja porta imaju učinak sljedeći put kada pokrenete TCP/IP. Ako je TCP/IP aktivan kada postavljate ograničenja porta, trebate zaustaviti TCP/IP i ponovo ga pokrenuti.

2) RFC1700 pruža više informacija o dodjelama broja zajedničkog porta.

__ Korak f. Za protokol, specificirajte *TCP.

__ Korak g. Za polje korisničkog profila, specificirajte ime korisničkog profila koje je zaštićeno u vašem sistemu. (Zaštićeni korisnički profil je korisnički profil koji ne posjeduje programe koji usvajaju ovlaštenje i nema lozinku koju znaju ostali korisnici.) Ograničavanjem porta na određenog korisnika, automatski isključujete sve druge korisnike.

__ Korak h. Ponavljajte korake 2c kroz 2g za *UDP protokol.

Kontrola LPD pristupa

Ako želite dozvoliti LPD klijentima pristup vašem sistemu, pazite na sljedeća sigurnosna pitanja:

- Da spriječite korisnika od preplavljanja vašeg sistema s neželjenim objektima, uvjerite se da imate prikladno postavljena ograničenja praga za vaša pomoćna spremišta memorije (ASP-i). Možete prikazati i postaviti pragove za ASP-e koristeći ili Sistemske servisne alate (SST) ili Namjenske servisne alate (DST). Knjiga *Sigurnosno kopiranje i obnavljanje* osigurava više informacija o ASP pragovima.
- Možete koristiti ovlaštenje za izlazne redove da ograničite spool datoteke na vaš sistem. LPD korisnici bez korisničkog ID-a koriste QTMPLPD korisnički profil. Možete dati pristup ovog korisničkog profila samo nekim izlaznim redovima.

Sigurnosna razmatranja za SNMP

iSeries poslužitelj se može ponašati kao simple network management protocol agent (SNMP) u mreži. SNMP osigurava sredstva za upravljanje gateway-ima, usmjerivačima i hostovima u mrežnoj okolini. SNMP agent skuplja informacije o sistemu i izvodi funkcije koje udaljeni SNMP mrežni upravitelji zahtijevaju.

Spriječavanje SNMP pristupa

Ako *ne* želite da bilo tko koristi SNMP za pristup vašem sistemu, trebate zaštiti SNMP poslužitelj od izvođenja. Napravite sljedeće:

__ Korak 1. Da spriječite poslove SNMP poslužitelja od automatskog pokretanja kada pokrenete TCP/IP, upišite sljedeće:

```
CHGSNMPA AUTOSTART(*NO)
```

Bilješke:

a. AUTOSTART(*YES) je defaultna vrijednost.

b. “Kontrola koju TCP/IP poslužitelji pokreću automatski” na stranici 108 pruža više informacija o kontroliranju koje TCP/IP poslužitelji pokreću automatski.

__ Korak 2. Da spriječite nekoga od pridruživanja korisničke aplikacije, kao što je aplikacija utičnica, s portom koji sistem normalno koristi SNMP, učinite sljedeće:

__ Korak a. Upišite GO CFGTCP za prikaz izbornika Konfiguriranje TCP/IP-a.

__ Korak b. Izaberite opciju 4 (Rad s ograničenjima TCP/IP porta).

__ Korak c. Na prikazu Rad s ograničenjima TCP/IP porta, specificirajte opciju 1 (Dodavanje).

__ Korak d. Za nižu razinu porta, specificirajte 161.

__ Korak e. Za višu razinu porta, specificirajte *ONLY.

Bilješke:

1) Ograničenja porta imaju učinak sljedeći put kada pokrenete TCP/IP. Ako je TCP/IP aktivan kada postavljate ograničenja porta, trebate zaustaviti TCP/IP i ponovo ga pokrenuti.

2) RFC1700 pruža više informacija o dodjelama broja zajedničkog porta.

__ Korak f. Za protokol, specificirajte *TCP.

__ Korak g. Za polje korisničkog profila, specificirajte ime korisničkog profila koje je zaštićeno u vašem sistemu. (Zaštićeni korisnički profil je korisnički profil koji ne posjeduje programe koji

usvajaju ovlaštenje i nema lozinku koju znaju ostali korisnici.) Ograničavanjem porta na određenog korisnika, automatski isključujete sve druge korisnike.

__ Korak h. Ponavljajte korake 2c do 2g za *UDP protokol.

Kontrola SNMP pristupa

Ako želite dozvoliti SNMP upraviteljima pristup vašem sistemu, pazite na sljedeća sigurnosna pitanja:

- Netko tko može pristupiti vašoj mreži sa SNMP-om može skupiti informacije o vašoj mreži. Informacije koje ste sakrili koristeći zamjenska imena i poslužitelj za imena domene postaju dostupne mogućem uljezu preko SNMP-a. Dodatno, uljez može koristiti SNMP da promijeni vašu mrežnu konfiguraciju i da prekine vašu komunikaciju.
- SNMP se oslanja na zajedničko ime za pristup. Konceptualno, zajedničko ime je slično lozinki. Zajedničko ime nije šifrirano. Stoga, nije osjetljivo na njuškanje. Koristite naredbu Dodavanje zajednice za SNMP (ADDCOMSNMP) da postavite parametar upravitelja Internet adresom (INTNETADR) na jednu ili više specifičnih adresa umjesto na *ANY. Također možete postaviti parametar OBJACC naredbi ADDCOMSNMP ili CHGCOMSNMP na *NONE da spriječite upravitelja u zajednici da pristupa MIB objektima. Namjera je da se ovo radi samo privremeno da se ne dopusti pristup upraviteljima u zajednici, a bez uklanjanja zajednice.

Sigurnosna razmatranja za INETD poslužitelj

Za razliku od većine TCP/IP poslužitelja, INETD poslužitelj ne pruža klijentima jednu jednostruku uslugu. Umjesto toga, on pruža raznolike mješovite usluge koje administratori mogu prilagoditi. Iz tog razloga, INETD poslužitelj se ponekad naziva ″super poslužitelj″. INETD poslužitelj ima sljedeće ugrađene usluge:

- vrijeme
- dnevno vrijeme
- jeka
- odbacivanje
- promjena

Ove usluge su podržane i za TCP i za UDP. Za UDP, usluge jeke, vremena, dnevnog vremena i promjena primaju UDP pakete, tada šalju pakete natrag davaocu. Poslužitelj jeke vraća natrag pakete jeke koje prima, poslužitelj vremena i dnevnog vremena generira vrijeme u određenom formatu i šalje ga natrag i poslužitelj promjene generira pakete ASCII znakova koji se mogu ispisati i šalje ih natrag.

Priroda ovih UDP usluga čini sistem osjetljivim na napad odbijanja usluga. Na primjer, pretpostavite da imate dva poslužitelja iSeries: SYSTEMA i SYSTEMB. Zloban programer može izmijeniti IP zaglavlje i UDP zaglavlje s izvorišnom adresom SYSTEMA i UDP brojem porta poslužitelja vremena. Tada može poslati paket poslužitelju vremena na SYSTEMB, koji će poslati vrijeme SYSTEMA, koji će odgovoriti natrag SYSTEMB i tako dalje, generirajući neprekidnu petlju i konzumirajući CPU resurse na oba sistema, ali i pojasnu širinu mreže.

Stoga, trebate razmotriti rizike takvog napada na vaš iSeries sistem i izvoditi ove usluge jedino na sigurnim mrežama. INETD poslužitelj je otpremljen tako da se ne pokrene automatski kad pokrećete TCP/IP. Možete konfigurirati da li ili ne pokrenuti usluge kad je INETD pokrenut. Po defaultu, TCP i UDP poslužitelji vremena i poslužitelji dnevnog vremena se pokreću kad pokrenete INETD poslužitelj.

Postoje dvije konfiguracijske datoteke za INETD poslužitelj:

```
/QIBM/UserData/OS400/inetd/inetd.conf
/QIBM/ProdData/OS400/inetd/inetd.conf
```

Ove datoteke određuju koji se programi pokreću kada se pokreće INETD poslužitelj. One također određuju pod kojim korisničkim profilom se izvode ovi programi kada ih pokrene INETD.

Bilješka: Konfiguracijska datoteka u proddata se ne smije nikad mijenjati. Ona se zamjenjuje svaki put kad se sistem ponovno učitava. Korisnikove konfiguracijske promjene trebaju se jedino smještati u datoteku, u direktorijskom stablu korisničkih podataka, zato što se ova datoteka **ne** ažurira za vrijeme nadogradnje izdanja.

Ako zloban programer dobije pristup ovim datotekama, treba se tako konfigurirati da pokrene bilo koji program kada se pokrene INETD. Stoga je vrlo važno da se zaštite ove datoteke. Po defaultu one zahtijevaju QSECOFR ovlaštenje da bi se napravile promjene. Ne trebate smanjiti ovlaštenje potrebno da im se pristupi.

Bilješka: Ne modificirajte konfiguracijsku datoteku u ProdData direktoriju. Ta datoteka se zamjenjuje svaki put kada se sistem ponovo učitava. Korisnikove konfiguracijske promjene trebaju se jedino smještati u datoteku u stablu direktorija Korisnički podaci, budući da se ta datoteka ne ažurira za vrijeme nadogradnje izdanja.

Sigurnosna razmatranja za ograničavanje TCP/IP roaminga

Ako je vaš sistem povezan na mrežu, možda ćete htjeti ograničiti sposobnost vaših korisnika da se slobodno kreću mrežom s TCP/IP aplikacijama. Jedan način da se ovo napravi je da se ograniči pristup sljedećim naredbama TCP/IP klijenta:

Bilješka: Ove naredbe mogu postojati u nekoliko knjižnica na vašem sistemu. One su minimalno i u QSYS knjižnici i u QTCP knjižnici. Pronađite i osigurajte sva pojavljivanja.

- STRTCPFTP
- FTP
- STRTCPTELN
- TELNET
- LPR
- SNDTCPSPLF
- RUNRMTCMD (REXEC klijent)

Moguća odredišta vaših korisnika su određena sljedećim:

- Unosi u vašoj TCP/IP host tablici.
- *DFTROUTE unos u TCP/IP tablici usmjeravanja. Ovo dozvoljava korisnicima da upišu IP adresu sljedećeg sistema na putu kada je njihovo odredište nepoznata mreža. Korisnik može dosegnuti ili kontaktirati udaljenu mrežu koristeći defaultni smjer.
- Konfiguracija imena udaljenog poslužitelja. Ova podrška dozvoljava drugom poslužitelju u mreži da locira imena hosta za vaše korisnike.
- Tablica udaljenog sistema.

Vi trebate kontrolirati tko može dodati unose u ove tablice i promijeniti vašu konfiguraciju. Također trebate razumjeti implikacije vaših unosa u tablicu i vaše konfiguracije.

Budite svjesni da korisnik s dobrim znanjem i s pristupom ILC C prevodiocu može kreirati program utičnicu koji se može pripojiti TCP ili UDP portu. Ovo možete otežati ograničavajući pristup sljedećim datotekama sučelja utičnice u knjižnici QSYSINC:

- SYS

- NETINET
- H
- ARPA
- utičnice i SSL

Za servisne programe, možete ograničiti upotrebu utičnica i SSL aplikacija koji su već prevedene ograničavajući upotrebu ovih servisnih programa:
- QSOSRV1
- QSOSRV2
- QSOSKIT(SSL)
- QSOSSLSR(SSL)

Servisni programi se otpremaju s javnim ovlaštenjem *USE, ali ovlaštenje može biti promijenjeno na *EXCLUDE (ili na drugu vrijednost kako je potrebno)

Poglavlje 14. Pristup sigurnoj radnoj stanici

Mnogi od korisnika vašeg sistema imaju osobna računala (PC-e) na svojim stolovima kao radne stanice. Oni koriste alate koje rade na PC-u i koriste PC za povezivanje na iSeries poslužitelj.

Većina metoda povezivanja PC na iSeries poslužitelj omogućuje više funkcija od emulacije radne stanice. PC može izgledati kao ekran za iSeries i omogućiti korisniku interaktivne sesije prijave. Dodatno, PC može izgledati iSeries poslužiteljima kao drugo računalo i omogućiti funkcije kao što su prijenos datoteka i poziv udaljene procedure.

Kao administrator sigurnosti iSeries poslužitelja, trebate biti svjesni sljedećeg:

- Funkcija koje su dostupne PC korisnicima koji su povezani na vaš sistem
- Resursa iSeries poslužitelja kojima PC korisnici mogu pristupiti.

Možda trebate spriječiti napredne PC funkcije (kao što su prijenos datoteka i poziv udaljene procedure) ako sigurnosna shema vašeg iSeries poslužitelja još nije pripremljena za te funkcije. Vjerojatno je vaš dugoročni cilj dozvoliti napredne PC funkcije dok još uvijek štitite informacije na vašem sistemu. Poglavlja koja slijede raspravljaju o nekim sigurnosnim pitanjima koja su pridružena PC pristupu.

Spriječavanje virusa radne stanice

Ove informacije predlažu načine koje administratori sigurnosti mogu poduzeti protiv PC virusa.

Pristup podacima sigurne radne stanice

Neki softver PC klijenta koristi dijeljene foldere za pohranjivanje informacija na poslužitelju. Za pristup datotekama iSeries baze podataka, PC korisnik ima ograničen, dobro definiran skup sučelja. Sa sposobnosti prijenosa datoteke koja je dio većine klijent/poslužitelj softvera, PC korisnik može kopirati datoteke između poslužitelja i PC-a. Sa sposobnosti pristupa bazi podataka; kao što je DDM datoteka, udaljeni SQL ili ODBC pogonitelj; PC korisnik može pristupati podacima na poslužitelju.

U ovom okruženju možete kreirati programe za presretanje i procjenu zahtjeva PC-korisnika za pristup poslužiteljskim resursima. Kad zahtjevi koriste DDM datoteku, specificirajte izlazni program u mrežnom atributu pristupu upravljanja distribuiranim podacima (DDMACC). Za neke metode PC prijenosa datoteka specificirajte izlazni program u mrežnom atributu pristupa klijentskog zahtjeva (PCSACC). Ili možete specificirati PCSACC (*REGFAC) za upotrebu funkcije registracije. Kad zahtjevi koristite druge funkcije poslužitelja za pristup podacima, možete koristiti naredbu WRKREGINF za registriranje izlaznih programa za te funkcije poslužitelja.

Međutim, izlazne programe može biti teško oblikovati, a i rijetko su jednostavni. Izlazni programi nisu zamjena za objektno ovlaštenje koje je oblikovano za zaštititi vaše objekte od neovlaštenih pristupa od bilo kojeg izvora.

Neki klijentski softver, kao što je IBM iSeries Access za Windows, koristi integrirani sistem datoteka za pohranjivanje i pristup podacima na iSeries poslužiteljima. S integriranim sistemom datoteka, cijeli poslužitelj postaje lakše dostupan PC korisnicima. Objektno ovlaštenje postaje još važnije. Kroz integrirani sistem datoteka, korisnik s dovoljnim

© Autorska prava IBM Corp. 1996, 2004

ovlaštenjem može gledati knjižnicu poslužitelja kao da je PC direktorij. Jednostavne naredbe premještanja i kopiranja mogu odmah premjestiti podatke iz knjižnice iSeries poslužitelja u PC direktorij ili obratno. Sistem automatski radi prikladne promjene na formatu podataka.

Bilješke:

1. Možete koristiti autorizacijsku listu za kontrolu upotrebe objekata u QSYS.LIB sistemu datoteka. Pogledajte “Ograničavanje pristupa QSYS.LIB sistemu datoteka” na stranici 88 za još informacija.
2. Poglavlje 11, “Upotreba Integriranog sistema datoteka za osiguravanje datoteka”, na stranici 83 daje još informacija o pitanjima sigurnosti za integrirani sistem datoteka.

Snaga integriranog sistema datoteka je u njegovoj jednostavnosti za korisnike i razvijače. S pojedinačnim sučeljem, korisnik može raditi s objektima u višestrukim okruženjima. PC korisnik ne treba poseban softver ili API-e za pristup objektima. Umjesto toga, PC korisnik može koristiti poznate PC naredbe ili “označi i klikni” za izravan rad s objektima.

Za sve sisteme koji imaju spojene PC-ove, ali osobito za sisteme koji imaju klijentski softver koji koristi integrirani sistem datoteka, dobra shema objektnih ovlaštenja je kritična. Zbog toga što je sigurnost integrirana u OS/400 proizvod, svaki zahtjev pristupa podacima mora proći kroz obradu provjeravanja ovlaštenja. Provjera ovlaštenja se primjenjuje na zahtjeve iz bilo kojeg izvora i za pristup podacima koji koristi bilo koju metodu.

Objektno ovlaštenje s pristupom radnoj stanici

Kad postavite ovlaštenje za objekte, trebate procijeniti što ovlaštenje omogućuje PC korisniku. Na primjer, kad korisnik ima *USE ovlaštenje za datoteku, korisnik može gledati ili pisati podatke u tu datoteku. Korisnik ne može promijeniti informacije u datoteci ili brisati datoteku. Za PC korisnika, gledanje je ekvivalentno “čitanju”, što korisniku daje dovoljno ovlaštenje da načini kopiju datoteke na PC. To možda nije ono što ste namjeravali.

Za neke kritične datoteke, možda trebate postaviti javno ovlaštenje na *EXCLUDE da spriječite učitavanje. Tad možete omogućiti drugu metodu za “gledanje” datoteke na poslužitelju, kao što je upotreba izbornika i programa koji prihvaćaju ovlaštenja.

Druga je opcija za spriječavanje učitavanja upotreba izlaznog programa koji se izvodi svaki put kad PC korisnik starta funkciju poslužitelja (osim interaktivne prijave). Možete specificirati izlazni program u PCSACC mrežnom atributu upotrebom naredbe Promjena mrežnog atributa (CHGNETA). Ili, možete registrirati izlazne programe upotrebom naredbe Rad s informacijama registracije (WRKREGINF). Metoda koju koristite ovisi o tome kako PC-i pristupaju podacima na vašem sistemu koji klijentski program PC-i koriste. Izlazni program (QIBM_QPWFS_FILE_SERV) se odnosi na iSeries Access i Net Server pristup na IFS. On ne spriječava pristup s PC-a s drugim mehanizmima, kao što je FTP ili ODBC.

PC softver tipično još nudi i sposobnost slanja, tako da korisnik može kopirati podatke iz PC-a u datoteku baze podataka poslužitelja. Ako niste ispravno postavili vašu shemu ovlaštenja, PC korisnik može prekriti sve podatke u datoteci s podacima iz PC-a. Ovlaštenje *CHANGE trebate pažljivo dodjeljivati. Ponovo pregledajte Dodatak D u knjizi *Uputa iSeries sigurnosti* da razumijete koje je ovlaštenje potrebno za operacije s datotekama.

iSeries Informacijski Centar daje više informacija o ovlaštenjima za PC funkcije i načinu upotrebe izlaznih programa. Pogledajte “Preduvjeti i povezane informacije” na stranici xii za detalje.

Administracija aplikacija

Administracija aplikacija je opcijski-instalabilna komponenta iSeries Navigatora, Graphical User Interface (GUI) za iSeries poslužitelj. Administracija aplikacija dozvoljava

administratorima sistema kontrolu funkcija ili aplikacija dostupnih korisnicima i grupama na određenom poslužitelju. To uključuje kontrolu funkcija dostupnih korisnicima koji pristupaju njihovom poslužitelju kroz klijente. Ovdje je važno istaknuti, da ukoliko pristupate poslužitelju iz Windows klijenta, korisnik iSeries poslužitelja, a ne Windows korisnik određuje koje su funkcije dostupne za administraciju.

Za potpunu dokumentaciju o iSeries Navigator Administraciji aplikacija, pogledajte iSeries Informacijski Centar–>Povezivanje na iSeries—>Što povezati s —>iSeries Navigatorom (../html/as400/v5r2/ic2924/info/rzaj3/rzaj3overview.htm).

Administracija politika

Politike su alat za pomoć administratorima, kad konfiguriraju softver na PC-ovima njihovih klijenata. Politike mogu ograničiti kojima funkcijama i aplikacijama korisnik može pristupati na PC-u. Politike također mogu predlagati ili stavljati na upravljanje konfiguracije koje će koristiti korisnici ili određeni PC-ovi.

Bilješka: Politike ne nude kontrolu preko resursa poslužitelja. Politike nisu zamjena za sigurnost poslužitelja. Politike se mogu koristiti da utječu na to kako iSeries Access može pristupati poslužitelju iz određenog PC-a, od određenog korisnika. Međutim, one ne mijenjaju kako se može pristupati resursima poslužitelja putem drugih mehanizama.

Politike su pohranjene na poslužitelju datoteka. Svaki put kad se korisnik prijavi na svoju Windows radnu stanicu, politike koje se primjenjuju na tog Windows korisnika, se učitavaju iz poslužitelja datoteka. Politike se primjenjuju na registar prije no što korisnik učini bilo što na radnoj stanici.

Microsoft politike u usporedbi s administracijom aplikacija

iSeries Access Express podržava dvije različite strategije za implementiranje administrativne kontrole unutar vaše mreže: Microsoft sistemske politike i iSeries Navigator Administraciju aplikacija. Razmotrite sljedeće pri odluci koja je strategija najpogodnija za vaše potrebe.

Microsoft sistemske politike

Politike su PC pogonjene, nisu ovisne o specifičnim OS/400 izdanjima. Politike se mogu primijeniti na PC-ove, kao i na Windows korisnike. To znači da se korisnici odnose na Windows korisnički profil, ne na korisnički profil poslužitelja. Politike se mogu koristiti za ″konfiguriranje″ kao i za ograničavanje. Politike će tipično ponuditi veću zrnatost od Administracije aplikacija i mogu ponuditi veći opseg funkcija. To je stoga što povezivanje na poslužitelja nije potrebno za određivanje da li korisnik može koristiti funkciju ili ne. Primjena politika je kompliciranija od primjene Administracije aplikacija, zato što je potrebna upotreba Microsoft sistemskog editora politika, a PC-ovi se moraju pojedinačno konfigurirati za učitavanje politika.

iSeries Navigator administracija aplikacija

Administracija aplikacija pridružuje podatke korisničkom profilu, umjesto Windows profilu s kojim se Microsoft sistemske politike pridružuju. Dok su iSeries poslužitelji koji izvode V4R3 ili kasnije od OS/400 proizvoda potrebni da bi koristili Administraciju aplikacija, neke su funkcije jedino dostupne u V4R4 ili kasnije. Administracija aplikacija koristi grafičko sučelje korisnika iSeries Navigatora za administraciju, što je dosta jednostavnije koristiti od editora politika. Informacije Administracije aplikacija se primjenjuju na korisnika bez obzira na PC s kojeg se prijavljuje. Određene funkcije unutar iSeries Navigatora mogu se ograničiti.

Administracija aplikacija se preporučuje ako su sve funkcije koje želite koristiti Administracijsko aplikacijsko-omogućene i ako verzija OS/400 koja se koristi podržava Administraciju aplikacija.

Upotreba SSL-a s iSeries Access za Windows

Za informacije o upotrebi iSeries Access Express sa SSL-om, pregledajte iSeries Informacijski Centar poglavlja *Administracija Sloja sigurnih utičnica, Osiguravanje iSeries Access Express i iSeries Navigator, iSeries Developer Kit za Java , i iSeries Java Toolbox* pod Java glavnim poglavljem. Također možete ponovo pregledati ove informacije na CD-u koji je dostavljen s vašim sistemom.

iSeries Navigator sigurnost

iSeries Navigator osigurava sučelje koje je jednostavno za korištenje na vašem poslužitelju, za korisnike koji imaju iSeries Access. Sa svakim novim izdanjem OS/400 proizvoda, postaje dostupno više funkcija poslužitelja kroz iSeries Navigator. Sučelje koje je lako za korištenje daje mnoge koristi, uključujući smanjene troškove tehničke podrške i poboljšanu sliku vašeg sistema. Ono također predstavlja izazov sigurnosti.

Kao administrator sigurnosti, više se ne možete pouzdati u neznanje vaših korisnika pri zaštititi vaših resursa. iSeries Navigator čini mnoge funkcije laganim i vidljivim za vaše korisnike. Trebate osigurati da ste oblikovali i implementirali sigurnosne politike za korisničke profile i za objektnu sigurnost da zadovoljite vaše sigurnosne potrebe.

V4R4 i kasnije verzije IBM e(logo)server iSeries Access za Windows-a daju sljedeće metode kontrole funkcija koje korisnici mogu izvoditi kroz iSeries Navigatora:

- Selektivno instaliranje
- Administracija aplikacija
- Windows NT sistemska podrška politika

iSeries Navigator je pakiran u višestruke komponente koje možete posebno instalirati. To vam omogućuje instaliranje samo onih funkcija koje vam trebaju. Administracija aplikacija omogućuje administratoru kontrolu funkcija kojima korisnik ili grupa može pristupiti kroz iSeries Navigator. Administracija aplikacija organizira aplikacije u sljedeće kategorije:

iSeries Navigator
Uključuje iSeries Navigator i plug-inove.

Aplikacije klijenta
Sadrži sve druge aplikacije klijenta, uključujući iSeries Access, koji osigurava funkcije na klijentima koji se administriraju preko Administracije aplikacija.

Aplikacije hosta
Uključuju sve aplikacije koje se u potpunosti nalaze na vašem poslužitelju i omogućuju funkcije koje su administrirane kroz Administraciju aplikacija.

Možete koristiti selektivno instaliranje, administraciju aplikacija i politike da ograničite iSeries Navigator funkcije koje može koristiti korisnik. Nijedno od ovih, ipak, ne treba koristiti za sigurnost resursa.

Počevši od V4R4, IBM e(logo)server iSeries Access za Windows također podržava upotrebu Windows NT Editora politika sistema za kontrolu koje se funkcije mogu izvoditi iz određenog PC klijenta, bez obzira tko koristi PC.

Pogledajte iSeries Informacijski Centar za dodatne informacije o selektivnom instaliranju, Administraciji aplikacija i Administraciji politika. “Ograničenje pristupa funkcijama programa” na stranici 5 sekcija ove knjige također sadržava neke rasprave o administraciji aplikacija.

Spriječavanje ODBC pristupa

Povezljivost otvorenih baza podataka (ODBC) je alat koji PC aplikacije mogu koristiti za pristup iSeries podacima kao da su podaci PC podaci. ODBC programer može načiniti fizičku lokaciju podataka transparentnu korisniku PC aplikacije. Za više informacija o ODBC sigurnosnim razmatranjima, otiđite na ″iSeries Access za Windows ODBC sigurnost″ informacije (/rzaii/rzaiiodbc09.HTM), locirane u iSeries Informacijskom Centru.

Razmatranja sigurnosti za lozinke sesija radne stanice

Tipično, kad PC korisnik pokrene softver za povezivanje, kao što je iSeries Access, korisnik jednom upisuje ID korisnika i lozinku za poslužitelja. Lozinka se šifrira i pohranjuje u memoriju PC-a. Kad god korisnik uspostavi novu sesiju na istom poslužitelju, PC automatski šalje ID korisnika i lozinku.

Neki klijent/poslužitelj softver također nudi opcije premošćenja ekrana za Prijavu za interaktivne sesije. Softver će poslati ID korisnika i šifriranu lozinku kad korisnik pokrene interaktivnu (5250 emulacija) sesiju. Za podršku ove opcije, sistemska vrijednost QRMTSIGN na poslužitelju mora biti postavljena na *VERIFY.

Kad izaberete dozvoljavanje premošćivanja ekrana Prijave, trebate razmotriti sigurnosne rizike.

Izlaganje sigurnosti: Za 5250 emulaciju ili bilo koji drugi tip interaktivne sesije, ekran Prijave je isti kao bilo koji drugi ekran. Iako lozinka nije prikazana na ekranu kad se upisuje, lozinka se šalje putem veze u nešifriranom obliku kao i bilo koje drugo polje podataka. Za neke tipove veza, ovo može omogućiti priliku mogućim uljezima da nadgledaju vezu i otkriju ID korisnika i lozinku. Nadgledanje veze upotrebom elektroničke opreme često se naziva **njuškanje**. Počevši s V4R4, možete koristiti Sloj sigurnih utičnica (SSL) kako bi šifrirali informacije između iSeries Access i iSeries poslužitelja. Ovo štiti vaše podatke, uključujući i lozinke, od njuškanja.

Kad izaberete opciju premošćivanja ekrana Prijave, PC šifrira lozinku prije njenog slanja. Šifriranje izbjegava mogućnost krađe lozinke pomoću njuškanja. Međutim, morate osigurati da vaši PC korisnici vježbaju operativnu sigurnost. Nenadzirani PC s aktivnom sesijom na iSeries sistemu daje nekome priliku da pokrene drugu sesiju bez poznavanja ID-a korisnika i lozinke. PC-ove treba postaviti tako da se zaključavaju kad je sistem duže razdoblje neaktivan i trebali bi tražiti lozinku za nastavak sesije.

Čak i ako ne izaberete premošćivanje ekrana Prijave, nenadzirani PC s aktivnom sesijom predstavlja izlaganje sigurnosti. Upotrebom PC softvera, netko može pokrenuti sesiju poslužitelja i pristupiti podacima, opet bez poznavanja ID-a i lozinke korisnika. Izlaganje s 5250 emulacijom je donekle veće, jer treba manje znanja za pokretanje sesije i početak pristupa podacima.

Morate i školovati svoje korisnike o učincima koje ima prekidanje veze njihovih iSeries Access sesija. Mnogi korisnici pretpostavljaju (logično, ali netočno) da opcija odspajanja potpuno zaustavlja njihovu vezu na poslužitelj. Zapravo, kad korisnik bira opciju odspajanja, poslužitelj napravi korisničku sesiju (licencu) dostupnom drugom korisniku. Međutim, klijentova veza na poslužitelj još je otvorena. Drugi korisnik može doći do nezaštićenog PC-a i dobiti pristup resursima poslužitelja i bez unosa korisničkog ID-a i lozinke.

Svojim korisnicima koji trebaju prekinuti svoje sesije možete predložiti dvije opcije:

- Osigurajte da njihovi PC-ovi imaju funkciju koja traži lozinku. Ovo uzrokuje da nenadzirani PC postane neraspoloživ za bilo koga tko ne zna lozinku.
- Da potpuno prekinete sesiju ili se odjavite iz Windowsa ili ponovno pokrenite (ponovno podignite) PC. To prekida sesiju na iSeriesu.

Također trebate naučiti vaše korisnike o mogućim izlaganjima sigurnosti kad koriste iSeries Access za Windows. Kad korisnik specificira UNC (univerzalna konvencija za imenovanje) da identificira iSeries resurs, Win95 ili NT klijent izgrađuje mrežno povezivanje na vezu s poslužiteljem. Zbog toga što korisnik specificira UNC, korisnik ovo ne vidi kao mapirani Mrežni pogon. Često, korisnik i nije svjestan postojanja mrežne veze. Međutim, ova mrežna veza predstavlja izlaganje sigurnosti na nenadziranom PC-u, jer se poslužitelj pojavljuje u stablu direktorija na PC-u. Ako korisnička sesija ima moćan korisnički profil, resursi poslužitelja mogu biti razotkriveni na nenadziranom PC-u. Kao i kod prethodnog primjera, lijek je osiguravanje da i korisnici razumiju izlaganje i da koriste funkciju zaključavanja svoga PC-a.

Zaštita poslužitelja od udaljenih naredbi i procedura

Upućen PC korisnik sa softverom kao što je iSeries Access može izvoditi naredbe na poslužitelju bez prolaska kroz ekran Prijave. Slijedi nekoliko metoda koje su dostupne PC korisnicima za izvođenje naredbi poslužitelja. Vaš klijent/poslužitelj softver određuje metode koje su dostupne vašim PC korisnicima.

- Korisnik može otvoriti DDM datoteku i koristiti funkciju udaljene naredbe za izvođenje naredbe.
- Neki softver, kao što je iSeries Access optimizirani klijenti, omogućuje funkciju udaljene naredbe kroz API-je Poziva distribuiranog programa (DPC), bez upotrebe DDM-a.
- Neki softver, kao što je udaljeni SQL i ODBC, omogućuju funkciju udaljene naredbe bez DDM-a ili DPC-a.

Za klijent/poslužitelj softver koji koristi DDM za podršku udaljene naredbe, možete koristi DDMACC mrežni atribut da potpuno spriječite udaljene naredbe . Za klijent/poslužitelj softver koji koristi drugu poslužiteljsku podršku, možete registrirati izlazne programe za poslužitelja. Ako želite dozvoliti udaljene naredbe, morate provjeriti da li vaša shema objektnih ovlaštenja primjereno štititi vaše podatke. Sposobnost udaljene naredbe je ekvivalentna davanju reda za naredbe korisniku. Dodatno, kad iSeries primi udaljenu naredbu kroz DDM, sistem ne forsira postavljanje Ograničene sposobnosti (LMTCPB) korisničkog profila.

Zaštita radnih stanica od udaljenih naredbi i procedura

IBM iSeries Access za Windows omogućuje sposobnost primanja udaljenih naredbi na PC. Možete koristiti naredbu Izvođenje udaljene naredbe (RUNRMTCMD) na poslužitelju da izvedete proceduru na pripojenom PC-u. RUNRMTCMD sposobnost je vrijedan alat za sistemske administratore i pomoćno osoblje. Međutim, on također daje priliku za oštećenje PC podataka ili namjerno ili slučajno.

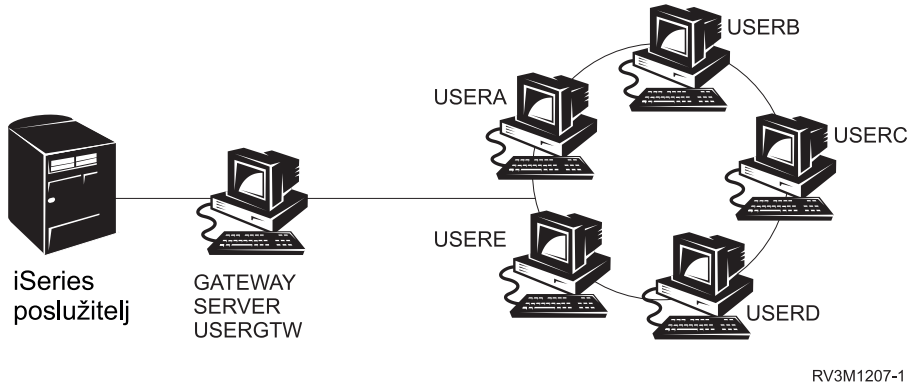
PC-ovi nemaju iste funkcije objektnih ovlaštenja kao iSeries poslužitelji. Vaša najbolja zaštita od problema s RUNRMTCMD naredbom je pažljivo ograničavanje korisnika sistema koji imaju pristup ovoj naredbi. IBM iSeries Access za Windows omogućuje sposobnost registriranja korisnika koji mogu izvoditi udaljene naredbe na određenom PC-u. Kad je veza preko TCP/IP-a, možete koristiti kontrolni panel svojstava na klijentu za kontrolu pristupa udaljenih naredbi. Korisnike možete ovlastiti putem ID-a korisnika ili imena udaljenog

sistema. Kad je veza preko SNA, neki softver klijenta omogućuje sposobnost postavljanja sigurnosti konverzacije. S drugim klijentskim softverom, jednostavno birate hoćete li ili ne postaviti sposobnost dolazne naredbe.

Za svaku kombinaciju klijentskog softvera i tipa veze (kao što je TCP/IP ili SNA), trebate pregledati mogućnosti za dolazne naredbe na pripojenim PC-ovima. Pogledajte u dokumentaciju klijenta i nađite "dolazna naredba" ili "RUNRMTCMD". Budite spremni savjetovati PC korisnike i mrežne administratore o ispravnom (sigurnom) načinu konfiguriranja klijenata da dozvole ili spriječe ovu sposobnost.

Gateway poslužitelji

Vaš sistem može sudjelovati u mreži s posrednim ili prilaznim poslužiteljem između iSeries sistema i PC-a. Na primjer, vaš iSeries sistem može biti pripojen na LAN s PC poslužiteljem koji ima PC-e koji su pripojeni na poslužitelja. Sigurnosna pitanja u ovoj situaciji ovise o sposobnostima softvera koji se izvodi na gateway poslužitelju. Slika 13 pokazuje primjer konfiguracije gateway-poslužitelja:



Slika 13. iSeries sistem s gateway poslužiteljem

S nekim softverom, vaš iSeries sistem neće znati o bilo kojim korisnicima (kao što su USERA ili USERC) koji su nizvodno od gateway poslužitelja. Poslužitelj će se prijaviti na sistem kao pojedinačan korisnik (USERGTW). On će koristiti USERGTW korisnički ID za rukovanje svim zahtjevima nizvodnih korisnika. Zahtjev od USERA će poslužitelju izgledati kao zahtjev od korisnika USERGTW.

U ovakvom slučaju, morate se pouzdati u gateway poslužitelja za forsiranje sigurnosti. Morate razumjeti i upravljati sigurnosnim sposobnostima prilaznog poslužitelja. Iz perspektive iSeries poslužitelja, svaki korisnik ima ista ovlaštenja kao korisnički ID koji gateway poslužitelj koristi za pokretanje sesije. Na ovo možete gledati kao na ekvivalent izvođenja programa koji prihvaća ovlaštenja i omogućuje red za naredbe.

S drugim softverom, gateway poslužitelj prosljeđuje zahtjeve od pojedinačnih korisnika iSeries poslužiteljima. iSeries poslužitelj zna da USERA zahtijeva pristup određenom objektu. Gateway je takoreći proziran za sistem.

Ako je vaš sistem u mreži koja ima gateway poslužitelje, trebate procijeniti koliko ćete ovlaštenja dati korisničkim ID-evima koji se koriste od gateway poslužitelja. Također trebate razumjeti sljedeće:
- Sigurnosne mehanizme koje gateway poslužitelji forsiraju.
- Kako će nizvodni korisnici izgledati vašem iSeries sistemu.

Bežične LAN komunikacije

Neki klijenti mogu koristi iSeries Bežični LAN da komuniciraju s vašim sistemom bez žica. iSeries Bežični LAN koristi tehnologiju komunikacije pomoću radio frekvencija. Kao administrator sigurnosti trebate biti svjesni sljedećih sigurnosnih karakteristika iSeries Bežičnih LAN proizvoda:

- Ovi bežični LAN proizvodi koriste tehnologiju raširenog spektra. Ovu istu tehnologiju je koristila vlada u prošlosti kako bi osigurala radio prijenose. Za nekoga tko pokuša elektronički nadgledati prijenose podataka, prijenosi izgledaju prije kao šum nego kao pravi prijenos.
- Bežično povezivanje ima tri konfiguracijska parametra vezana uz sigurnost.
  - Podatkovna brzina (dvije moguće brzine podataka)
  - Frekvencija (pet mogućih frekvencija)
  - Sistemski identifikator (8 milijuna identifikatora)

  Kombinacija ovih konfiguracijskih elemenata pruža 80 milijuna mogućih konfiguracija, što čini hakerovu vjerojatnost pogađanja ispravne konfiguracije posebno niskom.
- Upravo kao i s ostalim komunikacijskim metodama, na sigurnost bežičnih komunikacija utječe sigurnost uređaja klijenta. Sistemske ID informacije i drugi konfiguracijski parametri su u datoteci na uređaju klijenta i trebaju biti zaštićene.
- Ako je bežični uređaj izgubljen ili ukraden, normalne poslužiteljske sigurnosne mjere, kao na primjer lozinke za prijavu i sigurnost objekta, osiguravaju zaštitu kada neovlašteni korisnik pokuša koristiti izgubljenu ili ukradenu jedinicu da pristupi vašem sistemu.
- Ako je jedinica bežičnog klijenta izgubljena ili ukradena, trebate razmotriti promjenu sistemskih ID informacija za sve korisnike, pristupne točke i sisteme. Razmislite o ovome kao o mijenjanju brave na vašim vratima ako je ukraden svežanj ključeva.
- Možda ćete htjeti particionirati vaš poslužitelj u grupe klijenata koji imaju jedinstvene sistemske ID-ove. Ovo ograničava utjecaj ako se jedinica izgubi ili ukrade. Ova metoda radi samo ako možete ograničiti grupu korisnika na specifičan dio vaših instalacija.
- Za razliku od tehnologije ožičenog LAN-a, tehnologija bežičnog LAN-a je vlasnička. Stoga, elektronička njuškala nisu javno dostupna za ove bežične LAN proizvode. Njuškalo je elektronički uređaj koji izvodi neovlašteno nadgledanje prijenosa.

Poglavlje 15. Sigurnosni izlazni programi

Neke funkcije iSeries poslužitelja daju izlaz tako da vaš sistem može izvoditi korisnik-kreirane programe da obavi dodatno provjeravanje i provjeru valjanosti. Na primjer, možete postaviti sistem da izvoditi izlazni program svaki put kad netko pokuša otvoriti DDM (upravljanje distribuiranim podacima) datoteku na vašem sistemu. Možete koristiti funkciju registracije da specificirate programe izlaza koji se izvode pod određenim uvjetima.

Nekoliko iSeries publikacija sadržavaju primjere programa izlaza koji obavljaju funkcije sigurnosti. Tablica 24 daje listu tih izlaznih programa i izvora za programe primjere.

Tablica 24. Izvori primjera izlaznih programa

Tip izlaznog programa	Svrha	Gdje naći primjere
Provjera valjanosti lozinke	Sistemska vrijednost QPWDVLDPGM može specificirati ime programa ili pokazivati da programi provjere valjanosti registrirani za QIBM_QSY_VLD_PASSWRD izlaznu točku budu korišteni za provjeru nove lozinke za dodatne zahtjeve kojima ne rukuju sistemske vrijednosti QPWDxxx. Upotrebu ovog programa treba pažljivo nadgledati jer prima nešifrirane lozinke. Ovaj program **ne treba** pohranjivati lozinke u datoteku ili ih prosljeđivati drugom programu.	• *Implementacijski vodič za iSeries Sigurnost i revizija, GG24–4200* • *Uputa iSeries sigurnosti*, SC41-5302-07
PC Podrška/400 ili Client Access pristup[1]	Možete specificirati ime ovog programa u parametru Pristupa zahtjeva klijenta (PCSACC) mrežnih atributa za kontrolu sljedećih funkcija: • Funkciju virtualnog pisača • Funkciju prijenosa datoteke • Funkciju dijeljenih foldera tipa 2 • Funkciju poruke pristupa klijenta • Redove podataka • Funkciju udaljenog SQL-a	*Implementacijski vodič za iSeries Sigurnost i revizija, GG24–4200*
Pristup Upravljanja distribuiranim podacima (DDM)	Možete specificirati ime ovog programa u parametru Pristupa DDM zahtjeva (DDMACC) mrežnih atributa za kontrolu sljedećih funkcija: • Funkciju dijeljenih foldera tipa 0 i 1 • Funkciju Submitiranja udaljene naredbe	*Implementacijski vodič za iSeries Sigurnost i revizija, GG24–4200*
Daljinska prijava	Možete specificirati program u QRMTSIGN sistemskoj vrijednosti za kontrolu koji se korisnici mogu automatski prijaviti iz kojih lokacija (prolaz-kroz.)	*Implementacijski vodič za iSeries Sigurnost i revizija, GG24–4200*
Povezljivost otvorenih baza podataka (ODBC) s iSeries Access[1]	Kontrolirajte sljedeće funkcije ODBC-a: • Da li je ODBC uopće dozvoljen. • Koje su funkcije dozvoljene za datoteke iSeries baze podataka. • Koji su SQL izrazi dozvoljeni. • Koje se informacije mogu dohvatiti o objektima poslužitelja baze podataka. • Koje su funkcije SQL kataloga dozvoljene.	Nijedan dostupan.

© Autorska prava IBM Corp. 1996, 2004

Tablica 24. Izvori primjera izlaznih programa (nastavak)

Tip izlaznog programa	Svrha	Gdje naći primjere
Program rukovanja QSYSMSG prekidom	Možete kreirati program za nadgledanje QSYSMSG reda poruka i poduzeti prikladnu akciju (kao što je obavještavanje administratora sigurnosti) ovisno o tipu poruke.	*Implementacijski vodič za iSeries Sigurnost i revizija, GG24–4200*
TCP/IP	Nekoliko TCP/IP poslužitelja (kao što su FTP, TFTP, TELNET i REXEC) omogućuju izlazne točke. Možete dodati izlazne programe za rukovanje prijave provjere valjanosti korisničkih zahtjeva, kao što je zahtjev za dohvaćanjem ili stavljanjem određene datoteke. Ove izlaze također možete koristiti da omogućite anoniman FTP na vašem sistemu.	"TCP/IP Postojanje korisnika u *iSeries Sistemske API reference* knjiga"
Promjene korisničkog profila	Možete kreirati izlazne programe za sljedeće naredbe korisničkog profila: CHGUSRPRF CRTUSRPRF DLTUSRPRF RSTUSRPRF	• *Uputa iSeries sigurnosti*, SC41-5302-07 • "TCP/IP Postojanje korisnika u *iSeries Sistemske API reference* knjiga"

Bilješke:

1. Dodatne se informacije o ovom predmetu mogu naći u iSeries Informacijskom Centru. Pogledajte "Preduvjeti i povezane informacije" na stranici xii za više detalja.

Poglavlje 16. Razmatranja sigurnosti za Internet pretražitelje

Mnogi PC korisnici u vašoj organizaciji imaju pretražitelje na svojim radnim stanicama. Oni se mogu povezati na Internet. Oni se također mogu povezati na vaš poslužitelj. Slijede neka razmatranja o sigurnosti i za PC-je i za vaš poslužitelj.

Rizik: oštećenje radne stanice

Web stranica koju vaš korisnik posjećuje može imati pridružen ″program,″ kao što je Java aplet, Active-X kontrolu ili neki drugi tip plug-ina. Iako je to rijetko, kad se ovaj tip ″programa″ izvodi na PC-ju postoji mogućnost da se oštete informacije na PC-ju. Kao administrator sigurnosti, razmotrite sljedeće za zaštitu PC-ja u vašoj organizaciji:

- Shvatite sigurnosne opcije različitih pretražitelja koje imaju vaši korisnici. Na primjer, s nekim pretražiteljima, Vi možete kontrolirati pristup koji Java apleti imaju izvan pretražitelja (ograničena operacijska okolina Jave zove se *sandbox*). Ovo može spriječiti aplete od oštećivanja PC podataka.

  Bilješka: Koncept sandboxa i njegova pridružena sigurnosna ograničenja ne postoje za Active-X i druge plug-inove.
- Dajte preporuke svojim korisnicima o postavkama njihovih pretražitelja. Vi vjerojatno nemate ni vrijeme niti resurse da osigurate da vaši korisnici slijede vaše preporuke. Stoga, morate ih educirati o potencijalnim rizicima neprikladnih postavki.
- Razmotrite standardizaciju na Web pretražiteljima koji daju sigurnosne opcije koje vam trebaju.
- Uputite vaše korisnike da vas informiraju o bilo kakvom sumnjivom ponašanju ili simptomima koji mogu biti pridruženi određenim Web stranicama.

Rizik: pristup do iSeries direktorija kroz mapirane pogone

Pretpostavimo da je PC povezan na vaš poslužitelj s IBM iSeries Access za Windows sesijom. Sesija postavlja mapirane pogone da se poveže s iSeries integriranim sistemom datoteka. Na primjer, **G** pogon na PC-u se može mapirati na integrirani sistem datoteka poslužitelja SYSTEM1 u mreži.

Sad pretpostavimo da PC korisnik ima pretražitelj i može pristupiti Internetu. Korisnik zahtijeva Web stranicu koja izvodi nevaljali ″program″ kao što je Java aplet ili Active-X kontrola. Razumljivo, program može pokušati izbrisati sve na PC-ovom G pogonu.

Imate nekoliko zaštita od šteta za mapirane pogone:

- Vaša najvažnija zaštita je zaštita resursa na vašem poslužitelju. Java aplet ili Active-X kontrola poslužitelju izgledaju kao korisnici koji su uspostavili PC sesiju. Trebate pažljivo upravljati s onim za što su PC korisnici ovlašteni raditi na vašem poslužitelju.
- Savjetujte vaše PC korisnike da postave svoje pretražitelje da spriječe pokušaje pristupa mapiranim pogonima. Ovo radi za Java aplete ali ne za Active-X kontrole, koji nemaju sandbox koncept.
- Educirajte vaše korisnike o opasnostima povezivanja na vašeg poslužitelja i Internet u istoj sesiji. Također, osigurajte da vaši PC korisnici (sa Windows 95 klijentima, na primjer) razumiju da pogoni ostaju mapirani i kad izgleda kao da se iSeries Access sesija završava.

© Autorska prava IBM Corp. 1996, 2004

Rizik: pouzdani potpisani apleti

Vaši su korisnici možda slijedili vaše savjete i postavili svoje pretražitelje da spriječe aplete od pisanja u bilo koji PC pogon. Međutim, vaši PC korisnici trebaju biti svjesni da *potpisan aplet* može nadjačati postavke za njihovog pretražitelja.

Potpisani aplet ima pridružen digitalni potpis da postavi svoju autentičnost. Kad korisnik pristupa Web stranici koja ima potpisan aplet, korisnik vidi poruku. Poruka označava potpis apleta (tko ga je potpisao i kad je potpisan). Kad vaš korisnik prihvati aplet, korisnik dopušta apletu nadjačavanje sigurnosnih postavki za pretražitelja. Potpisan aplet može pisati na lokalne pogone PC-ja, iako defaultna postavka za pretražitelja to spriječava. Potpisan aplet također može pisati u mapirane pogone na vašem poslužitelju jer oni PC-ju izgledaju kao lokalni pogoni.

Za vaše vlastite Java aplete koji dolaze od vašeg poslužitelja, možda ćete trebati koristiti potpisane aplete. Međutim, trebate uputiti vaše korisnike da općenito ne prihvaćaju potpisane aplete od nepoznatih izvora.

Poglavlje 17. Povezane informacije

Priručnici

- *APPC programiranje*, SC41-5443-00opisuje naprednu podršku program-program komunikacije (APPC) za iSeries sistem. Ova knjiga je vodič za razvoj aplikacijskih programa koji koriste APPC i definiranje komunikacijskog okruženja za APPC komunikacije. Ona uključuje razmatranja o aplikacijskim programima, konfiguracijskim zahtjevima i naredbama, upravljanju problemima za APPC i općenita razmatranja o mrežnom radu. Pogledajte CD-ROM iSeries Informacijski Centar.
- *AS/400 Internet sigurnost: Zaštita vašeg AS/400 od ŠTETE na Internetu* Redbook, SG24-4929 objašnjava sigurnosna pitanja i rizike koji se odnose na povezivanje vašeg iSeries na Internet. On daje primjere, preporuke, savjete i tehnike za TCP/IP aplikacije.
- *Sigurnosno kopiranje i obnavljanje*, SC41-5304-07 daje informacije o planiranju strategije sigurnosnog kopiranja i obnavljanja, spremanju informacija vašeg sistema, i obnavljanju vašeg sistema. Pogledajte iSeries Informacijski Centar. Dodatne informacije o ovim predmetima se također mogu naći u iSeries Informacijski Centar. Pogledajte “Preduvjeti i povezane informacije” na stranici xii za više detalja.
- *CL programiranje*, SC41-5721-06, daje detaljne opise za kodiranje specifikacija za opis podataka (DDS) za datoteke koje se mogu eksterno opisati. Te datoteke su fizičke, logičke, datoteke ekrana, pisača i funkcija međusistemske komunikacije (ICF). Pogledajte iSeries Informacijski Centar.
- CL poglavlje u Informacijskom Centru (Pogledajte “Preduvjeti i povezane informacije” na stranici xii za više detalja.) daje opis cijelog iSeries kontrolnog jezika (CL) i njegovih OS/400 naredbi. OS/400 naredbe se koriste kako bi se zatražile funkcije Operating System/400 (5722-SS1) licencnog programa. Sve ne-OS/400 CL naredbe--one povezane s drugim licencnim programima, uključujući sve raznolike jezike i pomoćne programe--su opisane u drugim knjigama koje podržavaju te licencne programe.
- *Implementiranje iSeries sigurnosti, 3. izdanje* od Wayne Madden-a i Carol Woodbury. Loveland, Colorado: 29th Street Press, a division of Duke Communications International, 1998. Daje upute i praktične prijedloge za planiranje, postavljanje i upravljanje iSeries sigurnosti.

  ISBN narudžbeni broj:

  1-882419-78-2
- Za više informacija koje se tiču HTTP poslužitelja, pogledajte sljedeći URL:

  `http://www.ibm.com/eserver/iseries/software/http/docs/doc.htm`
- *Uputa iSeries sigurnosti*, SC41-5302-07, daje potpune informacije o vrijednostima sistemske sigurnosti, korisničkim profilima, sigurnosti resursa i reviziji sigurnosti. Ovaj priručnik ne opisuje sigurnost za specifične licencne programe, jezike, i pomoćne programe. Pogledajte iSeries Informacijski Centar.
- Poglavlje ″Osnovne sistemske operacije″ u Informacijskom Centru daje informacije o nekim od ključnih koncepata i zadataka potrebnih za iSeries osnovne operacije. Pogledajte “Preduvjeti i povezane informacije” na stranici xii za više detalja.
- Informacijski Centar opisuje kako koristiti i konfigurirati TCP/IP i nekoliko TCP/IP aplikacija, kao što su FTP, SMTP i TELNET. Pogledajte “Preduvjeti i povezane informacije” na stranici xii za više detalja.
- *TCP/IP Poslužiteljska podrška za datoteku za OS/400 Instalacija i Vodič za korisnike*, SC41-0125, daje uvodne informacije, instalacijske upute i procedure postavljanja za

© Autorska prava IBM Corp. 1996, 2004

Poslužiteljska podrška za datoteku ponudu licencnih programa. On objašnjava funkcije dostupne s proizvodom i uključuje primjere i savjete za njihovo korištenje s drugim sistemima.

- *Kriterij procjene pouzdanosti računalnih sistema* DoD 5200.28.STD, opisuje kriterij za razine povjerenja za računalne sisteme. TCSEC je publikacija vlade Sjedinjenih Država. Kopije se mogu dobiti od:

  Office of Standards and Products
  National Computer Security Center
  Fort Meade, Maryland 20755-6000 USA
  Pažnja: Chief, Computer Security Standards
- Informacijski Centar sadržava nekoliko poglavlja koja se tiču Upravljanja sistemom i Upravljanja poslom u iSeries. Neki od ovih poglavlja uključuju zbirku podataka performansi, upravljanje sistemskim vrijednostima i upravljanje memorijom. Za detalje o pristupu Informacijskom Centru, pogledajte “Preduvjeti i povezane informacije” na stranici xii. Upravljanje poslom, SC41-5306-03, daje informacije o načinu kreiranja i mijenjanja okruženja upravljanja poslom. Pogledajte iSeries Informacijski Centar.

Dodatno ovim poglavljima Informacijskog Centra i Dopunskim priručnicima, za pomoć možete koristiti sljedeće resurse:

- **IBM SecureWay**
  IBM SecureWay sadrži uobičajene proizvode za IBM portfelj ponuda sigurnosti; hardver, softver, konzalting i usluge kako bi se pomoglo korisnicima da osiguraju svoju informacijsku tehnologiju. Bez obzira da li se radi o pojedinačnim potrebama ili o kreiranju rješenja za čitavo poduzeće, IBM SecureWay ponude osiguravaju vještine koje su potrebne za planiranje, oblikovanje, implementiranje i djelovanje rješenja sigurnosti za posao. Kako bi dobili više informacija o IBM SecureWay ponudama, posjetite IBM SecureWay početnu stranicu:

  `http://www.ibm.com/secureway`
- **Ponude usluga**
  Instaliranje novog hardvera ili softvera može na koncu povećati vašu djelotvornost i poslovne operacije. Ali također postavlja prijetnju za prekid posla i vrijeme kvara i može trošiti vaše vrijedne interne resurse. IBM Globalne usluge osiguravaju usluge koje se odnose na iSeries sigurnost. Sljedeća vam Web stranica omogućuje traženje potpunog ispisivanja usluga za vaš iSeries:

  `http://www.as.ibm.com/asus`

Napomene

Ove informacije su razvijene za proizvode i usluge koji se nude u SAD.

IBM ne mora nuditi proizvode, usluge ili dodatke razmatrane u ovom dokumentu u drugim zemljama. Posavjetujte se sa svojim lokalnim IBM predstavnikom za informacije o proizvodima i uslugama koji su trenutno dostupni u vašem području. Bilo koje upućivanje na IBM proizvod, program ili uslugu nema namjeru tvrditi da se samo taj IBM proizvod, program ili usluga mogu koristiti. Bilo koji funkcionalno ekvivalentan proizvod, program ili usluga koji ne narušava nijedno IBM pravo na intelektualno vlasništvo, se može koristiti kao zamjena. Međutim, na korisniku je odgovornost da procijeni i verificira operacije bilo kojeg ne-IBM proizvoda, programa ili usluge.

IBM može imati patente ili aplikacijske patente koje su još u toku, a koji pokrivaju predmet o kojem se govori u ovom dokumentu. Posjedovanje ovog dokumenta vam ne daje nikakve licence na ove patente. Možete poslati upit za licence, u pismenom obliku, na:

| IBM Director of Licensing
| IBM Corporation
| 500 Columbus Avenue
| Thornwood, NY 10594-1785
| U.S.A.

Za upite o licenci koji se tiču dvo-bajtnih (DBCS) informacija, kontaktirajte IBM Odjel intelektualnog vlasništva u vašoj zemlji ili pošaljite pismeni upit na:

| IBM World Trade Asia Corporation
| Licensing
| 2-31 Roppongi 3-chome, Minato-ku
| Tokyo 106, Japan

Sljedeći odlomak se ne primjenjuje na Ujedinjeno Kraljevstvo ili bilo koju drugu zemlju gdje su takve izjave nekonzistentne s lokalnim zakonima: INTERNATIONAL BUSINESS MACHINES CORPORATION DAJE OVU PUBLIKACIJU “KAKVA JE ”, BEZ IKAKVIH JAMSTAVA, BILO IZRAVNIH ILI POSREDNIH, UKLJUČUJUĆI, ALI NE OGRANIČAVAJUĆI SE NA, UKLJUČENA JAMSTVA O NE-POVREĐIVANJU, PROĐI NA TRŽIŠTU ILI SPOSOBNOSTI ZA ODREĐENU SVRHU. Neke zemlje ne dozvoljavaju odricanje od izravnih ili posrednih jamstava u određenim transakcijama, zbog toga se ova izjava možda ne odnosi na vas.

Ove informacije mogu sadržavati tehničke netočnosti ili tipografske pogreške. Povremeno se rade promjene na ovim informacijama; te promjene bit će uključene u nova izdanja ove publikacije. IBM može raditi poboljšanja i/ili promjene u proizvodu(ima) i/ili programu/ima opisanim u ovoj publikaciji, bilo kad, bez prethodne obavijesti.

Bilo koje upućivanje u ovim informacijama na ne-IBM Web stranice, služi samo kao pomoć i ni na kakav način ne služi za promicanje tih Web stranica. Materijali na tim Web stranicama nisu dio materijala za ovaj IBM proizvod i upotreba tih Web stranica je na vaš osobni rizik.

| IBM može koristiti ili distribuirati informacije koje mu dobavite na bilo koji način za koji
| smatra da je prikladan i to bez bilo kakvih obaveza prema vama.

© Autorska prava IBM Corp. 1996, 2004

Vlasnici licence za ovaj program, koji žele imati informacije o njemu u svrhu omogućavanja: (i) izmjene informacija između neovisno kreiranih programa i drugih programa (uključujući i ovaj) i (ii) uzajamne upotrebe informacija koje su bile izmijenjene, trebaju kontaktirati:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Takve informacije mogu biti dostupne, uz odgovarajuće termine i uvjete, uključujući u nekim slučajevima i plaćanje pristojbe.

Licencni program opisan u ovim informacijama i svi licencni materijali dostupni za to, su osigurani od strane IBM-a, pod uvjetima od IBM Customer Agreement, IBM International Program License Agreement ili bilo kojeg ekvivalentnog ugovora između nas.

Svi podaci o izvedbi koji su ovdje sadržani su utvrđeni u kontroliranoj okolini. Stoga rezultati postignuti u drugim operacijskim okolinama mogu biti značajno drukčiji. Neka mjerenja su možda bila izvedena na sistemima na razvojnoj razini i ne postoji nikakvo jamstvo da će ta mjerenja biti ista na općenito dostupnim sistemima. Osim toga, neka mjerenja su možda bila procijenjena pomoću ekstrapolacije. Stvarni rezultati se mogu razlikovati. Korisnici ovog dokumenta trebaju provjeriti primjenljive podatke za njihove specifične okoline.

Informacije koje se tiču ne-IBM proizvoda su dobivene od dobavljača tih proizvoda, njihovih objavljenih najava ili drugih dostupnih javnih izvora. IBM nije testirao te proizvode i ne može potvrditi točnost performansi, kompatibilnosti ili bilo koji drugi zahtjev vezan uz ne-IBM proizvod. Pitanja o sposobnostima ne-IBM proizvoda bi trebala biti adresirana na dobavljače tih proizvoda.

Sve izjave u vezi budućih IBM namjera ili smjernica su podložne promjeni ili povlačenju bez prethodne obavijesti i predstavljaju samo ciljeve i namjere.

Ovo su informacije samo u svrhu planiranja. Ove informacije se mogu promijeniti prije nego proizvodi postanu dostupni.

Ove informacije sadržavaju primjere podataka i izvještaja korištenih u svakodnevnim poslovnim operacijama. Radi što boljeg objašnjenja, ti primjeri uključuju imena pojedinaca, poduzeća, brandova i proizvoda. Sva ta imena su izmišljena i bilo koja sličnost s imenima i adresama koja se koriste u stvarnom poslovnom okruženju, je u potpunosti slučajna.

LICENCA ZA AUTORSKO PRAVO:

Ove informacije sadrže primjere aplikacijskih programa u izvornom jeziku koji ilustriraju tehnike programiranja na različitim operativnim platformama. Možete kopirati, modificirati i distribuirati ove primjere programa u bilo kojoj formi bez plaćanja IBM-u, u svrhu razvoja, korištenja, marketinga ili distribuiranja aplikacijskih programa prilagođavajući ih sučelju aplikativnog programiranja za operacijsku platformu za koju su primjeri programa pisani. Ti primjeri nisu bili temeljito testirani u svim uvjetima. IBM, stoga, ne može jamčiti ili potvrditi pouzdanost, upotrebljivost ili funkcionalnost tih programa. Možete kopirati, modificirati i distribuirati ove primjere bez bilo kakvog plaćanja IBM-u u svrhu razvoja, korištenja, marketinga ili distribuiranja aplikacijskih programa prilagođavajući ih sučeljima programiranja IBM aplikacija.

Ako gledate nepostojanu kopiju ovih informacija, fotografije i ilustracije u boji se možda neće vidjeti.

Zaštitni znaci

Sljedeći termini su zaštitni znaci International Business Machines Corporation u Sjedinjenim Državama, ostalim zemljama ili oboje.

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 i ProShare su zaštitni znaci ili registrirani zaštitni znaci Intel Corporation u Sjedinjenim Državama, drugim zemljama ili oboje.

Microsoft, Windows, Windows NT i Windows logo su zaštitni znaci Microsoft Corporation u Sjedinjenim Državama, drugim zemljama ili oboje.

Java i svi Java-zasnovani zaštitni znaci su zaštitni znaci Sun Microsystems, Inc. u Sjedinjenim Državama, drugim zemljama ili oboje.

UNIX je registrirani zaštitni znak The Open Group u Sjedinjenim Državama i drugim zemljama.

Ostala imena poduzeća, proizvoda, i usluga mogu biti zaštitni znaci ili servisne oznake drugih.

Kazalo

Posebni znakovi

Brojevi

A

B

C

© Autorska prava IBM Corp. 1996, 2004

Č

D

E

F

G

I

J

K

L

M

N

NJ

O

P

Q

R

S

Š

T

U

V

Z

Opaske čitatelja

iSeries
Savjeti i alati za osiguranje vašeg iSeriesa
Verzija 5

Broj publikacije: SA12-6294-07

Koristiti će nam Vaša ocjena ove publikacije. Molimo Vas ukažite na eventualne greške u tekstu, osvrnite se na točnost, organizaciju, sadržaj i cjelovitost knjige. Vaši komentari neka se odnose samo na ovaj priručnik, njegov izgled i sadržaj.

S pitanjima tehničke prirode i o cijenama proizvoda obratite se IBM predstavništvu, IBM poslovnim partnerima ili ovlaštenim distributerima.

Nazovite ″Halo IBM″ na broj telefona (u SAD) 001-803-313233 gdje ćete dobiti sve ostale opće informacije.

Suglasni ste da Vaše opaske IBM koristi za svoje potrebe na odgovarajući način, iz čega ne proizlaze nikakve međusobne obaveze.

Opaske:

Zahvaljujemo na suradnji

Vaše opaske šaljite:
- Vaše opaske šaljite na adresu otisnutu na poleđini ovog obrasca.
- Ako odgovor šaljete telefaksom birajte slijedeći broj: Sjedinjene države i Kanada: 1-800-937-3430
- Vaše opaske možete poslati e-mailom na: RCHCLERK@us.ibm.com

Ako želite odgovor od IBM-a, molimo Vas za slijedeće podatke:

Ime	Adresa
Tvrtka	
Telefonski broj	E-mail adresa

IBM

IBM CORPORATION
ATTN DEPT 542 IDCLERK
3605 Highway 52 N
ROCHESTER MN

Tiskano u Hrvatskoj

SA12-6294-07