IBM

eserver

iSeries

Nasveti in orodja za zaščito iSeries

Različica 5

SA12-6308-07

IBM

@server

iSeries

Nasveti in orodja za zaščito iSeries

Različica 5

SA12-6308-07

Opomba

Pred uporabo teh informacij in izdelka, ki ga opisujejo, preberite “Opombe” na strani 149.

Osma izdaja (april 2004)

Ta izdaja velja za različico 5, izdajo 3, raven popravkov 0 IBM-ovega Operating System/400 (številka izdelka 5722-SS1) in za vse naslednje izdaje in ravni popravkov, dokler ne bo v novih izdajah navedeno drugače. Ta različica ne deluje na vseh modelih RISC (računalnik z zoženim naborom ukazov) niti ne deluje na modelih CISC.

Ta izdaja nadomesti SC41-5300-06.

Kazalo

Slike

Tabele

O nasvetih in orodjih za zaščito iSeries (SC41-5300-07)

Vloga računalnikov v podjetjih se zelo hitro spreminja. Vodje, ponudniki programske opreme, skrbniki za zaščito in kontrolorji morajo začeti razmišljati o številnih področjih, ki so se jim v preteklosti zdela samoumevna. Med ta področja spada tudi zaščita iSeries.

Sistemi nudijo številne nove funkcije, ki se močno razlikujejo od tradicionalnih računovodskih aplikacij. Uporabniki dostopajo do sistemov na nove načine: prek lokalnih omrežij (LAN-ov), naročniških linij (klicni dostop), brezžično in prek omrežij vseh vrst. Zelo pogosto je, da uporabniki sploh ne vidijo prijavnega zaslona. Številna podjetja so se "razširila" z lastniškimi omrežji ali prek interneta.

Nenadoma se zdi, da imajo sistemi cel kup novih vrat in oken. Vodje sistemov in skrbnike zaščite upravičeno skrbi, kako zaščititi informacijska sredstva v tem hitro spreminjajočem se okolju.

Te informacije nudijo niz praktičnih nasvetov za uporabo funkcij zaščite iSeries in za vzpostavitev operacijskih postopkov, ki upoštevajo zaščito. Priporočila v teh informacijah se nanašajo na namestitev s povprečnimi zahtevami za zaščito in izpostavitvijo. Te informacije ne nudijo popolnega opisa vseh razpoložljivih funkcij za zaščito iSeries. Če se želite podučiti o dodatnih možnostih ali potrebujete popolnejše informacije, preberite publikacije, ki so opisane v razdelku Poglavje 18, "S tem povezane informacije", na strani 147.

V teh informacijah opisujemo tudi, kako nastaviti in uporabiti orodja za zaščito, ki so del OS/400. V razdelku Poglavje 4, "Konfiguriranje iSeries za uporabo orodij za zaščito", na strani 25 in "Ukazi in meniji ukazov za zaščito" na strani 26 boste našli referenčne informacije o orodjih za zaščito. Te informacije nudijo zglede za uporabo orodij.

Komu je namenjena ta knjiga

Za zaščito sistema sta odgovorna**varnostnik** ali **skrbnik za zaščito**. Ta odgovornost običajno vključuje naslednje naloge:

- nastavitev in upravljanje profilov uporabnikov
- nastavitev sistemskih vrednosti, ki vplivajo na zaščito
- upravljanje pooblastil za objekte
- uveljavitev in nadzorovanje načel zaščite

Če ste odgovorni za upravljanje zaščite v enem ali več sistemih iSeries, so te informacije namenjene vam. Navodila v teh informacijah so napisana na podlagi naslednjega:

- Poznate osnovne operacijske postopke iSeries kot sta podpisovanje in uporaba ukazov.
- Poznate osnovne elemente zaščite iSeries: ravni zaščite, sistemske vrednosti za zaščito, profili uporabnikov in zaščita objektov.

  Opomba: Pregled teh elementov boste našliv razdelkuPoglavje 1, "Osnovni elementi zaščite iSeries", na strani 3. Če teh osnovnih elementov še ne poznate, preberite temo Informacijskega centra iSeries z naslovom *Osnovna zaščita in načrtovanje*. Za podrobnosti preglejte razdelek "Predpogoji in s tem povezane informacije" na strani xii.
- Zaščito v sistemu ste aktivirali z nastavitvijo sistemske vrednosti za raven zaščite QSECURITY na vsaj 30.

IBM neprestano izboljšuje zmožnosti zaščite na iSeries. Če želite izkoristiti te izboljšave, redno pregledujte zbirni paket popravkov, ki je trenutno na voljo za vašo izdajo. Preglejte, ali vsebuje popravke, ki so ustrezni za zaščito.

Kako uporabiti te informacije

Če sistema niste nastavili za uporabo orodij za zaščito ali imate nameščen komplet programskih orodij za zaščito za OS/400 za starejšo izdajo, naredite naslednje:

1. Začnite z Poglavje 2, "Čarovnik za zaščito iSeries in Planer zaščite za eServer", na strani 9. Ta opisuje, kako uporabiti te funkcije za izbiro priporočenih orodij za zaščito in kako jih začeti uporabljati.
2. Če potrebujete osnovne informacije o zaščiti, lahko pregledate informacije v priročniku Security Reference v Informacijskem centru iSeries.

Opomba

Te informacije vsebujejo *številne* nasvete za zaščito iSeries. Toda morda je v vašem sistemu potrebno zaščititi samo nekatera področja. S pomočjo teh informacij so podučite o možnih luknjah v zaščiti in njihovih posledicah, nato pa se usmerite na področja, ki so najpomembnejša za vaš sistem.

Predpogoji in s tem povezane informacije

V Informacijskem centru lahko začnete iskati tehnične informacije o sistemu iSeries.

Do Informacijskega centra lahko dostopite na dva načina:

- Na naslednji spletni strani:

  `http://www.ibm.com/eserver/iseries/infocenter`
- S pomočjo *Informacijski center iSeries*, SK3T-4091-04 CD-ROM-a. Tega prejmete skupaj z novo nadgradnjo iSeries strojne ali IBM Operating System/400 programske opreme. CD-ROM lahko tudi naročite prek IBM-ovega Centra za publikacije:

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

Informacijski center iSeries vsebuje nove in dopolnjene iSeries informacije o namestitvi programske in strojne opreme, okolju Linux, WebSphere, Java, visoki razpoložljivosti, bazah podatkov, logičnih particijah, ukazih CL in aplikacijskih programerskih vmesnikih (API-jih). Poleg tega nudi tudi svetovalce in iskalnike, ki vam nudijo pomoč pri načrtovanju, odpravljanju težav in konfiguriranju iSeries strojne in programske opreme.

Z vsakim naročilom nove strojne opreme prejmete *iSeries Setup and Operations CD-ROM*, SK3T-4098-02. CD-ROM vsebuje IBM @server IBM e(logo)server iSeries Access za Windows in čarovnika EZ-Setup. iSeries Access Family nudi vrsto učinkovitih funkcij odjemalca in strežnika za povezavo PC-jev s strežniki iSeries. Čarovnik EZ-Setup avtomatizira večino nalog namestitve iSeries.

Nasveti za pošiljanje pripomb

Vaš odziv je pomemben in nam pomaga, da vam nudimo najnovejše in najpopolnejše informacije. Če imate kakšne pripombe na vsebino te knjige ali katerokoli drugo dokumentacijo iSeries, izpolnite obrazec za pripombe bralca na koncu te knjige.

- Če želite pripombe poslati po pošti, ta obrazec pošljite skupaj z naslovom, ki je natisnjen na drugi strani. Če pripomb ne pošiljate iz ZDA, temveč iz druge države, lahko obrazec predate lokalni podružnici IBM ali IBM-ovemu predstavniku in ne bo vam treba plačati poštnine.
- Če želite pripombe poslati po telefaksu, pokličite eno izmed naslednjih številk:
  - Združene države Amerike, Kanada in Portoriko: 1-800-937-3430
  - Druge države: 1-507-253-5192
- Če želite pripombe poslati prek elektronske pošte, jih pošljite na enega izmed naslednjih naslovov elektronske pošte:
  - Pripombe o knjigah:

    RCHCLERK@us.ibm.com
  - Pripombe o Informacijskem centru iSeries

    RCHINFOC@us.ibm.com

Pri tem pa vključite tudi naslednje:

- Ime knjige ali temo Informacijskega centra iSeries
- Številko publikacije
- Številko strani ali temo knjige, na katere se pripombe nanašajo

Del 1. Osnovna zaščita iSeries

Poglavje 1. Osnovni elementi zaščite iSeries

V tej temi boste našli kratek pregled osnovnih elementov, ki s skupnim delovanjem nudijo zaščito iSeries. V drugih delih te knjige presežemo osnove in nudimo nasvete za uporabo teh elementov zaščite, tako da zadostijo potrebam vašega podjetja.

Ravni zaščite

Z nastavitvijo sistemske vrednosti za raven zaščite (QSECURITY) lahko izberete, kolikšno raven zaščite naj uveljavi sistem. Sistem nudi pet ravni zaščite:

Raven 10:

Sistem ne uveljavi nobene zaščite. Potrebno ni nobeno geslo. Če podan profil uporabnika ne obstaja v sistemu, ko se nekdo prijavi, ga sistem izdela.

OPOZORILO:

V V4R3 in v bodočih izdajah ni mogoče nastaviti sistemske vrednosti QSECURITY na 10. Če v sistemu trenutno uporabljate raven zaščite 10, bo pri namestitvi različic 4 izdaje 3 ostala na tej ravni. Če spremenite raven zaščite v katero drugo vrednost, je ne morete več vrniti na raven 10. Ker raven 10 ne nudi nobene zaščite, je IBM ne priporoča. **IBM ne bo nudil nobene pomoči zaradi težav, do katerih pride na ravni 10, razen če je težava mogoča tudi na višji ravni zaščite.**

Raven 20:

Sistem zahteva za prijavo ID uporabnika in geslo. Raven zaščite 20 se pogosto imenuje **prijavna zaščita**.Po privzetku imajo vsi uporabniki pooblastilo do vseh objektov, ker imajo vsi uporabniki posebno pooblastilo *ALLOBJ.

Raven 30:

Sistem zahteva za prijavo ID uporabnika in geslo. Uporabniki morajo imeti pooblastilo za uporabo objektov, ker po privzetku nimajo nobenega pooblastila. To se imenuje **zaščita sredstev**.

Raven 40:

Sistem zahteva za prijavo ID uporabnika in geslo. Poleg zaščite sredstev nudi sistem tudi funkcije **zaščite integritete**. Funkcije zaščite integritete, kot je preverjanje veljavnosti parametrov za vmesnike operacijskega sistema, so namenjene za zaščito pred vdorom izkušenih sistemskih uporabnikov v sistem in njegove objekte. Za večino namestitev je raven 40 priporočena raven zaščite. Ko prejmete nov sistem iSeries z izdajo V4R5 ali novejšo, je raven zaščite nastavljena na 40.

Raven 50:

Sistem zahteva za prijavo ID uporabnika in geslo. Sistem uveljavi zaščito sredstev in zaščito integritete ravni 40,vendar doda tudi **izboljšano zaščito integritete**, kot je omejitev obravnave sporočil med programi sistemskega stanja in programi uporabniškega stanja. Raven zaščite 50 je namenjena za sisteme iSeries z zahtevami za visoko zaščito.

Opomba: Raven 50 je zahtevana raven za potrdila C2 (in potrdila FIPS-140).

V 2. poglavju knjige *iSeries Security Reference* boste našli podrobnejše informacije o ravneh zaščite in opise za preklop iz ene ravni zaščite v drugo.

Globalne nastavitve

V sistemu imate globalne nastavitve, ki vplivajo na to, kako delo vstopi v sistem in kako vidijo sistem sistemski uporabniki. Te nastavitve vključujejo naslednje:

Sistemske vrednosti zaščite:
Sistemske vrednosti zaščite se uporabljajo za nadzorovanje zaščite v sistemu. Te vrednosti so razdeljene v štiri skupine:
- splošne sistemske vrednosti zaščite
- druge sistemske vrednosti, povezane z zaščito
- sistemske vrednosti, ki nadzorujejo gesla
- sistemske vrednosti, ki nadzorujejo beleženje

Številne teme te knjige razlagajo vplive specifičnih vrednosti na zaščito. V 3. poglavju knjige *iSeries Security Reference* so opisane vse sistemske vrednosti, povezane z zaščito.

Omrežni atributi:
Omrežni atributi nadzorujejo, kako vaš sistem sodeluje (ali izbere, da ne bo sodeloval) v omrežju z drugimi sistemi. Podrobnejše informacije o omrežnih atributih lahko najdete v knjigi *Work Management*.

Opisi podsistemov in drugi elementi za upravljanje dela:
Elementi za upravljanje dela določajo, kako delo vstopi v sistem in v katerem okolju se izvaja. Številne teme v teh informacijah razlagajo vpliv nekaterih vrednosti za upravljanje dela na zaščito. Popolne informacije lahko najdete v knjigi *Work Management*.

Konfiguriranje komunikacij:
Tudi konfiguriranje komunikacij vpliva na to, kako delo vstopi v sistem. V številnih temah teh informacij boste našli predloge za zaščito sistema, ki sodeluje v omrežju.

Profili uporabnikov

Vsak uporabnik sistema **mora** imeti profil uporabnika. Profil uporabnika morate izdelati, preden se lahko uporabnik prijavi. S pomočjo profilov uporabnikov lahko tudi krmilite dostop do servisnih orodij kot so DASD in izpisi glavnega pomnilnika. Podrobnejše informacije poiščite v razdelku “Upravljanje servisnih orodij” na strani 56.

Profil uporabnika je močno in prožno orodje, ki nadzoruje, kaj lahko naredi uporabnik in prilagodi način, na katerega vidi uporabnik sistem. Knjiga *iSeries Security Reference* opisuje vse parametre profila uporabnika.

Profili skupin

Profil skupine je posebna vrsta profila uporabnika. Uporabite ga lahko za definiranje pooblastila za skupino uporabnikov, namesto da bi vsakemu med njimi dodelili ločeno pooblastilo. Profil skupine lahko uporabite tudi kot vzorec pri izdelavi posameznih profilov uporabnikov, tako da uporabite funkcijo kopiranja profila ali meni načel zaščite Navigatorja iSeries, s pomočjo katerega uredite pooblastila uporabnikov.

V 5. in 7. poglavju knjige *iSeries Security Reference* boste našli podrobnejše informacije o načrtovanju in uporabi profilov skupin.

Zaščita sredstev

Zaščita sredstev v sistemu omogoča, da definirate, kdo lahko uporabi objekte, in način njihove uporabe. Zmožnost za dostop do objekta se imenuje **pooblastilo**. Pri nastavitvi objektnih pooblastil morate paziti, da uporabnikom dodelite dovolj pooblastil za izvajanje svojega dela, ne pa tudi pooblastil, ki bi jim omogočala pregledovanje in spreminjanje sistema. Objektno pooblastilo dodeli uporabniku pravice za določen objekt in lahko podaja, kaj lahko naredi uporabnik z objektom. Sredstvo objekta je lahko omejeno prek specifičnih podrobnejših pooblastil uporabnikov, kot sta dodajanje ali spreminjanje zapisov. Sistemska sredstva je mogoče uporabiti za dodelitev uporabniškega dostopa do določenih sistemsko definiranih podnizov pooblastil: *ALL, *CHANGE, *USE in *EXCLUDE.

Datoteke, programi, knjižnice in imeniki so najpogostejši sistemski objekti, ki zahtevajo zaščito sredstev, vendar lahko podate pooblastilo za katerikoli posamezen objekt v sistemu.

Poglavje 5, “Zaščita informacijskih sredstev z objektnim pooblastilom” razlaga pomembnost nastavitve objektnih pooblastil v sistemu. 5. poglavje knjige *iSeries Security Reference* opisuje možnosti za nastavitev zaščite sredstev.

Funkcija omejitve dostopa do programa

Funkcija omejitve dostopa do programa omogoča, da podate zaščito programa, če nimate objekta iSeries, ki bi ščitil program. Preden smo v V4R3 dodali podporo za funkcijo omejitve dostopa do programa, ste lahko opravili to nalogo z izdelavo seznama pooblastil ali drugega objekta in s preverjanjem pooblastila za objekt, da ste preverili dostop do funkcije programa. Zdaj lahko s pomočjo funkcije omejitve dostopa do programa preprosteje nadzorujete dostop do aplikacije, delov aplikacije ali funkcij znotraj programa.

Za upravljanje dostopa uporabnikov do funkcij aplikacije prek Navigatorja iSeries lahko uporabite dva načina. Prvi uporablja podporo za upravljanje aplikacij:

1. Z desno tipko miške kliknite sistem, ki vsebuje funkcijo, katere nastavitev dostopa želite spremeniti.
2. Izberite **Upravljanje aplikacij**.
3. Če ste v sistemu za upravljanje, izberite **Lokalne nastavitve**. V nasprotnem primeru nadaljujte z naslednjim korakom.
4. Izberite funkcijo z zmožnostjo upravljanja.
5. Če je ustrezno, izberite **Privzeti dostop**. Z izbiro te možnosti po privzetku omogočite vsem uporabnikom dostop do funkcije.
6. Če je ustrezno, izberite **Dostop do vseh objektov**. Z izbiro te možnosti omogočite vsem uporabnikom s sistemskim pooblastilom za vse objekte dostop do te funkcije.
7. Če je ustrezno, izberite **Prilagodi**. S pomočjo gumbov **Dodaj** in **Odstrani** v pogovornem oknu **Prilagajanje dostopa** dodajte ali odstranite uporabnike ali skupine s seznamov **Dovoljen dostop** in **Zavrnjen dostop**.
8. Če je ustrezno, izberite **Odstrani prilagoditev**. Z izbiro te možnosti zbrišete prilagojen dostop za izbrano funkcijo.
9. S klikom gumba **Potrdi** zaprite pogovorno okno **Upravljanje aplikacij**.

Drugi način upravljanja dostopa uporabnikov vključuje podporo Navigatorja iSeries za uporabnike in skupine:

1. V Navigatorju iSeries razširite ikono **Uporabniki in skupine**.
2. Izberite **Vsi uporabniki**, **Skupine** ali **Uporabniki, ki niso v skupini**, da boste prikazali seznam uporabnikov in skupin.
3. Z desno tipko miške kliknite uporabnika ali skupino in izberite **Lastnosti**.

4. Kliknite **Zmožnosti**.
5. Kliknite jeziček **Aplikacije**.
6. Na tej strani spremenite nastavitev dostopa za uporabnika ali skupino.
7. Dvakrat kliknite **Potrdi**, da boste zaprli pogovorno okno **Lastnosti**.

V razdelku"Zaščita Navigatorja iSeries" na strani 138 lahko najdete podrobnejše informacije o vprašanjih zaščite, povezanih z Navigatorjem iSeries.

Če ste pisec aplikacij, lahko s pomočjo API-jev funkcije omejitve dostopa do programa naredite naslednje:

- registrirate funkcijo
- pridobite informacije o funkciji
- definirate, kdo lahko uporabi funkcijo in kdo je ne more
- preverite, ali lahko uporabnik uporablja funkcijo

Opomba: Ta podpora **ni** nadomestilo za zaščito sredstev. Funkcija omejitve dostopa do programa uporabniku ne preprečuje dostopa do sredstva (kot sta datoteka ali program) iz drugega vmesnika.

Za uporabo te podpore znotraj aplikacije mora ponudnik aplikacije registrirati funkcije pri namestitvi aplikacije. Registrirana funkcija ustreza bloku kode za določene funkcije v aplikaciji. Če uporabnik zažene aplikacijo, le-ta pokliče API, preden pokliče blok kode. API pokliče API za preverjanje uporabe, da preveri, ali ima uporabnik dovoljenje za uporabo funkcije. Če ima uporabnik dovoljenje za uporabo registrirane funkcije, se zažene blok kode. Če uporabnik nima dovoljenja za uporabo funkcije, ne more zagnati bloka kode.

Opomba: API vključuje registracijo 30-mestnega ID-ja funkcije v registracijsko bazo podatkov (WRKREGINF). Čeprav ne obstajajo nobene izhodne točke, povezane z ID-ji funkcij, ki jih uporabljajo API-ji funkcije za omejitev dostopa, izhodne točke morate imeti. Če želite v registru karkoli registrirati, **morate** podate ime formata izhodne točke. V ta namen izdela API Registriraj funkcijo navidezno ime formata, ki ga nato uporabi za vse registrirane funkcije. Ker je to navidezno ime formata, ni program izhodne točke nikoli poklican.

Skrbnik sistema določi, kdo lahko dostopi do funkcije in kdo ne sme. Skrbnik lahko upravlja dostop s pomočjo API-ja ali grafičnega uporabniškega vmesnika za upravljanje aplikacij Navigatorja iSeries. V knjigi *iSeries server API Reference* boste našli informacije o API-jih funkcije za omejitev dostopa do programa. Dodatne informacije o nadzorovanju dostopa do funkcij poiščitev razdelku"Zaščita Navigatorja iSeries" na strani 138.

Dnevniki zaščite

Beleženje za zaščito sistema se izvaja zaradi več razlogov:

- Za preverjanje, ali je načrt zaščite popoln.
- Za zagotovitev, da so načrtovani krmilni elementi zaščite na mestu in delujejo. To vrsto beleženja običajno izvaja varnostnik za zaščito kot del dnevnega upravljanja zaščite. Včasih se podrobneje izvaja tudi kot del občasnega pregleda zaščite, ki ga opravijo notranji ali zunanji kontrolorji.
- Za zagotovitev, da je zaščita sistema v skladu s spremembami v okolju sistema. Sledi nekaj zgledov sprememb, ki vplivajo na zaščito:
  - novi objekti, ki jih izdelajo uporabniki sistema
  - novi uporabniki z dostopom do sistema
  - sprememba lastništva objekta (pooblastilo ni prilagojeno)

  - sprememba odgovornosti (spremenjena skupina uporabnikov)
  - začasno pooblastilo (ki ni časovno preklicano)
  - na novo nameščeni izdelki
- Za pripravo na dogodek kot je namestitev nove aplikacij, preklop v višjo raven zaščite ali nastavitev komunikacijskega omrežja.

Tehnike, opisane tu, so primerne za vse med temi situacijami. Za katere stvari boste izvajali beleženje in kako pogosto, je odvisno od velikosti in zaščitnih zahtev vašega podjetja.

Beleženje zaščite vključuje uporabo ukazov v sistemu in dostop do dnevnika beleženja. Izdelate lahko poseben profil, ki ga bo uporabljala oseba, ki izvaja beleženje zaščite v sistemu. Profil kontrolorja potrebuje posebno pooblastilo *AUDIT za spreminjanje značilnosti beleženja sistema. Nekatere izmed nalog beleženja, predlagane v tem poglavju, zahtevajo profil uporabnika v posebnima pooblastiloma *ALLOBJ in *SECADM. Ko se beleženje konča, nastavite geslo za profil kontrolorja na *NONE.

Podrobnejše informacije o beleženju zaščite poiščite v 9. poglavju knjige *Security Reference*.

Zgled: poročilo o atributih zaščite sistema

Slika 1 kaže zgled izhodnih podatkov ukaza Natisni atribute zaščite sistema (PRTSYSSECA). Poročilo kaže nastavitve za sistemske vrednosti in omrežne atribute, povezane z zaščito, ki si priporočeni za sisteme z običajnimi zahtevami za zaščito. Kaže tudi trenutne nastavitve v sistemu.

Opomba: Stolpec *Trenutna vrednost* v poročilu prikazuje trenutno nastavitev sistema. Primerjajte ga s priporočeno vrednostjo, da boste videli, ali obstajajo luknje v zaščiti.

```
Atributi zaščite sistema

Ime
Sis. vrednosti   Trenutna vrednost      Priporočena vrednost
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. Vzorčno poročilo o atributih zaščite sistema (Del 1 od 4)

```
QAUTOCFG         0                    0
QAUTORMT         1                    0
QAUTOVRT         9999                 0
QCMNRCYLMT       0 0                  0 0
QCRTAUT          *CHANGE              Nadzor na ravni knjižnice
QCRTOBJAUD       *NONE                Nadzor na ravni 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. Vzorčno poročilo o atributih zaščite sistema (Del 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. Vzorčno poročilo o atributih zaščite sistema (Del 3 od 4)

```
Atributi zaščite sistema

Ime
omr. atributa    Trenutna vrednost    Priporočena vrednost
DDMACC           *OBJAUT              *REJECT
JOBACN           *FILE                *REJECT
PCSACC           *OBJAUT              *REJECT
```

Slika 1. Vzorčno poročilo o atributih zaščite sistema (Del 4 od 4)

Poglavje 2. Čarovnik za zaščito iSeries in Planer zaščite za eServer

Orodji Čarovnik za zaščito strežnika iSeries in Planer zaščite za eServer vam pomagata pri odločitvi, katere zaščitne ukrepe boste uveljavili za vaš iSeries strežnik. Če iSeries Čarovnika za zaščito uporabite v Navigatorju iSeries, lahko izdelate poročila, ki odražajo vaše potrebe po zaščiti, glede na odgovore, ki jih izberete. Ta poročila lahko nato uporabite za konfiguriranje zaščite v sistemu.

S pomočjo Čarovnika za zaščito iSeries ali Planerja zaščite za eServer lahko zasnujete in izdelate osnovna varnostna načela za strežnike iSeries. Cilj obeh orodij je poenostaviti izvedbo in upravljanje zaščite v sistemih. Čarovnik, ko je na voljo kot del OS/400, postavi več vprašanj o okolju strežnika in na osnovi odgovorov prikaže niz priporočil, ki jih lahko čarovnik takoj uveljavi v sistemu.

Planer zaščite za eServer je spletna različica čarovnika za zaščito. Omogoča vam izbiro glede na vaše potrebe po zaščiti, nato pa izdela poročilo, v katerem prikaže možnosti, potrebne za zaščito vaše strani.

Planer zaščite za eServer je različica čarovnika, ki temelji na spletu. Ravno tako kot čarovnik tudi svetovalec poda niz priporočil za izvedbo zaščite v sistemu. Vendar pa svetovalec priporočil ne more uveljaviti. Namesto tega izdela seznam vrednosti za zaščito sistema in druge vrednosti, ki jih je potrebno uveljaviti v sistemu, in sicer na osnovi vprašanj na vprašanja svetovalca.

Čarovnik za zaščito

Odločitev, katere vrednosti za zaščito sistema iSeries uporabiti v podjetju, je lahko precej zapletena. Če še ne poznate izvedbe zaščite na strežnikih iSeries ali če ste okolje, v katerem se izvaja strežnik iSeries, pred nedavnim spremenili, vam bo čarovnik za zaščito pomagal pri odločitvah.

Kaj je čarovnik?

- Čarovnik je orodje, namenjeno uporabnikom začetnikom, s pomočjo katerega lahko nekaj namestijo v sistem ali nekaj konfigurirajo.
- Čarovnik postavi uporabniku vprašanja in na ta način zbere informacije. Odgovor na vsako vprašanje določa, katero bo naslednje postavljeno vprašanje.
- Ko čarovnik postavi vsa vprašanja, se uporabniku prikaže zaključno pogovorno okno. Uporabnik nato klikne gumb **Dokončaj** in namesti ali konfigurira postavko.

Cilji čarovnika za zaščito

Cilj čarovnika za zaščito je na osnovi odgovorov uporabnikov konfigurirati naslednje:

- Z zaščito povezane sistemske vrednosti in omrežni atributi.
- Poročanje, povezano z zaščito, za nadzorovanje sistema
- Za izdelavo poročila z informacijami za skrbnika in poročila z informacijami za uporabnika:
  - Poročilo z informacijami za skrbnika vsebuje priporočene nastavitve zaščite in postopke, ki jih morate opraviti, preden uveljavite priporočila.
  - Poročilo z informacijami za uporabnika vsebuje informacije, ki jih lahko uporabite za načelo zaščite podjetja. V to poročilo so na primer vključena pravila za sestavo gesel.
- Za nudenje priporočenih nastavitev za različne postavke, povezane z zaščito v sistemu.

Cilji čarovnika za zaščito

- Cilji čarovnika za zaščito so naslednji:
  - Na osnovi odgovorov, ki jih uporabniku zastavi čarovnik, določiti nastavitve za zaščito sistema in jih nato uveljaviti.
  - Čarovnik ustvari podrobna informacijska poročila, vključno z naslednjim:
    - Poročilo, ki razlaga priporočila čarovnika
    - Poročilo, ki razlaga postopke, ki jih je potrebno opraviti pred izvedbo
    - Poročilo, ki navaja koristne informacije, namenjene uporabnikom sistema
- Te postavke uveljavijo osnovno načelo zaščite v sistemu.
- Čarovnik priporoči izdelavo poročil beleženja, ki jih morate občasno zagnati. Ta poročila vam pomagajo pri naslednjem:
  - Zagotoviti ravnanje v skladu z načeli zaščite
  - Zagotoviti, da so načela zaščite spremenjena samo z vašo odobritvijo
  - Načrtovati poročila za nadzorovanje dogodkov, povezanih z zaščito v sistemu
- Čarovnik omogoča, da shranite priporočila ali v sistemu uveljavite vsa ali nekatera med njimi.

Opomba: Čarovnika za zaščito lahko v istem sistemu uporabite več kot enkrat, da uporabnikom s starejšo namestitvijo omogočite, da pregledajo svojo trenutno zaščito. Uporaba čarovnika za zaščito je mogoča od izdaje sistema V3R7 naprej (ko smo vpeljali Navigator iSeries).

Če želite uporabljatiiSeries Navigatorja, morate imeti na vašem PC-ju Windows 95/NT nameščenIBM iSeries Access za Windows ter vzpostavljeno povezavo med PC-jemiSeries in strežnikom. Uporabnik čarovnika mora biti povezan s strežnikom iSeries. Imeti mora ID uporabnika s posebnimi pooblastili *ALLOBJ, *SECADM, *AUDIT in *IOSYSCFG. Kot pomoč pri povezovanju PC-ja Windows 95/NT PC s sistemom iSeries preberite temo Informacijskega centra IBM iSeries Access za Windows topic (podrobnosti poiščitev razdelku“Predpogoji in s tem povezane informacije” na strani xii).

Do čarovnika za zaščito dostopite takole:

1. V Navigatorju iSeries razširite ikono strežnika.
2. Z desno tipko miške kliknite **Zaščita** in izberite **Konfiguriraj**.
   - Ko zažene uporabnik možnost **Zaščita** Navigatorja iSeries, je poslana strežniku iSeries zahteva za preverjanje posebnega pooblastila uporabnika.
   - Če uporabnik nima vseh zahtevanih posebnih pooblastil (*ALLOBJ, *AUDIT, *IOSYSCFG, *SECADM), ne bo prikazana možnost **Konfiguriraj**, dostop do čarovnika za zaščito pa ne bo mogoč.
3. Če ima uporabnik vsa zahtevana pooblastila:
   - So poiskani prejšnji odgovori čarovnika
   - So priklicane trenutne nastavitve zaščite.

Čarovnik za zaščito prikaže enega izmed treh pozdravnih zaslonov. Kateri zaslon se prikaže, je odvisno od tega, kateri izmed naslednjih pogojev obstaja:

- Čarovnik ni bil še nikoli zagnan za ciljni strežnik iSeries
- Čarovnik je bil zagnan predhodno, vendar so bile spremembe v zaščiti odložene
- Čarovnik je bil zagnan predhodno in spremembe v zaščiti so bile uveljavljene

Če ne uporabljate Navigatorja iSeries, lahko kljub temu uporabljate pomoč pri načrtovanju zaščite. Planer zaščite za eServer je spletna različica čarovnika za zaščito, z eno razliko. Svetovalec namreč ne bo samodejno konfiguriral sistema. Vendar pa bo na osnovi vaših odgovorov ustvaril poročilo s priporočenimi možnostmi za zaščito. Za dostop do Planerja zaščite za eServer obiščite informacijski center za eServer:

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

Planer zaščite za eServer

Planer zaščite za eServer je spletna različica čarovnika za zaščito. Postavi vam ista vprašanja kot čarovnik za zaščito in na osnovi odgovorov ustvari ista priporočila. Glavne razlike med tema orodjema so naslednje:

- Planer zaščite za eServer **ne**—
  - ustvari poročil
  - primerja trenutnih nastavitev s priporočenimi nastavitvami
  - nastavi sistemskih vrednosti samodejno
- Iz Planerja zaščite za eServer ni mogoče uveljaviti priporočil.

Planer zaščite za eServer ustvari program CL, ki ga prikrojite lastnim potrebam in tako avtomatizirate konfiguriranje zaščite. Iz Planerja zaščite za eServer se lahko neposredno povežete z dokumentacijo strežnika iSeries. Tu boste našli informacije o sistemskih vrednostih ali poročila, ki vam bodo pomagala določiti, ali te nastavitve ustrezajo vašemu okolju.

Če želite dostopati do Planerja zaščite za eServer, nastavite vaš spletni pregledovalnik na naslednji URL:

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

Poglavje 3. Nadzorovanje interaktivne prijave

Ko razmišljate o omejitvi vstopa v sistem, začnite v samem začetku - to je s prijavnim zaslonom. Sledijo možnosti, ki jih lahko uporabite, da otežite prijavo v sistem z uporabo prijavnega zaslona.

Nastavitev pravil za gesla

Prijavo v sistem lahko zaščitite takole:
- Nastavite načelo, ki določa, da gesla ne smejo biti trivialna in ne smejo biti v skupni rabi.
- Nastavite sistemske vrednosti, ki vam bodo pomagale pri uveljavljanju. Tabela 1 kaže priporočene nastavitve sistemskih vrednosti.

Kombinacija vrednosti v razdelku Tabela 1 je precej omejevalna in je namenjena, da močno zmanjša zmožnost trivialnih gesel. Toda morda bodo imeli vaši uporabniki težave pri izbiri gesel, ki zadovoljujejo te omejitve.

Uporabnikom lahko pomagate tako, da jim podate naslednje:
1. seznam kriterijev za gesla
2. zglede neveljavnih gesel
3. predloge za tvorbo dobrih gesel

Zaženite ukaz CFGSYSSEC (Konfiguriraj zaščito sistema), da boste nastavili te vrednosti. S pomočjo ukaza PRTSYSSECA (Natisni atribute zaščite sistema) natisnite trenutne nastavitve za te sistemske vrednosti.

V 3. poglavju knjige *iSeries Security Reference* “Vrednosti, nastavljene z ukazom Konfiguriraj zaščito sistema” na strani 33 boste našli podrobnejše informacije o ukazu CFGSYSSEC.

Tabela 1. Sistemske vrednosti za gesla

Ime sistemske vrednosti	Opis	Priporočena vrednost
QPWDEXPITV	Kako pogosto morajo uporabniki sistema spremeniti svoja gesla. Za posamezne uporabnike v profilu uporabnika lahko podate različne vrednosti.	60 (dni)
QPWDLMTAJC	Ali sistem prepreči iste sosednje znake.	1 (da)
QPWDLMTCHR	Katerih znakov ni mogoče uporabiti v geslih.[2]	AEIOU#$@
QPWDLMTREP	Ali sistem prepreči več kot eno uporabo istega znaka v geslu.	2 (ni dovoljen zaporedoma)
QPWDLVL	Ali so gesla profilov uporabnikov omejena na 10 znakov ali na maksimum 128 znakov.	0[3]
QPWDMAXLEN	Največje dovoljeno število znakov v geslu.	8
QPWDMINLEN	Najmanjše zahtevano število znakov v geslu.	6
QPWDPOSDIF	Ali se mora vsak znak v geslu razlikovati od znaka na istem mestu v prejšnjem geslu.	1 (da)
QPWDRQDDGT	Ali morajo gesla vsebovati vsaj en številski znak.	1 (da)
QPWDRQDDIF	Kako dolgo mora uporabnik čakati, da lahko znova uporabi isto geslo.[2]	5 ali manj (intervalov izteka)[1]
QPWDVLDPGM	Kateri izhodni program je poklican za preverjanje veljavnosti na novo dodeljenih gesel.	*NONE

Tabela 1. Sistemske vrednosti za gesla (nadaljevanje)

Ime sistemske vrednosti	Opis	Priporočena vrednost

Opombe:

1. Sistemska vrednost QPWDEXPITV podaja, kako pogosto morate spremeniti geslo, kot je na primer vsakih 60 dni. To je **interval izteka**. Sistemska vrednost QPWDRQDDIF podaja, koliko intervalov izteka mora preteči, da lahko znova uporabite isto geslo. V 3. poglavju knjige *iSeries Security Reference* boste našli podrobnejše informacije o skupnem delovanju teh sistemskih vrednosti.
2. QPWDLMTCHR ni uveljavljen za ravni gesel 2 ali 3. Podrobnosti lahko najdetev razdelku“Ravni gesel”.
3. Preglejte razdelek “Načrtovanje sprememb v ravni gesel”, da boste določili raven gesla, ki ustreza vašim potrebam.

Ravni gesel

Od izdaje operacijskega sistema V5R1 naprej nudi sistemska vrednost QPWDLVL večjo zaščito gesel. V prejšnjih izdajah so bili uporabniki omejeni na gesla dolžine 10 znakov, sestavljena iz omejenega območja znakov. Zdaj lahko izberejo uporabniki geslo dolžine do 128 znakov glede na raven gesel, na katero je nastavljen sistem. Ravni gesel so naslednje:

- **Raven 0:** sistemi so naloženi s to ravnijo. Na ravni 0 imajo gesla dolžino 10 znakov in lahko vsebujejo samo črke od A do Z ter znake 0–9, #, @, $ in _. Gesla ravni 0 so manj varna od gesel višje ravni.
- **Raven 1:** Veljajo ista pravila kot za raven 0, toda gesla za podporo iSeries za Omrežno soseščino Windows (ki se od tu naprej imenuje omrežni strežnik iSeries) niso nikoli shranjena.
- **Raven 2:** gesla na tej ravni so zaščitena. To raven lahko uporabite za preizkušanje. Gesla so shranjena za uporabnike ravni 0 ali 1, če imajo 10 znakov ali manj, in za gesla ravni 0 ali 1 je uporabljen nabor znakov. Gesla te ravni imajo naslednje značilnosti:
  - do 128 znakov dolžine
  - sestavljena so iz vseh razpoložljivih znakov tipkovnice
  - ne smejo biti v celoti sestavljena iz praznih mest; prazna mesta na koncu gesla so odstranjena
  - upoštevajo velike in male črke
- **Raven 3:** gesla te ravni so najbolj varna in uporabljajo najbolj razvite razpoložljive algoritme šifriranja. Gesla na tej ravni imajo iste značilnosti kot na ravni 2. Gesla za omrežni strežnik iSeries na tej ravni niso shranjena.

Gesla ravni 2 in 3 uporabite samo, če vsi sistemi v omrežju zadovoljujejo naslednji kriterij:

- nameščen imajo operacijski sistem izdaje V5R1 ali novejše
- raven gesel je nastavljena na 2 ali 3

Vsi uporabniki se morajo prijaviti z uporabo iste ravni gesel. Ravni gesel so globalne, kar pomeni, da uporabniki ne morejo izbrati ravni za njihovo zaščito.

Načrtovanje sprememb v ravni gesel

Spremembe v ravneh gesel je potrebno natančno načrtovati. Če ne izdelate ustreznega načrta za spremembo ravni gesel, se lahko zgodi, da operacije z drugimi sistemi ne bodo uspele ali da se uporabniki ne bodo mogli prijaviti v sistem. Preden spremenite sistemsko vrednost QPWDLVL, shranite podatke o zaščiti s pomočjo ukaza SAVSECDTA ali SAVSYS. Če imate trenutno varnostno kopijo, lahko na novo nastavite gesla za vse profile uporabnikov, če boste morali vrniti nastavitev v nižjo raven gesel.

Izdelki, ki jih uporabljate v sistemu in na odjemalcih, s katerimi sodeluje sistem, imajo lahko težave, če je sistemska vrednost za raven gesel (QPWDLVL) nastavljena na 2 ali 3. Vse izdelke ali odjemalce, ki pošljejo geslo sistemu v šifrirani obliki in ne v čistem besedilu, ki ga vnese uporabnik na prijavnem zaslonu, morate nadgraditi, tako da bodo delovali z novimi pravili šifriranja gesel za QPWDLVL 2 ali 3. Pošiljanje šifriranega gesla se imenuje **nadomestitev gesla**.

Nadomestitev gesla se uporablja za preprečevanje zajetja gesla med prenosom prek omrežja. Nadomestitve za gesla, ustvarjena s starejšimi odjemalci, ki ne podpirajo novega algoritma za QPWDLVL 2 ali 3, tudi če so specifični znaki pravilni, ne bodo sprejeta. To velja tudi za dostop vseh enakovrednih partnerjev od iSeries do iSeries, ko so za overjanje sistemov uporabljene šifrirane vrednosti.

Težava je v tem, da so nekateri prizadeti izdelki (kot je na primer komplet programskih orodij Java) na voljo kot vmesna programska oprema. Izdelki drugih proizvajalcev, ki vključujejo prejšnjo različico enega od teh izdelkov, ne bodo pravilno delovali, dokler jih ne izdelate na novo z nadgrajeno različico vmesne programske opreme.

Glede na zgoraj povedano in na druge scenarije je jasno, zakaj je pred spremembo sistemske vrednosti QPWDLVL potrebno izdelati natančen načrt.

Problematika spreminjanja QPWDLVL iz 0 v 1

Geslo ravni 1 omogoča sistemu, ki mu ni potrebno komunicirati z odjemalsko podporo Windows 95/98/ME AS/400 za izdelek Omrežna soseščina Windows (omrežni strežnik iSeries), odstranitev gesel omrežnega strežnika iSeries iz sistema. Z odstranitvijo nepotrebnih šifriranih gesel iz sistema se poveča splošna zaščita sistema.

Na ravni QPWDLVL 1 bodo delovali vsi trenutni mehanizmi overjanja in nadomestitve gesel in vsi mehanizmi pred V5R1. Možnost za potencialni vdor je zelo majhna, razen za funkcije in storitve, ki zahtevajo geslo omrežnega strežnika iSeries.

Problematika spreminjanja QPWDLVL iz 0 ali 1 v 2

Geslo ravni 2 uvaja uporabo gesel, ki upoštevajo velike in male črke, imajo dolžino do 128 znakov in nudijo največjo možnost za vrnitev v QPWDLVL 0 ali 1.

Ne glede na raven gesel sistema so gesla ravni 2 in 3 izdelana pri vsaki spremembi gesla ali pri prijavi uporabnika v sistem. Če uporabljate gesla ravni 2 in 3, med tem ko sistem še vedno uporablja raven gesel 0 ali 1, pomagate pri pripravi na spremembo v raven gesel 2 ali 3.

Preden spremenite QPWDLVL v 2, s pomočjo ukazov DSPAUTUSR ali PRTUSRPRF TYPE(*PWDINFO) poiščite vse profile uporabnikov, ki nimajo gesel, ki jih je mogoče uporabiti na ravni gesel 2. Glede na profile, ki jih najdeta ta ukaza, lahko z enim izmed naslednjih načinov v profil dodate gesla ravni 2 in 3.

- Spremenite geslo za profil uporabnika s pomočjo ukazov CL CHGUSRPRF ali CHGPWD ali API-ja QSYCHGPW. S tem boste povzročili, da bo sistem spremenil geslo, ki ga je mogoče uporabiti na ravni gesel 0 in 1. Sistem bo izdelal tudi dve enakovredni gesli, ki upoštevata velike in male črke, ki ju je mogoče uporabiti na ravni gesel 2 in 3. Za uporabo gesel ravni 2 ali 3 je izdelana ena različica gesla samo z velikimi črkami in ena različica samo z malimi črkami.

  Če na primer spremenite geslo v C4D2RB4Y, ustvari sistem gesli ravni 2 C4D2RB4Y in c4d2rb4y.
- Prijavite se v sistem na način, ki predstavi geslo v čistem besedilu (ne uporablja nadomestitve gesla). Če je geslo veljavno in profil uporabnika nima gesla, ki ga je mogoče uporabiti na ravni gesel 2 in 3, sistem ustvari dve enakovredni gesli, ki upoštevata velike in

male črke, ki ju je mogoče uporabiti na ravni gesel 2 in 3. Za uporabo na ravni gesel 2 ali 3 je izdelana ena različica gesla samo z velikimi črkami in ena različica gesla samo z malimi črkami.

Če geslo, ki ga je mogoče uporabiti na ravni gesel 2 ali 3 ne obstaja, to lahko predstavlja težavo, če profil uporabnika tudi nima gesla, ki ga je mogoče uporabiti na ravni gesel 0 in 1 ali če se uporabnik poskusi prijaviti prek izdelka, ki uporablja nadomestitev gesel. V teh primerih se uporabnik ne bo mogel prijaviti, če spremenite raven gesel v 2.

Če profil uporabnika nima gesla, ki ga je mogoče uporabiti na ravni gesel 2 in 3 in če profil uporabnika nima gesla, ki ga je mogoče uporabiti na ravni gesel 0 in 1 in se uporabnik prijavi prek izdelka, ki pošlje gesla v čistem besedilu, sistem primerja uporabnika z geslom ravni 0 in izdela za profil uporabnika dve gesli ravni 2 (kot je opisano zgoraj). Nadaljnje prijave bodo primerjane z gesli ravni 2.

Noben odjemalec ali storitev, ki uporabljata nadomestitev gesel, ne bosta pravilno delovala na ravni QPWDLVL 2, če ju ne nadgradite za uporabo nove nadomestitvene sheme gesel. Skrbnik naj preveri, ali sta odjemalec ali storitev, ki nista bila nadgrajena v novo nadomestitveno shemo gesel, potrebna.

Odjemalci in storitve, ki uporabljajo nadomestitev gesel, so naslednji:

- TELNET
- iSeries Access
- Gostiteljski strežniki iSeries
- QFileSrv.400
- Tiskalna podpora za omrežni strežnik iSeries
- DDM
- DRDA
- SNA LU6.2

Preden opravite spremembo v QPWDLVL 2, priporočamo, da shranite podatke o zaščiti. Če bo potrebna vrnitev v QPWDLVL 0 ali 1, bo veliko preprostejša.

Priporočamo, da drugih sistemskih vrednosti gesel, kot sta QPWDMINLEN in QPWDMAXLEN, ne spremenite, dokler ne opravite nekaj preizkusov v QPWDLVL 2. Če bo potrebna vrnitev v QPWDLVL 1 ali 0 veliko preprostejša. Toda sistemska vrednost QPWDVLDPGM mora podajati *REGFAC ali *NONE, preden bo sistem dovolil, da spremenite QPWDLVL v 2. Če uporabite program za preverjanje veljavnosti gesel, boste najbrž napisali novega, ki ga lahko s pomočjo ukaza ADDEXITPGM registrirate za izhodno točko QIBM_QSY_VLD_PASSWRD.

Gesla iSeries NetServer so v QPWDLVL 2 še zmeraj podprta, tako da bi morale vse funkcije/storitve, ki zahtevajo geslo iSeries NetServer, še zmeraj pravilno delovati.

Ko se skrbnik navadi na izvajanje sistema v ravni QPWDLVL 2, lahko začne spreminjati sistemske vrednosti gesel za uporabo daljših gesel. Toda zavedati se mora, da je z dolgimi gesli povezano naslednje:

- Če podate gesla, daljša od 10 znakov, sta ravni gesel 0 in 1 odstranjeni. Ta profil uporabnika se ne bo mogel prijaviti, če vrnete sistem na raven gesel 0 ali 1.
- Če vsebujejo gesla posebne znake ali ne upoštevajo pravil sestave za preprosta imena objektov (vključno z upoštevanjem velikih in malih črk), so gesla ravni 1 in 2 odstranjena.
- Če podate gesla, daljša od 14 znakov, je geslo omrežnega strežnika iSeries za profil uporabnika odstranjeno.

- Sistemske vrednosti gesel veljajo samo za vrednost novega gesla ravni 2, ne pa tudi za sistemsko ustvarjeno geslo ravni 0 in 1 ali za vrednosti gesel omrežnega strežnika iSeries (če so ustvarjene).

Problematika spreminjanja QPWDLVL iz 2 v 3

Ko nekaj časa izvajate sistem na ravni QPWDLVL 2, lahko skrbnik preklopi v raven QPWDLVL 3, da še poveča zaščito gesel.

Na ravni QPWDLVL 3 so gesla omrežnega strežnika iSeries odstranjena, zato sistema ne prenesite v QPWDLVL 3, dokler ni več nobene potrebe za uporabo gesel omrežnega strežnika iSeries.

Na ravni QPWDLVL 3 so vsa gesla ravni 0 in 1 odstranjena. Skrbnik lahko s pomočjo ukazov DSPAUTUSR ali PRTUSRPRF poišče profile uporabnikov, s katerimi niso povezana gesla ravni 2 ali 3.

Sprememba v nižjo raven gesel

Vrnitev v nižjo raven QPWDLVL, dokler je mogoča, ni tako preprosta operacija. Na splošno bi morali razmišljati o ravneh kot o enosmerni poti iz nižjih vrednosti QPWDLVL v višje vrednosti QPWDLVL. Toda včasih je potrebno vrednost QPWDLVL vrniti prejšnje stanje.

Naslednji razdelki razlagajo, kaj je potrebno opraviti za vrnitev v nižjo raven gesel.

Problematika spreminjanja iz QPWDLVL 3 v 2: Ta sprememba je dokaj preprosta. Ko je QPWDLVL nastavljen v 2, mora skrbnik določiti, ali mora kateri izmed profilov uporabnikov vsebovati gesla omrežnega strežnika iSeries in gesla ravni 0 ali 1; v primeru, da jih potrebuje, mora spremeniti geslo profila uporabnika v dovoljeno vrednost.

Poleg tega je potrebno spremeniti sistemske vrednosti gesla nazaj v vrednosti, združljive z omrežnim strežnikom iSeries in z gesli ravni 0 ali 1, če so le-ta potrebna.

Problematika spreminjanja iz QPWDLVL 3 v 1 ali 0: Zaradi velike možnosti, da bo ta sprememba povzročala težave v sistemu (kot je na primer, da se nihče ne more prijaviti, ker so vsa gesla ravni 0 in 1 odstranjena), ni neposredno podprta. Če želite opraviti spremembo iz QPWDLVL 3 v QPWDLVL 1 ali 0, morate najprej opraviti vmesno spremembo v QPWDLVL 2.

Problematika spreminjanja iz QPWDLVL 2 v 1: Preden spremenite QPWDLVL v 1, naj skrbnik s pomočjo ukaza DSPAUTUSR ali PRTUSRPRF TYPE(*PWDINFO) poišče profile uporabnikov, ki nimajo gesla ravni 0 ali 1. Če bo profil uporabnika bo spremembi QPWDLVL zahteval geslo, naj skrbnik z enim izmed naslednjih načinov zagotovi, da bo za profil izdelano geslo ravni 0 in 1:

- Spremenite geslo za profil uporabnika s pomočjo ukazov CL CHGUSRPRF ali CHGPWD ali API-ja QSYCHGPW. S tem boste povzročili, da bo sistem spremenil geslo, ki ga je mogoče uporabiti na ravni gesel 2 in 3. Sistem bo izdelal tudi enakovredno geslo iz velikih črk, ki ga je mogoče uporabiti na ravni 0 in 1. Sistem lahko izdela geslo ravni 0 in 1 samo, če so zadovoljeni naslednji pogoji:
  - Dolžina gesla je 10 znakov ali manj.
  - Geslo je mogoče pretvoriti v znake EBCDIC iz velikih črk A-Z, 0-9, @, #, $ in podčrtaj.
  - Geslo se ne začne s številko ali s podčrtajem.

  Če na primer spremenite geslo v vrednost LepDan, to povzroči, da sistem ustvari geslo ravni 0 in 1 LEPDAN. Toda če spremenite vrednost gesla v Lepi dnevi v aprilu, bo sistem odstranil geslo ravni 0 in 1 (ker je geslo predolgo in vsebuje presledke).

  Če gesla ravni 0 ali 1 ni mogoče izdelati, ni izdelano nobeno sporočilo ali navedba.

- Prijavite se v sistem na način, ki predstavi geslo v čistem besedilu (ne uporablja nadomestitve gesla). Če je geslo veljavno in profil uporabnika nima gesla, ki ga je mogoče uporabiti na ravni gesel 0 in 1, ustvari sistem enakovredno geslo iz velikih črk, ki ga je mogoče uporabiti na ravni gesel 0 in 1. Sistem lahko ustvari geslo ravni 0 in 1 samo, če so zadovoljeni zgoraj navedeni pogoji.

Skrbnik lahko nato spremeni QPWDLVL v 1. Vsa gesla omrežnega strežnika iSeries so odstranjena, ko stopi v veljavo sprememba v QPWDLVL 1 (naslednji IPL).

Problematika spreminjanja iz QPWDLVL 2 v 0: Problematika je ista kot pri spreminjanju iz QPWDLVL 2 v 1, z razliko, da so vsa gesla omrežnega strežnika iSeries pri uveljavitvi spremembe ohranjena.

Problematika spreminjanja iz QPWDLVL 1 v 0: Ko spremenite QPWDLVL v 0, naj skrbnik s pomočjo ukaza DSPAUTUSR ali PRTUSRPRF poišče profile uporabnikov, ki nimajo gesla omrežnega strežnika iSeries. Če profil uporabnika zahteva geslo omrežnega strežnika iSeries, ga lahko izdelate tako, da spremenite geslo uporabnika ali s prijavo na način, ki predstavi geslo v čistem besedilu.

Skrbnik lahko nato spremeni QPWDLVL v 0.

Spreminjanje znanih gesel

Naslednji načini kažejo, kako zaprete nekaj znanih vhodov na strežnik iSeries, ki lahko obstajajo v sistemu.

__ Korak 1. Zagotovite, da noben profil uporabnika ne uporablja privzetega gesla (ki je enako imenu profila uporabnika). Uporabite lahko ukaz ANZDFTPWD (Analiziraj privzeta gesla). (Preglejte razdelek “Izogibanje privzetim geslom” na strani 23.)

__ Korak 2. Poskusite se prijaviti v sistem s kombinacijo profilov uporabnikov in gesel, prikazanih v Tabela 2 na strani 19. Ta gesla so objavljena in so prva izbira vsakogar, ki poskusi vdreti v sistem. Če se lahko prijavite, s pomočjo ukaza CHGUSRPRF (Spremeni profil uporabnika) spremenite geslo v priporočeno vrednost.

__ Korak 3. Zaženite namenska servisna orodja (DST) in se poskusite prijaviti z gesli, prikazanimi v razdelku Tabela 2 na strani 19. Preglejte Informacijski center iSeries —>Zaščita—>Storitvena orodja. Preglejte razdelek “Predpogoji in s tem povezane informacije” na strani xii, kjer boste našli informacije o dostopu do Informacijskega centra iSeries.

__ Korak 4. Če se lahko prijavite v DST z enim od teh gesel, jih spremenite. V Informacijskem centru iSeries —>Zaščita—>Storitvena orodja boste našli podrobne informacije o spremembi ID-jev uporabnikov in gesel servisnih orodij. Podrobnejše informacije o dostopu do Informacijskega centra iSeries poiščitev razdelku“Predpogoji in s tem povezane informacije” na strani xii.

__ Korak 5. Na koncu zagotovite, da se ne morete prijaviti s preprostim pritiskom tipke Enter na prijavnem zaslonu, ne da bi vnesli ID uporabnika in geslo. Poskusite več različnih zaslonov. Če se lahko prijavite, ne da bi na prijavni zaslon vnesli informacije, naredite nekaj od naslednjega:

- Uporabite raven zaščite 40 ali 50 (sistemska vrednost QSECURITY).

  Opomba: Če povečate raven zaščite v 40 ali 50, se lahko aplikacije drugače izvajajo.

- Spremenite vse postavke delovne postaje za interaktivne podsisteme, tako da bodo kazale na opise opravil, ki podajajo USER(*RQD).

Tabela 2. Gesla za profile, ki jih poda IBM

ID uporabnika	Geslo	Priporočena vrednost
QSECOFR	QSECOFR[1]	Netrivialna vrednost, ki jo pozna samo skrbnik za zaščito. **Zapišite si izbrano geslo in ga shranite na varno mesto.**
QSYSOPR	QSYSOPR	*NONE[2]
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2, 3]
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

Opombe:

1. Sistem je dobavljen tako, da je vrednost *Nastavi geslo na pretečeno* za QSECOFR nastavljena na *YES. Ko se prvič prijavite v nov sistem, morate spremeniti geslo QSECOFR.
2. Sistem potrebuje te profile uporabnikov za sistemske funkcije, toda uporabnikom ne pustite, da se prijavijo s temi profili. Za nove sisteme, nameščene z izdajo V3R1 ali novejšo, je to geslo nastavljeno na *NONE.

   Če zaženete ukaz CFGSYSSEC, nastavi sistem ta gesla na *NONE.
3. Če želite zagnati iSeries Access za Windows s pomočjo TCP/IP, morate omogočiti profil uporabnika QUSER.

Tabela 3. Gesla za namenska servisna orodja

Raven DST	ID uporabnika[1]	Geslo	Priporočena vrednost
Osnovna zmožnost	11111111	11111111	Netrivialna vrednost, ki jo pozna samo skrbnik za zaščito.[2]
Vse zmožnosti	22222222	22222222[3]	Netrivialna vrednost, ki jo pozna samo skrbnik za zaščito.[2]
Zmožnost zaščite	QSECOFR	QSECOFR[3]	Netrivialna vrednost, ki jo pozna samo skrbnik za zaščito.[2]
Zmožnost storitev	QSRV	QSRV[3]	Netrivialna vrednost, ki jo pozna samo skrbnik za zaščito.[2]

Opombe:

1. ID uporabnika je potreben samo za izdaje PowerPC AS (RISC) operacijskega sistema.
2. Če se mora predstavnik servisne službe prijaviti s tem ID-jem uporabnika in geslom, po njegovem odhodu spremenite geslo v novo vrednost.
3. Profil uporabnika servisnih orodij se izteče takoj po prvi uporabi.

Opomba: Gesla DST lahko spremenite samo z overjeno napravo. To velja tudi za vsa gesla in ustrezne ID-je uporabnikov, ki so identični. Podrobnejše informacije o overjenih napravah preberite v informacijah Informacijskega centra iSeries o nastavitvi operacijske ukazne mize.

Nastavitev vrednosti za prijavo

Tabela 4 na strani 20 kaže številne vrednosti, ki jih lahko nastavite, da otežite prijavo nepooblaščene osebe v sistem. Če zaženete ukaz CFGSYSSEC, nastavi te sistemske vrednosti na priporočene nastavitve. Več o teh sistemskih vrednostih lahko preberete v 3. poglavju knjige *iSeries Security Reference*.

Tabela 4. Sistemske vrednosti za prijavo

Ime sistemske vrednosti	Opis	Priporočena nastavitev
QAUTOCFG	Ali sistem samodejno konfigurira nove naprave.	0 (Ne)
QAUTOVRT	Število opisov navideznih naprav, ki jih samodejno izdela sistem, če ni za uporabo na voljo nobena naprava.	0
QDEVRCYACN	Kaj naredi sistem, če se naprava na novo poveže po napaki.[1]	*DSCMSG
QDSCJOBITV	Kako dolgo sistem počaka, preden konča prekinjeno opravilo.	120
QDSPSGNINF	Ali sistem pri prijavi uporabnika prikaže informacije o prejšnji prijavi.	1 (Da)
QINACTITV	Kako dolgo sistem čaka, preden izvede dejanje, če je interaktivno opravilo neaktivno.	60
QINACTMSGQ	Kaj naredi sistem, ko je doseženo časovno obdobje QINACTITV.	*ENDJOB
QLMTDEVSSN	Ali sistem prepreči uporabniku, da se sočasno prijavi na več kot eno delovno postajo.	1 (Da)
QLMTSECOFR	Ali se lahko uporabniki s posebnim pooblastilom *ALLOBJ ali *SERVICE prijavijo samo na določene delovne postaje.	1 (Da)[2]
QMAXSIGN	Največje dovoljeno število zaporednih, nepravilnih poskusov prijav (profil uporabnika ali geslo nista pravilna).	3
QMAXSGNACN	Kaj naredi sistem, ko je dosežena omejitev QMAXSIGN.	3 (Onemogoči profil uporabnika in napravo)

Opombe:

1. Sistem lahko prekine in znova vzpostavi seje TELNET, če je opis naprave za sejo izrecno dodeljen.
2. Če nastavite sistemsko vrednost na 1 (Da), morate za naprave izrecno pooblastiti uporabnike s posebnim pooblastilom *ALLOBJ ali *SERVICE. To najpreprosteje naredite tako, da dodelite profilu uporabnika QSECOFR pooblastilo *CHANGE za določene naprave.

Spreminjanje sporočil o napakah pri prijavi

Hekerji radi vedo, kadar jim uspeva vdor v sistem. Če sporočilo o napaki na prijavnem zaslonu pravi, da geslo ni pravilno, lahko heker sklepa, da je ID uporabnika pravilen. Če uporabite ukaz CHGMSGD (Spremeni opis sporočila), ki spremeni besedilo za dve prijavni sporočili o napakah, lahko onemogočite hekerja. Tabela 5 kaže priporočeno besedilo.

Tabela 5. Sporočila o napakah pri prijavi

ID sporočila	Naloženo besedilo	Priporočeno besedilo
CPF1107	CPF1107 – Geslo za profil uporabnika ni pravilno.	Prijavne informacije niso pravilne. **Opomba:** V besedilo sporočila ne vključite ID-ja sporočila.
CPF1120	CPF1120 – Uporabnik XXXXX ne obstaja.	Prijavne informacije niso pravilne. **Opomba:** V besedilo sporočila ne vključite ID-ja sporočila.

Načrtovanje razpoložljivosti profilov uporabnikov

Nekatere profile uporabnikov lahko nastavite tako, da so na voljo za prijavo samo ob določenih urah ali ob določenih dneh. Če imate na primer nastavljen profil za kontrolorja zaščite, ga lahko nastavite samo za tiste ure, ko veste, da bo kontrolor opravljal svoje delo. V času, ko veste, da so profili uporabnikov izven uporabe, jih lahko onemogočite s posebnim pooblastilom *ALLOBJ (vključno s profilom uporabnika QSECOFR).

S pomočjo ukaza CHGACTSCDE (Spremeni postavko urnika aktiviranja) lahko nastavite profile uporabnikov tako, da so samodejno omogočeni in onemogočeni. Za vsak profil uporabnika, ki ga želite načrtovati, izdelajte postavko, ki definira njegov urnik.

Če na primer želite, da je profil QSECOFR na voljo samo od sedmih zjutraj do desetih zvečer, vpišite na zaslon CHGACTSCDE naslednje:

```
              Spremeni postavko urnika aktiviranja (CHGACTSCDE)

Vpišite izbire in pritisnite tipko Enter.

Profil uporabnika  . . . . . . . . . . . > QSECOFR       Ime
Čas aktiviranja. . . . . . . . . . . . . > '7:00'        Čas, *NONE
Čas deaktiviranja. . . . . . . . . . . . > '22:00'       Čas, *NONE
Dnevi. . . . . . . . . . . . . . . . . . > *MON          *ALL, *MON, *TUE, *WED...
                                 > *TUE
                                 > *WED
                                 > *THU
                + za dodatne vrednosti > *FRI
```

Slika 2. Zaslon Načrtovanje aktiviranja profila - zgled

Pravzaprav lahko omogočite profil QSECOFR samo za nekaj ur dnevno. Za izvedbo večine sistemskih funkcij lahko uporabite kakšen drug profil uporabnika z razredom *SECOFR. Na ta način se izognete izpostavi znanega profila uporabnika napadom hekerjev.

Občasno lahko uporabite ukaz DSPAUDJRNE (Prikaži postavke dnevnika beleženja) in natisnete postavke dnevnika beleženja CP (Spremeni profil). S pomočjo teh postavk lahko preverite, ali sistem omogoči in onemogoči profile uporabnikov v skladu z načrtovanim urnikom.

Drug način, s katerim lahko zagotovite, da so profili uporabnikov onemogočeni v skladu z načrtovanim urnikom, je uporaba ukaza PRTUSRPRF (Natisni profil uporabnika). Če podate *PWDINFO za tip poročila, vključuje poročilo status vseh izbranih profilov uporabnikov. Če na primer redno onemogočite vse profile uporabnikov s posebnim pooblastilom *ALLOBJ, lahko takoj za tem, ko onemogočite profile, načrtujete zagon naslednjega ukaza:

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

Odstranitev neaktivnih profilov uporabnikov

Vaš sistem naj vsebuje samo profile uporabnikov, ki so potrebni. Če profila uporabnika ne potrebujete več, ker je uporabnik odšel ali je dobil drugo mesto znotraj podjetja, profil odstranite. Če uporabnika dalj časa ne bo v podjetju, onemogočite (deaktivirajte) ta profil uporabnika. Nepotreben profil uporabnika lahko omogoči nepooblaščen vstop v sistem.

Samodejno onemogočanje profilov uporabnikov

Ukaz ANZPRFACT (Analiziraj dejavnost profila) lahko redno onemogoča profile uporabnikov, ki so neaktivnih določeno število dni. Če uporabite ukaz ANZPRFACT, podate

število dni neaktivnosti, ki jih išče sistem. Sistem išče datum zadnje uporabe, datum obnovitve in datum izdelave profila uporabnika.

Ko podate vrednost za ukaz ANZPRFACT, sistem izdela načrt za tedensko izvajanje opravila ob 13.00 (začenši z dnem za prvo določitvijo vrednosti). Opravilo pregleda vse profile in onemogoči tiste, ki niso aktivni. Ukaza ANZPRFACT ni potrebno uporabiti znova, razen če želite spremeniti število dni neaktivnosti.

Če uporabite ukaz CHGACTPRFL (Spremeni seznam aktivnih profilov), lahko nekatere profile izvzamete iz obdelave ANZPRFACT. Ukaz CHGACTPRFL izdela seznam profilov uporabnikov, ki jih ukaz ANZPRFACT ne bo onemogočil, ne glede na to, kako dolgo se neaktivni.

Ko sistem zažene ukaz ANZPRFACT, zapiše postavko CP v dnevnik beleženja za vsak profil uporabnika, ki je onemogočen. S pomočjo ukaza DSPAUDJRNE lahko navedete seznam profilov uporabnikov, ki so na novo onemogočeni.

Opomba: Sistem zapiše postavko beleženja samo, če vrednost QAUDCTL podaja *AUDLVL in sistemska vrednost QAUDLVL podaja *SECURITY.

Drug način, s katerim lahko zagotovite, da so profili uporabnikov onemogočeni v skladu z načrtovanim urnikom, je uporaba ukaza PRTUSRPRF (Natisni profil uporabnika). Če podate *PWDINFO za tip poročila, vključuje poročilo status vseh izbranih profilov uporabnikov.

Samodejna odstranitev profilov uporabnikov

Ukaz CHGEXPSCDE (Spremeni postavko urnika izteka) lahko uporabite za upravljanje odstranitve ali onemogočanja profilov uporabnikov. Če veste, da uporabnika nekaj časa ne bo, lahko njegov profil uporabnika odstranite ali onemogočite.

Ko prvič uporabite ukaz CHGEXPSCDE, izdela postavko urnika opravila, ki se zažene vsak dan minuto čez polnoč. Opravilo pregleda datoteko QASECEXP in določi, ali je ta dan za odstranitev določen kakšen profil uporabnika.

Z ukazom CHGEXPSCDE lahko profil uporabnika onemogočite ali zbrišete. Če se odločite, da ga boste zbrisali, morate podati, kaj bo naredil sistem z objekti, katerih lastnik je uporabnik. Preden zbrišete profil uporabnika, morate pregledati objekte uporabnika. Če je na primer uporabnik lastnik programov, ki prevzamejo pooblastilo, ali boste želeli, da ti programi prevzamejo pooblastilo novega lastnika? Ali pa ima nov lastnik morda več pooblastil, kot je potrebno (kot je posebno pooblastilo)? Morda boste morali izdelati nov profil uporabnika s posebnimi pooblastili, ki bo lastnik programov, ki morajo prevzeti pooblastilo.

Raziskati morate tudi, ali bo brisanje profila uporabnika povzročilo kakšen težave v aplikacijah. Ali na primer kakšen opis opravila podaja profil uporabnika kot privzetega uporabnika?

S pomočjo ukaza DSPEXPSCD (Prikaži urnik izteka) lahko prikažete seznam profilov, ki so terminirani za brisanje ali onemogočenje.

Z ukazom DSPAUTUSR (Prikaži pooblaščene uporabnike) lahko navedete vse profile uporabnikov v sistemu. Zastarele profile zbrišite z ukazom DLTUSRPRF (Zbriši profil uporabnika).

Opomba k zaščiti:: Profil uporabnika onemogočite tako, da nastavite njegov status v *DISABLED. Če onemogočite profil uporabnika, ni na voljo za

interaktivno uporabo. Z onemogočenim profilom uporabnika se ne morete prijaviti. Paketna opravila se lahko izvajajo pod onemogočenim profilom uporabnika.

Izogibanje privzetim geslom

Ko izdelate nov profil uporabnika, je po privzetku izdelano geslo, ki je isto kot ime profila uporabnika. To je priložnost za nekoga, da vstopi v sistem, če pozna vaša načela za dodeljevanje imen profilov in ve, da se vam bo v podjetju pridružil nov sodelavec.

Pri izdelavi novih profilov uporabnikov uporabite namesto privzetega gesla unikatno, nevsakdanje geslo. Novemu uporabniku predajte geslo zaupno, kot je na primer v pismu "Dobrodošli v sistem", ki razlaga načela za zaščito. Z nastavitvijo profila uporabnika v PWDEXP(*YES) zahtevajte, da uporabnika spremeni geslo pri prvi uporabi.

S pomočjo ukaza ANZDFTPWD (Analiziraj privzeta gesla) lahko pregledate vse profile uporabnikov v sistemu in preverite, ali kateri med njimi uporablja privzeto geslo. Pri natisu poročila lahko podate, naj sistem v primeru, da je geslo isto kot ime profila uporabnika, opravi določeno dejanje (kot je na primer, da onemogoči profil uporabnika). Ukaz ANZDFTPWD natisne seznam profilov, ki jih najde, in dejanj, ki jih opravi.

Opomba: Gesla so shranjena v sistemu v obliki šifriranja v eni smeri. To pomeni, da jih ni mogoče dešifrirati. Sistem šifrira podano geslo in ga primerja s shranjenim geslom, ravno tako kot preveri geslo pri prijavi v sistem. Če izvajate beleženje za napake v pooblastilih (*AUTFAIL), bo sistem zapisal postavko dnevnika beleženja PW za vsak profil uporabnika, ki *nima* privzetega gesla (za sisteme, v katerih se izvaja izdaja V4R1 ali starejša). Od izdaje V4R2 naprej sistem pri izvedbi ukaza ANZDFTPWD ne zapiše postavk dnevnika beleženja PW.

Nadzorovanje delovanja prijave in gesel

Če vas skrbijo poskusi nepooblaščenega vstopa v sistem, lahko uporabite ukaz PRTUSRPRF, ki vam bo pomagal pri nadzorovanju delovanja prijave in gesel.

Sledi nekaj predlogov za uporabo tega poročila:

- Določite, ali je interval za potek gesel za nekatere profile uporabnikov daljši od sistemske vrednosti in ali je opravičen. USERY ima na primer v poročilu nastavljen interval za potek gesla 120 dni.
- To poročilo redno izvajajte, da boste nadzorovali poskuse neuspešnih prijav. Nekdo, ki poskuša vdreti v vaš sistem, se lahko zaveda, da sistem po določenem številu neuspešnih poskusov opravi neko dejanje. Možni vdiralec lahko tako na primer vsako noč poskusi vdor manjkrat, kot dopušča vrednost QMAXSIGN, in vas tako ne opozori na poskuse. Če to poročilo zaženete vsako jutro in opazite, da imajo določeni profili uporabnikov pogosto neuspele poskuse prijave, lahko sumite, da gre za težavo.
- Določite profile uporabnikov, ki že nekaj časa niso v bili uporabi ali katerih gesla že nekaj časa niso bila spremenjena.

Informacije o shranitvi gesel

Za podporo nekaterim omrežnim funkcijam in komunikacijskim zahtevam nudijo strežniki iSeries varen način za shranjevanje gesel, ki jih je mogoče dešifrirati. Vaš sistem na primer uporablja ta gesla za vzpostavitev povezave SLIP z drugim sistemom. ("Zaščita in seje izhodnih klicev" na strani 115 opisuje to uporabo shranjenih gesel.)

Strežniki iSeries shranijo ta posebna gesla v zaščitenem področju, do katerega ne more dostopiti noben uporabniški program ali vmesnik. Ta gesla lahko nastavijo in pridobijo samo izrecno pooblaščene sistemske funkcije.

Če uporabite na primer shranjeno geslo za izhodne povezave SLIP, nastavite geslo s sistemskim ukazom, ki izdela konfiguracijski profil (WRKTCPPTP). Za uporabo ukaza potrebujete *IOSYSCFG. Posebej kodiran povezovalni skript pridobi geslo, ki ga dešifrira v postopku izhodnega klica. Dešifrirano geslo ni vidno za uporabnika in za noben dnevnik opravil.

Kot skrbnik za zaščito se morate odločiti, ali boste dovolili v sistemu shranjevanje gesel, ki jih je mogoče dešifrirati. To podate s pomočjo sistemske vrednosti Ohrani podatke o zaščiti strežnika (QRETSVRSEC). Privzeta vrednost je 0 (Ne). Če izrecno ne nastavite te sistemske vrednosti, sistem zato ne bo shranil gesel, ki jih je mogoče dešifrirati.

Če obstajajo omrežne ali komunikacijske zahteve za shranjena gesla, morate nastaviti ustrezna načela in razumeti načela in postopke vaših komunikacijskih partnerjev. Če na primer uporabite SLIP za komuniciranje z drugim strežnikom iSeries, je najbolje, če v obeh sistemih nastavite posebne profile uporabnikov za vzpostavljanje sej. Posebni profili naj imajo omejeno pooblastilo v sistemu. S tem omejite vpliv v vašem sistemu, če pride do okvare shranjenega gesla v sistemu partnerja.

Poglavje 4. Konfiguriranje iSeries za uporabo orodij za zaščito

V teh informacijah bomo opisali, kako nastaviti sistem za uporabo orodij za zaščito, ki so del OS/400. Ko namestite OS/400, so orodja za zaščito pripravljena za uporabo. V nadaljnjih temah boste našli predloge za operacijske postopke z orodji za zaščito.

Varno delovanje orodij za zaščito

Ko namestite OS/400, so objekti, ki so povezani z orodji za zaščito, varni. Da bi orodja za zaščito delovala varno, se izogibajte izvajanju sprememb v objektih orodij za zaščito.

Sledijo nastavitve in zahteve zaščite za objekte orodij za zaščito:

- Programi in ukazi orodij za zaščito so v knjižnici QSYS. Naloženi so z javnim pooblastilom *EXCLUDE. Številni ukazi orodij za zaščito izdelajo datoteke v knjižnici QUSRSYS. Ko sistem izdela te datoteke, imajo javno pooblastilo *EXCLUDE.

  Datoteke, ki vsebujejo informacije za tvorbo poročil o spremembah, imajo imena, ki se začno s QSEC. Datoteke, ki vsebujejo informacije za upravljanje profilov uporabnikov, imajo imena, ki se začno s QASEC. Te datoteke vsebujejo zaupne informacije o vašem sistemu, zato njihovega javnega pooblastila ne spremenite.
- Orodja za zaščito uporabljajo običajno nastavitev sistema za usmeritev natisnjenih izhodnih podatkov. Ta poročila vsebujejo zaupne informacije o sistemu. Če želite usmeriti izhodne podatke v zaščiteno izhodno čakalno vrsto, opravite ustrezne spremembe v profilu uporabnika ali v opisu opravila za uporabnike, ki bodo izvajali orodja za zaščito.
- Zaradi funkcij zaščite, ki jih nudijo ukazi orodij za zaščito in zaradi tega, ker dostopajo do številnih objektov v sistemu, zahtevajo posebno pooblastilo *ALLOBJ. Nekateri ukazi zahtevajo tudi posebno pooblastilo *SECADM, *AUDIT ali *IOSYSCFG. Da bi zagotovili uspešno izvajanje ukazov, se pri uporabi orodij za zaščito prijavite kot varnostnik za zaščito. Zato ni potrebno dodeliti zasebnega pooblastila nobenemu ukazu orodij za zaščito.

Odpravljanje navzkrižij med datotekami

Številni ukazi poročil orodij za zaščito ustvarijo datoteko baze podatkov, ki jo lahko uporabite za natis različice poročila o spremembah. V razdelku“Ukazi in meniji ukazov za zaščito” na strani 26 boste našli ime datoteke za vsak ukaz. Sočasno lahko zaženete ukaz samo iz enega opravila. Večina ukazov zdaj vključuje funkcijo preverjanja, ki uveljavi to zahtevo. Če zaženete ukaz, ko ga uporablja še drugo opravilo, se prikaže sporočilo o napaki.

Številna tiskalna opravila so dolgotrajna opravila. Ko predložite poročila v paket ali jih dodate v planer opravil, morate biti previdni, da se izognete navzkrižjem med datotekami. Natisnete lahko na primer dve različici poročila PRTUSRPRF z različnim izbiralnim kriterijem. Če predložite poročila v paket, uporabite čakalno vrsto opravil, ki izvaja sočasno samo eno opravilo, in zagotovite, da se opravila poročil izvajajo zaporedoma.

Če uporabite planer opravil, morate načrtovati dve opravili tako, da je med njima dovolj velika časovnega razmika, da se prva različica konča, preden se začne drugo opravilo.

Shranitev orodij za zaščito

Programe orodij za zaščito shranite vsakič, ko zaženete ukaz SAVSYS (Shrani sistem) ali možnost z menija Shranjevanje, ki izvede ukaz SAVSYS.

Datoteke orodij za zaščito so v knjižnici QUSRSYS. To knjižnico shranite kot del običajnih shranjevalnih postopkov. Knjižnica QUSRSYS vsebuje podatke za številne licenčne programe v sistemu. Podrobnejše informacije o ukazih in možnostih, ki shranijo knjižnico QUSRSYS, lahko najdete v Informacijskem centru.

Ukazi in meniji ukazov za zaščito

Ta razdelek opisuje ukaze in menije orodij za zaščito. V teh informacijah boste našli več zgledov za uporabo teh ukazov.

Za orodja za zaščito sta na voljo dva menija:

- Meni SECTOOLS (Orodja za zaščito), ki izvaja ukaze interaktivno.
- Meni SECBATCH (Predloži ali načrtuj poročila zaščite v paket), ki izvede ukaze poročila v paketu. Meni SECBATCH je sestavljen iz dveh delov. Prvi del menija uporabi ukaz SBMJOB (Predloži opravilo), ki predloži poročila za takojšnjo obdelavo v paketu.

  Drugi del menija uporabi ukaz ADDJOBSCDE (Dodaj postavko urnika opravila). Z njim lahko načrtujete redno izvajanje poročil zaščite ob določenih dneh in urah.

Menijske možnosti orodij za zaščito

Tabela 6 opisuje te menijske možnosti in z njimi povezane ukaze:

Tabela 6. Ukazi orodij za profile uporabnikov

Možnost menija [1]	Ime ukaza	Opis	Uporabljena datoteka baze podatkov
1	ANZDFTPWD	Ukaz Analiziraj privzeta gesla uporabite za poročanje o profilih uporabnikov, v katerih je geslo isto kot ime profila uporabnika.	QASECPWD[2]
2	DSPACTPRFL	Ukaz Prikaži seznam aktivnih profilov uporabite za prikaz in natis seznama profilov uporabnikov, ki so izvzeti iz obdelave ANZPRFACT.	QASECIDL[2]
3	CHGACTPRFL	Ukaz Spremeni seznam aktivnih profilov uporabite za dodajanje profilov uporabnikov na seznam izjem in odstranitev z njega za ukaz ANZPRFACT. Profil uporabnika, ki je na seznamu aktivnih profilov, je trajno aktiven (dokler ga ne odstranite s seznama). Ukaz ANZPRFACT ne onemogoči profila, ki je na seznamu aktivnih profilov, ne glede na to, kako dolgo je profil neaktiven.	QASECIDL[2]
4	ANZPRFACT	Z ukazom Analiziraj dejavnost profila onemogočite profile uporabnikov, ki niso bili uporabljeni določeno število dni. Ko z ukazom ANZPRFACT podate število dni, ga izvede sistem ponoči. Ukaz CHGACTPRFL lahko uporabite za izvzetje profilov uporabnikov iz onemogočanja.	QASECIDL[2]
5	DSPACTSCD	Ukaz Prikaži urnik aktiviranja profilov uporabite za prikaz in natis informacij o urniku omogočanja in onemogočanja določenih profilov uporabnikov. Urnik lahko izdelate z ukazom CHGACTSCDE.	QASECACT[2]
6	CHGACTSCDE	Ukaz Spremeni postavko urnika aktiviranja uporabite, da omogočite profil uporabnika na voljo za prijavo samo ob določenih urah dneva ali tedna. Za vsak profil uporabnika, ki ga načrtujete, izdela sistem postavke urnika opravil za čas omogočanja in onemogočanja.	QASECACT[2]

Tabela 6. Ukazi orodij za profile uporabnikov (nadaljevanje)

Možnost menija [1]	Ime ukaza	Opis	Uporabljena datoteka baze podatkov
7	DSPEXPSCD	Ukaz Prikaži urnik izteka uporabite za prikaz ali natis seznama profilov uporabnikov, ki jih želite v bodoče onemogočiti ali odstraniti iz sistema. Ukaz CHGEXPSCDE uporabite za nastavitev profilov uporabnikov za iztek.	QASECEXP[2]
8	CHGEXPSCDE	Ukaz Spremeni postavko urnika izteka omogoča, da načrtujete odstranitev profila uporabnika. Profil lahko odstranite začasno (tako da ga onemogočite) ali ga zbrišete iz sistema. Ta ukaz uporablja postavko urnika opravil, ki se izvaja vsak dan ob 00:01 (minuto čez polnoč). Opravilo pregleda datoteko QASECEXP in določi, ali je ta dan za potek določen kakšen profil uporabnika. S pomočjo ukaza DSPEXPSCD prikažite profile uporabnikov, ki so terminirani za iztek.	QASECEXP[2]
9	PRTPRFINT	Ukaz Natisni podatke profila uporabite za natis poročila, ki vsebuje informacije o število postavk, ki jih vsebuje profil uporabnika. Število postavk določa velikost profila uporabnika.	

Opombe:

1. Možnosti so z menija SECTOOLS.
2. Ta datoteka je v knjižnici QUSRSYS.

Za prikaz dodatnih možnosti se lahko pomaknete po meniju navzdol. Tabela 7 opisuje menijske možnosti in povezane ukaze za beleženje zaščite:

Tabela 7. Ukazi orodij za beleženje zaščite

Možnost menija [1]	Ime ukaza	Opis	Uporabljena datoteka baze podatkov
10	CHGSECAUD	Z ukazom Spremeni beleženje zaščite nastavite beleženje zaščite in spremenite sistemske vrednosti, ki krmilijo beleženje zaščite. Če zaženete ukaz CHGSECAUD in dnevnik beleženja zaščite (QAUDJRN) še ne obstaja, ga sistem izdela. Ukaz CHGSECAUD nudi možnosti, ki poenostavljajo nastavitev sistemske vrednosti QAUDLVL (raven beleženja). Če podate *ALL, lahko aktivirate vse možne nastavitve za raven beleženja. Podate lahko tudi *DFTSET in aktivirate najpogosteje uporabljane nastavitve (*AUTFAIL, *CREATE, *DELETE, *SECURITY in *SAVRST). **Opomba:** Če uporabite za nastavitev beleženja orodja za zaščito, morate izdelati tudi načrt za upravljanje sprejemnikov dnevnikov beleženja, sicer boste hitro naleteli na težave pri uporabi diska.	
11	DSPSECAUD	Ukaz Prikaži beleženje zaščite uporabite za prikaz informacij o dnevniku beleženja zaščite in sistemskih vrednosti, ki krmilijo beleženje zaščite.	

Tabela 7. Ukazi orodij za beleženje zaščite (nadaljevanje)

Možnost menija [1]	Ime ukaza	Opis	Uporabljena datoteka baze podatkov
Opombe: 1. Možnosti so z menija SECTOOLS.			

Uporaba menija Paket zaščite

Sledi prvi del menija SECBATCH:

```
SECBATCH         Predložitev
ali terminiranje poročil zaščite v paket
                                                                  Sistem:
Izberite eno od naslednjega:

  Predložitev poročil v paket
     1. Prevzem objektov
     2. Postavke dnevnika beleženja
     3. Pooblastila pooblastitvenega seznama
     4. Pooblastila ukazov
     5. Zasebna pooblastila ukazov
     6. Zaščita komunikacij
     7. Pooblastila imenikov
     8. Zasebna pooblastila imenikov
     9. Pooblastila dokumentov
    10. Zasebna pooblastila dokumentov
    11. Pooblastila datotek
    12. Zasebna pooblastila datotek
    13. Pooblastila map
```

Če izberete možnost s tega menija, se prikaže zaslon Predložitev opravila (SBMJOB). Če želite spremeniti privzete možnosti za ukaz, lahko v vrstici *Ukaz za zagon* pritisnete F4 (Poziv).

Če želite videti možnost Načrtovanje paketnih poročil, se pomaknite na meni SECBATCH. Možnosti s tega prvega dela menija omogočajo, da na primer nastavite sistem tako, da redno izvaja različice poročil o spremembah. Za prikaz dodatnih menijskih možnosti se lahko pomaknete navzdol. Če izberete možnost s tega prvega dela menija, se prikaže zaslon Dodajanje postavke urnika opravil (ADDJOBSCDE).

Če želite izbrati za poročilo druge nastavitve, lahko postavite utripalko v vrstico *Ukaz za zagon* in pritisnete F4 (Poziv). Uporabite pomenljivo ime opravila, da boste prepoznali postavko pri prikazu postavk urnika opravil.

Možnosti menija Paket zaščite

Tabela 8 na strani 29 opisuje menijske možnosti in povezane ukaze za poročila zaščite.

Če zaženete poročila zaščite, natisne sistem samo tiste informacije, ki ustrezajo izbiralnemu kriteriju, ki ste ga podali vi, in izbiralnemu kriteriju za orodje. Opisi opravil, ki na primer podajajo ime profila uporabnika, so povezani z zaščito. Zato poročilo opisa opravil (PRTJOBDAUT) natisne opise opravil v podani knjižnici, samo če javno pooblastilo za opis opravila ni *EXCLUDE *in* če opis opravila podaja ime profila uporabnika v parametru USER.

Podobno velja, če tiskate informacije o podsistemu (ukaz PRTSBSDAUT), ko sistem natisne informacije o podsistemu samo, če ima opis podsistema komunikacijsko postavko, ki podaja profil uporabnika.

Če določeno poročilo natisne manj informacij kot ste pričakovali, uporabite zaslonske informacije pomoči in poiščite izbiralni kriterij za poročilo.

Tabela 8. Ukazi za poročila zaščite

Možnost menija [1]	**Ime ukaza**	**Opis**	**Uporabljena datoteka baze podatkov**
1, 40	PRTADPOBJ	Ukaz Natisni objekte s prevzemom uporabite za natis seznama objektov, ki prevzamejo pooblastilo podanega profila uporabnika. Podate lahko en profil uporabnika, splošno ime profila (kot so na primer vsi profili, ki se začno s Q) ali vse profile uporabnikov v sistemu. To poročilo ima dve različici. Celotno poročilo navede vse objekte s prevzemom, ki ustrezajo izbiralnemu kriteriju. Poročilo o spremembah navede razlike med objekti s prevzemom, ki so trenutno v sistemu, in med objekti s prevzemom, ki so bili v sistemu pri zadnji izvedbi poročila.	QSECADPOLD[2]
2, 41	DSPAUDJRNE	Ukaz Prikaži postavke dnevnika beleženja uporabite za prikaz ali natis informacij o postavkah v dnevniku beleženja zaščite. Izberete lahko določene vrste postavk, določene uporabnike in časovno obdobje.	QASYxxJ4[3]
3, 42	PRTPVTAUT *AUTL	Če uporabite ukaz Natisni zasebna pooblastila za objekte *AUTL, se prikaže seznam vseh pooblastitvenih seznamov v sistemu. Poročilo vključuje uporabnike, ki imajo pooblastilo za posamezne sezname in kakšno vrsto pooblastila imajo za seznam. Te informacije vam bodo služile kot pomoč pri analiziranju izvorov za pooblastila objektov v sistemu. To poročilo ima tri različice. Celotno poročilo navede vse pooblastitvene sezname v sistemu. Poročilo o spremembah navede dodajanja in spremembe, izvedene v pooblastilih od zadnje izvedbe poročila. Poročilo o brisanju navede uporabnike, katerih pooblastilo za pooblastitveni seznam je bilo od zadnje izvedbe poročila zbrisano. Če natisnete celotno poročilo, imate na voljo možnost za natis seznama objektov, ki jih ščitijo posamezni pooblastitveni seznami. Sistem izdela ločeno poročilo za vsak pooblastitveni seznam.	QSECATLOLD[2]
6, 45	PRTCMNSEC	Ukaz Natisni zaščito komunikacij uporabite za natis nastavitev, povezanih z zaščito, za objekte, ki vplivajo na komunikacije v sistemu. Te nastavitve vplivajo na način vstopa uporabnikov in opravil v sistem. Ta ukaz ustvari dve poročili: poročilo, ki prikaže nastavitve za konfiguracijske sezname v sistemu in poročilo, ki navede parametre, povezane z zaščito, za opise linij, krmilnike in opise naprav. Vsako od teh poročil ima celotno različico in različico s spremembami.	QSECCMNOLD[2]

Tabela 8. Ukazi za poročila zaščite (nadaljevanje)

Možnost menija [1]	Ime ukaza	Opis	Uporabljena datoteka baze podatkov
15, 54	PRTJOBDAUT	Ukaz Natisni pooblastilo opisa opravila uporabite za natis seznama z opisom opravil, ki podajajo profil uporabnika in imajo javno pooblastilo, ki ni *EXCLUDE. Poročilo prikaže posebna pooblastila za profil uporabnika, ki je podan v opisu opravila. To poročilo ima dve različici. Celotno poročilo navede vse objekte opisov opravil, ki ustrezajo izbiralnemu kriteriju. Poročilo o spremembah navede razlike med objekti opisov opravil, ki so trenutno v sistemu, in med objekti opisov opravil, ki so bili v sistemu pri zadnji izvedbi poročila.	QSECJBDOLD[2]
Glejte 4. opombo	PRTPUBAUT	Ukaz Natisni objekte z javnimi pooblastili uporabite za natis seznama objektov, katerih javno pooblastilo ni *EXCLUDE. Ko zaženete ukaz, podate tip objekta in knjižnico ali knjižnice za poročilo. Ukaz PRTPUBAUT uporabite za natis informacij o objektih, do katerih lahko dostopijo vsi uporabniki v sistemu. To poročilo ima dve različici. Celotno poročilo navede vse objekte, ki ustrezajo izbiralnemu kriteriju. Poročilo o spremembah navede razlike med podanimi objekti, ki so trenutno v sistemu in med objekti (istega tipa in v isti knjižnici), ki so bili v sistemu pri zadnji izvedbi poročila.	QPBxxxxxx[5]
Glejte opombo 5.	PRTPVTAUT	Ukaz Natisni zasebna pooblastila uporabite za natis seznama zasebnih pooblastil za objekte podanega tipa v podani knjižnici. To poročilo vam bo v pomoč pri določanju virov pooblastil za objekte. To poročilo ima tri različice. Celotno poročilo navede vse objekte, ki ustrezajo izbiralnemu kriteriju. Poročilo o spremembah navede razlike med podanimi objekti, ki so trenutno v sistemu in med objekti (istega tipa in v isti knjižnici), ki so bili v sistemu pri zadnji izvedbi poročila. Poročilo o brisanju navede uporabnike, katerih pooblastilo za objekte je bilo od zadnjega natisa poročila zbrisano.	QPVxxxxxx[5]
24, 63	PRTQAUT	Ukaz natisni poročilo čakalne vrste uporabite za natis nastavitev zaščite za izhodne čakalne vrste in čakalne vrste opravil v sistemu. Te nastavitve krmilijo, kdo si lahko ogleda in spremeni postavke v izhodni čakalni vrsti in v čakalni vrsti opravil. To poročilo ima dve različici. Celotno poročilo navede vse objekte izhodne čakalne vrste in čakalne vrste opravil, ki ustrezajo izbiralnemu kriteriju. Poročilo o spremembah navede razlike med objekti izhodne čakalne vrste in čakalne vrste opravil, ki so trenutno v sistemu, in med objekti izhodne čakalne vrste in čakalne vrste opravil, ki so bili v sistemu pri zadnji izvedbi poročila.	QSECQOLD[2]

Tabela 8. Ukazi za poročila zaščite (nadaljevanje)

Možnost menija [1]	Ime ukaza	Opis	Uporabljena datoteka baze podatkov
25, 64	PRTSBSDAUT	Ukaz Natisni opis podsistema uporabite za natis komunikacijskih postavk, povezanih z zaščito, za opis podsistemov v sistemu. Te nastavitve krmilijo, kako lahko delo vstopi v sistem in kako se izvajajo opravila. Poročilo natisne opis podsistema samo, če ima komunikacijske postavke, ki podajajo ime profila uporabnika. To poročilo ima dve različici. Celotno poročilo navede vse objekte opisov podsistema, ki ustrezajo izbiralnemu kriteriju. Poročilo o spremembah navede razlike med objekti opisov podsistema, ki so trenutno v sistemu, in med objekti opisov podsistema, ki so bili v sistemu pri zadnji izvedbi poročila.	QSECSBDOLD[2]
26, 65	PRTSYSSECA	Ukaz Natisni atribute zaščite sistema uporabite za natis seznama sistemskih vrednosti in omrežnih atributov, povezanih z zaščito. Poročilo prikaže trenutno vrednost in priporočeno vrednost.	
27, 66	PRTTRGPGM	Ukaz Natisni programe prožil uporabite za natis seznama programov prožil, ki so povezani z datotekami baze podatkov v sistemu. To poročilo ima dve različici. Celotno poročilo navede vse dodeljene programe prožil, ki ustrezajo izbiralnemu kriteriju. Poročilo o spremembah navede programe prožil, ki so bili dodeljeni od zadnje izvedbe poročila.	QSECTRGOLD[2]
28, 67	PRTUSROBJ	Ukaz Natisni uporabniške objekte uporabite za natis seznama uporabniških objektov (objektov, ki niso IBM-ov) v knjižnici. To poročilo lahko uporabite za natis seznama uporabniških objektov v knjižnici (kot je QSYS), ki so v sistemskem delu seznama knjižnic. To poročilo ima dve različici. Celotno poročilo navede vse uporabniške objekte, ki ustrezajo izbiralnemu kriteriju. Poročilo o spremembah navede razlike med uporabniškimi objekti, ki so trenutno v sistemu, in med uporabniškimi objekti, ki so bili v sistemu pri zadnji izvedbi poročila.	QSECPUOLD[2]
29, 68	PRTUSRPRF	Ukaz Natisni profil uporabnika uporabite za analizo profilov uporabnikov, ki ustrezajo podanemu kriteriju. Profile uporabnikov lahko izberete na osnovi posebnih pooblastil, uporabniškega razreda ali na osnovi neujemanja med posebnimi pooblastili in uporabniškim razredom. Natisnete lahko informacije o pooblastilih, informacije o okolju, informacije o geslih ali informacije o ravni gesel.	
30, 69	PRTPRFINT	Ukaz Natisni podatke profila uporabite za natis poročila z notranjimi informacijami o številu postavk.	

Tabela 8. Ukazi za poročila zaščite (nadaljevanje)

Možnost menija [1]	Ime ukaza	Opis	Uporabljena datoteka baze podatkov
31, 70	CHKOBJITG	Ukaz Preveri integriteto objekta uporabite za določitev, ali so bili operacijski objekti (kot so programi) spremenjeni brez uporabe prevajalnika. Ta ukaz vam bo pomagal odkriti poskuse pošiljanj virusnega programa v sistemu ali spremembe programa, ki bi izvedel nepooblaščena navodila. V knjigi *iSeries Security Reference* boste našli podrobnejše informacije o ukazu CHKOBJITG.	

Opombe:

1. Možnosti so z menija SECBATCH.
2. Ta datoteka je v knjižnici QUSRSYS.
3. xx je dvomestni tip postavke dnevnika. Vzorčna izhodna datoteka za postavke dnevnika AE je na primer QSYS/QASYAEJ4. Vzorčne izhodne datoteke so opisane v dodatku F knjige *iSeries Security Reference* .
4. Meni SECBATCH vsebuje možnosti za tipe objektov, ki običajno skrbijo skrbnike za zaščito. Možnost 11 ali 50 na primer izvedeta ukaz PRTPUBAUT za objekte *FILE. Splošne možnosti (18 in 57) uporabite za tip objekta.
5. Meni SECBATCH vsebuje možnosti za tipe objektov, ki običajno skrbijo skrbnike za zaščito. Možnosti 12 in 51 na primer zaženeta ukaz PRTPVTAUT za objekte *FILE. Splošne možnosti (19 in 58) uporabite za podajanje tipa objekta.
6. xxxxxx v imenu datoteke je tip objekta. Datoteka za programske objekte se na primer imenuje QPBPGM za javna pooblastila in QPVPGM za zasebna pooblastila. Datoteke so v knjižnici QUSRSYS.

   Datoteka vsebuje člana za vsako knjižnico, za katero ste natisnili poročilo. Ime člana je isto kot ime knjižnice.

Ukazi za prilagajanje zaščite

Tabela 9 opisuje ukaze, ki jih lahko uporabite za prilagoditev zaščite v sistemu. Ti ukazi so na meniju SECTOOLS.

Tabela 9. Ukazi za prilagajanje sistema

Možnost menija [1]	Ime ukaza	Opis	Uporabljena datoteka baze podatkov
60	CFGSYSSEC	Ukaz Konfiguriraj zaščito sistema uporabite za nastavitev sistemskih vrednosti, povezanih z zaščito, v njihove priporočene nastavitve. Ukaz nastavi tudi beleženje zaščite v sistemu. “Vrednosti, nastavljene z ukazom Konfiguriraj zaščito sistema” na strani 33 opisuje, kaj naredi ukaz. **Opomba:** Če želite prikazati priporočila za zaščito, prilagojena vaši situaciji, namesto tega ukaza zaženite čarovnika za zaščito iSeries ali svetovalca za zaščito iSeries. Informacije o teh orodjih lahko najdete v razdelku Poglavje 2, “Čarovnik za zaščito iSeries in Planer zaščite za eServer”, na strani 9.	
61	RVKPUBAUT	Ukaz Prekliči javno pooblastilo uporabite za nastavitev javnega pooblastila na *EXCLUDE za niz ukazov v sistemu, ki so zelo občutljivi glede zaščite. “Funkcije ukaza Prekliči javno pooblastilo” na strani 34 navaja dejanja, ki jih izvede ukaz RVKPUBAUT.	

Opombe:

1. Možnosti so z menija SECTOOLS.

Vrednosti, nastavljene z ukazom Konfiguriraj zaščito sistema

Tabela 10 navaja sistemske vrednosti, ki so nastavljene, če zaženete ukaz CFGSYSSEC. Ukaz CFGSYSSEC zažene program, ki se imenuje QSYS/QSECCFGS.

Tabela 10. Vrednosti, nastavljene z ukazom CFGSYSSEC

Ime sistemske vrednosti	Nastavitev	Opis sistemske vrednosti
QALWOBJRST	*NONE	Ali je mogoče obnoviti programe sistemskega stanja in programe, ki prevzamejo pooblastilo.
QAUTOCFG	0 (Ne)	Samodejno konfiguriranje novih naprav.
QAUTOVRT	0	Število opisov navideznih naprav, ki jih samodejno izdela sistem, če ni za uporabo na voljo nobena naprava.
QDEVRCYACN	*DSCMSG (Prekini povezavo s sporočilom)	Sistemsko dejanje pri vnovični vzpostavitvi komunikacij.
QDSCJOBITV	120	Časovno obdobje preden sistem opravi dejanje za opravilo s prekinjeno povezavo.
QDSPSGNINF	1 (Da)	Ali se uporabnikom prikaže zaslon s prijavnimi informacijami.
QINACTITV	60	Časovno obdobje preden sistem opravi dejanje za neaktivno interaktivno opravilo.
QINACTMSGQ	*ENDJOB	Dejanje, ki ga izvede sistem za neaktivno opravilo.
QLMTDEVSSN	1 (Da)	Ali so uporabniki omejeni na sočasno prijavo na eno napravo.
QLMTSECOFR	1 (Da)	Ali so uporabniki *ALLOBJ in *SERVICE omejeni na določene naprave.
QMAXSIGN	3	Koliko zaporednih, neuspešnih poskusov prijave je dovoljenih.
QMAXSGNACN	3 (oba)	Ali sistem onemogoči delovno postajo ali profil uporabnika, ko je dosežena omejitev QMAXSIGN.
QRMTSIGN	*FRCSIGNON	Kako sistem obravnava poskus oddaljene prijave (prehod ali TELNET).
QRMTSVRATR	0 (izključeno)	Omogoča oddaljeno analiziranje sistema.
QSECURITY [1 na strani 34]	50	Uveljavljena raven zaščite.
QVFYOBJRST	3 (preveri podpise pri obnovitvi)	Preveri objekte pri obnovitvi.
QPWDEXPITV	60	Kako pogosto morajo uporabniki spremeniti svoja gesla.
QPWDMINLEN	6	Najmanjša dovoljena dolžina gesel.
QPWDMAXLEN	8	Največja dovoljena dolžina gesel.
QPWDPOSDIF	1 (Da)	Ali se mora vsako mesto v novem geslu razlikovati od istega mesta v zadnjem geslu.
QPWDLMTCHR	Glejte opombo 2 na strani 34	Znaki, ki niso dovoljeni v geslih.
QPWDLMTAJC	1 (Da)	Ali so sosednji znaki v geslih prepovedani.
QPWDLMTREP	2 (zaporedna ponovitev ni mogoča)	Ali so ponavljajoči se znaki prepovedani v geslih.
QPWDRQDDGT	1 (Da)	Ali morajo gesla vsebovati vsaj eno številko.
QPWDRQDDIF	1 (32 unikatnih gesel)	Koliko unikatnih gesel je zahtevanih, preden je mogoče ponoviti geslo.
QPWDVLDPGM	*NONE	Uporabniški izhodni program, ki ga pokliče sistem za preverjanje veljavnosti gesel.

Tabela 10. Vrednosti, nastavljene z ukazom CFGSYSSEC (nadaljevanje)

Ime sistemske vrednosti	Nastavitev	Opis sistemske vrednosti
Opombe: 1. Če trenutno uporabljate vrednost QSECURITY 40 ali manj, pred spremembo v višjo raven zaščite zagotovo preberite 2. poglavje knjige *iSeries Security Reference*. 2. Omejeni znaki so shranjeni v ID-ju sporočila CPXB302 datoteke sporočil QSYS/QCPFMSG. Naloženi so kot AEIOU@$#. Omejene znake lahko spremenite s pomočjo ukaza CHGMSGD (Spremeni opis sporočila). Sistemska vrednost QPWDLMTCHR ni uveljavljena za raven gesel 2 ali 3.		

Ukaz CFGSYSSEC tudi nastavi geslo na *NONE za naslednje IBM-ove profile uporabnikov:

QSYSOPR

QPGMR

QUSER

QSRV

QSRVBAS

Na koncu nastavi ukaz CFGSYSSEC beleženje zaščite s pomočjo ukaza CHGSECAUD (Spremeni beleženje zaščite). Ukaz CFGSYSSEC vklopi beleženje dejanj in objektov in poda tudi privzeti niz dejanj za beleženje v ukazu CHGSECAUD.

Prilagajanje programa

Če katera od teh nastavitev ni primerna za vašo namestitev, lahko izdelate lastno različico programa, ki obdela ukaz. Naredite naslednje:

__ Korak 1. S pomočjo ukaza RTVCLSRC (Pridobi izvor CL) prekopirajte izvor za program, ki se zažene, ko uporabite ukaz CFGSYSSEC. Program, ki ga boste pridobili, je QSYS/QSECCFGS. Ko ga poiščete, mu dajte *drugo ime*.

__ Korak 2. V programu opravite želene spremembe, nato pa ga prevedite. Pri prevajanju pazite, da *ne* boste zamenjali IBM-ovega programa QSYS/QSECCFGS. Vaš program naj ima drugo ime.

__ Korak 3. S pomočjo ukaza CHGCMD (Spremeni ukaz) spremenite program, tako da bo obdelal parameter (PGM) ukaza za ukaz CFGSYSSEC. Vrednost PGM nastavite na ime vašega programa. Če na primer v knjižnici QGPL izdelate program, ki se imenuje MYSECCFG, vpišite naslednje:

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

Opomba: Če spremenite program QSYS/QSECCFGS, IBM ne zagotavlja njegove zanesljivosti, uporabnosti, zmogljivosti ali delovanja. Posredna jamstva za tržnost in primernost za določen namen so izrecno zavrnjena.

Funkcije ukaza Prekliči javno pooblastilo

Ukaz RVKPUBAUT (Prekliči javno pooblastilo) lahko uporabite za nastavitev javnega pooblastila za niz ukazov in programov na *EXCLUDE. Ukaz RVKPUBAUT zažene program, ki se imenuje QSYS/QSECRVKP. Ko naložite QSECRVKP, prekliče javno pooblastilo (z nastavitvijo javnega pooblastila na *EXCLUDE) za ukaze, navedene v Tabela 11 na strani 35, in aplikacijske programerske vmesnike (API-je), navedene v Tabela 12 na strani 35. Ko dobite sistem, je javno pooblastilo za te ukaze in API-je nastavljeno na *USE.

Ukazi, navedeni v Tabela 11, in API-ji, navedeni v Tabela 12, v sistemu izvajajo funkcije, ki nudijo možnost nekomu, da povzroči škodo. Kot skrbnik za zaščito morate izrecno pooblastiti uporabnike za izvajanje teh ukazov in programov, ne pa jih omogočiti za vse sistemske uporabnike.

Ko zaženete ukaz RVKPUBAUT, podate knjižnico, ki vsebuje ukaze. Privzetek je knjižnica QSYS. Če imate v sistemu več kot en državni jezik, morate zagnati ukaz za vse knjižnice QSYSxxx.

Tabela 11. Ukazi, katerih javno pooblastilo je nastavljeno z ukazom 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, navedeniv razdelkuTabela 12, so vsi v knjižnici QSYS:

Tabela 12. Programi, katerih javno pooblastilo je nastavljeno z ukazom RVKPUBAUT

QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

Ko zaženete ukaz RVKPUBAUT, nastavi sistem javno pooblastilo za korenski imenik na *USE (razen če že ni *USE ali manj).

Prilagajanje programa

Če katera od teh nastavitev ni primerna za vašo namestitev, lahko izdelate lastno različico programa, ki obdela ukaz. Naredite naslednje:

__ Korak 1. S pomočjo ukaza RTVCLSRC (Pridobi izvor CL) prekopirajte izvor za program, ki se zažene, ko uporabite ukaz RVKPUBAUT. Program, ki ga boste pridobili, je QSYS/QSECRVKP. Ko ga poiščete, mu dajte *drugo ime*.

__ Korak 2. V programu opravite želene spremembe, nato pa ga prevedite. Pri prevajanju pazite, da *ne* boste zamenjali IBM-ovega programa QSYS/QSECRVKP. Vaš program naj ima drugo ime.

__ Korak 3. S pomočjo ukaza CHGCMD (Spremeni ukaz) spremenite program, tako da bo obdelal parameter (PGM) ukaza za ukaz RVKPUBAUT. Vrednost PGM nastavite na ime vašega programa. Če na primer v knjižnici QGPL izdelate program, ki se imenuje MYRVKPGM, vpišite naslednje:

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

Opomba: če spremenite program QSYS/QSECRVKP, IBM ne zagotavlja njegove zanesljivosti, uporabnosti, zmogljivosti ali delovanja. Posredna jamstva za tržnost in primernost za določen namen so izrecno zavrnjena.

Del 2. Zahtevnejša zaščita iSeries

Poglavje 5. Zaščita informacijskih sredstev z objektnim pooblastilom

Kot skrbniku za zaščito vam je gotovo izziv zaščititi informacijska sredstva podjetja, ne da bi s tem prizadeli uporabnike sistema. Zagotoviti morate, da imajo uporabniki dovolj pooblastil za izvajanje svojega dela, in paziti, da jim ne dodelite pooblastil za pregledovanje sistema in izvajanje nepooblaščenih sprememb.

Nasvet za zaščito

Pooblastilo, ki je preveč omejujoče, ima lahko nasprotnem učinek. Uporabniki včasih namreč reagirajo na preveč omejujoča pooblastila tako, da med seboj delijo gesla.

Operacijski sistem OS/400 nudi integrirano zaščito objektov. Uporabniki morajo za dostop do objektov uporabiti vmesnike, ki jih nudi sistem. Če želite na primer dostopiti do datoteke baze podatkov, morate uporabiti ukaze ali programe, ki so namenjeni za dostopanje do datotek baze podatkov. Ukaza, ki je namenjen za dostop do čakalne vrste sporočil ali dnevnika opravil, ne morete uporabiti.

Vsakič, ko s pomočjo sistemskega vmesnika dostopite do objekta, sistem preveri, ali imate pooblastilo za objekt, ki ga zahteva ta vmesnik. Objektno pooblastilo je močno in prožno orodje za zaščito sredstev v sistemu. Vaš izziv kot skrbnika za zaščito je, da nastavite učinkovito shemo za zaščito objektov, ki jih lahko upravljate in vzdržujete.

Uveljavitev objektnega pooblastila

Vsakič, ko poskusite dostopiti do objekta, operacijski sistem preveri vaše pooblastilo za ta objekt. Toda če je raven zaščite v vašem sistemu (sistemska vrednost QSECURITY) nastavljena na 10 ali 20, imajo vsi uporabniki samodejno pooblastilo za dostop do vseh objektov, ker imajo vsi profili uporabnikov posebno pooblastilo *ALLOBJ.

Nasvet za objektna pooblastila: Če niste prepričani, ali uporabljate zaščito objektov, preverite sistemsko vrednost QSECURITY (raven zaščite). Če je QSECURITY nastavljen na 10 ali 20, ne uporabljate zaščite objektov.

Preden spremenite zaščito v raven 30 ali več, morate izdelati načrt in se pripraviti, sicer uporabniki ne bodo mogli dostopiti do informacij, ki jih potrebujejo.

V temi Informacijskega centra z naslovom **Osnovna zaščita in načrtovanje sistema** boste našli način za analiziranje aplikacij in odločitev, kako nastaviti zaščito objektov. Če še ne uporabljate zaščite objektov ali če je shema za zaščito objektov zastarela in zapletena, preberite to temo, ki vam bo pomagala pri prvih korakih.

Zaščita menijev

Strežnik iSeries je bil v začetku oblikovna kot nasledek izdelkov S/36 in S/38. Številne namestitve strežnika iSeries so bile na določeni točki namestitve S/36 ali namestitve S/38. Da bi lahko skrbniki za zaščito v teh zgodnjih sistemih nadzorovali, kaj lahko delajo uporabniki, so pogosto uporabljali način, ki se imenuje **zaščita menijev** ali **nadzorovanje dostopa do menijev**.

Nadzorovanje dostopa do menijev pomeni, da se uporabniki po prijavi prikaže meni. Uporabnik lahko izvaja samo tiste funkcije, ki so na meniju. Uporabnik ne more uporabiti ukazne vrstice v sistemu, kjer bi izvedel funkcije, ki jih ni na meniju. Teoretično gledano skrbnikom za zaščito ni treba skrbeti glede pooblastil za objekte, ker meniji in programi nadzorujejo, kaj lahko delajo uporabniki.

Strežnik iSeries nudi številne možnosti profilov uporabnikov, ki vam bodo pomagale pri nadzorovanju dostopa do menijev:
- Parameter **začetnega menija** (INLMNU) krmili, kateri meni se prikaže uporabniku po prijavi.
- Parameter **začetnega programa** (INLPGM) zažene namestitveni program, preden se uporabniku prikaže meni. S pomočjo parametra INLPGM lahko tudi omejite uporabnika na izvajanje enega samega programa.
- Parameter **Omeji zmožnosti** (LMTCPB) omeji uporabnika na omejen niz ukazov. Uporabniku tudi preprečuje, da bi na prijavnem zaslonu podal drug začetni program ali meni. (Parameter LMTCPB omeji samo ukaze, ki jih vnesete prek ukazne vrstice.)

Omejitve krmiljenja menijskega dostopa

Računalniki in uporabniki računalnikov so se v zadnjih nekaj letih močno spremenili. Na voljo so številna orodja kot so programi poizvedb in preglednic, ki uporabnikom omogočajo tudi lastno programiranje, da nekoliko razbremenijo oddelke z informacijskimi sistemi. Nekatera orodja kot sta SQL ali ODBC, nudijo zmožnost za prikaz in spreminjanje informacij. Omogočiti ta orodja znotraj menijske strukture je zelo težko.

Delovne postaje s stalno funkcijo (“zelen zaslon”) hitro nadomeščajo osebni računalniki in omrežja računalnikov. Če vaš sistem sodeluje v omrežju, lahko uporabniki vstopijo v sistem, ne da bi sploh kdajkoli videli prijavni zaslon ali meni.

Kot skrbnik za zaščito, ki poskuša uveljaviti krmiljenje menijskega dostopa, imate dve osnovni težavi:
- Če uspete omejiti uporabnike na menije, uporabniki najbrž ne bodo zadovoljni, ker bo njihova uporaba modernih orodij omejena.
- Če ne uspete, lahko spravite v nevarnost pomembne, zaupne informacije, ki naj bi jih ščitilo krmiljenje menijskega dostopa. Če vaš sistem sodeluje v omrežju, se zmožnost za uveljavitev krmiljenja menijskega dostopa zmanjša. Parameter LMTCPB na primer velja samo za ukaze, ki jih vnesete iz ukazne vrstice v interaktivnih seji. Parameter LMTCPB ne vpliva na zahteve iz komunikacijskih sej kot so prenosi datotek PC, FTP ali oddaljeni ukazi.

Izboljšanje krmiljenja menijskega dostopa z zaščito objektov

S številnimi novimi možnostmi, ki so na voljo za povezavo s sistemi, se shema za zaščito strežnika iSeries ne more zanašati zgolj na krmiljenje menijskega dostopa. Ta tema nudi predloge za prehod v okolje zaščite objektov, ki bo dopolnilo krmiljenje menijskega dostopa.

Tema Informacijskega centra z naslovom *Osnovna zaščita in načrtovanje sistema* opisuje način za analiziranje pooblastila, ki ga morajo imeti uporabniki za objekte za izvajanje trenutnih aplikacij. Uporabnike nato dodelite skupinam, skupinam pa ustrezno pooblastilo. Ta pristop je pripraven in logičen. Toda če vaš sistem deluje že več let in vsebuje številne aplikacije, se vam zdi najbrž naloga analiziranja aplikacij in nastavitve objektnih pooblastil ogromna.

Nasvet za objektno pooblastilo: Če združite trenutne menije s programi, ki prevzamejo pooblastilo lastnikov programov, omogočite prehod, ki presega krmiljenje menijskega dostopa. Ne pozabite, da morate zaščititi programe, ki prevzamejo pooblastilo in profile uporabnikov, ki so njihovi lastniki.

Kot pomoč pri nastavitvi prehodnega okolja, medtem ko postopoma analizirate aplikacije in objekte, boste morda lahko uporabili trenutne menije. Sledi zgled, ki uporablja meni OEMENU (Postavka razvrstitve) ter povezane datoteke in programe.

Zgled: nastavitev prehodnega okolja

Ta zgled se začne z naslednjimi predpostavkami in zahtevami:

- Vse datoteke so v knjižnici ORDERLIB.
- Imen vseh datotek ne poznate. Prav tako ne veste, katero pooblastilo zahtevajo menijske možnosti za različne datoteke.
- Meni in vsi programi, ki jih pokliče, so v knjižnici ORDERPGM.
- Želite, da si lahko vsi, ki se prijavijo v sistem, ogledajo informacije v vseh datotekah naročil, v datotek strank in v datotekah postavk (na primer s poizvedbami ali preglednicami).
- Datoteke lahko spreminjajo samo uporabniki, katerih trenutni prijavni meni je OEMENU. V ta namen morajo uporabiti programe na meniju.
- Sistemski uporabniki razen skrbnikov za zaščito nimajo posebnega pooblastila *ALLOBJ ali *SECADM.

Naslednji koraki kažejo, kako spremenite to okolje krmiljenja menijskega dostopa in ga prilagodite za poizvedbe:

__ Korak 1. Izdelajte seznam uporabnikov, katerih začetni meni je OEMENU.

Za izpis okolja za vse profile uporabnikov v sistemu lahko uporabite ukaz PRTUSRPRF *ENVINFO (Natisni profil uporabnika). Poročilo vključuje začetni meni, začetni program in trenutno knjižnico. Slika 7 na strani 55 kaže zgled poročila.

__ Korak 2. Zagotovite, da je lastnik objekta OEMENU (ki je lahko objekt *PGM ali *MENU) profil uporabnika, ki ni uporabljen za prijavo. Profil uporabnika mora biti onemogočen ali imeti geslo *NONE. Za ta zgled denimo, da je OEOWNER lastnik objekta programa OEMENU.

__ Korak 3. Zagotovite, da ni profil uporabnika, ki je lastnik objekta programa OEMENU, profil skupine. Uporabite lahko naslednji ukaz:

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

__ Korak 4. Spremenite program OEMENU, tako da bo prevzel pooblastilo profila uporabnika OEOWNER. (S pomočjo ukaza CHGPGM spremenite parameter USRPRF v *OWNER.)

Opomba: Objekti *MENU ne morejo prevzeti pooblastil. Če je OEMENU objekt *MENU, lahko ta zgled prilagodite tako, da naredite eno od naslednjega:

- Izdelajte program, ki prikaže meni.
- Uporabite prevzeto pooblastilo za programe, ki se zaženejo, ko izbere uporabnik možnosti z menija OEMENU.

__ Korak 5. Nastavite javno pooblastilo za vse datoteke v ORDERLIB na *USE, tako da vnesete naslednja dva ukaza:

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

Če izberete pooblastilo *USE, lahko uporabniki prekopirajo datoteko tako, da uporabijo prenos datotek PC ali FTP.

__ Korak 6. Profilu, ki je lastnik programa menija dodelite pooblastilo *ALL za datoteke tako, da vpišete naslednje:

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

Za večino aplikacij je pooblastilo *CHANGE za datoteke zadostno. Toda vaše aplikacije lahko izvajajo tudi funkcije kot je čiščenje članov fizične datoteke, ki zahtevajo višje pooblastilo kot *CHANGE. Analizirati morate aplikacije in podati samo minimalno pooblastilo, ki je potrebno za aplikacijo. Toda v prehodnem obdobju se s prevzemom pooblastila *ALL izognete napakam v aplikacijah, ki jih lahko povzroči nezadostno pooblastilo.

__ Korak 7. Omejite pooblastilo za programe v knjižnici naročil tako, da vpišete naslednje:

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

__ Korak 8. Profilu OEOWNER dodelite pooblastilo za programe v knjižnici tako, da vpišete naslednje:

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

__ Korak 9. Uporabnikom, ki ste jih določili v koraku 1, dodelite pooblastilo za program menija; to naredite tako, da za vsakega uporabnika vpišete naslednje:

```
GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM)
     USER(ime-profila-uporabnika) AUT(*USE)
```

Ko opravite te korake, bodo lahko vsi uporabniki sistema, ki niso izrecno izključeni, dostopili (ne pa tudi spremenili) do datotek v knjižnici ORDERLIB. Uporabniki, ki imajo pooblastilo za program OEMENU, bodo lahko uporabljali programe na meniju za ažuriranje datotek v knjižnici ORDERLIB. Zdaj bodo datoteke v tej knjižnici lahko spremenili samo uporabniki, ki imajo pooblastilo za program OEMENU. Datoteke ščiti kombinacija zaščite objektov in krmiljenje menijskega dostopa.

Ko opravite podobne korake za vse knjižnice, ki vsebujejo uporabniške podatke, izdelate preprosto shemo za krmiljenje sprememb v bazi podatkov. Ta način omogoča, da uporabniki ažurirajo datoteke baze podatkov samo z uporabo odobrenih menijev in programov. Uporabniki si lahko zdaj tudi ogledajo datoteke, jih analizirajo in kopirajo s pomočjo orodij, ki podpirajo odločanje ali s povezavami iz drugega sistema ali s PC-ja.

Nasvet za objektno pooblastilo: Če vaš sistem sodeluje v omrežju, bo pooblastilo *USE morda nudilo večje pooblastilo kot pričakujete. Če imate na primer pooblastilo *USE za datoteko, lahko s pomočjo FTP izdelate kopijo datoteke v drugem sistemu (vključno s PC-jem).

Uporaba zaščite knjižnice kot dopolnilo zaščiti menijev

Za dostop do objektov v knjižnici morate imeti pooblastilo za objekt in za knjižnico. Večina operacij zahteva pooblastilo *EXECUTE ali *USE za knjižnico.

Od vaše situacije je odvisno, ali boste lahko uporabili pooblastilo za knjižnico kot preprosto sredstvo za zaščito objektov. Za zgled vzemimo meni Postavka razvrščanja in denimo, da lahko vsakdo, ki ima pooblastilo do tega menija, uporabi vse programe v knjižnici ORDERPGM. Namesto da bi zaščitili posamezne programe, lahko nastavite javno pooblastilo za knjižnico ORDERPGM na *EXCLUDE. Določenim uporabnikom lahko nato dodelite

pooblastilo *USE za knjižnico, s čimer jim omogočite uporabo programov v knjižnici. (To predpostavlja, da je javno pooblastilo za programe *USE ali več.)

Pooblastilo za knjižnico je lahko preprost in učinkovit način za upravljanje objektnih pooblastil. Vendar pa morate poznati vsebino knjižnice, ki jo ščitite, da ne boste omogočili neželenega dostopa do objektov.

Konfiguriranje lastništva objektov

Lastništvo objektov v sistemu predstavlja pomemben del sheme objektnih pooblastil. Po privzetku ima lastnik objekta pooblastilo *ALL za objekt. V 5. poglavju knjige *iSeries Security Reference* boste našli priporočila in zglede za načrtovanje lastništva objektov. Sledi nekaj nasvetov:

- Na splošno naj profili skupin ne bodo lastniki objektov. Če je profil skupine lastnik objekta, imajo vsi člani skupine pooblastilo *ALL za objekt, razen če je član skupine izrecno izključen.
- Če uporabite prevzeto pooblastilo, razmislite, ali naj bodo profili uporabnikov, ki so lastniki programov, tudi lastniki objektov aplikacij kot so datoteke. Morda ne boste želeli, da imajo uporabniki, ki zaženejo programe, ki prevzamejo pooblastilo, pooblastilo *ALL za datoteke.

Če uporabljate Navigator iSeries, lahko to dosežete tako, da dokončate spremembe s pomočjo funkcije **načel** zaščite. Podrobnejše informacije lahko najdete v Informacijskem centru (podrobnosti boste našliv razdelku“Predpogoji in s tem povezane informacije” na strani xii).

Objektno pooblastilo za sistemske ukaze in programe

Sledi več predlogov pri omejitvi pooblastila na IBM-ove objekte:

- Če uporabljate v sistemu več kot en državni jezik, imate v sistemu več kot eno sistemsko knjižnico (QSYS). V sistemu obstaja knjižnica QSYSxxxx za vsak državni jezik v sistemu. Če s pomočjo objektnega pooblastila krmilite dostop do sistemskih ukazov, ne pozabite zaščititi ukaza v knjižnici QSYS in v vseh knjižnicah QSYSxxx v sistemu.
- Knjižnica System/38 včasih nudi ukaz s funkcijo, ki je enakovredna ukazom, ki jih želite omejiti. Omejiti morate enakovreden ukaz v knjižnici QSYS38.
- Če uporabljate okolje System/36, bo morda potrebno omejiti dodatne programe. Program QY2FTML na primer nudi prenos datotek System/36.

Beleženje funkcij zaščite

V tem poglavju bomo opisali načine za beleženje učinkovitosti zaščite v sistemu. Beleženje za zaščito sistema se izvaja zaradi več razlogov:

- Za preverjanje, ali je načrt zaščite popoln.
- Za zagotovitev, da so načrtovani krmilni elementi zaščite na mestu in delujejo. To vrsto beleženja običajno izvaja varnostnik za zaščito kot del dnevnega upravljanja zaščite. Včasih se natančneje izvaja tudi kot del občasnega pregleda zaščite, ki ga opravijo notranji ali zunanji kontrolorji.
- Za zagotovitev, da je zaščita sistema v skladu s spremembami v okolju sistema. Sledi nekaj zgledov sprememb, ki vplivajo na zaščito:
  - novi objekti, ki jih izdelajo uporabniki sistema
  - novi uporabniki z dostopom do sistema
  - sprememba lastništva objekta (pooblastilo ni prilagojeno)
  - sprememba odgovornosti (spremenjena skupina uporabnikov)

  - začasno pooblastilo (ki ni časovno preklicano)
  - na novo nameščeni izdelki
- Za pripravo na dogodek kot je namestitev nove aplikacij, preklop v višjo raven zaščite ali nastavitev komunikacijskega omrežja.

Tehnike, opisane v tem poglavju, so primerne za vse med temi situacijami. Za katere stvari boste izvajali beleženje in kako pogosto, je odvisno od velikosti in zaščitnih zahtev vašega podjetja. Namen tega poglavja je razložiti, katere informacije so na voljo, kako jih pridobiti in zakaj so potrebne, ne pa nuditi smernic za pogostost izvajanja beleženja.

Te informacije so sestavljene iz treh delov:

- Potrditveni seznam postavk zaščite, ki jih lahko načrtujete in beležite.
- Informacije o nastavitvi in uporabi dnevnika beleženja, ki ga nudi sistem.
- Druge tehnike, ki so na voljo za zbiranje informacij o zaščiti v sistemu.

Beleženje zaščite vključuje uporabo ukazov v sistemu iSeries in dostop do dnevnika in informacij beleženja v sistemu. Izdelate lahko poseben profil, ki ga bo uporabljala oseba, ki bo izvajala beleženje zaščite v sistemu. Profil kontrolorja bo potreboval posebno pooblastilo *AUDIT, da bo lahko spremenil značilnosti beleženja v sistemu. Nekatere izmed nalog beleženja, predlagane v tem poglavju, zahtevajo profil uporabnika v posebnima pooblastiloma *ALLOBJ in *SECADM. Ko se beleženja konča, ne pozabite nastaviti gesla za profil kontrolorja na *NONE.

Podrobnejše informacije o beleženju zaščite lahko najdete v 9. poglavju knjige *Security Reference*.

Analiziranje profilov uporabnikov

S pomočjo ukaza DSPAUTUSR (Prikaži pooblaščene uporabnike) lahko prikažete ali natisnete celoten seznam vseh uporabnikov v sistemu. Seznam lahko uredite po imenih profilov ali po imenih profilov skupin. Sledi zgled zaporedja pa profilu skupine:

```
                          Prikaz pooblaščenih uporabnikov

                        Nazadnje
Profil      Profil    spremenjeno    Brez
skupine    uporabnika  geslo         gesla  Besedilo
DPTSM
            ANDERSOR    08/04/0x            Roger Anders
            VINCENTM    09/15/0x            Mark Vincent
DPTWH
            ANDERSOR    08/04/0x            Roger Anders
            WAGNERR     09/06/0x            Rose Wagner
QSECOFR
            JONESS      09/20/0x            Sharon Jones
            HARRISOK    08/29/0x            Ken Harrison
*NO GROUP
            DPTSM       09/05/0x    X       Sales and Marketing
            DPTWH       08/13/0x    X       Warehouse
            RICHARDS    09/05/0x            Janet Richards
            SMITHJ      09/18/0x            John Smith
```

Natis izbranih profilov uporabnikov

S pomočjo ukaza DSPUSRPRF (Prikaži profil uporabnika) lahko izdelate izhodno datoteko, ki jo lahko obdelate z orodjem poizvedbe.

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

Z orodjem poizvedbe lahko izdelate različna analitična poročila izhodne datoteke kot sta naslednji:

- seznam vseh uporabnikov s posebnima pooblastiloma *ALLOBJ in *SPLCTL
- seznam vseh uporabnikov, ki so razvrščeni po polju profila uporabnika kot sta začetni program ali uporabniški razred

Za izdelavo različnih poročil iz izhodne datoteke lahko izdelate programe poizvedb. Na primer:

- Seznam vseh profilov uporabnikov, ki imajo katerokoli posebno pooblastilo; to naredite z izbiro zapisov, v katerih polje UPSPAU ni enako *NONE.
- Seznam vseh uporabnikov, ki lahko vnesejo ukaze; to naredite z izbiro zapisov, v katerih je polje *Omejitev zmožnosti* (v vzorčni izhodni datoteki baze podatkov se imenuje UPLTCP) enako *NO ali *PARTIAL.
- Seznam vseh uporabnikov, ki imajo določen začetni meni ali začetni program.
- Seznam neaktivnih uporabnikov; to naredite s pomočjo polja datuma zadnje prijave.

Pregled velikih profilov uporabnikov

Profili uporabnikov z velikim številom pooblastil, za katere se zdi, da so naključno razpršena v večjem delu sistema, lahko odražajo nepravilno načrtovanje zaščite. Sledi način iskanja velikih profilov uporabnikov in njihove ocenitve:

1. S pomočjo ukaza DSPOBJD (Prikaži opis objekta) lahko izdelate izhodno datoteko, ki vsebuje informacije o vseh profilih uporabnikov v sistemu:

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

2. Izdelava programa poizvedbe, ki bo navedel ime in velikost vsakega profila uporabnika v padajočem zaporedju po velikosti.
3. Natis podrobnih informacij o največjih profilih uporabnikov in ocenitev pooblastil in objektov v lasti, da vidite, ali so ustrezna:

   ```
   DSPUSRPRF USRPRF(ime-profila-uporabnika) +
             TYPE(*OBJAUT) OUTPUT(*PRINT)
   DSPUSRPRF USRPRF(ime-profila-uporabnika) +
             TYPE(*OBJOWN) OUTPUT(*PRINT)
   ```

   Nekateri IBM-ovi profili uporabnikov so zelo veliki zaradi števila objektov, katerih lastniki so. Izpis in njihovo analiziranje običajno ni potrebno. Vendar pa preverite programe, ki prevzamejo pooblastilo profilov uporabnikov, ki jih je podal IBM, in imajo posebno pooblastilo *ALLOBJ kot sta QSECOFR in QSYS.

Podrobnejše informacije o beleženju zaščite poiščite v 9. poglavju knjige *Security Reference*.

Analiziranje objektnih pooblastil

S pomočjo naslednjega načina lahko določite, kdo ima pooblastilo za knjižnice v sistemu:

1. Z ukazom DSPOBJD izpišite seznam vseh knjižnic v sistemu:

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

   Opomba: Ta ukaz ne bo prikazal knjižnic v neodvisnih pomnilniških prostorih, ki nimajo statusa razpoložljivosti.

2. Z ukazom DSPOBJAUT (Prikaži objektno pooblastilo) izpišite pooblastila za določeno knjižnico:

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

3. Z ukazom DSPLIB (Prikaži knjižnico) izpišite objekte v knjižnici:
   ```
   DSPLIB LIB(QSYS/ime-knjižnice) ASPDEV(ime-naprave-asp) OUTPUT(*PRINT)
   ```

S pomočjo teh poročil lahko določite, kaj je v knjižnici in kdo ima dostop do nje. Če je potrebno, si lahko s pomočjo ukaza DSPOBJAUT ogledate tudi pooblastilo za izbrane objekte v knjižnici.

Iskanje spremenjenih objektov

S pomočjo ukaza CHKOBJITG (Preveri integriteto objekta) lahko poiščete objekte, ki so bili spremenjeni. Spremenjen objekt je običajno znak vdora v sistem. Ta ukaz lahko zaženete, če je nekdo:

- obnovil programe v sistemu
- uporabil namenska servisna orodja (DST)

Ko zaženete ukaz, izdela sistem datoteko baze podatkov, ki vsebuje informacije o možnih težavah v integriteti. Preverite lahko objekte, katerih lastnik so en profil, več različnih profilov ali vsi profili. Poiščete lahko objekte, katerih domena je bila spremenjena. Če želite, lahko tudi znova izračunate vrednosti za preverjanje programa in poiščete objekte tipa *PGM, *SRVPGM, *MODULE in *SQLPKG, ki so bili spremenjeni.

Za izvajanje programa CHKOBJITG potrebujete posebno pooblastilo *AUDIT. Izvajanje ukaza je lahko zaradi pregledovanj in računanj, ki jih izvaja, precej dolgotrajno. Zaženite ga, ko vaš sistem ni preveč zaposlen.

Opomba: Profili, ki so lastniki velikega števila objektov s številnimi zasebnimi pooblastili, lahko postanejo zelo veliki. Velikost profila lastnika vpliva na zmogljivost pri prikazu in delu s pooblastilom za objekte v lasti ter pri shranjevanju ali obnavljanju profilov. Vpliva lahko tudi na sistemske operacije. Če želite preprečiti ta vpliv na zmogljivost ali sistemske operacije, porazdelite lastništvo objektov na več profilov. **Vseh (ali skoraj vseh) objektov ne dodelite samo enemu profilu lastnika.**

Analiziranje programov, ki prevzamejo pooblastilo

Programi, ki prevzamejo pooblastilo uporabnika s posebnim pooblastilom *ALLOBJ, predstavljajo luknjo v zaščiti. Za iskanje in pregled teh programov lahko uporabite naslednji način:

1. Za vsakega uporabnika s posebnim pooblastilom *ALLOBJ uporabite ukaz DSPPGMADP (Prikaži programe, ki prevzamejo), da boste navedli programe, ki prevzamejo pooblastilo uporabnika:
   ```
   DSPPGMADP
   USRPRF(ime-profila-uporabnika) +
             OUTPUT(*PRINT)
   ```

   Opomba: Tema “Natis izbranih profilov uporabnikov” na strani 44 kaže, kako izpisati uporabnike s pooblastilom *ALLOBJ.
2. S pomočjo ukaza DSPOBJAUT določite, kdo ima pooblastilo za uporabo vsakega programa s prevzemom, in kakšno je javno pooblastilo za program:
   ```
   DSPOBJAUT OBJ(ime-knjižnice/ime-programa) +
             OBJTYPE(*PGM) ASPDEV(ime-knjižnice/ime-programa) +
             OUTPUT(*PRINT)
   ```
3. Preglejte izvorno kodo in opis programa in ocenite naslednje:
   - Ali je uporabniku programa med izvajanjem pod prevzetim profilom preprečena uporaba dodatne funkcije kot je uporaba ukazne vrstice.

- Ali program prevzame minimalno raven pooblastila, ki je potrebna za nameravano funkcijo. Aplikacije, ki uporabljajo napako programa, je mogoče oblikovati z istim profilom uporabnika za objekte in programe. Če je pooblastilo lastnika programa prevzeto, ima uporabnik pooblastilo *ALL za aplikacijske objekte. V večini primerov ne potrebuje profil lastnika nobenega posebnega pooblastila.

4. S pomočjo ukaza DSPOBJD preverite, kdaj je bil program nazadnje spremenjen:

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

Upravljanje dnevnika beleženja in sprejemnikov dnevnikov

Dnevnik beleženja QSYS/QAUDJRN je namenjen izključno za beleženje zaščite. V dnevnik beleženja ne zapisujte objektov. Dnevnika beleženja naj ne uporablja krmiljenje potrditev. V ta dnevnik ne pošiljajte uporabniških postavk z ukazom SNDJRNE (Pošlji postavko dnevnika) ali API-ja QJOSJRNE (Pošlji postavko dnevnika).

Za zagotovitev, da lahko sistem zapiše postavke beleženja v dnevnik beleženja, se uporablja posebna zaščita zaklepanja. Če je beleženje aktivno (sistemska vrednost QAUDCTL ni *NONE), ima sistemsko razsodniško opravilo (QSYSARB) ključavnico za dnevnik QSYS/QAUDJRN. Če je beleženje aktivno, v dnevniku beleženja ne morete izvajati določenih operacij kot so naslednje:

- ukaz DLTJRN
- ukaz ENDJRNxxx
- ukaz APYJRNCHG
- ukaz RMVJRNCHG
- ukaz DMPOBJ ali DMPSYSOBJ
- prenos dnevnika
- obnovitev dnevnika
- operacije, ki uporabljajo pooblastila, kot je ukaz GRTOBJAUT
- ukaz WRKJRN

Informacije iz postavk dnevnika zaščite so opisane v knjigi *Security Reference*. Vse postavke zaščite v dnevniku beleženja imajo kodo beleženja T. Poleg postavk zaščite so v dnevniku QAUDJRN prikazane tudi sistemske postavke. To so postavke s kodo beleženja J, ki je povezana z nalaganjem začetnega programa (IPL) in splošnimi operacijami, ki se izvajajo v sprejemnikih dnevnikov (na primer shranitev sprejemnika).

Če pride v dnevniku ali v njegovem trenutnem sprejemniku do napake, tako da ni več mogoče zapisovati postavk beleženja, sistemska vrednost QAUDENDACN določi, katero dejanje bo opravil sistem. Obnovitev okvarjenega dnevnika ali sprejemnika dnevnika je ista kot za druge dnevnike.

Če želite, lahko sistem upravlja spreminjanje sprejemnikov dnevnikov. Pri izdelavi dnevnika QAUDJRN podajte MNGRCV(*SYSTEM) ali spremenite dnevnik v to vrednost. Če podate MNGRCV(*SYSTEM), sistem samodejno odpne sprejemnik, ko doseže prag ter izdela in pripne nov sprejemnik dnevnika. To se imenuje **sistemsko upravljanje spreminjanja dnevnikov**. Podrobnejše informacije poiščite v Informacijskem centru iSeries —>Upravljanje sistemov–> Upravljanje dnevnikov–>Upravljanje lokalnih dnevnikov–>Upravljanje dnevnikov. Podrobnejše informacije o dostopu do Informacijskega centra iSeries poiščitev razdelku“Predpogoji in s tem povezane informacije” na strani xii.

Poglavje 6. Upravljanje pooblastil

Kot pomoč pri vodenju nastavitve pooblastil v sistemu je na voljo niz poročil zaščite. Ko v začetku zaženete ta poročila, lahko natisnete vse (na primer pooblastilo za vse datoteke ali za vse programe).

Ko vzpostavite bazo informacij, lahko redno izvajate različice poročil o spremembah. Različice poročil o spremembah vam bodo pomagale določiti spremembe v sistemu, povezane z zaščito, ki zahtevajo vašo pozornost. Tako lahko na primer vsak teden zaženete poročilo, ki prikaže javno pooblastilo za datoteke. Zahtevate lahko samo različico poročila o spremembah. Poročilo bo prikazalo nove datoteke v sistemu, ki so na voljo za vse, in obstoječe datoteke, katerih javno pooblastilo je bilo od zadnje izvedbe poročila spremenjeno.

Za izvajanje orodij za zaščito sta na voljo dva menija:

- Uporaba menija SECTOOLS za interaktivno izvajanje programov
- Uporaba menija SECBATCH za paketno izvajanje programov. Meni SECBATCH je sestavljen iz dveh delov: prvi je namenjen za takojšnjo predložitev opravil v čakalno vrsto opravil, drugi pa za postavitev opravil v planer opravil.

Če uporabljate Navigator iSeries, naslednji koraki kažejo, kako zaženete orodja za zaščito:

1. V Navigatorju iSeries razširite vaš strežnik —>**Zaščita**.
2. Z desno tipko miške kliknite **Načela** in izberite **Razišči**, da boste prikazali seznam načel, ki jih lahko izdelate in upravljate.

Nadzorovanje javnih pooblastil za objekte

Zaradi preprostosti in zmogljivosti je večina sistemov nastavljenih tako, da je večina objektov na voljo skoraj vsem uporabnikom. Namesto da bi bili uporabniki izrecno pooblaščeni za vsak objekt, imajo izrecno zavrnjen dostop do določenih zaupnih, na zaščito občutljivih objektov. V nekaterih sistemih z visokimi zahtevami za zaščito je uveljavljen obraten pristop, in so pooblastila za objekte izdana po potrebi. V teh sistemih je večina objektov izdelana z javnim pooblastilom, nastavljenim na *EXCLUDE.

iSeries je na objektih temelječ sistem, ki vsebuje številne različne vrste objektov. Večina tipov objektov ne vsebuje občutljivih informacij ali izvaja funkcij, povezanih z zaščito. Kot skrbnik za zaščito v sistemu iSeries z značilnimi potrebami za zaščito se boste najbrž usmerili na objekte, ki zahtevajo zaščito, kot so datoteke baz podatkov in programi. Za druge tipe objektov lahko nastavite javno pooblastilo, ki zadostuje za vaše aplikacije, ki je za večino tipov objektov *USE.

S pomočjo ukaza PRTPUBAUT (Natisni javno pooblastilo) lahko natisnete informacije o objektih, do katerih lahko dostopijo javni uporabniki. (**Javni uporabnik** je vsakdo s prijavnim pooblastilom, ki nima izrecnega pooblastila za objekt.) Če uporabite ukaz PRTPUBAUT, lahko podate tipe objektov ter knjižnice ali imenike, ki jih želite pregledati. Na menijih SECBATCH in SECTOOLS so na voljo možnosti za natis poročil o objektih z javnimi pooblastili za tipe objektov, ki navadno vplivajo na zaščito. Redno lahko natisnete različico tega poročila o spremembah, da boste videli, kateri objekti zahtevajo vašo pozornost.

Upravljanje pooblastil za nove objekte

OS/400 nudi funkcije, ki vam bodo pomagale pri upravljanju pooblastil in lastništva novih objektov v sistemu. Ko uporabnik izdela nov objekt, sistem določi naslednje:
- kdo bo lastnik objekta
- kakšno je javno pooblastilo za objekt
- ali ima objekt kakšno zasebno pooblastilo
- kam bo shranjen objekt (v katero knjižnico ali imenik)
- ali se bo za dostop do objekta izvajalo beleženje

Za to odločanje uporablja sistem sistemske vrednosti, parametre knjižnice in parametre profilov uporabnikov. “V 5. poglavju ”Dodelitev pooblastil in lastništva novim objektom knjige *iSeries Security Reference* boste našli številne zglede možnosti, ki so na voljo.

S pomočjo ukaza PRTUSRPRF lahko natisnete parametre profilov uporabnikov, ki vplivajo na lastništvo in pooblastila novih objektov. Slika 5 na strani 54 kaže zgled tega poročila.

Nadzorovanje pooblastitvenih seznamov

S pomočjo pooblastitvenih seznamov lahko združite objekte s podobnimi zahtevami za zaščito. Konceptualno gledano vsebuje pooblastitveni seznam seznam uporabnikov in pooblastil, ki jih imajo uporabniki za objekte, ki jih ščiti seznam. Pooblastitveni seznami nudijo učinkovit način za upravljanje pooblastil za podobne objekte v sistemu, toda včasih lahko otežijo vodenje pooblastil za objekte.

S pomočjo ukaza PRTPVTAUT (Natisni zasebno pooblastilo) lahko natisnete informacije o pooblastilih s pooblastitvenih seznamov. Slika 3 kaže zgled poročila.

```
                          Zasebna pooblastila (celotno poročilo)
SYSTEM4
Pooblastitveni                Primarna                              Seznam----------Objekt-----------  ------------Podatki---------
seznam          Lastnik       skupina       Uporabnik   Pooblastilo Upr   Oper Upr  Obst   Sprem  Ref  Bran  Dod  Ažu  Bri  Izvedba
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. Poročilo o zasebnih pooblastilih za pooblastitvene sezname

To poročilo prikazuje iste informacije, ki jih lahko vidite na zaslonu Urejanje pooblastitvenega seznama (EDTAUTL). Prednost poročila je, da nudi informacije o vseh pooblastitvenih seznamih na enem mestu. Če na primer nastavljate zaščito za novo skupino objektov, lahko hitro pregledate poročilo in ugotovite, ali obstoječi pooblastitveni seznam ustreza vašim potrebam za te objekte.

Natisnete lahko različico poročila o spremembah in si ogledate nove pooblastitvene sezname ali pooblastitvene sezname, v katerih so bile od zadnjega natisa poročila opravljene spremembe v pooblastilih. Na voljo je tudi možnost za natis seznama objektov, ki jih ščitijo posamezni pooblastitveni seznami. Slika 4 na strani 51 kaže zgled poročila za en pooblastitveni seznam:

```
                    Prikaz objektov pooblastitvenega seznama
Pooblastitveni seznam. . . . . :   CUSTAUTL
Knjižnica. . . . . :     QSYS
Lastnik. . . . . :   AROWNER
Primarna skupina . . . . . :   *NONE

                                                        Primarna
Objekt         Knjižnica      Tip          Lastnik      skupina       Besedilo
CUSTMAS        CUSTLIB        *FILE        AROWNER      *NONE
CUSTORD        CUSTORD        *FILE        OEOWNER      *NONE
```

Slika 4. Prikaz poročila o objektih pooblastitvenega seznama

To poročilo lahko na primer uporabite, da boste razumeli učinek dodajanja novega uporabnika na pooblastitveni seznam (katera pooblastila bo prejel uporabnik).

Uporaba pooblastitvenih seznamov

Navigator iSeries nudi funkcije zaščite, oblikovane tako, da vam bodo pomagale pri razvijanju načrta in načel zaščite ter pri konfiguriranju sistema, tako da bo ustrezal potrebam vašega podjetja. Ena izmed razpoložljivih funkcij je uporaba pooblastitvenih seznamov.

Pooblastitveni seznami nudijo naslednje možnosti.

- Pooblastitveni seznam združi objekte s podobnimi zahtevami za zaščito.
- Konceptualno gledano vsebuje pooblastitveni seznam seznam uporabnikov in skupin ter pooblastil, ki jih imajo uporabniki za objekte, ki jih ščiti seznam.
- Vsak uporabnik in skupina imata različno pooblastilo za niz objektov, ki jih ščiti seznam.
- Pooblastilo je dodeljeno prek seznama in ne posameznim uporabnikom in skupinam.

Naloge, ki jih lahko opravite s pomočjo pooblastitvenih seznamov, vključujejo naslednje:

- izdelava pooblastitvenega seznama
- spreminjanje pooblastitvenega seznama
- dodajanje uporabnikov in skupin
- spreminjanje dovoljenj uporabnikov
- prikaz zaščitenih objektov

Za uporabo te funkcije opravite naslednje korake:

1. V Navigatorju iSeries razširite ikono strežnika—>Zaščita. Prikažejo se **pooblastitveni seznami** in **načela**.
2. Z desno tipko miške kliknite **Pooblastitveni seznami** in izberite **Nov pooblastitveni seznam**. **Nov pooblastitveni seznam** omogoča naslednje.
   - **Uporaba:** omogoča dostop do atributov objekta in uporabo objekta. Uporabniki z javnim pooblastilom si lahko objekt ogledajo, ne morejo pa ga spremeniti.
   - **Spreminjanje:** omogoča spreminjanje vsebine objekta (z nekaterimi izjemami).
   - **Vse:** omogoča vse operacije v objektu razen tistih, ki so omejene na lastnika. Uporabnik ali skupina lahko krmilita obstoj objekta, podata zaščito za objekt, objekt spremenita in zanj izvajata osnovne operacije. Uporabnik ali skupina lahko tudi spremenita lastništvo objekta.
   - **Izključitev:** vse operacije v objektu so prepovedane. Uporabniki in skupine, ki jim dodelite to dovoljenje, nimajo dostopa do objekta in zanj ne morejo izvajati nobenih operacij. Podaja, da uporabniki z javnim pooblastilom ne morejo uporabljati objekta.

Pri delu s pooblastitvenimi seznami boste dodelili dovoljenja za objekte in podatke. Dovoljenja za objekte, med katerimi lahko izberete, so navedena spodaj.

- **Operacijsko:** nudi dovoljenje za pregled opisa objekta in uporabo objekta, kot to določa podatkovno dovoljenje, ki ga imata uporabnik ali skupina za objekt.

- **Upravljanje:** nudi dovoljenje za podajanje zaščite za objekt, prenos ali preimenovanje objekta in dodajanje članov v datoteke baze podatkov.
- **Obstoj:** nudi dovoljenje za krmiljenje obstoja in lastništva objekta. Uporabnik ali skupina lahko zbrišeta objekt, sprostita njegov pomnilnik, za objekt izvedeta operacije shranitve in obnovitve in preneseta lastništvo objekta. Če imata uporabnik ali skupina posebno dovoljenje za shranitev, ne potrebujeta dovoljenja za obstoj.
- **Spreminjanje** (uporablja se samo za datoteke baz podatkov in pakete SQL): nudi dovoljenje, potrebno za spreminjanje atributov objekta. Če imata uporabnik ali skupina dovoljenje za datoteko baze podatkov, lahko dodata in odstranita prožila, dodata in odstranita referenčne in unikatna omejitve ter spremenita atribute datoteke baze podatkov. Če imata uporabnik ali skupina to dovoljenje za paket SQL, lahko spremenite njegove atribute. To dovoljenje se trenutno uporablja samo za datoteke baze podatkov in pakete SQL.
- **Referenca** (uporablja se samo za datoteke baze podatkov in pakete SQL): nudi dovoljenje, potrebno za sklic na objekt iz drugega objekta, tako da operacije v tem objektu lahko omeji drugi objekt. Če imata uporabnik ali skupina to dovoljenje za fizično datoteko, lahko dodata referenčne omejitve, v katerih je fizična datoteka nadrejena. To dovoljenje se trenutno uporablja samo za datoteke baze podatkov.

Dovoljenja za podatke, med katerimi lahko izberete, so navedena spodaj.
- **Branje:** nudi dovoljenje, potrebno za prikaz vsebine objekta, kot je na primer prikaz zapisov datoteke.
- **Dodajanje:** nudi pravico za dodajanje postavk v objekt, kot je na primer dodajanje sporočil v čakalno vrsto sporočil ali dodajanje zapisov v datoteko.
- **Ažuriranje:** nudi dovoljenje za spreminjanje postavk v objektu, kot je na primer spreminjanje zapisov v datoteki.
- **Brisanje:** nudi dovoljenje za odstranitev postavk iz objekta, kot je na primer odstranjevanje sporočil iz čakalne vrste sporočil ali brisanje zapisov iz datoteke.
- **Izvedba:** nudi dovoljenje, potrebno za izvedbo programa, servisnega programa ali paketa SQL. Uporabnik lahko objekt poišče tudi v knjižnici ali v imeniku.

Za podrobnejše informacije o posameznih postopkih pri izdelavi ali urejanju pooblastitvenih seznamov uporabite zaslonsko pomoč, ki je na voljo v Navigatorju iSeries.

Dostopanje do načel v Navigatorju iSeries

S pomočjo Navigatorja iSeries si lahko ogledate in upravljate načela strežnika iSeries. Navigator iSeries ima pet področij načel:

- **Načelo beleženja**
  To načelo omogoča, da nastavite nadzorovanje določenih dejanj in dostopa do določenih sredstev v sistemu.
- **Načelo zaščite**
  To načelo omogoča, da podate raven zaščite in dodatnih možnosti, povezanih z zaščito sistema.
- **Načelo gesel**
  To načelo omogoča, da podate raven gesel za sistem.
- **Načelo obnovitve**
  To načelo omogoča, da podate način obnovitve določenih objektov v sistemu.
- **Načelo prijave**
  To načelo omogoča, da podate, kako se lahko uporabniki prijavijo v sistem.

Za prikaz ali spreminjanje načel v Navigatorju iSeries opravite naslednje korake:

1. V Navigatorju iSeries razširite strežnik —>**Zaščita**.

2. Z desno tipko miške kliknite **Načela** in izberite **Razišči**, da boste prikazali seznam načel, ki jih lahko izdelate in upravljate. Podrobnejše informacije o teh načelih poiščite v pomoči Navigatorja iSeries.

Nadzorovanje zasebnih pooblastil za objekte

Možnosti menija SECBATCH:
12 *za takojšnjo predložitev* **41** *za uporabo planerja opravil*

S pomočjo ukaza PRTPVTAUT (Natisni zasebno pooblastilo) lahko natisnete seznam vseh zasebnih pooblastil za objekte podanega tipa v podani knjižnici.

To poročilo lahko uporabite kot pomoč pri odkrivanju novih pooblastil v objektih. Pomaga vam lahko tudi pri ohranitvi sheme zasebnih pooblastil na ravni, ki ni preveč zapletena in neupravljiva.

Nadzorovanje dostopa do izhodnih čakalnih vrst in čakalnih vrst opravil

Včasih skrbnik za zaščito odlično zaščiti dostop do datotek, nato pa pozabi, kaj se zgodi pri natisu vsebine datoteke. Strežnik iSeries nudi funkcije, ki omogočajo zaščito občutljivih izhodnih čakalnih vrst in čakalnih vrst opravil. Izhodno čakalno vrsto lahko na primer zaščitite tako, da nepooblaščeni uporabniki ne morejo prikazati ali prekopirati zaupnih vmesnih datotek, ki čakajo na natis. Čakalne vrste opravil zaščitite tako, da nepooblaščeni uporabniki ne morejo preusmeriti zaupnega opravila v nezaupno izhodno čakalno vrsto in v celoti preklicati opravila.

Možnosti menija SECBATCH:
24 za takojšnjo predložitev63 *za uporabo planerja opravil*

Tema Informacijskega centra z naslovom *Osnovna zaščita in načrtovanje sistema* in knjiga *iSeries Security Reference* opisujeta, kako zaščititi izhodne čakalne vrste in čakalne vrste opravil.

S pomočjo ukaza PRTQAUT (Natisni pooblastilo čakalne vrste) lahko natisnete nastavitve zaščite za čakalne vrste opravil in izhodne čakalne vrste v sistemu. Nato lahko ocenite tiskalna opravila, ki tiskajo zaupne informacije in zagotovite, da gredo v zaščitene izhodne čakalne vrste in čakalne vrste opravil.

Za izhodne čakalne vrste in čakalne vrste opravil, za katere menite, da so občutljive na zaščito, lahko primerjate nastavitve zaščite z informacijami v dodatku D knjige *iSeries Security Reference*. Tabele v dodatku D navajajo, katere nastavitve so potrebne za izvedbo različnih funkcij izhodne čakalne vrste in čakalne vrste opravil.

Nadzorovanje posebnih pooblastil

Če imajo uporabniki v sistemu nepotrebna posebna pooblastila, je lahko vaš trud za izdelavo dobre sheme objektnih pooblastil zaman. Objektno pooblastilo je brez pomena, če ima profil uporabnika posebno pooblastilo *ALLOBJ. Uporabnik s posebnim pooblastilom *SPLCTL lahko prikaže vse vmesne datoteke v sistemu, ne glede na to, koliko truda vložite v zaščito izhodnih čakalnih vrst. Uporabnik s posebnim pooblastilom *JOBCTL lahko vpliva na

operacije sistema in preusmeri opravila. Uporabnik s posebnim pooblastilom *SERVICE lahko z uporabo servisnih orodij dostopi do podatkov brez uporabe operacijskega sistema.

Možnosti menija SECBATCH:
29 za takojšnjo predložitev 68 *za uporabo planerja opravil*

S pomočjo ukaza PRTUSRPRF (Natisni profil uporabnika) lahko natisnete informacije o posebnih pooblastilih in uporabniških razredih za profile uporabnikov v sistemu. Pri izvedbi poročila imate na voljo več možnosti:
- vsi profili uporabnikov
- profili uporabnikov z določenimi posebnimi pooblastili
- profili uporabnikov z določenimi uporabniškimi razredi
- profili uporabnikov z neujemanjem med uporabniškim razredom in posebnimi pooblastili.

Slika 5 kaže zgled poročila, ki prikazuje posebna pooblastila za vse profile uporabnikov:

```
                                    Informacije o profilu uporabnika
  Tip poročila . . . . . :   *AUTINFO
  Izbran z . . . . . :   *SPCAUT
  Posebna pooblastila  . . . . . :   *ALL
                   -------------Posebna pooblastila-------------
                                *IO                                                          Skupina
Profil    Profili   *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  Upor.          Lastnik   Pooblastilo  Tip         Omejna
uporabn.  skupin     OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  razred                  skupine      pooblastila  zmožnosti
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. Poročilo z uporabniškimi informacijami: zgled 1

Poleg posebnih pooblastil prikaže poročilu tudi naslednje:
- Ali ima profil uporabnika omejene zmožnosti.
- Ali sta uporabnik ali skupina uporabnika lastnika novih objektov, ki jih izdela uporabnik.
- Katero pooblastilo samodejno prejme skupina uporabnika za nove objekte, ki jih izdela uporabnik

Slika 6 kaže zgled poročila za neujemanje med posebnimi pooblastili in uporabniškimi razredi:

```
Informacije o profilu uporabnika
Tip poročila . . . . . :   *AUTINFO
Izbran z . . . . . :   *MISMATCH
-------------------------------Posebna pooblastila-------------
                               *IO                                                       Skupina
Profil    Profili   *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  Upor.          Lastnik    Pooblastilo  Tip         Omejena
uporabn.  skupin     OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  razred                   skupine     pooblastila  zmožnost
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. Poročilo z uporabniškimi informacijami: zgled 2

V sliki Slika 6 ne spreglejte naslednjega:
- USERX ima uporabniški razred operaterja sistema (*SYSOPR), vendar ima posebni pooblastili *ALLOBJ in *SPLCTL.

- USERY ima uporabniški razred uporabnika (*USER), vendar ima posebno pooblastilo *SECADM.
- Tudi USERZ ima uporabniški razred uporabnika (*USER) in posebno pooblastilo *SECADM. Vidite lahko tudi, da je USERZ član skupine QPGMR, ki ima posebni pooblastili *JOBCTL in *SAVSYS.

Ta poročila lahko redno izvajate kot pomoč pri nadzorovanju upravljanja profilov uporabnikov.

Nadzorovanje uporabniških okolij

Ena izmed vlog profila uporabnika je definirati okolje za uporabnika, vključno z izhodno čakalno vrsto, začetnim menijem in opisom opravila. Okolje uporabnika vpliva na to, kako uporabnik vidi sistem in do določene mere tudi na to, kaj lahko naredi uporabnik. Uporabnik mora imeti pooblastilo za objekte, ki so podani v profilu uporabnika. Toda če je shema pooblastil še v postopku izdelave ali če ni zelo omejujoča, lahko uporabniško okolje, ki je definirano v profilu uporabnika, povzroči neželene rezultate. Sledi nekaj zgledov:

Možnosti menija SECBATCH:

29 *za takojšnjo predložitev***68** *za uporabo planerja opravil*

- Opis opravila uporabnika lahko podaja profil uporabnika, ki ima več pooblastil kot uporabnik.
- Uporabniku se lahko prikaže začetni meni, ki nima ukazne vrstice. Toda ukazno vrstico lahko poda uporabnikov program za obravnavo tipke Attention.
- Uporabnik ima lahko pooblastilo za izvajanje zaupnih poročil, toda izhodni podatki uporabnika so lahko usmerjeni v izhodno čakalno vrsto, ki je na voljo za uporabnike, ki poročil ne bi smeli videti.

Možnost *ENVINFO ukaza Natisni profil uporabnika (PRTUSRPRF) lahko uporabite kot pomoč pri nadzorovanju okolij, ki so definirana za uporabnike sistema. Slika 7 kaže zgled poročila:

```
                                    Informacije o profilu uporabnika
  Tip poročila . . . . . :   *ENVINFO
  Izbran z . . . . . :   *USRCLS
                        Začetni        Začetni          Opis/       Čak.vrsta/     Izhodna        Program/
Profil          Trenutna meni/          program/       knjižnica     knjižnica      čakal.vrsta/   knjižica
uporabnika      knjižnica knjižnica     knjižnica      opravila      sporočil       knjižnica      Attention
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. Zgled natisa uporabniškega okolja za profil uporabnika

Upravljanje servisnih orodij

Storitvena orodja se uporabljajo za konfiguriranje, upravljanje in servisiranje strežnika. Do servisnih orodij lahko dostopite iz namenskih servisnih orodij (DST) ali iz sistemskih servisnih orodij (SST). ID-ji uporabnikov servisnih orodij so zahtevani za dostop do DST in SST ter za uporabo funkcij Navigatorja iSeries za upravljanje logičnih particij (LPAR) in diskovnih enot.

DST je na voljo, ko zaženete licenčno notranjo kodo, tudi če OS/400 ni naložen. SST je na voljov razdelkuOS/400. Naslednja tabela podaja osnovne razlike med DST in SST.

Značilnost	DST	SST
Dostop	Fizičen dostop prek ukazne mize med ročnim IPL-om ali z izbiro možnosti 21 na Nadzorni plošči.	Dostop prek interaktivnega opravila z zmožnostjo prijave z QSRV ali z naslednjimi pooblastili: • Pooblastilo za ukaz CL STRSST (Zaženi SST) • Posebno pooblastilo za storitve (*SERVICE) ali posebno pooblastilo za objekte (*ALLOBJ). • Funkcionalno pooblastilo za uporabo SST.
Razpoložljivost	Na voljo je tudi, če ima strežnik omejene zmožnosti. Za dostop do DST ni zahtevan OS/400.	Na voljo je, ko zaženete OS/400. Za dostop do SST je zahtevan OS/400.
Overjanje	Zahteva ID uporabnika in geslo servisnih orodij	Zahteva ID uporabnika in geslo servisnih orodij

Preglejte Informacijski center iSeries —>Zaščita—>Storitvena orodja, kjer boste našli informacije o uporabi servisnih orodij za izvedbo naslednjih nalog:

- Dostop do servisnih orodij z DST
- Dostop do servisnih orodij s SST
- Dostop do servisnih orodij z Navigatorjem iSeries
- Izdelava ID-ja uporabnika servisnih orodij
- Sprememba funkcionalnih pooblastil za ID uporabnika servisnih orodij
- Sprememba opisa za ID uporabnika servisnih orodij
- Prikaz ID-ja uporabnika servisnih orodij
- Omogočanje ali onemogočanje ID-ja uporabnika servisnih orodij
- Brisanje ID-ja uporabnika servisnih orodij
- Spreminjanje ID-jev uporabnikov in gesel servisnih orodij s pomočjo SST ali DST
- Spreminjanje gesla ID-ja uporabnika servisnih orodij s pomočjo STRSST
- Spreminjanje ID-jev uporabnikov in gesel servisnih orodij
- API Spremeni ID uporabnika servisnih orodij (QSYCHGDS)
- Vnovična nastavitev gesla profila uporabnika QSECOFR OS/400
- Vnovična nastavitev ID-ja uporabnika in gesla servisnih orodij QSECOFR
- Shranitev in obnovitev zaščitnih podatkov servisnih orodij
- Izdelava lastne različice ID-ja uporabnika servisnih orodij QSECOFR
- Konfiguriranje strežnika servisnih orodij za DST
- Konfiguriranje strežnika servisnih orodij za OS/400
- Nadzorovanje uporabe servisne funkcije prek DST
- Nadzorovanje uporabe servisnih orodij prek dnevnika beleženja zaščite OS/400

Preglejte razdelek “Predpogoji in s tem povezane informacije” na strani xii, kjer boste našli informacije o dostopu do Informacijskega centra iSeries.

Poglavje 7. Uporaba zaščite logičnih particij (LPAR)

Uporaba več logičnih particij na enem strežniku iSeries je lahko koristna v naslednjih scenarijih.

- **Vzdrževanje neodvisnih sistemov**: Z dodelitvijo dela sredstev (pomnilniške enote, procesorjev, pomnilnika in V/I naprav) particiji dosežete logično osamitev programske opreme. Če so logične particije pravilno konfigurirane, lahko dopustijo nekaj napak v strojni opremi. Interaktivno in paketno delo, ki se na eni delovni postaji skupaj ne izvaja najbolje, lahko osamite in učinkovito izvajate na ločenih particijah.
- **Združitev**: Sistem z logičnimi particijami lahko zmanjša število strežniških sistemov iSeries, potrebnih znotraj podjetja. Več sistemov lahko združite v en sistem z logičnimi particijami. S tem si prihranite potrebo in stroške za dodatno opremo. Ker se potrebe spreminjajo, lahko prenesete sredstva z ene logične particije na drugo.
- **Izdelava mešanega proizvodnega in preizkusnega okolja:** Izdelate lahko kombinacijo proizvodnega in preizkusnega okolja. Na primarni particiji lahko izdelate eno proizvodno particijo. Za izdelavo več proizvodnih particij preberite spodnjo temo *Izdelava okolja z več proizvodnimi particijami*.

  Logična particija je preizkusna ali proizvodna particija. Na proizvodni particiji se izvajajo vaše glavne poslovne aplikacije. Napaka na proizvodni particiji lahko v veliki meri ovira operacije podjetja in vas stane časa in denarja. Preizkusna particija preizkuša programsko opremo. Napaka na preizkusni particiji, ki ni nujno načrtovana, ne bo vplivala na običajne poslovne operacije.
- **Izdelava okolja z več proizvodnimi particijami:** Več proizvodnih particij izdelajte samo na sekundarnih particijah. V tej situaciji namenite primarno particijo za upravljanje particij.
- **Vroča varnostna kopija:** Če prekopirate sekundarno particijo na drugo logično particijo znotraj istega sistema, bo preklop na nadomestno particijo v primeru napake povzročil minimalne neugodnosti. Ta konfiguracija tudi zmanjša učinek dolgih shranjevalnih oken. Nadomestno particijo lahko izključite in shranite, medtem ko druga logična particija nadaljuje z delom. Za uporabo strategije vročih varnostnih kopij potrebujete posebno programsko opremo.
- **Integrirana gruča:** S pomočjo OptiConnect/400 in visoko razpoložljive aplikacijske programske opreme se lahko izvaja particionirani sistem kot integrirana gruča. Z integrirano gručo lahko zaščitite sistem pred večino neterminiranih napak na sekundarni particiji.

Opomba: Pri nastavitvi sekundarne particije morate nameniti posebno pozornost mestom kartic. Če ima vhodno/izhodni procesor (IOP), ki ga izberete za ukazno mizo, tudi kartico LAN in le-ta ni namenjena za uporabo z operacijsko ukazno mizo, bo aktivirana za uporabo s ukazno mizo in je morda ne boste mogli uporabiti za načrtovane namene. Podrobnejše informacije o delu z operacijsko ukazno mizo poiščite v temi Poglavje 9, “iSeries”, na strani 63.

Podrobnejše informacije o tej temi lahko najdete v ″Logičnih particijah″ Informacijskega centra iSeries.

Upravljanje zaščite za logične particije

Naloge, povezane z zaščito, ki jih opravite v particioniranem sistemu, so iste kot v sistemu brez logičnih particij. Toda če izdelate logične particije, delate z več neodvisnimi sistemi. Zato morate opraviti iste naloge na vsaki logični particiji za razliko od sistema brez logičnih particij, kjer jih opravite samo enkrat.

Pri delu z zaščito na logičnih particijah si zapomnite nekaj osnovnih pravil:

- Pri dodajanju uporabnikov v sistem morate upoštevati, da jih lahko naenkrat dodate samo na eno logično particijo. Uporabnike morate dodati na vsako logično particijo, do katere želite, da imajo dostop.
- Omejite število uporabnikov, ki imajo pooblastilo za uporabo namenskih servisnih orodij (DST) in sistemskih servisnih orodij (SST) na primarni particiji. Več informacij o DST in SST vam je na voljo v temi ″Upravljanje logičnih particij z uporabo Navigatorja iSeries, DST in SST″ v Informacijski center iSeries. V razdelku “Upravljanje servisnih orodij” na strani 56 lahko najdete informacije o uporabi profilov uporabnikov servisnih orodij za nadzor dostopa do dejavnosti particij.

  Opomba: Pred uporabo Navigatorja iSeries za dostop do funkcij LPAR, morate inicializirati strežnik servisnih orodij. S tem povezane informacije poiščite v Informacijskem centru iSeries —>Zaščita—>Storitvena orodja. V razdelku “Predpogoji in s tem povezane informacije” na strani xii poiščite informacije o dostopu do Informacijskega centra iSeries.
- Sekundarne particije ne morejo videti ali uporabljati glavnega pomnilnika in diskovnih enot druge logične particije.
- Sekundarne particije lahko vidijo samo lastna sredstva strojne opreme.
- Primarna particija lahko vidi vsa sistemska sredstva strojne opreme na zaslonih DST in SST Delo s sistemskimi particijami.
- Operacijski sistem primarne particije še vedno vidi samo lastna razpoložljiva sredstva.
- Primarno particijo nadzoruje sistemska nadzorna plošča. Če nastavite način okna na Zaščiten, ni mogoče na zaslonu SST Delo s statusom particije opraviti nobenega dejanja. Če želite uveljaviti DST iz sistemske nadzorne plošče, morate spremeniti način v Ročen.
- Če nastavite operacijski način sekundarne particije na Zaščiten, omejite uporabo zaslona Delo s statusom particije na naslednje načine:
  - Za spreminjanje statusa particije lahko uporabite samo DST na sekundarni particiji; za spreminjanje statusa particije ne morete uporabiti SST.
  - DST na sekundarni particiji lahko uveljavite samo z zaslona primarne particije Delo s statusom particije z uporabo DST ali SST.
  - Za spreminjanje načina sekundarne particije iz Zaščiten v katerokoli drugo vrednost lahko uporabite samo DST.

Če način sekundarne particije ni več zaščiten, lahko za spreminjanje statusa particije uporabite DST in SST na sekundarni particiji.

Podrobnejše informacije o zaščiti strežnika iSeries lahko najdete v knjigi Security Reference in na straneh Osnovna zaščita in načrtovanje sistema Informacijskega centra iSeries.

Poglavje 9. iSeries

Poglavje 9. iSeries

Operacijska ukazna miza omogoča, da s pomočjo PC-ja dostopite do strežnika iSeries in ga nadzorujete. Operacijska ukazna miza vključuje podporo za oddaljeno klicanje PC-jev v omrežje strežnikov iSeries brez naprav operacijske mize, s čimer omogoči, da postanejo ukazne mize oddaljeni PC-ji. Pri uporabi operacijske ukazne mize pazite na naslednje:

- Z operacijske ukazne mize lahko opravite katerokoli nalogo, ki jo lahko opravite na običajni ukazni mizi. Profili uporabnikov, ki imajo posebno pooblastilo *SERVICE ali *ALLOBJ, se lahko na primer prijavijo v sejo operacijske ukazne mize, tudi če so onemogočeni.
- Operacijska ukazna miza s pomočjo profilov uporabnikov in gesel servisnih orodij omogoča povezavo s strežnikom iSeries. Zaradi tega je še posebej pomembno, da spremenite profile uporabnikov in gesla servisnih orodij. Hekerji gotovo poznajo privzete ID-je uporabnikov in gesla profilov uporabnikov servisnih orodij in jih lahko uporabijo za poskus vzpostavitve oddaljene seje ukazne mize s strežnikom iSeries. Nasvete o geslih lahkonajdete v razdelku“Spreminjanje znanih gesel” na strani 18 in “Izogibanje privzetim geslom” na strani 23.
- Za zaščito informacij pri uporabi oddaljene ukazne mize uporabite možnost povratnega klica Omrežja na klic Windows.
- Pri nastavitvi sekundarne particije morate nameniti posebno pozornost mestom kartic. Če ima vhodno/izhodni procesor (IOP), ki ga izberete za ukazno mizo, tudi kartico LAN in le-ta ni namenjena za uporabo z operacijsko ukazno mizo, bo aktivirana za uporabo s ukazno mizo in je morda ne boste mogli uporabiti za načrtovane namene.

V izdajo V5R1 smo operacijsko ukazno mizo izboljšali tako, da omogoča izvajanje dejavnosti ukazne mize pred lokalnega omrežja (LAN). Izboljšano overjanje in šifriranje podatkov omogočata omrežno zaščito za postopke ukazne mize. Če želite uporabljati operacijsko ukazno mizo s povezljivostjo LAN, priporočamo, da namestite naslednje izdelke:

- Cryptographic Access Provider, 5722–AC2 ali 5722–AC3 na strežniku iSeries
- Client Encryption, 5722–CE2 ali 5722–CE3 na PC-ju operacijske ukazne mize

Če želite šifrirati podatke ukazne mize, mora biti na strežniku iSeries nameščen eden izmed izdelkov ponudnika šifriranega dostopa; **tudi** na PC-ju mora biti nameščen eden izmed izdelkov za šifriranje odjemalcev.

Opomba: Če ne namestite nobenega izmed izdelkov za šifriranje, podatki ne bodo šifrirani.

Spodnja tabela povzema rezultate šifriranja razpoložljivih izdelkov:

Tabela 13. Rezultati šifriranja

Ponudnik šifriranega dostopa na strežniku iSeries	Šifriranje odjemalca na PC-ju operacijske ukazne mize	Nastalo šifriranje podatkov
Nič	Nič	Nič
5722–AC2	5722–CE2	56-bitno
5722–AC2	5722–CE3	56-bitno
5722–AC3	5722–CE2	56-bitno
5722–AC3	5722–CE3	128-bitno

Dodatne informacije o nastavitvi in upravljanju iSeries operacijska ukazna miza, lahko najdete v Informacijskem centru iSeries.

Operacijska ukazna miza - pregled zaščite

Zaščita operacijske ukazne mize je sestavljena iz naslednjega:

- overjanje naprave ukazne mize
- overjanje uporabnika
- zasebnost podatkov
- integriteta podatkov

Operacijska ukazna miza z neposredno povezljivostjo ima zaradi povezave od točke do točke implicitno overjanje naprav, zasebnost podatkov in integriteto podatkov. Za prijavo na zaslon ukazne mize je zahtevana zaščita z overjanjem uporabnikov.

Overjanje naprave ukazne mize

Overjanje naprave ukazne mize se prepriča, katera fizična naprava je ukazna miza. Operacijska ukazna miza z neposredno povezljivostjo uporablja fizično povezavo, podobno ukazni mizi twinax. Operacijska ukazna miza, ki uporablja neposredno povezavo, je lahko fizično zaščitena podobno kot povezava twinax, ki krmili dostop do fizične naprave ukazne mize.

Operacijska ukazna miza s povezljivostjo LAN uporablja različico plasti zaščitenih vtičnic (SSL), ki podpira overjanje naprav in uporabnikov brez uporabe potrdil. Overjanje naprav za to obliko povezave temelji na profilu naprave servisnih orodij. Podrobnosti poiščitev razdelku65.

Overjanje uporabnikov

Overjanje uporabnikov preverja, kdo uporablja napravo ukazne mize. Vsa vprašanja, povezana z overjanjem uporabnikov, so enaka, ne glede na vrsto ukazne mize.

Zasebnost podatkov

Zasebnost podatkov zagotavlja, da bo podatke ukazne mize prebral samo zaželen uporabnik. Operacijska ukazna miza z neposredno povezljivostjo uporablja fizično povezavo, podobno ukazni mizi twinax ali zaščiteni omrežni povezavi za povezljivost LAN, ki ščiti podatke ukazne mize. Operacijska ukazna miza, ki uporablja neposredno povezavo, nudi isto zasebnost podatkov kot povezava twinax. Če je fizično mesto zaščiteno, so zaščiteni tudi podatki ukazne mize.

Operacijska ukazna miza s povezljivostjo LAN uporablja zaščiteno omrežno povezavo, če namestite ustrezne izdelke šifriranega dostopa (ACx in CEx). Seja ukazne mize uporabi najvišje možne šifriranje glede na šifrirne izdelke, nameščene na strežniku iSeries in na PC-ju, na katerem se izvaja operacijska ukazna miza.

Opomba: Če ne namestite nobenega izmed izdelkov za šifriranje, podatki ne bodo šifrirani.

Integriteta podatkov

Integriteta podatkov zagotavlja, da podatki ukazne mize na poti so prejemnika niso bili spremenjeni. Operacijska ukazna miza z neposredno povezljivostjo uporablja fizično povezavo, podobno ukazni mizi twinax ali zaščiteni omrežni povezavi za povezljivost LAN, ki ščiti podatke ukazne mize. Operacijska ukazna miza, ki uporablja neposredno povezavo, nudi isto zasebnost podatkov kot povezava twinax. Če je fizično mesto zaščiteno, so zaščiteni tudi podatki ukazne mize.

Operacijska ukazna miza s povezljivostjo LAN uporablja zaščiteno omrežno povezavo, če namestite ustrezne izdelke šifriranega dostopa (ACx in CEx). Seja ukazne mize uporabi najvišje možne šifriranje glede na šifrirne izdelke, nameščene na strežniku iSeries in na PC-ju, na katerem se izvaja operacijska ukazna miza.

Opomba: Če ne namestite nobenega izmed izdelkov za šifriranje, podatki ne bodo šifrirani.

Uporaba operacijske ukazne mize s povezljivostjo LAN

Opomba: Ukazna miza je lahko katerakoli naprava operacijske ukazne mize, toda profil uporabnika servisnih orodij uporabljajo samo konfiguracije, ki temeljijo na lokalnem omrežju.

Strežnik iSeries je naložen s privzetim profilom naprave servisnih orodij QCONSOLE in s privzetim geslom QCONSOLE. Operacijska ukazna miza s povezljivostjo LAN bo spremenila geslo med vsako uspešno povezavo. Podrobnejše informacije poiščitev razdelku“Uporaba čarovnika za namestitev operacijske ukazne mize”.

Dodatne informacije o operacijski ukazni mizi s povezljivostjo LAN iSeries lahko najdete v temi Informacijskega centra z naslovom Operacijska ukazna miza s povezljivostjo LAN.

Zaščita operacijske ukazne mize s povezljivostjo LAN

Pri uporabi operacijske ukazne mize s povezljivostjo LAN priporočamo naslednje:

- Izdelajte drug profil naprave servisnih orodij z atributi ukazne mize in shranite informacije o profilu na varno mesto.
- Na strežnik iSeries namestite ponudnik šifriranega dostopa 5722–AC2 ali 5722–AC3D, na PC operacijske ukazne mize pa izdelek za šifriranje odjemalca 5722–CE2 ali 5722–CE3.
- Izberite netrivialno geslo servisne naprave.
- PC z operacijsko ukazno mizo zaščitite na enak način kot bi zaščitili ukazno mizo twinax ali operacijsko ukazno mizo z neposredno povezljivostjo.

Uporaba čarovnika za namestitev operacijske ukazne mize

Ta čarovnik bo pri uporabi operacijske ukazne mize s povezljivostjo LAN dodal na PC potrebne informacije. Čarovnik za namestitev zahteva vnos profila naprave servisnih orodij, gesla profila naprave servisnih orodij in gesla za zaščito informacij o profilu naprave servisnih orodij.

Opomba: Geslo informacij profila naprave servisnih orodij se uporablja za zaklepanja in odklepanje informacij profila naprave servisnih orodij (profila naprave servisnih orodij in gesla) na PC-ju.

Pri vzpostavitvi omrežne povezave vas bo čarovnik za namestitev operacijske ukazne mize pozval, da vnesete geslo informacij servisne naprave za dostop do šifriranega profila in gesla naprave servisnih orodij. Vnesti boste morali tudi veljavno identifikacijo in geslo uporabnika servisnih orodij.

Poglavje 10. Odkrivanje sumljivih programov

Najnovejši trendi uporabe računalnikov so povečali možnost, da se v sistemu izvajajo programi iz neoverjenih virov ali programi, ki izvajajo neznane funkcije. Sledi nekaj zgledov:

- Uporabnik osebnega računalnika včasih dobi programe od drugih uporabnikov osebnih računalnikov. Če je PC priključen v sistem iSeries, lahko ta program vpliva na strežnik iSeries.
- Tudi uporabniki, ki so povezani v omrežje, lahko pridobijo programe, kot na primer z elektronskih oglasnih desk.
- Hekerji so vedno bolj aktivni in slavni, saj pogosto objavijo svoje načine in rezultate. To lahko vodi do posnemanja programerjev, ki sicer upoštevajo predpise.

Ti trendi vodijo do težav v zaščiti računalnikov, ki se imenuje **računalniški virus**. Virus je program, ki lahko spremeni druge programe, tako da vključijo kopijo samega sebe. Takrat rečemo, da so drugi programi okuženi z virusom. Poleg tega lahko virus izvaja druge operacije, ki izrabljajo sistemska sredstva ali uničujejo podatke.

Arhitektura strežnika iSeries nudi nekaj zaščite pred virusnimi značilnostmi računalniškega virusa. To je opisano v razdelku "Zaščita pred računalniškimi virusi". Toda skrbnika za zaščito iSeries morajo bolj skrbeti programi, ki izvajajo nepooblaščene funkcije. Preostale teme tega poglavja opisujejo načine, na katere lahko nekdo z zlobnimi nameni nastavi škodljive programe v vašem sistemu. Teme nudijo nasvete, ki kažejo, kako programom preprečiti izvajanje nepooblaščenih funkcij.

Nasvet za zaščito

Objektno pooblastilo predstavlja vedno prvo linijo zaščite. Če nimate dobrega načrta za zaščito objektov, je vaš sistem nezaščiten. Te informacije razlagajo načine, na katere lahko poskusijo nepooblaščeni uporabniki izkoristiti luknje v zankah sheme objektnih pooblastil.

Zaščita pred računalniškimi virusi

Računalnik, ki je okužen z virusom, vsebuje program, ki lahko spremeni druge programe. Napadalci, ki poskušajo izdelati in razširiti to vrsto virusa, imajo v arhitekturi iSeries, temelječi na objektih, v primerjavi z drugimi računalniškimi arhitekturami težje delo. Na strežniku iSeries lahko uporabite določene ukaze in navodila za delo s posameznimi tipi objektov. S pomočjo datotečnih navodil ne morete spremeniti objekta operacijskega programa (kar počne večina tvorcev virusov), niti ne morete preprosto izdelati programa, ki spremeni drug programski objekt. V to je potrebno vložiti veliko čas, truda in znanja, in imeti dostop do orodij in dokumentacije, ki na splošno ni na voljo.

Toda ker so nove funkcije strežnika iSeries postale na voljo za okolja odprtih sistemov, nekatere funkcije za zaščito strežnikov iSeries, temelječe na objektih, niso več v uporabi. Tako lahko na primer uporabniki integrirani datotečni sistem (IFS) neposredno delajo z nekaterimi objekti v imenikih, kot so tokovne datoteke.

Toda čeprav arhitektura strežnika iSeries otežuje razširitev virusa med programi strežnika iSeries, je lahko strežnik iSeries še vedno prenašalec virusa. Kot datotečni strežnik lahko shranjuje strežnik iSeries programe, ki jih souporabljajo številni uporabniki osebnih računalnikov. Katerikoli od teh programov lahko vsebuje virus, ki ga strežnik iSeries ne

odkrije. Da bi preprečili okužbo PC-jev, priključenih na strežnik iSeries, s to vrsto virusa, morate uporabiti programsko opremo za pregledovanje virusov na PC-jih.

Na strežniku iSeries obstajajo številne funkcije, ki preprečujejo uporabo jezika nižje ravni z zmožnostjo kazalca za spreminjanje operacijskega objekta programa:

- Če v sistemu uporabljate raven zaščite 40 ali več, vključuje zaščita integritete tudi zaščito pred spreminjanjem programskih objektov. Tako ne primer ni mogoče uspešno zagnati programa, ki vsebuje v bloke združena (zaščitena) računalniška navodila.
- Tudi vrednost za preverjanje veljavnosti programov je namenjena za zaščito pri obnovitvi programa, ki je bil shranjen (in morda tudi spremenjen) v drugem sistemu. 2. poglavje knjige *iSeries Security Reference* opisuje funkcije zaščite integritete za raven zaščite 40 in več, vključno z vrednostmi za preverjanje veljavnosti programov.

  Opomba: Vrednost za preverjanje veljavnosti programov ni popolnoma varna in ne predstavlja zamenjave za programe, namenjene opazovanju in ocenjevanju, ki so obnovljeni v sistemu.

Na voljo so tudi številna orodja, ki vam bodo pomagala pri odkrivanju poskusa vpeljave spremenjenega programa v sistem:

- Ukaz CHKOBJITG (Preveri integriteto objekta) lahko uporabite za pregledovanje objektov (operacijskih objektov), ki ustrezajo iskalnim vrednostim, in zagotovite, da ti objekti niso bili spremenjeni. To je podobno funkciji odkrivanja virusov.
- Za nadzorovanje spremenjenih ali obnovljenih programov lahko uporabite funkcijo beleženja zaščite. Vrednosti *PGMFAIL, *SAVRST in *SECURITY za sistemsko vrednost ravni pooblastil nudijo zapise beleženja, ki vam lahko pomagajo pri odkrivanju poskusov vpeljave virusnih programov v sistem. V 9. poglavju in v dodatku F knjige *iSeries Security Reference* boste našli podrobnejše informacije o vrednostih beleženja in postavkah dnevnika beleženja.
- Parameter FRCCRT (Prisili izdelavo) ukaza Spremeni program (CHGPGM) lahko uporabite za vnovično izdelavo kateregakoli programa, ki je bil obnovljen v sistemu. Sistem znova izdela program s pomočjo programske predloge. Če je programski objekt po prevodu spremenjen, sistem na novo izdela spremenjen objekt in ga zamenja. Če vsebuje programska predloga v bloke združena (zaščitena) navodila, sistem ne bo uspel na novo izdelati programa.
- Za vnovično izdelavo kateregakoli programa, obnovljenega v sistemu, lahko uporabite sistemsko vrednost QFRCCVNRST (Prisili pretvorbo pri obnovitvi). Sistem znova izdela program s pomočjo programske predloge. Ta sistemska vrednost nudi številne izbire za programe, ki jih lahko znova izdelate.
- Sistemsko vrednost QVFYOBJRST (Preveri objekte pri obnovitvi) lahko uporabite, da preprečite obnovitev programov, ki nimajo digitalnega podpisa ali veljavnega digitalnega podpisa. Če digitalni podpis ni veljaven, to pomeni, da je bil od takrat, ko ga je podpisal njegov razvijalec, spremenjen. Na voljo so API-ji, ki omogočajo, da podpišete lastne programe, shranjevalne datoteke in tokovne datoteke.

Podrobnejše informacije o podpisovanju in njegovi uporabi za zaščito sistema pred napadi lahko najdetev razdelku“Podpisovanje objektov” na strani 78.

Nadzorovanje uporabe prevzetega pooblastila

Na strežniku iSeries lahko izdelate program, ki prevzame pooblastilo lastnika programa. To pomeni, da ima vsak uporabnik, ki zažene program, ista pooblastila (zasebna in posebna pooblastila) kot profil uporabnika, ki je lastnik programa.

Če prevzeto pooblastilo pravilno uporabljate, je lahko zelo koristno orodje za zaščito. “Izboljšanje krmiljenja menijskega dostopa z zaščito objektov” na strani 40 na primer opisuje, kako združiti prevzeto pooblastilo in menije kot pomoč, ki presega krmiljenje menijskega dostopa. S prevzetim pooblastilom lahko zaščitite pomembne datoteke pred spreminjanjem z nepooblaščenimi uporabniškimi programi, pri tem pa za te datoteke še vedno omogočite poizvedbe.

Kot skrbnik za zaščito morate zagotoviti, da je prevzeto pooblastilo pravilno uporabljeno:

- Programi naj prevzemajo pooblastilo profila uporabnika, ki ima samo toliko pooblastil, kot je zahtevano za izvajanje potrebnih funkcij. Še posebej pazite pri programih, ki prevzamejo pooblastilo profila uporabnika s posebnim pooblastilom *ALLOBJ ali profila, ki je lastnik pomembnih objektov.
- Programi, ki prevzamejo pooblastilo, naj imajo določeno, omejeno delovanje, in naj ne nudijo splošne zmožnosti za vnašanje ukazov.
- Programe, ki prevzamejo zaščite, je potrebno pravilno zaščititi.
- Prekomerna uporaba prevzetega pooblastila ima lahko negativen vpliv na zmogljivost sistema. Da bi se izognili težavam v zmogljivosti, v 5. poglavju knjige *iSeries Security Reference* preglejte diagrame poteka za preverjanje pooblastil in predloge za uporabo prevzetega pooblastila.

Možnosti menija SECBATCH:
1 *za takojšnjo predložitev* **40 za uporabo planerja opravil**

Ukaz PRTADPOBJ (Natisni objekte s prevzemom) (možnost 21 na meniju SECTOOLS) lahko uporabite kot pomoč pri nadzorovanju uporabe prevzetega pooblastila v sistemu.

Poročilo prikaže posebna pooblastila podanega profila uporabnika, programe, ki prevzamejo pooblastilo profila uporabnika, kot tudi naprave ASP, ki uporabljajo pooblastila profila. Ko vzpostavite bazo informacij, lahko redno tiskate različice poročil o spremembah v objektih s prevzemom. Ta poročila navedejo nove programe, ki prevzamejo pooblastilo, in programe, v katerih so bile od zadnje izvedbe poročila opravljene spremembe v prevzemu pooblastil.

Če sumite na zlorabo prevzetega pooblastila v sistemu, lahko nastavite sistemsko vrednost QAUDLVL tako, da vključuje *PGMADP. Če je ta vrednost aktivna, izdela sistem postavko dnevnika beleženja vsakič, ki nekdo zažene ali zaustavi program, ki prevzame pooblastilo. Postavka vključuje ime uporabnika, ki je zagnal program in ime programa.

Omejitev uporabe prevzetega pooblastila

Ko se zažene program iSeries, lahko s pomočjo prevzetega pooblastila pridobi dostop do objektov na dva različna načina:

- Sam program lahko prevzame pooblastilo njegovega lastnika. To je podano v parametru profila uporabnika (USRPRF) programa ali servisnega programa.
- Program lahko uporabi (nasledi) prevzeto pooblastilo iz prejšnjega programa, ki je še vedno v klicnem skladu opravila. Program lahko prevzame prevzeto pooblastilo iz prejšnjih programov, tudi če sam program ne prevzame pooblastila. Uporaba parametra prevzetega pooblastila (USEADPAUT) programa ali servisnega programa nadzoruje, ali nasledi program prevzeto pooblastilo iz prejšnjih programov v skladu programov.

Sledi zgled uporabe prevzetega pooblastila iz prejšnjih programov.

Denimo, da ima profil uporabnika ICOWNER pooblastilo *CHANGE za datoteko ITEM in da je javno pooblastilo za datoteko ITEM nastavljeno na *USE. Noben drug profil uporabnika nima izrecno definiranega pooblastila za datoteko ITEM. Tabela 14 kaže atribute za tri programe, ki uporabljajo datoteko ITEM:

Tabela 14. Zgled za uporabo prevzetega pooblastila (USEADPAUT)

Ime programa	Lastnik programa	Vrednost USRPRF	Vrednost USEADPAUT
PGMA	ICOWNER	*OWNER	*YES
PGMB	ICOWNER	*USER	*YES
PGMC	ICOWNER	*USER	*NO

Zgled 1–prevzem pooblastila:
1. USERA zažene program PGMA.
2. Program PGMA poskusi odpreti datoteko ITEM s funkcijo ažuriranja.

Rezultat: poskus ne uspe. USERA ima dostop *CHANGE do datoteke ITEM, ker PGMA prevzame pooblastilo od ICOWNER.

Zgled 2–uporaba prevzetega pooblastila:
1. USERA zažene program PGMA.
2. Program PGMA pokliče program PGMB.
3. Program PGMB poskusi odpreti datoteko ITEM s funkcijo ažuriranja.

Rezultat: poskus ne uspe. Čeprav program PGMB ne prevzame pooblastila (*USRPRF je *USER), omogoča uporabo prejšnjega prevzetega pooblastila (*USEADPAUT je *YES). Program PGMA je še vedno v skladu programov. Zato dobi USERA dostop *CHANGE do datoteke ITEM, ker PGMA prevzame pooblastilo od ICOWNER.

Zgled 3–Brez uporabe prevzetega pooblastila:
1. USERA zažene program PGMA.
2. Program PGMA pokliče program PGMC.
3. Program PGMC poskusi odpreti datoteko ITEM s funkcijo ažuriranja.

Rezultat: napaka v pooblastilu. Program PGMC ne prevzame pooblastila. Program PGMC prav tako ne dopušča uporabe prevzetega pooblastila iz prejšnjih programov. Čeprav je PGMA še vedno v klicnem skladu, njegovo prevzeto pooblastilo ni uporabljeno.

Preprečevanje uporabe prevzetih pooblastil za nove programe

Posredovanje prevzetega pooblastila novejšim program v skladu nudi izkušenemu programerju možnost za izdelavo programa trojanskega konja. Program trojanskega konja lahko iz prejšnjih programov v skladu pridobi pooblastilo, ki ga potrebuje za povzročitev škode. Da bi to preprečili, lahko omejite uporabnike, ki lahko izdelajo programe, ki uporabljajo prevzeto pooblastilo prejšnjih programov.

Ko izdelate nov program, sistem samodejno nastavi parameter USEADPAUT na *YES. Če ne želite, da program nasledi prevzeto pooblastilo, morate uporabiti ukaz CHGPGM (Spremeni program) ali CHGSRVPGM (Spremeni servisni program), s katerim nastavite parameter USEADPAUT na *NO.

Za krmiljenje, kdo lahko izdela programe, ki nasledijo prevzeto pooblastilo, lahko uporabite pooblastitveni seznam in sistemsko vrednost za prevzem pooblastila (QUSEADPAUT). Če podate v sistemski vrednosti QUSEADPAUT ime pooblastitvenega seznam, sistem uporabi ta pooblastitveni seznam za določitev, kako izdelati nove programe.

Ko uporabnik izdela program ali servisni program, preveri sistem pooblastilo uporabnika za pooblastitveni seznam. Če ima uporabnik pooblastilo *USE, je parameter USEADPAUT za nov program nastavljen na *YES. Če uporabnik nima pooblastila *USE, je parameter USEADPAUT nastavljen na *NO. Pooblastilo uporabnika za pooblastitveni seznam ne more izhajati iz prevzetega pooblastila.

Pooblastitveni seznam, ki ga podate v sistemski vrednosti QUSEADPAUT, prav tako krmili, ali lahko uporabnik s pomočjo ukaza CHGxxx nastavi vrednost USEADPAUT za program ali servisni program.

Opombe:

1. Ime pooblastitvenega seznam ni nujno QUESADPAUT. Izdelate lahko pooblastitveni seznam z drugim imenom in ga nato podate za sistemsko vrednost QUSEADPAUT. V ukazih v tem zgledu zamenjajte ime z vašim pooblastitvenim seznamom.
2. Sistemska vrednost QUSEADPAUT ne vpliva na obstoječe programe v sistemu. S pomočjo ukaza CGHPGM ali CHGSRVPGM nastavite parameter USEADPAUT za obstoječe programe.

Bolj omejevalno okolje: Če želite, da večina uporabnikov izdela nove programe s parametrom USEADPAUT, nastavljenim na *NO, naredite naslednje:

1. Za nastavitev javnega pooblastila za pooblastitveni seznam na *EXCLUDE vpišite naslednje:

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

2. Za nastavitev določenih uporabnikov za izdelavo programov, ki uporabljajo prevzeto pooblastilo prejšnjih programov, vpišite naslednje:

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

Manj omejevalno okolje: Če želite, da večina uporabnikov izdela nove programe s parametrom USEADPAUT, nastavljenim na *YES, naredite naslednje:

1. Javno pooblastilo za pooblastitveni seznam pustite nastavljeno na *USE.
2. Če želite preprečiti, da bi določeni uporabniki izdelali programe, ki uporabljajo prevzeto pooblastilo prejšnjih programov, vpišite naslednje:

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

Nadzorovanje uporabe programov prožil

DB2 UDB nudi zmožnost za povezavo programov prožil z datotekami baze podatkov. Zmožnost za programe prožil je v splošni uporabi industrije upravljalnikov baz podatkov z močnimi funkcijami.

Če povežete program prožila z datoteko baze podatkov, podate, kdaj se zažene program prožila. Tako lahko na primer nastavite datoteko naročil stranke tako, da zažene program prožila vsakič, ko je v datoteko dodan nov zapis. Ko neplačani dolgovi stranke presežejo kreditno omejitev, lahko program prožila natisne opozorilno pismo za stranko in pošlje sporočilo vodji za kredite.

Programi prožil predstavljajo produktiven način za nudenje funkcij aplikacij in za upravljanje informacij. Toda tudi nekomu z nepoštenimi nameni omogočajo izdelavo “trojanskega konja” v sistemu. Uničevalen program lahko čaka na zagon ob določenem dogodku v datoteki baze podatkov v sistemu.

Opomba: V zgodovini je bil trojanski konj velik, prazen lesen konj, v katerem so bili grški vojaki. Ko so konja pripeljali znotraj zidov Troje, so vojaki splezali iz konja in začeli bitko s Trojanci. V računalniškem svetu se ime trojanski konj pogosto uporablja za program, ki skriva uničevalne funkcije.

Možnosti menija SECBATCH:
27 *za takojšnjo predložitev* **66** *za uporabo planerja opravil*

Ko dobite sistem, je zmožnost za dodajanje programa prožila v datoteko baze podatkov omejena. Če skrbno upravljate objektna pooblastila, značilen uporabnik ne bo imel zadosti pooblastil za dodajanje programa prožila v datoteko baze podatkov. (V dodatku D knjige *iSeries Security Reference* boste našli zahtevana pooblastila ali vse ukaze, vključno z ukazom ADDPFTRG (Dodaj prožilo fizične datoteke).

S pomočjo ukaza PRTTRGPGM (Natisni programe prožil) lahko natisnete seznam vseh programov prožil v podani knjižnici ali v vseh knjižnicah.

Začetno poročilo lahko uporabite kot osnovo za ocenitev programov prožil, ki že obstajajo v sistemu. Nato lahko redno tiskate poročilo o spremembah in pregledate, kateri novi programi prožil so bili dodani v sistem.

Pri pregledu programov prožil pazite na naslednje:

- Kdo je izdelal program prožila? Za določitev tega lahko uporabite ukaz DSPOBJD (Prikaži opis objekta).
- Kaj dela program? Za določitev tega si morate ogledati izvorni program ali se pogovoriti z njegovim tvorcem. Ali program prožila na primer preveri, kdo je uporabnik? Morda čaka program prožila na določenega uporabnika (QSECOFR), da bi omogočil dostop do sistemskih sredstev.

Ko vzpostavite bazo informacij, lahko redno tiskate poročilo o spremembah in nadzorujete nove programe prožil, ki so bili dodani v sistem.

Preverjanje skritih programov

Programi prožil ne predstavljajo edinega načina za vnos trojanskega konja v sistem. Programi prožil so primer **izhodnega programa**. Ko pride do določenega dogodka, kot je na primer ažuriranje datoteke v primeru programa prožila, zažene sistem izhodni program, ki je povezan s tem dogodkom.

Tabela 15 opisuje druge zglede izhodnih programov, ki so lahko v vašem sistemu. Iste načine uporabite za ocenitev uporabe in vsebine teh izhodnih programov, ki jih uporabljate za programe prožil.

Opomba: Tabela 15 ni celoten seznam vseh možnih izhodnih programov.

.

Tabela 15. Sistemsko podani izhodni programi

Ime programa	Kdaj se program zažene
Uporabniško podano ime v omrežnem atributu DDMACC.	Ko uporabnik poskusi odpreti datoteko DDM v sistemu ali vzpostavi povezavo DRDA.
Uporabniško podano ime v omrežnem atributu PCSACC.	Ko poskusi uporabnik uporabiti funkcije Client Accessa s pomočjo izvirnih objektov za dostop do objektov v sistemu.

Tabela 15. Sistemsko podani izhodni programi (nadaljevanje)

Ime programa	Kdaj se program zažene
Uporabniško podano ime v sistemski vrednosti QPWDVLDPGM	Ko uporabnik zažene funkcijo za spreminjanje gesla.
Uporabniško podano ime v sistemski vrednosti QRMTSIGN.	Ko se uporabnik poskusi interaktivno prijaviti iz oddaljenega sistema.
QSYS/QEZUSRCLNP	Ko se zažene funkcija samodejnega čiščenja.
Uporabniško podano ime v parametru EXITPGM ukaza CHGBCKUP.	Ko uporabite funkcijo varnostnega kopiranja Operacijskega pomočnika.
Uporabniško podana imena v ukazu CRTPRDLOD.	Preden shranite, obnovite ali zbrišete izdelek, izdelan z ukazom, ali za tem.
Uporabniško podano ime parametra DFTPGM v ukazu CHGMSGD.	Če je za sporočilo podan privzet program, sistem zažene program pri izdaji sporočila. Ker obstaja v značilnem sistemu veliko število opisov sporočil, je uporabo privzetih programov težko nadzorovati. Če želite preprečiti javnim uporabnikom dodajanje privzetih programov za sporočila, lahko nastavite javno pooblastilo za datoteke sporočil (objekti *MSGF) na *USE.
Uporabniško podano ime v parametru FKEYPGM ukaza STREML3270.	Ko uporabnik pritisne funkcijsko tipko med emulacijsko sejo naprave 3270. Sistem vrne nadzor emulacijski seji naprave 3270, ko se izhodni program zaključi.
Uporabniško podano ime v parametru EXITPGM ukazov nadzornika zmogljivosti	Za obdelavo podatkov, ki jih zbirajo naslednji ukazi: STRPFRMON, ENDPFRMON, ADDPFRCOL in CHGPFRCOL. Program se zažene, ko se konča zbirka podatkov.
Uporabniško podano ime v parametru EXITPGM ukaza RCVJRNE.	Za vsako postavko dnevnika ali skupino postavk dnevnikov, prebranih iz podanega dnevnika in sprejemnikov dnevnikov.
Uporabniško podano ime v API-ju QTNADDCR.	Med operacijo potrditve (COMMIT) ali povrnitve (ROLLBACK).
Uporabniško podana imena v API-ju QHFRGFS.	Za izvedbo funkcij datotečnega sistema.
Uporabniško podano ime v parametru opisa tiskalne naprave.	Za določitev, kaj natisniti na ločevalni strani pred vmesno datoteko ali tiskalnim opravilom ali za njima.
QGPL/QUSCLSXT	Ko se datoteka baze podatkov zapre in omogoči zajetje informacij o uporabi datoteke.
Uporabniško podano ime v parametru FMTSLR logične datoteke.	Ko vnesete zapis v datoteko baze podatkov in ime formata zapisa ni vključeno v programski jezik visoke ravni. Program izbiralca prejme zapis kot vhodni podatek, določi uporabljen format zapisa in ga vrne bazi podatkov.
Uporabniško podano ime v sistemski vrednosti QATNPGM, v parametru ATNPGM profila uporabnika ali v parametru PGM ukaza SETATNPGM.	Ko uporabnik pritisne tipko Attention.
Uporabniško podano ime v parametru EXITPGM ukaza TRCJOB.	Pred zagonom postopka sledenja opravilu.

Za ukaze, ki omogočajo, da podate izhodni program, morate zagotoviti, da privzeta vrednost ukaza ni bila spremenjena tako, da podaja izhodni program. Zagotoviti morate tudi, da javno pooblastilo za te ukaze ne zadostuje za spreminjanje privzetih vrednosti ukazov. Ukaz CHGCMDDFT zahteva pooblastilo *OBJMGT za ukaz. Za izvajanje ukaza ne potrebujete pooblastila *OBJMGT.

Vrednotenje registriranih izhodnih programov

S pomočjo sistemske funkcije za registriranje lahko registrirate izhodne programe, ki se zaženejo ob določenih dogodkih. Če želite izpisati registracijske informacije v sistemu, vpišite WRKREGINF OUTPUT(*PRINT). Slika 8 kaže zgled poročila:

```
              Delo z registracijskimi informacijami
Izhodna točka. . . . . . . . . . . . . :   QIBM_QGW_NJEOUTBOUND
Format izhodne točke . . . . . . . . . :   NJEO0100
Registrirana izhodna točka . . . . . . :   *YES
Omogoči deregistracijo . . . . . . . . :   *YES
Naj. št. izhodnih programov  . . . . . :   *NOMAX
Trenutno št. izhodnih programov  . . . :   0
Vnaprejšnja obdelava za dodajanje. . . :   *NONE
  Knjižnica. . . . . . . . . . . . . . :
  Format . . . . . . . . . . . . . . . :
Vnaprejšnja obdelava za odstranitev. . :   *NONE
  Knjižnica. . . . . . . . . . . . . . :
  Format . . . . . . . . . . . . . . . :
Vnaprejšnja obdelava za pridobivanje . :   *NONE
  Library  . . . . . . . . . . . . . . :
```

Slika 8. Delo z registracijskimi informacijami - zgled

Za vsako izhodno točko v sistemu kaže poročilo, ali je trenutno registriran kakšen izhodni program. Če ima izhodna točka trenutno registrirane programe, lahko z različice zaslona WRKREGINF izberete možnost 8 (Prikaži program) in prikažete informacije o programih:

```
                    Delo z registracijskimi informacijami

Vpišite možnosti in pritisnite Enter.
5=Prikaži izhodno točko    8=Delo z izhodnimi programi

                           Format
     Izhodna               izhodne
Mož  točka                 točke     Registriran Besedilo
     QIBM_QGW_NJEOUTBOUND  NJEO0100     *YES     Izhodna postavka omrežnega opravila
8    QIBM_QHQ_DTAQ         DTAQ0100     *YES     Strežnik izvorne pod. čakalne vrste
     QIBM_QLZP_LICENSE     LICM0100     *YES     Izvirni strežnik za upravljanje licenc
     QIBM_QMF_MESSAGE      MESS0100     *YES     Izvirni strežnik sporočil
     QIBM_QNPS_ENTRY       ENTR0100     *YES     Omrežni tiskalni strežnik - postavka
     QIBM_QNPS_SPLF        SPLF0100     *YES     Omrežni tiskalni strežnik - spool
     QIBM_QNS_CRADDACT     ADDA0100     *YES     Dejavnost dodajanja opisa CRQ
     QIBM_QNS_CRCHGACT     CHGA0100     *YES     Dejavnost spreminjanja opisa CRQ
```

Za vrednotenje teh izhodnih programov uporabite način, ki ga uporabljate za druge izhodne programe in programe prožil.

Preverjanje terminiranih programov

iSeries nudi številne načine za terminiranje opravil, ki se lahko izvajajo kasneje, vključno s Planerjem opravil. Ti načini običajno ne predstavljajo luknje v zaščiti, ker mora imeti uporabnik, ki načrtuje opravila, isto pooblastilo, ki je zahtevano za predložitev opravila v paket.

Vendar pa občasno preverite opravila, ki so terminirana za v prihodnje. Nezadovoljen uporabnik, ki ni več zaposlen v podjetju, lahko s tem načinom načrtuje nesrečo.

Omejitev zmožnosti shranitve in obnovitve

Večini uporabnikov ni potrebno shranjevati in obnavljati objektov v sistemu. Ukazi za shranjevanje nudijo zmožnost za kopiranje pomembnih sredstev vašega podjetja na nosilec ali v drug sistem. Večina ukazov za shranjevanje podpira shranjevalne datoteke, ki jih lahko pošljete v drug sistem (z uporabo datotečnega ukaza SNDNETF) brez dostopa do nosilca ali shranitvene/obnovitvene naprave.

Ukazi za obnovitev nudijo zmožnost za obnovitev nepooblaščenih objektov v sistemu, kot so programi, ukazi in datoteke. Z uporabo shranjevalnih datotek lahko tudi obnovite informacije brez dostopa do nosilca ali shranitvene/obnovitvene naprave. Shranjevalne datoteke lahko pošljete iz drugega sistema z ukazom SNDNETF ali s funkcijo FTP.

Sledi nekaj predlogov za omejitev operacij shranitve in obnovitve v sistemu:

- Nadzorujte, kateri uporabniki imajo posebno pooblastilo *SAVSYS. Posebno pooblastilo *SAVSYS omogoča uporabniku, da shrani in obnovi objekte, tudi če nima ustreznega pooblastila do objektov.
- Nadzorujte fizičen dostop do shranitvenih in obnovitvenih naprav.
- Omejite dostop do shranitvenih in obnovitvenih ukazov. Ko namestite licenčne programe OS/400, je javno pooblastilo za ukaze RSTxxx nastavljeno na *EXCLUDE. Javno pooblastilo za ukaze SAVxxx je *USE. Razmislite o spremembi javnega pooblastila za ukaze SAVxxx v *EXCLUDE. Previdno omejite uporabnike, ki jim dodelite pooblastilo za ukaze RSTxxx.
- S pomočjo sistemske vrednosti QALWOBJRST omejite obnovitev programe za stanje sistema, programe, ki prevzamejo pooblastilo in objekte, v katerih je prišlo do napak pri preverjanju veljavnosti.
- S pomočjo sistemske vrednosti QVFYOBJRST krmilite objekte, namenjene za obnovitev v sistemu..
- S pomočjo sistemske vrednosti QFRCCVNRST nadzorujte vnovično izdelavo določenih objektov, za katere se izvaja obnavljanje v sistemu.
- Za nadzorovanje operacij obnovitve uporabite beleženje zaščite. Vključite sistemsko vrednost *SAVRST v QAUDLVL in občasno natisnite zapise beleženja, ki jih izdelajo operacije obnovitve. (V 9. poglavju in v dodatku F knjige *iSeries Security Reference* boste našli podrobnejše informacije o operacijah postavk beleženja.).

Preverjanje uporabniških objektov v zaščitenih knjižnicah

Vsako opravilo strežnika iSeries ima seznam knjižnic. Seznam knjižnic določa vrstni red, v katerem išče sistem objekt, če ime knjižnice ni podano z imenom objekta. Če na primer pokličete program, ne da bi podali, kje se nahaja, sistem preišče seznam knjižnic v podanem vrstnem redu in zažene prvo kopijo programa, ki ga najde.

V knjigi *iSeries Security Reference* boste našli podrobnejše informacije o luknjah v zaščiti na seznamih knjižnic in o klicanju programov brez podanega imena knjižnice (to se imenuje **nekvalificiran klic**). V njej boste našli tudi predloge za nadzorovanje vsebine seznamov knjižnic in zmožnost za spreminjanje seznamov sistemskih knjižnic.

Da bi se sistem pravilno izvajal, morajo biti določene sistemske knjižnice, kot sta QSYS in QGPL, na seznamu knjižnic za vsako opravilo. Za nadzorovanje, kdo lahko dodaja programe tem knjižnicam, uporabite objektno pooblastilo. To vam bo pomagalo preprečiti, da bi nekdo v eno od teh knjižnic shranil lažni program, ki ima isto ime kot program, ki je prikazan v knjižnici kasneje na seznamu knjižnic.

Preveriti morate tudi, kdo ima pooblastilo za ukaz CHGSYSLIBL in nadzorovanje zapisov SV v dnevniku beleženja zaščite. Nepošten uporabnik lahko postavi knjižnico na seznamu knjižnic pred QSYS in povzroči, da izvajajo uporabniki nepooblaščene ukaze, ki imajo isto ime kot IBM-ovi ukazi.

Možnosti menija SECBATCH:
28 *za takojšnjo predložitev* **67** *za uporabo planerja opravil*

S pomočjo ukaza PRTUSROBJ (Natisni uporabniške objekte) lahko natisnete seznam uporabniških objektov (objekti, ki jih ni izdelal IBM) v podani knjižnici. Nato lahko ocenite programe na seznamu in določite, kdo jih je izdelal in kakšna je njihova funkcija.

Uporabniški objekti, ki niso programi, lahko predstavljajo tudi luknjo v zaščiti, če so shranjeni v sistemskih knjižnicah. Če na primer zapiše program zaupne podatke v datoteko, katere ime ni kvalificirano, je lahko program prevaran, tako da odpre nepravo različico te datoteke v sistemski knjižnici.

Poglavje 11. Preprečevanje in odkrivanje napadov hekerjev

Te informacije so sestavljene iz različnih vrst nasvetov, ki vam bodo pomagali pri odkrivanju možnih lukenj v zaščiti in vdiralcev v sistem.

Fizična zaščita

Sistemska enota predstavlja pomembno poslovno sredstvo in možna vrata v vaš sistem. Nekatere sistemske komponente znotraj sistema so majhne in veliko vredne. Sistemska enota mora biti na varnem mestu, da preprečite, da bi kdorkoli odstranil vredne sistemske komponente.

Sistemska enota vsebuje nadzorno ploščo, ki nudi izvajanje osnovnih funkcij brez delovne postaje. S pomočjo nadzorne plošče lahko naredite naslednje:

- zaustavite sistem
- zaženete sistem
- naložite operacijski sistem
- zaženete servisne funkcije

Vse te dejavnosti so lahko moteče za uporabnike sistema in predstavljajo tudi možno luknjo v zaščiti vašega sistema. Za nadzor nad tem, kdaj bodo te dejavnosti dovoljene, lahko uporabite ključavnico, ki ste jo dobili s sistemom. Če želite preprečiti uporabo nadzorne plošče, postavite ključavnico v položaj Zaščiteno, odstranite ključ in ga shranite na varno mesto.

Opombe:

1. Če morate v sistemu opraviti oddaljeni IPL ali oddaljeno diagnosticiranje, boste najbrž morali za ključavnico izbrati drugo nastavitev. V temi Prvi koraki Informacijskega centra iSeries boste našli podrobnejše informacije o nastavitvah ključavnice (podrobnosti poiščite v razdelku “Predpogoji in s tem povezane informacije” na strani xii).
2. Ključavnica ni vključena v vse sistemske modele kot standardna možnost.

Nadzorovanje dejavnosti profila uporabnika

Profili uporabnikov omogočajo vstop v sistem. Parametri v profilu uporabnika določajo uporabnikov okolje in značilnosti zaščite uporabnika. Kot skrbnik sistema morate nadzorovati in beležiti spremembe, ki so opravljene v profilih uporabnikov v sistemu.

Beleženje zaščite lahko nastavite tako, da sistem zabeleži zapis sprememb v profilih uporabnikov. S pomočjo ukaza DSPAUDJRNE lahko natisnete poročilo o teh spremembah.

Izdelate lahko tudi izhodne programe, ki ocenijo zahtevana dejanja v profilih uporabnikov. Tabela 16 kaže izhodne točke, ki so na voljo za ukaze profilov uporabnikov.

Tabela 16. Izhodne točke za dejavnost profila uporabnika

Ukaz profila uporabnika	Ime izhodne točke
CRTUSRPRF (Izdelaj profil uporabnika)	QIBM_QSY_CRT_PROFILE
CHGUSRPRF (Spremeni profil uporabnika)	QIBM_QSY_CHG_PROFILE
DLTUSRPRF (Zbriši profil uporabnika)	QIBM_QSY_DLT_PROFILE
RSTUSRPRF (Obnovi profil uporabnika)	QIBM_QSY_RST_PROFILE

Izhodni program lahko na primer poišče spremembe, ki lahko povzročijo, da uporabnik izvaja nepooblaščeno različico programa. Te spremembe lahko dodelijo drugačen opis knjižnice ali novo tekočo knjižnico. Izhodni program lahko obvesti čakalno vrsto sporočil ali opravi določeno dejanje (kot je na primer sprememba ali onemogočitev profila uporabnika) na osnovi informacij, ki jih prejme izhodni program.

V knjigi *iSeries Security Reference* lahko najdete podrobnejše informacije o izhodnih programih za dejanja profilov uporabnikov.

Podpisovanje objektov

Vsi zaščitni varnostni ukrepi so brez pomena, če jih lahko nekdo zaobide, tako da v sistem vpelje ponarejene podatke. Strežnik iSeries vsebuje številne vgrajene funkcije, ki preprečujejo nalaganje vdiralske programske opreme v sistem in odkrivanje takšne programske opreme. Ena izmed tehnik, dodana v V5R1, je podpisovanje objektov.

Podpisovanje objektov je izvedba koncepta šifriranja na strežniku iSeries, sicer imenovana ″digitalni podpisi″. Ideja je zelo preprosta: ko je proizvajalec programske opreme pripravljen dostaviti programsko opremo strankam, jo ″podpiše″. Ta podpis ne zagotavlja, da programska oprema izvaja določene funkcije, nudi pa način, ki omogoča, da preverite, ali izvira programska oprema v resnici od proizvajalca, ki jo je podpisal, in da programska oprema od izdelave in podpisa ni bila spremenjena. To je še posebej pomembno, če je bila programska oprema prenesena prek interneta ali je shranjena na nosilcu, za katerega menite, da je bil lahko spremenjen.

Uporaba digitalnih podpisov nudi večji nadzor nad tem, katero programsko opremo lahko naložite v sistem, in odkrivanjem sprememb, ko je oprema že naložena. Nova sistemska vrednost QVFYOBJRST (Preveri obnovitev objekta) nudi mehanizem za nastavitev omejitvenega načela, ki zahteva, da vso programsko opremo, ki jo naložite v sistem, podpišejo znani viri programske opreme. Izberete lahko tudi bolj odprto načelo in poenostavite preverjanje podpisov.

Vso programsko opremo OS/400, kot tudi programsko opremo za komponente in licenčne programe strežnika iSeries, je podpisal izvor, ki mu sistem zaupa. Ti podpisi pomagajo sistemu, da zaščiti svojo integriteto, in so preverjeni pri uveljavljanju popravkov v sistemu, da zagotovijo, da popravek izvira iz izvora, ki mu sistem zaupa, in da na poti ni bil spremenjen. Te podpise je mogoče tudi preveriti, ko je programska oprema v sistemu. Ukaz CHKOBJITG (Preveri integriteto objekta) smo razširili, tako da poleg drugih funkcij integritete objektov v sistemu preverja tudi podpise. Tudi Upravljalnik digitalnih potrdil vsebuje okna, ki jih lahko uporabite za preverjanje podpisov objektov, vključno z objekti v operacijskem sistemu.

Ravno tako kot je podpisan operacijski sistem, lahko s pomočjo digitalnih podpisov zaščitite tudi integriteto programske opreme, ki je bistvenega pomena za vaše poslovanje. Kupite lahko programsko opremo, ki jo je podpisal ponudnik programske opreme, ali podpišete programsko opremo, ki ste jo kupili ali napisali. Del načela zaščite je torej občasna uporaba ukaza CHKOBJITG ali Upravljalnika digitalnih potrdil, s katerima preverite, ali so podpisi v programski opremi še vedno veljavni in da objekti od podpisa niso bili spremenjeni. Nadalje lahko zahtevate, da vso programsko opremo, ki jo obnovite v sistemu, podpišete vi ali znan izvor. Toda ker večina programske opreme za strežnik iSeries, ki je ne proizvede IBM, trenutno ni podpisana, je lahko to načelo preveč omejujoče za vaš sistem. Novi digitalni podpisi nudijo prožnost pri izbiranju, kako najbolje zaščititi integriteto programske opreme.

Digitalni podpisi, ki ščitijo programsko opremo, predstavljajo samo enega izmed načinov za uporabo digitalnih potrdil. Dodatne informacije o upravljanju digitalnih potrdil lahko najdete v temi Upravljanje digitalnih potrdil Informacijskega centra (podrobnosti poiščite v temi “Predpogoji in s tem povezane informacije” na strani xii).

Nadzorovanje opisov podsistemov

Ko na strežniku iSeries zaženete podsistem, sistem izdela delovno okolje za vnos in izvajanje sistema. Opis podsistema definira, kakšno je videti to okolje, in zato lahko predstavlja tudi priložnost za zlonamerne uporabnike. Vdiralec lahko na primer s pomočjo opisa podsistema samodejno zažene program ali omogoči prijavo brez profila uporabnika.

Ko zaženete ukaz Prekliči javno pooblastilo (RVKPUBAUT), nastavi sistem javno pooblastilo za ukaze opisov podsistemov na *EXCLUDE. S tem preprečite, da bi uporabniki brez posebnih pooblastil (brez posebnega pooblastila *ALLOBJ) spreminjali ali izdelovali opise podsistemov.

V temah, ki sledijo, boste našli predloge za pregled opisov podsistemov, ki trenutno obstajajo v sistemu. Za izdelavo seznama vseh opisov podsistemov lahko uporabite ukaz WRKSBSD (Delo z opisi podsistemov). Če s seznama izberete možnost 5 (Prikaži), se prikaže meni za izbran opis sistema. Ta prikaže seznam delov okolja podsistema.

Za prikaz podrobnosti o delih izberete možnosti. Z ukazom CHGSBSD (Spremeni opis podsistema) spremenite prvi dve postavki menija. Če želite spremeniti ostale postavke, uporabite ustrezen ukaz za dodajanje, odstranitev ali spreminjanje tipa postavke. Če želite na primer spremeniti postavko delovne postaje, uporabite ukaz CHGWSE (Spremeni postavko delovne postaje).

V knjigi *Work Management* boste našli podrobnejše informacije o delu z opisi podsistemov. Navaja tudi naložene vrednosti za IBM-ove opise podsistemov.

Postavke opravil s samodejnim zagonom

Postavka opravila s samodejnim zagonom vsebuje ime opisa opravila. Opis opravila lahko vsebuje podatke zahteve (RQSDTA), ki povzroči zagon programa ali ukaza. RQSDTA je lahko na primer CALL LIB1/PROGRAM1. Pri vsakem zagonu podsistema bo sistem zagnal program PROGRAM1 v knjižnici LIB1.

Preglejte postavke opravil s samodejnim zagonom in povezane opise opravil. Razumeti morate funkcije vseh programov, ki se zaženejo samodejno pri zagonu podsistema.

Imena in tipi delovnih postaj

Ko se podsistem zažene, dodeli vse nedodeljene delovne postaje, ki so navedene (posebej ali na splošno) v njegovih postavkah za imena in tipe delovnih postaj. Ko se uporabnik prijavi, se prijavi v podsistem, ki je dodelil delovno postajo.

Postavka delovne postaje pove, kateri opis opravila bo uporabljen pri zagonu opravila na tej delovni postaji. Opis opravila lahko vsebuje podatke zahteve, ki povzroči izvajanje programa ali ukaza. Parameter RQSDTA je lahko na primer CALL LIB1/PROGRAM1. Vsakič, ko se uporabnik prijavi na delovno postajo v tem podsistemu, sistem zažene PROGRAM1 v LIB1.

Preglejte postavke delovne postaje in z njimi povezane opise opravil. Zagotovite, da ni nihče dodal ali ažuriral postavk za izvajanje programov, ki jih niste določili.

Postavka delovne postaje lahko podaja tudi privzeti profil uporabnika. Za določene konfiguracije podsistemov to omogoča, da se nekdo prijavi samo s preprostim pritiskom na tipko Enter. Če v sistemu uporabljate raven zaščite (sistemska vrednost QSECURITY), ki je manj kot 40, preglejte privzete uporabnike v postavkah delovne postaje.

Postavke čakalne vrste opravil

Ko se podsistem zažene, dodeli vse nedodeljene čakalne vrste opravil, ki so navedene v opisu podsistema. Postavke čakalne vrste opravil ne predstavljajo neposredne luknje v zaščiti, toda nudijo možnost, da se nekdo poigra z zmogljivostjo sistema, tako da povzroči izvajanje opravil v nenameravnih okoljih.

Občasno preglejte opise čakalne vrste opravil v opisih podsistemov in preverite, ali se izvajajo paketna opravila tam, kjer pričakujete.

Postavke usmerjanja

Postavka usmerjanja definira, kaj naredi opravilo, ko vstopi v podsistem. Podsistem uporablja postavke usmerjanja za vse tipe opravil: paketna, interaktivna in komunikacijska opravila. Postavka usmerjanja podaja naslednje:

- Razred opravila. Tako kot postavke čakalne vrste opravil lahko tudi razred, ki je povezan z opravilom, vpliva na njegovo delovanje, vendar ne predstavlja luknje v zaščiti.
- Program, ki se zažene pri zagonu opravila. Preglejte postavke usmerjanja in zagotovite, da ni nihče dodal ali ažuriral postavk za izvajanje programov, ki jih niste določili.

Komunikacijske postavke in imena oddaljenih mest

Ko komunikacijska postavka vstopi v vaš sistem, sistem določi način izvajanja komunikacijskega opravila s pomočjo komunikacijskih postavk in postavk imen oddaljenih mest v aktivnem podsistemu. Te postavke poiščite na naslednjih mestih:

- Komunikacijska opravila lahko izvajajo vsi podsistemi. Če podsistem, ki ste ga določili za komunikacije, ni aktiven, lahko najde opravilo, ki poskuša vstopiti v vaš sistem, drugo postavko v drugem opisu podsistema, ki ustreza njegovim potrebam. Pregledati morate postavke v vseh opisih podsistemov.
- Komunikacijska postavka vsebuje opis opravila. Opis opravila lahko vsebuje podatke zahteve, ki zažene ukaz ali program. Preglejte komunikacijske postavke in z njimi povezane opise opravil, da boste razumeli, kako se bodo zagnala opravila.
- Komunikacijska postavka podaja tudi privzeti profil uporabnika, ki ga uporabi sistem v določenih situacijah. Razumeti morate vlogo privzetih profilov. Če vsebuje vaš sistem privzete profile, morate zagotoviti, da imajo minimalno pooblastilo. Podrobnejše informacije o privzetih profilih uporabnikov lahkonajdete v razdelkuPoglavje 13, “Zaščitene komunikacije APPC”.

  S pomočjo ukaza PRTSBSDAUT (Natisni opis podsistema) lahko določite komunikacijske postavke, ki podajajo ime profila uporabnika.

Postavke vnaprej zagnanih opravil

Postavke vnaprej zagnanih opravil lahko uporabite za pripravo podsistema za določene vrste opravil, da se opravila hitreje zaženejo. Vnaprej zagnana opravila se lahko zaženejo pri zagonu podsistema ali po potrebi. Postavka vnaprej zagnanega opravila podaja naslednje:

- Program za izvajanje

  Privzeti profil uporabnika

  Opis opravila

Vse te možnosti predstavljajo možne luknje v zaščiti. Zagotovite, da bodo izvajale postavke vnaprej zagnanih opravil samo pooblaščene in nameravane funkcije.

Opravila in opisi opravil

Opisi opravil vsebujejo podatke zahteve in podatke usmerjanja, ki lahko povzročijo izvajanje določenega programa pri uporabi tega opisa opravila. Če podaja opis opravila program v parametru podatkov zahteve, sistem zažene program. Če podaja opis opravila podatke usmerjanja, sistem zažene program, podan v postavki usmerjanja, ki ustreza podatkom usmerjanja.

Sistem uporablja opise opravil za interaktivna in paketna opravila. Za interaktivna opravila podaja opis opravila postavka delovne postaje. Običajno je vrednost postavke delovne postaje *USRPRF, zato uporabi sistem opis opravila, ki je podan v profilu uporabnika. Za paketna opravila podate opis opravila pri predložitvi opravila.

Občasno preglejte opise opravil in zagotovite, da ne zaženejo nenameravanih programov. Uporabite tudi objektno pooblastilo, s katerim preprečite spremembe v opisih opravil. Pooblastilo *USE zadostuje za izvajanje opravila z opisom opravila. Značilen uporabnik ne potrebuje pooblastila *CHANGE za opise opravil.

Možnosti menija SECBATCH:
15 *za takojšnjo predložitev***54** *za uporabo planerja opravil*

Opisi opravil lahko podajajo tudi profil uporabnika, pod katerim se bo izvajalo opravilo. Če uporabite raven zaščite 40 in več, morate imeti pooblastilo *USE za opis opravila in za profil uporabnika, ki je podan v opisu opravila. Če uporabite ravni zaščite, manjše od 40, potrebujete pooblastilo *USE samo za opis opravila.

S pomočjo ukaza PRTJOBDAUT (Natisni pooblastilo opisa opravila) lahko natisnete seznam opisov opravil, ki podajajo profile uporabnikov in imajo javno pooblastilo *USE.

Poročilo kaže posebna pooblastila profila uporabnika, ki je podan v opisu opravila. Poročilo vključuje posebna pooblastila vseh skupinskih profilov, ki jih ima profil uporabnika. Za prikaz zasebnih pooblastil profila uporabnika lahko uporabite naslednji ukaz:

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

Opis opravila podaja seznam knjižnic, ki jih uporablja opravilo pri izvajanju. Če lahko nekdo spremeni seznam knjižnic uporabnika, lahko ta uporabnik zažene nenačrtovano različico programa v drugi knjižnici. Občasno preverite sezname knjižnic, ki so podane v opisu opravil vašega sistema.

Na koncu zagotovite še, da privzete vrednosti ukazov SBMJOB (Predloži opravilo) in CRTUSRPRF (Izdelaj profil uporabnika) niso bile spremenjene, tako da bi kazale na nenačrtovane opise opravil.

Imena transakcijskih programov arhitekture

Določene komunikacijske zahteve pošljejo v vaš sistem specifično vrsto signala. Ta zahteva se imenuje **ime transakcijskega programa (TPN) arhitekture**, ker je ime transakcijskega programa del arhitekture APPC za sistem. Zgled TPN arhitekture je zahteva za prehod zaslonske postaje. TPN-ji arhitekture predstavljajo običajen način za delovanje komunikacij in ni nujno, da je z njimi povezana luknja v zaščiti. Toda TPN-ji arhitekture lahko nudijo nepričakovan vhod v sistem.

Nekateri TPN-ji v zahtevi ne podajo profila. Če je zahteva povezana s komunikacijsko postavko, katere privzeti uporabnik je *SYS, lahko zahtevo vpeljete v sistem. Toda profil *SYS lahko izvaja samo sistemske funkcije, ne pa tudi uporabniških aplikacij.

Če ne želite, da se izvajajo TPN-ji arhitekture s privzetim profilom, lahko spremenite privzetega uporabnika v komunikacijskih postavkah iz *SYS v *NONE. “Zahteve TPN-jev arhitekture” navaja TPN-je arhitekture in povezane profile uporabnikov.

Če ne želite, da se določen TPN izvaja v vašem sistemu, naredite naslednje:

1. Izdelajte program CL, ki sprejme več parametrov. Program naj ne izvaja nobene funkcije. Vsebuje naj stavke navedbe (DCL) za parametre, nato pa naj se konča.
2. Dodajte postavko usmerjanja za TPN v vsak podsistem, ki vsebuje komunikacijske postavke ali postavke imen oddaljenih mest. Postavka usmerjanja naj podaja naslednje:
   - *Primerjalno vrednost* (CMPVAL), enako imenu programa za TPN (glejte Zahteve TPN-jev arhitekture) z začetnim položajem 37.
   - Vrednost *programa za klicanje* (PGM), ki je enaka imenu programa, ki ste ga izdelali v koraku 1. S tem preprečite, da bi TPN poiskal drugo postavko usmerjanja kot je *ANY.

Številni TPN-ji imajo v podsistemu že svoje postavke usmerjanja, ki so bile dodane zaradi zmogljivostnih vzrokov.

Zahteve TPN-jev arhitekture

Tabela 17. Programi in uporabniki za zahteve TPN

Zahteva TPN	Program	Profil uporabnika	Opis
X'30F0F8F1'	AMQCRC6A	*NONE	Shranjevanje sporočil v čakalno vrsto
X'06F3F0F1'	QACSOTP	QUSER	Transakcijski program prijave APPC
X'30F0F2D1'	QANRTP	QADSM	Konfiguracija APPC ADSM/400
X'30F0F1F9'	QCNPCSUP	*NONE	Mape v skupni rabi
X'07F0F0F1'	QCNTEDDM	QUSER	DDM
X'07F6C4C2'	QCNTEDDM	QUSER	Oddaljeni SQL–DRDA1
X'30F0F7F7'	QCQNRBAS	QSVCCS	Strežnik CC SNA
X'30F0F1F4'	QDXPRCV	QUSER	Sprejemnik DSNX–PC
X'30F0F1F3'	QDXPSEND	QUSER	Pošiljatelj DSNX–PC
X'30F0F2C4'	QEVYMAIN	QUSER	Strežnik ENVY**/400
X'30F0F6F0'	QHQTRGT	*NONE	Podatkovna čakalna vrsta PC
X'30F0F8F0'	QLZPSERV	*NONE	Upravljalnik licenc Client Access
X'30F0F1F7'	QMFRCVR	*NONE	Sprejemnik sporočil PC
X'30F0F1F8'	QMFSNDR	*NONE	Pošiljatelj sporočil PC
X'30F0F6F6'	QND5MAIN	QUSER	krmilnik delovne postaje APPN 5394
DB2DRDA	QCNTEDDDM	QUSER	DB2DRDA
APINGD	QNMAPINGD	QUSER	APINGD
X'30F0F5F4'	QNMEVK	QUSER	Pomožni programi za upravljanje sistema
X'30F0F2C1'	QNPSERVR	*NONE	Omrežni tiskalni strežnik PWS-I
X'30F0F7F9'	QOCEVOKE	*NONE	Koledar več sistemov
X'30F0F6F1'	QOKCSUP	QDOC	Senčenje imenikov
X'20F0F0F7'	QOQSESRV	QUSER	DIA različice 2

Tabela 17. Programi in uporabniki za zahteve TPN (nadaljevanje)

Zahteva TPN	Program	Profil uporabnika	Opis
X'20F0F0F8'	QOQSESRV	QUSER	DIA različice 2
X'30F0F5F1'	QOQSESRV	QUSER	DIA različice 2
X'20F0F0F0'	QOSAPPC	QUSER	DIA različice 1
X'30F0F0F5'	QPAPAST2	QUSER	Prehod S/36—S/38
X'30F0F0F9'	QPAPAST2	QUSER	Prehod tiskalnika
X'30F0F4F6'	QPWFSTP0	*NONE	Mape v skupni rabi tipa 2
X'30F0F2C8'	QPWFSTP1	*NONE	Datotečni strežnik Client Access
X'30F0F2C9'	QPWFSTP2	*NONE	Datotečni strežnik Windows** Client Access
X'30F0F6F9'	QRQSRVX	*NONE	Oddaljeni strežnik SQL–converged
X'30F0F6F5'	QRQSRV0	*NONE	Oddaljeni SQL brez potrditve
X'30F0F6F4'	QRQSRV1	*NONE	Oddaljeni SQL brez potrditve
X'30F0F2D2'	QSVRCI	QUSER	SOC/CT
X'21F0F0F8'	QS2RCVR	QGATE	Sprejemnik SNADS FS2
X'21F0F0F7'	QS2STSND	QGATE	Pošiljatelj SNADS FS2
X'30F0F1F6'	QTFDWNLD	*NONE	Funkcija prenosa PC
X'30F0F2F4'	QTIHNPCS	QUSER	Funkcija TIE
X'30F0F1F5'	QVPPRINT	*NONE	Navidezno tiskanje PC
X'30F0F2D3'	QWGMTP	QWGM	Strežnik Ultimedia Mail/400
X'30F0F8F3'	QZDAINIT	QUSER	Strežnik dostopa do podatkov PWS-I
X'21F0F0F2'	QZDRCVR	QSNADS	Sprejemnik SNADS
X'21F0F0F1'	QZDSTSND	QSNADS	Pošiljatelj SNADS
X'30F0F2C5'	QZHQTRG	*NONE	Strežnik podatkovne čakalne vrste PWS-I
X'30F0F2C6'	QZRCSRVR	*NONE	Oddaljeni ukazni strežnik PWS-I
X'30F0F2C7'	QZSCSRVR	*NONE	Osrednji strežnik PWS-I

Metode za nadzorovanje dogodkov zaščite

Nastavitev zaščite je trajen postopek. V sistemu morate ves čas nadzorovati spremembe in napake v zaščiti, nato pa v okolju zaščite opraviti ustrezne prilagoditve kot odziv na tisto, kar odkrijete.

Poročila zaščite vam bodo pomagala pri nadzorovanju sprememb, povezanih z zaščito, ki se izvajajo v sistemu. Sledijo še druge sistemske funkcije, ki jih lahko uporabite kot pomoč pri odkrivanju napak ali lukenj v zaščiti:

- Beleženje zaščite je močno orodje, ki ga lahko uporabite za opazovanje številnih vrst dogodkov, povezanih z zaščito, do katerih pride v sistemu. Sistem lahko na primer nastavite tako, da zapiše vnese beleženja vsakič, ko uporabnik odpre določeno datoteko baze podatkov za ažuriranje. Beležite lahko vse spremembe v sistemskih vrednostih. Beležite lahko dejanja, ki se zgodijo, ko uporabniki obnovijo objekte.

  V 9. poglavju knjige *iSeries Security Reference* boste našli popolne informacije o funkciji beleženja zaščite. Beleženje zaščite v sistemu lahko nastavite s pomočjo ukaza CHGSECAUD (Spremeni beleženje zaščite). Z ukazom DSPAUDJRNE (Prikaži postavke dnevnika beleženja) lahko tudi natisnete izbrane informacije iz dnevnika beleženja zaščite.

- Izdelate lahko čakalno vrsto sporočil QSYSMSG, ki bo zajemala sporočila, pomembna za operaterja sistema. Čakalna vrsta sporočil QSYSOPR sprejme med značilnim poslovnim dnem številna sporočila različne pomembnosti. Zaradi obsežnosti sporočil v čakalni vrsti sporočil QSYSOPR se lahko zgodi, da spregledate pomembna sporočila, povezana z zaščito.

  Če izdelate v knjižnici QSYS sistema čakalno vrsto sporočil QSYSMSG, sistem samodejno usmeri določena pomembna sporočila v čakalno vrsto sporočil QSYSMSG namesto v čakalno vrsto sporočil QSYSOPR.

  Izdelate lahko program, ki bo nadzoroval čakalno vrsto sporočil QSYSMSG ali pa jo v prekinitvenem načinu dodelite sebi ali kakšnemu drugemu uporabniku, ki mu zaupate.

Del 3. Aplikacije in omrežne komunikacije

Poglavje 12. Uporaba integriranega datotečnega sistema za zaščito datotek

Integrirani datotečni sistem nudi številne načine za shranitev in ogled informacij na strežniku iSeries. Integrirani datotečni sistem je del operacijskega sistema OS/400, ki podpira pretočne vhodne in izhodne operacije. Nudi načine za upravljanje pomnilnika, ki so podobni (in združljive) operacijskim sistemom na osebnih računalnikih in operacijskim sistemom UNIX.

S pomočjo integriranega datotečnega sistema si lahko ogledate vse objekte v sistemu v hierarhični imeniški strukturi. Toda v večini primerov si ogledajo uporabniki objekte na način, ki je najprimernejši za določen datotečni sistem. ″Tradicionalni″ objekti iSeries so na primer v datotečnem sistemu QSYS.LIB. Običajno si ogledajo uporabniki te objekte z vidika knjižnic, objekte v datotečnem sistemu QDLS pa z vidika dokumentov znotraj map. Korenski imenik (/), QOpenSys in uporabniško definirani datotečni sistemi predstavljajo strukturo hierarhičnih (ugnezdenih) imenikov.

Kot skrbnik sistema morate razumeti naslednje:

- kateri datotečni sistemi so uporabljeni v vašem sistemu
- unikatne značilnosti zaščite vsakega datotečnega sistema

Teme, ki sledijo, nudijo splošno problematiko, povezano z zaščito integriranega datotečnega sistema.

Pristop integriranega datotečnega sistema k zaščiti

Korenski datotečni sistem deluje kot osnova za vse druge datotečne sisteme na strežnikih iSeries. Na visoki ravni nudi integriran prikaz vseh objektov v sistemu. Drugi datotečni sistemi, ki obstajajo na strežnikih iSeries, nudijo različne pristope k upravljanju in integraciji objektov, odvisno od stranskega namena vsakega datotečnega sistema. Optični datotečni sistem (QOPT) na primer omogoča, da dostopijo aplikacije in strežniki iSeries (vključno z datotečnim strežnikom iSeries Access za Windows) do pogona CD-ROM na strežniku iSeries. Podobno omogoča datotečni sistem QFileSvr.400 aplikacijam dostop do podatkov integriranega datotečnega sistema na oddaljenih strežnikih iSeries. Datotečni strežnik QLANSrv omogoča dostop do datotek, shranjenih na integriranem strežniku xSeries za iSeries ali na drugih strežnikih, povezanih v omrežje.

Zaščitni pristop za vsak datotečni sistem je odvisen od podatkov, ki so na voljo v datotečnem sistemu. Datotečni sistem QOPT na primer ne nudi zaščite na ravni objektov, ker ne obstaja nobena tehnologija za zapisovanje pooblastitvenih informacij na zgoščenko. Za datotečni sistem QFileSvr.400 se izvaja nadzor dostopa v oddaljenem sistemu (kjer so datoteke fizično shranjene in upravljanje). Za datotečne sisteme kot je QLANSrv nudi nadzor dostopa integrirani strežnik xSeries za iSeries. Kljub različnim modelom zaščite podpirajo številni datotečni sistemi skladno upravljanje nadzora dostopa s pomočjo ukazov integriranega datotečnega sistema kot sta na primer CHGAUT (Spremeni pooblastilo) in CHGOWN (Spremeni lastnika).

Sledi nekaj nasvetov, povezanih z zaščito integriranega datotečnega sistema. Integrirani sistem je oblikovan tako, da čim bolj upošteva standarde POSIX. To vodi v zanimivo vedenje, kjer se pooblastilo strežnika iSeries in pravice POSIX ″pomešajo″:

1. Osebnega pooblastila uporabnika za imenik, katerega lastnik je ta uporabnik, ne odstranite, tudi če ima ta uporabnik pooblastilo prek javnega pooblastila, skupine ali seznama pooblastil. Pri delu s knjižnicami ali mapami v standardnem zaščitnem modelu

strežnika iSeries povzroči odstranitev zasebnega pooblastila lastnika zmanjšanje količine pooblastitvenih informacij, shranjenih za profil uporabnika in ne vpliva na druge operacije. Toda zaradi načina, na katerega standard POSIX definira prevzem pravic za imenike, bo imel lastnik novo izdelanega imenika ista objektna pooblastila za ta imenik kot jih ima nadrejeni lastnik za nadrejeni imenik, tudi če ima lastnik novo izdelanega imenika druga zasebna pooblastila za nadrejeni imenik. To je najbrž težko za razumeti, zato bomo prikazali zgled: USERA je lastnik imenika /DIRA, toda zasebna pooblastila za USERA so bila odstranjena. USERB ima zasebno pooblastilo za /DIRA. USERB izdela imenik /DIRA/DIRB. Ker USERA nima objektnih pooblastil za /DIRA, ne bo imel USERB nobenih objektnih pooblastil za /DIRA/DIRB. USERB ne mogel preimenovati ali zbrisati /DIRA/DIRB brez nadaljnjega dejanja spreminjanja objektnih pooblastil USERB. To velja tudi pri izdelavi datotek z API-jem open() s pomočjo oznake O_INHERITMODE. Če je USERB izdelal datoteko /DIRA/FILEB, USERB ne bo imel zanjo nobenih objektnih in podatkovnih pooblastil. USERB ne more pisati v novo datoteko.

2. Večina fizičnih datotečnih sistemov ne podpira prevzema pooblastil. To vključuje korenski datotečni sistem (/), QOpenSys, QDLS in uporabniško definirane datotečne sisteme.
3. Vsi objekti so v lasti profila uporabnika, ki je izdelal objekte, tudi če je polje OWNER profila uporabnika nastavljeno na *GRPPRF.
4. Številne operacije datotečnih sistemov zahtevajo podatkovno pooblastilo *RX za vsako komponento poti, vključno s korenskim imenikom (/). Če imate težave s pooblastili, ne pozabite preveriti pooblastila uporabnika za korenski imenik.
5. Prikaz ali pridobitev trenutnega delovnega imenika (DSPCURDIR, getcwd() itd.) zahteva podatkovno pooblastilo *RX za vsako komponento na poti. Toda sprememba trenutnega delovnega imenika (CD, chdir(), itd.) zahteva samo podatkovno pooblastilo *X za vsako komponento. Zato se lahko zgodi, da spremeni uporabnik trenutni delovni imenik na določeno pot, ki je potem ne more prikazati.
6. Namen ukaza COPY je podvojiti objekt. Nastavitve pooblastil za novo datoteko bodo iste kot v izvirniku, razen lastnika. Namen ukaza CPYTOSTMF pa je preprosta podvojitev podatkov. Uporabnik ne more nadzorovati nastavitev pooblastil nove datoteke. Tvorec/lastnik bo imel podatkovno pooblastilo *RWX, toda skupinsko in javno pooblastilo bosta *EXCLUDE. Uporabnik mora za dodelitev želenih pooblastil uporabiti druga sredstva (CHGAUT, chmod() itd.).
7. Če želi uporabnik pridobiti pooblastitvene informacije o objektu, mora biti njegov lastnik ali imeti objektno pooblastilo *OBJMGT. To se pojavi na nekaterih nepričakovanih mestih, kot na primer v ukazu COPY, ki mora pridobiti pooblastitvene informacije za izvirni objekt, da lahko nastavi enakovredna pooblastila ciljnega objekta.
8. Pri spreminjanju lastnika ali skupine objekta ni dovolj, da ima uporabnik samo ustrezno pooblastilo za objekt, pač pa mora imeti tudi podatkovno pooblastilo *ADD za nov profil uporabnika lastnika/skupine in podatkovno pooblastilo *DELETE za star profil lastnika/skupine. Ta podatkovna pooblastila niso povezana s podatkovnimi pooblastili datotečnega sistema. Ta podatkovna pooblastila lahko prikažete s pomočjo ukaza DSPOBJAUT in spremenite s pomočjo ukaza EDTOBJAUT. To se pojavi nepričakovano tudi v ukazu COPY, ko poskusi nastaviti ID skupine novega objekta.
9. V ukazu MOV pogosto pride do nenavadnih pooblastitvenih napak, še posebej pri prenosu iz enega fizičnega datotečnega sistema v drugega ali pri pretvorbi podatkov. V teh primerih postane prenos dejansko operacija kopiranja in brisanja. Zato lahko na ukaz MOV poleg težav, specifičnih zanj, vplivajo tudi iste pooblastitvene težave kot na ukazu COPY (glejte 7 in 8 zgoraj) in ukaz RMVLNK.

V naslednjih razdelkih boste našli nekaj težav za več datotečnih sistemov. Za podrobnejše informacije o specifičnem datotečnem sistemu na vašem strežniku iSeries boste morali pregledati dokumentacijo licenčnega programa, ki uporablja datotečni sistem.

Korenski datotečni sistem (/), QOpenSys in uporabniško definirani datotečni sistemi

Sledi problematika zaščite za korenski datotečni sistem, QOpenSys in uporabniško definirane datotečne sisteme.

Kako deluje pooblastilo

Korenski datotečni sistem, QOpenSys in uporabniško definirani datotečni sistemi nudijo združitev zmožnosti strežnika iSeries, PC-ja in UNIX** za upravljanje objektov in zaščito. Če uporabite ukaze integriranega datotečnega sistema iz strežniške seje iSeries (WRKAUT in CHGAUT), lahko nastavite vsa običajna objektna pooblastila strežnika iSeries. To vključuje tudi pooblastila *R, *W in *X, ki so združljiva s specifikacijo 1170 (operacijski sistemi tipa UNIX).

Opomba: Korenski datotečni sistem, QOpenSys in uporabniško definirani datotečni sistemi so funkcionalno enakovredni. Datotečni sistem QOpenSys upošteva velike in male črke, korenski datotečni sistem pa ne. Uporabniško definirane datotečne sisteme lahko po želji definirate tako, da upoštevajo velike in male črke. Ker imajo ti datotečni sistemi iste značilnosti zaščite, lahko v temah, ki sledijo, njihova imena uporabite izmenično.

Ko dostopite do korenskega datotečnega sistema kot skrbnik iz seje PC, lahko nastavite objektna pooblastila, ki jih uporablja PC za omejitev določenih vrst dostopa:
- sistem
- skrit
- arhivski
- samo za branje

Ti atributi PC so dodatek k vrednostim objektnih pooblastil strežnika iSeries in ne njihova zamenjava.

Ko poskusi uporabnik dostopiti do objekta v korenskem datotečnem sistemu, uveljavi OS/400 vse vrednosti objektnih pooblastili in atribute za objekt, ne glede na to, ali so ti atributi ″vidni″ iz vmesnika uporabnika. Denimo, da je za objekt vključen atribut samo za branje. Uporabnik objekta ne more zbrisati prek vmesnika za dostop iSeries. Objekta ne more zbrisati niti uporabnik strežnika iSeries z delovno postajo z nespremenljivo funkcijo, tudi če ima uporabnik strežnika iSeries posebno pooblastilo *ALLOBJ. Preden je mogoče zbrisati objekt, mora pooblaščen uporabnik s pomočjo funkcije PC na novo nastaviti vrednost samo za branje na izključeno. Podobno velja tudi za uporabnika PC, ki morda ne bo imel ustreznega pooblastila OS/400 za spreminjanje zaščitnih atributi objekta, povezanih s PC-jem.

Aplikacije tipa UNIX, ki se izvajajo na strežnikih iSeries, dostopajo do podatkov v korenskem datotečnem sistemu s pomočjo aplikacijskih programerskih vmesnikov (API-jev), podobnih UNIX. Z API-ji, podobnimi UNIX, lahko aplikacije prepoznajo in vzdržujejo naslednje informacije o zaščiti:
- lastnik objekta
- lastnik skupine (pooblastilo osnovne skupine strežnika iSeries)
- branje (datoteke)
- pisanje (spreminjanje vsebine)
- izvajanje (zagon programov ali pregledovanje imenikov)

Sistem preslika ta podatkovna pooblastila v obstoječa objektna in podatkovna pooblastila strežnika iSeries:

- Branje (*R) = *OBJOPR in *READ
- Pisanje (*W) = *OBJOPR, *ADD, *UPD, *DLT

- Izvajanje (*X) = *OBJOPR in *EXECUTE

Koncepti za druga objektna pooblastila (*OBJMGT, *OBJEXIST, *OBJALTER in *OBJREF) v okolju tipa UNIX ne obstajajo.

Toda ta objektna pooblastila ne obstajajo za vse objekte v korenskem datotečnem sistemu. Če izdelate objekt s pomočjo API-ja, podobnega UNIX, prevzame ta objekt pooblastila nadrejenega imenika, kar povzroči naslednje:

- Lastnik novega objekta ima ista objektna pooblastila kot lastnik nadrejenega imenika.
- Osnovna skupina novega objekta ima isto objektno pooblastilo kot osnovna skupina nadrejenega imenika.
- Javno pooblastilo novega objekta ima isto objektno pooblastilo kot javno pooblastilo nadrejenega imenika.

Podatkovno pooblastilo novega objekta za lastnika, osnovno skupino in javno pooblastilo je podano v API-ju s parametrom načina. Če so vsa objektna pooblastila vključena, bo vedenje pooblastil takšno kot v okolju tipa UNIX. Najbolje je, da pustite pooblastila vključena, sicer bo vedenje podobno kot v okolju POSIX.

Če izvajate aplikacije, ki uporabljajo API-je, podobne UNIX, uveljavi sistem vsa objektna pooblastila, ne glede na to, ali so ″vidna″ za aplikacije tipa UNIX. Tako bo na primer uveljavil sistem pooblastilo seznamov s pooblastili, tudi če koncepti seznamov s pooblastili ne obstajajo v operacijski okoljih tipa UNIX.

Če delate v okolju z mešanimi aplikacijami, morate paziti, da v enem okolju ne opravite sprememb v pooblastilih, ki bi poškodovale aplikacije v drugem okolju.

Delo z zaščito za korenski datotečni sistem (/), QOpenSys in uporabniško definirane datotečne sisteme

Z uvedbo integriranega datotečnega sistema je na strežnikih iSeries na voljo tudi nov niz ukazov za delo z objekti v več datotečnih sistemih. Ta niz ukazov vključuje ukaze za delo z zaščito:

- CHGAUD (Spremeni beleženje)
- CHGAUT (Spremeni pooblastilo)
- CHGOWN (Spremeni lastnika)
- CHGPGP (Spremeni osnovno skupino)
- DSPAUT (Prikaži pooblastilo)
- WRKAUT (Delo s pooblastilom)

Ti ukazi združujejo podrejena podatkovna in objektna pooblastila v podnize pooblastil, podobne kot v okolju UNIX:

***RWX** Branje/pisanje/izvajanje
***RW** Branje/pisanje
***R** Branje
***WX** Pisanje/izvajanje
***W** Pisanje
***X** Izvajanje

Poleg tega so na voljo še API-ji, podobni kot v okolju UNIX, ki omogočajo delo z zaščito.

Javno pooblastilo za korenski imenik

Ko dobite naložen sistem, je javno pooblastilo za korenski imenik nastavljeno na *ALL (vsa objektna in vsa podatkovna pooblastila). Ta nastavitev nudi prožnost in združljivost s pričakovanji aplikacij, podobnih UNIX, in s pričakovanji značilnih uporabnikov strežnika iSeries. Uporabnik strežnika iSeries z zmožnostjo ukazne vrstice lahko izdela novo knjižnico v datotečnem sistemu QSYS.LIB s preprosto uporabo ukaza CRTLIB. To običajno dopušča

pooblastilo na značilnem strežniku iSeries. Podobno kot velja za naloženo nastavitev korenskega datotečnega sistema lahko značilen uporabnik tudi izdela nov imenik v korenskem datotečnem sistemu (podobno kot lahko izdelate nov imenik na PC-ju).

Kot skrbnik za zaščito morate svoje uporabnike podučiti o ustrezni zaščiti objektov, ki jih izdelajo. Ko uporabnik izdela knjižnico, je najbolje, da javno pooblastilo zanjo ni *CHANGE (privzetek). Uporabnik naj nastavi javno pooblastilo na *USE ali *EXCLUDE, odvisno od vsebine knjižnice.

Če morajo izdelati uporabniki nove imenike v korenskem datotečnem sistemu (/), v QOpenSys ali v uporabniško definiranih datotečnih sistemih, imate na voljo več možnosti za zaščito:

- Uporabnike lahko podučite, naj pri izdelavi novih imenikov nadomestijo privzeto pooblastilo. Privzetek je prevzem pooblastila iz najbližjega nadrejenega imenika. V primeru novo izdelanega imenika v korenskem imeniku bo torej privzeto javno pooblastilo *ALL.
- Pod korenskim imenikom lahko izdelate ″glavni″ podimenik. Njegovo javno pooblastilo nastavite na ustrezno nastavitev za vaše podjetje. Nato dajte uporabnikom navodila, naj izdelajo vse nove osebne imenike v tem glavnem podimeniku. Njihovi novi imeniki bodo prevzeli pooblastilo glavnega imenika.
- Če želite, lahko spremenite javno pooblastilo za korenski imenik in tako uporabnikom preprečite izdelavo objektov v njem. (Odstranite pooblastila *W, *OBJEXIST, *OBJALTER, *OBJREF in *OBJMGT.) Vendar pa morate oceniti, ali bo ta sprememba povročila težave drugim aplikacijam. Morda imate aplikacije, podobne UNIX, ki pričakujejo, da bodo lahko brisale objekte iz korenskega imenika.

Ukaz PRTPVTAUT (Natisni zasebna pooblastila)

Ukaz PRTPVTAUT (Natisni zasebna pooblastila) omogoča, da natisnete poročilo o vseh zasebnih pooblastilih za objekte določenega tipa v podani knjižnici, mapi ali imeniku. Poročilo navede vse objekte podanega tipa in uporabnike, ki imajo pooblastilo za objekt. Na ta način lahko preverite različne vire pooblastil za objekte.

Ta ukaz natisne tri poročila za izbrane objekte. Prvo poročilo (celotno poročilo) vsebuje vsa zasebna pooblastila za izbrane objekte. Drugo poročilo (poročilo o spremembah) vsebuje dodatke in spremembe, ki ste jih opravili v zasebnih pooblastilih izbranih objektov, če ste predhodno zagnali ukaz PRTPVTAUT za podane objekte v podani knjižnici, mapi ali imeniku. V ’poročilu o spremembah’ so zabeleženi vsi novi objekti izbranega tipa, nova pooblastila za obstoječe objekte ali spremembe v obstoječih pooblastilih za obstoječe objekte. Če ukaza PRTPVTAUT niste predhodno zagnali za podane objekte v podani knjižnici, mapi ali imeniku, ’poročilo o spremembah’ ne bo izdelano. Če ste ukaz predhodno zagnali, vendar niste opravili nobene spremembe v pooblastilih objektov, bo ’poročilo o spremembah’ natisnjeno, toda naveden ne bo noben objekt.

Tretje poročilo (poročilo o brisanju) vsebuje vsa brisanja uporabnikov z zasebnimi pooblastili iz podanih objektov od predhodne izvedbe ukaza PRTPVTAUT. V ’poročilu o brisanju’ bodo prikazani vsi zbrisani objekti ali vsi uporabniki, ki so bili odstranjeni kot uporabniki z zasebnimi pooblastili. Če predhodno niste zagnali ukaza PRTPVTAUT, ’poročilo o brisanju’ ne bo izdelano. Če ste ukaz predhodno zagnali, vendar v objektih niste opravili nobene operacije brisanja, bo ’poročilo o brisanju’ natisnjeno, toda naveden ne bo noben objekt.

Omejitev: Za uporabo tega ukaza potrebujete posebno pooblastilo *ALLOBJ.

Zgledi:

Ta ukaz izdela celotno poročilo in poročili o spreminjanju in brisanje za vse datotečne objekte v PAYROLLLIB:

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

Ta ukaz izdela celotno poročilo in poročili o spreminjanju in brisanju za vse objekte tokovnih datotek v imeniku garry:

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

Ta ukaz izdela celotno poročilo in poročili o spreminjanju in brisanje za vse objekte tokovnih datotek v podimeniški strukturi, ki se začne v imeniku garry:

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

Ukaz PRTPUBAUT (Natisni objekte z javnimi pooblastili)

Ukaz PRTPUBAUT (Natisni objekte z javnimi pooblastili) omogoča natis poročila podanih objektov, ki nimajo javnega pooblastila *EXCLUDE. Za objekte *PGM bodo v poročilo vključeni samo programi brez javnega pooblastila *EXCLUDE, ki jih lahko pokliče uporabnik (program je uporabniška domena ali pa je raven sistemske zaščite (sistemska vrednost QSECURITY) 30 ali manj). Na ta način lahko preverite objekte, do katerih lahko dostopijo vsi uporabniki v sistemu.

Ta ukaz natisne dve poročili. Prvo poročilo (celotno poročilo) vsebuje vse podane objekte, ki nimajo javnega pooblastila *EXCLUDE. Drugo poročilo (poročilo o spremembah) vsebuje objekte, ki zdaj nimajo javnega pooblastila *EXCLUDE, ki so imeli javno pooblastilo *EXCLUDE ali pri izdaji ukaza PRTPUBAUT niso obstajali. Če ukaza PRTPUBAUT predhodno niste zagnali za podane objekte v knjižnici, mapi ali imeniku, 'poročilo o spremembah' ne bo izdelano. Če ste ukaz predhodno zagnali, vendar noben dodatni objekt nima javnega pooblastila *EXCLUDE, bo 'poročilo o spremembah' natisnjeno, vendar ne bo naveden noben objekt.

Omejitev: Za uporabo tega ukaza potrebujete posebno pooblastilo *ALLOBJ.

Zgledi:

Ta ukaz izdela celotno poročilo in poročilo o spremembah za vse datotečne objekte v knjižnici GARRY, ki nimajo javnega pooblastila *EXCLUDE:

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

Ta ukaz izdela celotno poročilo in poročili o spremembah in brisanju za vse objekte tokovnih datotek v podimeniški strukturi, ki se začne v imeniku garry, ki nimajo javnega pooblastila *EXCLUDE:

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

Omejitev dostopa do datotečnega sistema QSYS.LIB

Ker korenski datotečni sistem osnovni datotečni sistem, je datotečni sistem QSYS.LIB prikazan kot podimenik znotraj korenskega imenika. Zato lahko vsi uporabniki PC z dostopom do strežnika iSeries delajo z objekti, shranjenimi v knjižnicah strežnika iSeries (datotečni sistem QSYS.LIB) z običajnimi ukazi in dejanji PC. Uporabnik PC lahko na primer povleče objekt QSYS.LIB (kot je knjižnica s pomembnimi podatkovnimi datotekami) v rezalnik.

Kot ste se naučiliv razdelku"Korenski datotečni sistem (/), QOpenSys in uporabniško definirani datotečni sistemi" na strani 89, sistem uveljavi pooblastilo za vse objekte ne glede na to, ali je vidno za vmesnik. Zato uporabnik ne more razrezati (zbrisati) objekta, če zanj

nima pooblastila *OBJEXIST. Toda če je iSeries odvisen od zaščite menijskega dostopa in ne od zaščite objektov, lahko uporabnik PC odkrije objekte v datotečnem sistemu QSYS.LIB, ki so na voljo za rezanje.

Ko boste razširili uporabo sistema in različne načine dostopa, boste kmalu ugotovili, da zaščita menijskega dostopa ne zadostuje. Poglavje 5, “Zaščita informacijskih sredstev z objektnim pooblastilom”, na strani 39 razlaga strategije za nadzor menijskega dostopa z zaščito objektov. Toda strežniki iSeries nudijo tudi preprost način za preprečevanje dostopa do datotečnega sistema QSYS.LIB prek imeniške strukture korenskega datotečnega sistema. Za krmiljenje, kateri uporabniki lahko dostopijo do datotečnega sistema QSYS.LIB prek korenskega imenika, lahko uporabite pooblastitveni seznam QPWFSERVER .

Če je pooblastilo uporabnika za pooblastitveni seznam QPWFSERVER *EXCLUDE, uporabnik ne more vnesti imenika QSYS.LIB iz korenske imeniške strukture. Če je pooblastilo uporabnika *USE, lahko uporabnik vnese imenik. Če ima uporabnik pooblastilo za vnos imenika, velja običajno objektno pooblastilo za vsa dejanja, ki jih poskusi izvesti uporabnik na objektu znotraj datotečnega sistema QSYS.LIB. Z drugimi besedami povedano deluje pooblastilo za pooblastitveni seznam QPWFSERVER kot vrata za celoten datotečni sistem QSYS.LIB. Če ima uporabnik pooblastilo *EXCLUDE, so vrata zaklenjena. Za uporabnika s pooblastilom *USE (ali višjim pooblastilom) so vrata odklenjena.

V večini primerov uporabniki ne potrebujejo imeniškega vmesnika za dostop do objektov v datotečnem sistemu QSYS.LIB. Najbrž boste nastavili javno pooblastilo za pooblastitveni seznam QPWFSERVER na *EXCLUDE. Ne pozabite, da pooblastilo za pooblastitveni seznam odpre ali zapre vrata do vseh knjižnic znotraj datotečnega sistema QSYS.LIB, vključno z uporabniškimi knjižnicami. Če naletite na uporabnike, ki nasprotujejo tej odločitvi, lahko ocenite njihove zahteve na individualni osnovi. Če je primerno, lahko izrecno pooblastite posameznega uporabnika za pooblastitveni seznam. Vendar pa morate zagotoviti, da ima uporabnik ustrezno pooblastilo za objekte znotraj datotečnega sistema QSYS.LIB, sicer lahko nenamerno zbriše objekte ali celotne knjižnice.

Opombe:

1. Ko dobite naložen sistem, je javno pooblastilo za pooblastitveni seznam QPWFSERVER nastavljeno na *USE.
2. Če posameznega uporabnika izrecno pooblastite, seznam overjanja nadzoruje dostop samo s streženjem datotek iSeries Access, datotek NetServer in streženjem datotek mediSeries strežniki. S tem ni preprečen dostop do istih imenikov prek FTP, ODBC in drugih omrežij.

Zaščiteni imeniki

Za dostop do objekta znotraj korenskega datotečnega sistema preberete celotno pot do tega objekta. Za iskanje imenika morate imeti pooblastilo *X (*OBJOPR in *EXECUTE) za ta imenik. Denimo na primer, da želite dostopiti do naslednjega objekta:

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

Imeti morate pooblastilo *X za imenik companya in imenik customers.

V korenskem datotečnem sistemu lahko izdelate simbolično povezavo z objektom. Konceptualno gledano je simbolična povezava vzdevek za ime poti. Običajno je krajša in si jo je preprosteje zapomniti od celotne poti. Vendar pa simbolična povezava ne izdela druge fizične poti do objekta. Uporabnik še vedno potrebuje pooblastilo *X za vsak imenik in podimenik na fizični poti do objekta.

Za objekte v korenskem datotečnem sistemu lahko uporabite zaščito imenika, tako kot lahko uporabite v datotečnem sistemu QSYS.LIB zaščito knjižnic. Javno pooblastilo imenika lahko na primer nastavite na *EXCLUDE in preprečite javnim uporabnikom dostop do vseh objektov znotraj tega drevesa.

Zaščita novih objektov

Ko izdelate v korenskem datotečnem sistemu nov objekt, določa njegova pooblastila vmesnik, s pomočjo katerega ga izdelate. Če na primer uporabite ukaz CRTDIR in njegove privzete vrednosti, nov imenik prevzame vse značilnosti pooblastil nadrejenega imenika, vključno z zasebnimi pooblastili, pooblastilom osnovne skupine in povezavo pooblastitvenega seznama. Naslednji razdelki opisujejo, kako so določena pooblastila za vsak tip vmesnika.

Pooblastilo izhaja iz neposredno nadrejenega imenika in ne iz imenikov višje v drevesu. Zato morate kot skrbnik za zaščito oceniti pooblastilo, ki ga dodelite imenikom v hierarhiji, iz dveh vidikov:

- Kako vpliva pooblastilo na objekte v drevesu (kot pooblastilo knjižnice)
- Kako vpliva pooblastilo na novo izdelane objekte (kot je vrednost CRTAUT za knjižnice).

Priporočilo: Uporabnikom, ki delajo v integriranem datotečnem sistemu, lahko dodelite domači imenik (na primer /home/usrxxx), nato pa nastavite ustrezno zaščito (kot je PUBLIC *EXCLUDE). Vsi imeniki, ki jih izdela uporabnik pod domačim imenikom, prevzamejo pooblastila.

Sledijo opisi prevzema pooblastil za različne vmesnike:

Uporaba ukaza Izdelaj imenik

Če izdelate nov podimenik z ukazom CRTDIR, imate na voljo dve možnosti za podajanje pooblastila:

- Podate lahko javno pooblastilo (podatkovno pooblastilo, objektno pooblastilo ali oboje).
- Podate lahko *INDIR za podatkovno pooblastilo, objektno pooblastilo ali oboje. Če podate *INDIR za podatkovno in objektno pooblastilo, izdela sistem v novem objektu natančno kopijo vseh pooblastitvenih informacij iz nadrejenega imenika, vključno s pooblastitvenim seznamom, osnovno skupino, javnim pooblastilom in zasebnimi pooblastili. (Sistem ne prekopira zasebnega pooblastila, ki ga ima profil QSYS ali profil QSECOFR za objekt.)

Izdelava imenika z API-jem

Če izdelate imenik z API-jem mkdir(), podate podatkovna pooblastila za lastnika, osnovno skupino in javno pooblastilo (s preslikavo pooblastil *R, *W in *X). Sistem uporabi informacije v nadrejenem imeniku za nastavitev objektnih pooblastil za lastnika, osnovno skupino in javno pooblastilo.

Ker operacijski sistemi tipa UNIX nimajo koncepta objektnih pooblastil, API mkdir() ne podpira podajanja objektnih pooblastil. Če želite uporabiti različna objektna pooblastila, lahko uporabite ukaz strežnika iSeries (CHGAUT). Toda če odstranite nekatera objektna pooblastila, aplikacije, podobne UNIX, morda ne bodo delovale kot ste pričakovali.

Izdelava tokovne datoteke z API-jem open() ali creat()

Če izdelate tokovno datoteko z API-jem creat(), lahko podate podatkovna pooblastila za lastnika, osnovno skupino in javno pooblastilo (s pooblastili, podobnimi UNIX, *R, *W in *X). Sistem s pomočjo informacij v nadrejenem imeniku nastavi objektna pooblastila za lastnika, osnovno skupino in javno pooblastilo.

Ta pooblastila lahko podate tudi, če izdelate tokovno datoteko s pomočjo API-ja open(). Če uporabite API open(), lahko podate, naj prevzame objekt vsa pooblastila iz nadrejenega imenika. To se imenuje način prevzema. Če podate način prevzema, sistem izdela popolno ujemanje za nadrejena pooblastila, vključno s pooblastitvenim seznamom, osnovno skupino, javnim pooblastilom in zasebnimi pooblastili. Ta možnost deluje enako kot če za ukaz CRTDIR podate *INDIR.

Izdelava objekta s pomočjo vmesnika PC

Če izdelate objekt v korenskem datotečnem sistemu s pomočjo aplikacije PC, sistem samodejno prevzame vsa pooblastila iz nadrejenega imenika. To vključuje pooblastitveni seznam, osnovno skupino, javno pooblastilo in zasebna pooblastila. Aplikacije PC nimajo ekvivalenta za podajanje pooblastila pri izdelavi objekta.

Datotečni sistem QFileSvr.400

Z uporabo datotečnega sistema QFileSvr.400 lahko uporabnik (USERX) v enem sistemu iSeries (SYSTEMA) dostopi do podatkov v drugem povezanem sistemu iSeries (SYSTEMB). USERX vsebuje vmesnik, ki je ravno takšen kot vmesnik Client Access. Oddaljeni strežnik iSeries (SYSTEMB) je prikazan kot imenik z vsemi datotečnimi sistemi kot podimeniki.

Če poskusi USERX dostopiti do SYSTEMB s tem vmesnikom, SYSTEMA pošlje v SYSTEMB ime profila uporabnika USERX in šifrirano geslo. V SYSTEMB morata obstajati isti profil uporabnika in geslo, sicer SYSTEMB zavrne zahtevo.

Če SYSTEMB zavrne zahtevo, je USERX prikazan v SYSTEMB kot katerikoli drugi uporabnik Client Access. Za vsa dejanja, ki jih poskusi izvesti USERX, veljajo ista pravila za preverjanje pooblastil.

Kot skrbnik za zaščito se morate zavedati, da predstavlja datotečni sistem QFileSvr.400 še ena možna vrata v sistem. Tako ne morete kar preprosto sklepati, da omejite oddaljene uporabnike na interaktivno prijavo s prehodom zaslonske postaje. Če se izvaja podsistem QSERVER in je vaš sistem povezan z drugim sistemom iSeries, lahko dostopajo oddaljeni uporabniki do sistema kot če bi bili na lokalnem PC-ju, na katerem se izvaja Client Access. Zelo verjetno je, da ima vaš sistem povezavo, v kateri se mora izvajati podsistem QSERVER. To je še eden izmed razlogov, zaradi katerih je dobra shema objektnih pooblastil bistvenega pomena.

Omrežni datotečni sistem

Omrežni datotečni sistem (NFS) nudi dostop do sistemov (in iz njih), v katerih se izvaja NFS. NFS je industrijski standard za souporabo informacij med uporabniki v omrežnih sistemih. NFS nudi večina glavnih operacijskih sistemov (vključno z operacijskimi sistemi PC). Za sisteme UNIX je NFS osnovni način dostopa do podatkov. Strežniki iSeries lahko delujejo kot odjemalci ali strežniki NFS.

Kot skrbnik za zaščito sistema iSeries, ki deluje kot strežnik NFS, morate razumeti in upravljati vidike zaščite NFS. Sledi nekaj predlogov in težav:

- S pomočjo ukaza STRNFSSVR morate izrecno zagnati funkcijo strežnika NFS. Preverite, kdo ima pooblastilo za uporabo tega ukaza.
- Imenik ali objekt omogočite za odjemalce NFS tako, da ga izvozite. Zato imate zelo natančen nadzor nad deli sistema, ki bodo na voljo za odjemalce NFS v omrežju.
- Pri izvozu lahko podate, kateri odjemalci imajo dostop do objektov. Odjemalca določite z imenom sistema ali naslovom IP. Odjemalec je lahko posamezen PC ali celoten strežnik iSeries ali sistem UNIX. V terminologiji NFS se imenuje odjemalec (naslov IP) delovna postaja.

- Pri izvozu lahko podate za vsako delovno postajo, ki ima dostop do izvoženega imenika ali objekta, dostop samo za branje ali dostop za branje in pisanje. V večini primerov boste najbrž podali dostop samo za branje.
- NFS ne nudi zaščite z geslom. Oblikovan in namenjen je za souporabo podatkov znotraj sistemov, ki si medsebojno zaupajo. Ko uporabnik zahteva dostop, prejme strežnik identifikacijsko številko uporabnika. Sledi nekaj težav, povezanih z identifikacijsko številko uporabnika:
  - Strežnik iSeries poskusi najti profil uporabnika z isto identifikacijsko številko. Če najde ujemajočo se identifikacijsko številko, uporabi priporočila profila uporabnika. Priporočila so izraz NFS, ki opisuje uporabo pooblastila uporabnika. To je podobno izmenjavi profilov v drugih strežniških aplikacijah iSeries.
  - Pri izvozu imenika ali objekta lahko podate, ali boste omogočili dostop po profilu s korenskim imenikom. Strežnik NFS na strežnikih iSeries enači korensko pooblastilo s posebnim pooblastilom *ALLOBJ. Če podate, da ne dovolite korenskega pooblastila, uporabnik NFS z identifikacijsko številko uporabnika, ki se preslika v profil uporabnika s posebnim pooblastilom *ALLOBJ, ne bo imel dostopa do objekta pod tem profilom. Namesto tega bo zahtevnik v primeru, da je dovoljen anonimen dostop, preslikan v anonimen profil.
  - Pri izvozu imenika ali objekta lahko podate, ali boste dopustili anonimne zahteve. Anonimna zahteva je zahteva z identifikacijsko številko uporabnika, ki se ne ujema z nobeno identifikacijsko številko uporabnika v sistemu. Če se odločite, da boste omogočili anonimne zahteve, preslika sistem anonimnega uporabnika v IBM-ov profil uporabnika QNFSANON. Ta profil uporabnika nima nobenega posebnega ali izrecnega pooblastila. (Pri izvozu lahko po želji podate drug profil uporabnika za anonimne zahteve.)
- Če strežnik iSeries sodeluje v omrežju NFS (ali v kateremkoli omrežju s sistemi UNIX, ki so odvisni od identifikacijskih številk uporabnikov), boste najbrž morali voditi lastne identifikacijske številke uporabnikov in ne preprosto pustiti, da jih sistem dodeljuje samodejno. Identifikacijske številke uporabnikov boste morali uskladiti z drugimi sistemi v omrežju.

  Morda boste odkrili, da morate spremeniti identifikacijske številke uporabnikov (celo za IBM-ove profile uporabnikov), da bodo združljivi z drugimi sistemi v omrežju. Na voljo je program, ki omogoča preprosto spreminjanje identifikacijske številke za profil uporabnika. (Če spremenite identifikacijsko številko za profil uporabnika, morate spremeniti tudi identifikacijsko številko uporabnika za vse objekte, katerih lastnik je profil v korenskem imeniku ali v imeniku QOpenSrv.) Program QSYCHGID samodejno spremeni identifikacijsko številko uporabnika v profilu uporabnika in v vseh objektih, ki so v lasti. Informacije za uporabo tega programa poiščite v knjigi *iSeries System API Reference*.

Poglavje 13. Zaščitene komunikacije APPC

Če vaš sistem deluje v omrežju z drugimi sistemi, postane na voljo nov niz vrat in oken za vaš sistem. Kot skrbnik za zaščito morate poznati možnosti, ki jih lahko uporabite za nadzor vhodov v sistem v okolju APPC.

APPC (zahtevnejše komuniciranje programa s programom) predstavlja način, na katerega računalniki, vključno z osebnimi, komunicirajo med seboj. Komunikacije APPC lahko uporabijo prehod zaslonske postaje, porazdeljeno upravljanje podatkov in iSeries Access za Windows.

V temah, ki sledijo, so na voljo osnovne informacije o delovanju komunikacij APPC in o nastavitvi ustrezne zaščite. Te teme so v glavnem usmerjene na elemente konfiguracije APPC, povezane z zaščito. Da bi ta zgled prilagodili vaši situaciji, boste morda morali sodelovati z upravniki komunikacijskega omrežja in morda celo s ponudniki aplikacij. Te informacije uporabite kot osnovo, ki vam bo pomagala razumeti vprašanja, povezana z zaščito, in možnosti, ki so na voljo za APPC.

Zaščita ni nikoli "brezplačna". Nekateri predlogi za poenostavitev omrežne zaščite bodo otežili upravljanje omrežja. Tako na primer v teh informacijah nismo poudarili APPN (Advanced Peer-to-Peer Networking), ker je zaščito lažje razumeti in upravljati brez APPN. Toda brez APPN morajo skrbniki omrežja ročno izdelati konfiguracijske informacije, ki jih izdela APPN samodejno.

Tudi PC-ji uporabljajo komunikacije

Številni načini povezovanja PC-jev s strežniki iSeries so odvisni od komunikacij kot sta APPC ali TCP/IP. Pri branju naslednjih tem ne pozabite razmisliti o vprašanjih v zvezi z zaščito, ki se pojavijo pri povezavi obeh z drugimi sistemi in s PC-ji. Pri načrtovanju zaščite omrežja pazite, da ne boste za PC-je, priključene v sistem, povzročili nasprotnega učinka.

Izrazoslovje APPC

APPC nudi uporabniku v enem sistemu zmožnost izvajanja dela v drugem sistemu. Sistem, iz katerega izvira zahteva, se imenuje:

- **Izvorni sistem**
- **Lokalni sistem**
- **Odjemalec**

Sistem, ki prejme zahtevo, se imenuje:

- **Ciljni sistem**
- **Oddaljeni sistem**
- **Strežnik**

Osnovni elementi komunikacij APPC

Iz perspektive skrbnika za zaščito se mora v enem sistemu (SYSTEMA) zgoditi naslednje, preden lahko uporabnik v drugem sistemu (SYSTEMB) opravi pomembno delo:

- Izvorni sistem (SYSTEMA) mora podati pot ciljnemu sistemu (SYSTEMB). Ta pot se imenuje **seja APPC**.

- Ciljni sistem mora določiti uporabnika in ga povezati s profilom uporabnika. Ciljni sistem mora podpirati algoritem šifriranja izvornega sistema (podrobnejše informacije poiščitev razdelku“Ravni gesel” na strani 14).
- Ciljni sistem mora zagnati opravilo za uporabnika z ustreznim okoljem (vrednosti za upravljanje dela).

V temah, ki sledijo, bomo razložili te elemente, in kako so povezani z zaščito. Skrbnik za zaščito v ciljnem sistemu je odgovoren, da zagotovi, da uporabniki APPC ne bodo kršili zaščite. Toda če skrbnika za zaščito v obeh sistemih sodelujeta, bo upravljanje zaščite APPC veliko preprostejše.

Zgled: osnovna seja APPC

Če v okolju APPC zahtevata uporabnik ali aplikacija v enem sistemu dostop do drugega sistema, dva sistema vzpostavita sejo. Za vzpostavitev seje morata sistema povezati dva ujemajoča se opisa naprav APPC. Parameter imena oddaljenega mesta (RMTLOCNAME) v opisu naprave SYSTEMA se mora ujemati s parametrom imena lokalnega mesta (LCLLOCNAME) v opisu naprave SYSTEMB in obratno.

Da bi dva sistema vzpostavila sejo APPC, morata biti gesli mest v opisih naprav APPC v SYSTEMA in SYSTEMB identični. Obe morata podajati *NONE ali pa isto vrednost.

Če sta gesli nastavljeni na vrednost, ki ni *NONE, sta shranjeni in preneseni v šifrirani obliki. Če se gesli ujemata, sistem vzpostavi sejo. Če se gesli ne ujemata, je zahteva uporabnika zavrnjena. Če sistema podata za vzpostavitev seje geslo mesta, se to imenuje **varna povezava**.

Opomba: Podpore za funkcijo varne povezave ne nudijo vsi računalniški sistemi.

Omejitev sej APPC

Kot skrbnik za zaščito v izvornem sistemu lahko s pomočjo objektnega pooblastila krmilite, kdo lahko poskusi dostopiti do drugih sistemov. Nastavite javno pooblastilo za opise naprav na *EXCLUDE in določenim uporabnikom dodelite pooblastilo *CHANGE. S pomočjo sistemske vrednosti QLMTSECOFR preprečite uporabnikom s posebnim pooblastilom *ALLOBJ uporabo komunikacij APPC.

Kot skrbnik za zaščito v ciljnem sistemu lahko z uporabo pooblastila za naprave APPC preprečite uporabnikom, da bi zagnali sejo APPC v sistemu. Toda razumeti morate, kateri ID uporabnika bo poskusil dostopiti do opisa naprave APPC. “Dostop uporabnika APPC do ciljnega sistema” na strani 99 opisuje, kako povežejo strežniki iSeries ID uporabnika z zahtevo za sejo APPC.

Opomba: S pomočjo ukazov PRTPUBAUT *DEVD (Natisni objekte z javnimi pooblastili) in Natisni zasebna pooblastila (PRTPVTAUT *DEVD) lahko ugotovite, kdo v vašem sistemu ima pooblastilo za opise naprav.

Če v sistemu uporabljate APPN, ta samodejno izdela novo napravo APPC, če ni za smer, ki jo je izbral sistem, na voljo nobena obstoječa naprava. Eden izmed načinov za omejitev dostopa do naprav APPC v sistemu, ki uporablja APPN, je z izdelavo seznama pooblastil. Seznam pooblastil vsebuje seznam uporabnikov, ki imajo pooblastilo do naprav APPC. Nato lahko s pomočjo ukaza CHGCMDDFT (Spremeni privzetek ukaza) spremenite ukaz CRTDEVAPPC. Za parameter pooblastila (AUT) ukaza CRTDEVAPPC nastavite privzeto vrednost na seznam pooblastil, ki ste ga izdelali.

Opomba: Če v sistemu ne uporabljate angleščine, morate spremeniti privzetek ukaza v knjižnici QSYSxxxx za vsak narodni jezik v sistemu.

Veljavnost identitete drugega sistema, ki v vašem sistemu zahteva sejo (za uporabnika ali aplikacijo), lahko preverite s pomočjo parametra gesla mesta (LOCPWD) v opisu naprave APPC. Geslo mesta vam bo pomagalo odkriti lažni sistem.

Če uporabite gesla mest, se morate uskladiti z drugimi skrbniki za zaščito drugih sistemov v omrežju. Nadzorovati morate tudi, kdo lahko izdela ali spremeni opise naprav APPC in konfiguracijske sezname. Sistem zahteva posebno pooblastilo *IOSYSCFG za uporabo ukazov, ki omogočajo delo z napravami APPC in konfiguracijskimi seznami.

Opomba: Če uporabljate APPN, so gesla naprav shranjena na konfiguracijskem seznamu QAPPNRMT in ne v opisih naprav.

Dostop uporabnika APPC do ciljnega sistema

Ko sistem vzpostavi sejo APPC, izdela za uporabnika pot do vhoda v ciljni sistem. Številni drugi elementi določajo, kaj mora narediti uporabnik, da lahko vstopi v drug sistem.

Teme, ki sledijo, opisujejo elemente, ki določajo, kako pridobi uporabnik APPC dostop do ciljnega sistema.

Načini sistema za pošiljanje informacij o uporabniku

Arhitektura APPC nudi tri načine za pošiljanje zaščitnih informacij o uporabniku iz izvornega v ciljni sistem. Ti načini se imenujejo **oblikovane vrednosti zaščite**. Tabela 18 kaže te načine:

Opomba: V knjigi *APPC Programming* boste našli podrobnejše informacije o oblikovanih vrednostih zaščite.

Tabela 18. Vrednosti zaščite v arhitekturi APPC

Oblikovana vrednost zaščite	ID uporabnika, poslan v ciljni sistem	Geslo, poslano v ciljni sistem
None	Ne	Ne
Same	Da[1]	Glejte 2. opombo
Program	Da	Da[3]

Opombe:

1. Izvorni sistem pošlje ID uporabnika, če ciljni sistem poda SECURELOC(*YES) ali SECURELOC(*VFYENCPWD).
2. Uporabnik v zahtevo ne vnese gesla, ker ga je izvorni sistem že preveril. Izvorni sistem za SECURELOC(*YES) in SECURELOC(*NO) ne pošlje gesla. Za SECURELOC(*VFYENCPWD) pridobi izvorni sistem shranjeno, šifrirano geslo in ga pošlje (v šifrirani obliki).
3. Sistem pošlje geslo v šifrirani obliki, če podpirata šifriranje gesla izvorni in ciljni sistem. V nasprotnem primeru geslo ni šifrirano.

Aplikacija, ki jo zahteva uporabnika, določi oblikovano vrednost zaščite. Tako na primer SNADS vedno uporabi SECURITY(NONE). DDM uporablja SECURITY(SAME). S prehodom zaslonske postaje poda uporabnik vrednost zaščite z uporabo parametrov v ukazu STRPASTHR.

V vseh primerih ciljni primer izbere, ali bo sprejel zahtevo z vrednostjo zaščite, podano v izvornem sistemu. Včasih lahko ciljni sistem v celoti zavrne zahtevo, drugič pa zahteva drugo

vrednost zaščite. Če na primer uporabnik v ukazu STRPASTHR poda ID uporabnika in geslo, uporabi zahteva SECURITY(PGM). Toda če je sistemska vrednost QRMTSIGN v ciljnem sistemu *FRCSIGNON, bo uporabnik še vedno videl prijavni zaslon. Pri nastavitvi *FRCSIGNON sistem vedno uporabi SECURITY(NONE), kar je enako, kot če uporabnik za ukaz STRPASTHR ne bi vnesel ID-ja uporabnika in gesla.

Opombe:

1. Izvorni in ciljni sistem dogovorita vrednost zaščite, preden so poslani podatki. Če na primer poda ciljni sistem SECURELOC(*NO) in je zahteva SECURITY(SAME), ciljni sistem pove izvornemu sistemu, naj uporabi SECURITY(NONE). Izvorni sistem ne pošlje ID-ja uporabnika.
2. Ciljni sistem zavrne zahtevo za vzpostavitev seje, če je geslo uporabnika v ciljnem sistemu poteklo. To velja samo za povezovalne zahteve, ki pošljejo geslo, vključno z naslednjim:
   - zahteve za seje tipa SECURITY(PROGRAM)
   - zahteve za seje tipa SECURITY(SAME), če je vrednost SECURELOC nastavljena na *VFYENCPWD.

Možnosti za razdelitev odgovornosti za omrežno zaščito

Če je vaš sistem v omrežju, se morate odločiti, ali boste zaupali drugim sistemom pri preverjanju veljavnosti identitete uporabnika, ki poskuša vstopiti v vaš sistem. Ali boste sistemu SYSTEMA zaupali, da bo zagotovil, da je USERA v resnici USERA (ali da je QSECOFR v resnici QSECOFR)? Ali pa boste zahtevali, da uporabnik znova poda ID uporabnika in geslo?

Parameter varnega mesta (SECURELOC) v opisu naprave APPC v ciljnem sistemu podaja, ali je izvorni sistem varno (overjeno) mesto.

Če se v obeh sistemih izvaja izdaja, ki podpira *VFYENCPWD, SECURELOC(*VFYENCPWD), je na voljo dodatna zaščita, če uporabljajo aplikacije SECURITY(SAME). Čeprav zahtevnik v zahtevo ne vnese gesla, izvorni sistem pridobi geslo uporabnika in ga pošlje z zahtevo. Da bi zahteva uspela, mora imeti uporabnik isti ID uporabnika in geslo v obeh sistemih.

Če poda ciljni sistem SECURELOC(*VFYENCPWD) in izvorni sistem ne podpira te vrednosti, obravnava ciljni sistem zahtevo kot SECURITY(NONE).

Tabela 19 kaže skupno delovanje oblikovane vrednosti zaščite in vrednosti SECURELOC:

Tabela 19. Kako skupaj delujeta oblikovana vrednost zaščite APPC in vrednost SECURELOC

Izvorni sistem	**Ciljni sistem**	
Oblikovana vrednost zaščite	**Vrednost SECURELOC**	**Profil uporabnika za opravilo**
None	Any	Privzeti uporabnik [1]
Same	*NO	Privzeti uporabnik [1]
	*YES	Isto ime profila uporabnika kot ga ima zahtevnik izvornega sistema
	*VFYENCPWD	Isto ime profila uporabnika kot ga ima zahtevnik izvornega sistema. Uporabnik mora imeti v obeh sistemih isto geslo.
Program	Any	Profil uporabnika, ki je podan v zahtevi izvornega sistema.

Tabela 19. Kako skupaj delujeta oblikovana vrednost zaščite APPC in vrednost SECURELOC (nadaljevanje)

Izvorni sistem	Ciljni sistem	
Oblikovana vrednost zaščite	**Vrednost SECURELOC**	**Profil uporabnika za opravilo**
Opombe: 1. Privzeti uporabnik je določen s komunikacijsko postavko v opisu podsistema. To je opisano v razdelku “Dodelitev ciljnega sistema za profile uporabnikov opravil”.		

Dodelitev ciljnega sistema za profile uporabnikov opravil

Če zahteva uporabnik opravilo APPC v drugem sistemu, je z zahtevo povezano ime načina. Ime načina lahko izhaja iz zahteve uporabnika ali pa je privzeta vrednost iz omrežnih atributov izvornega sistema.

Ciljni sistem določi s pomočjo imena načina in imena naprave APPC kako se bo izvajalo opravilo. Ciljni sistem preišče aktivne podsisteme in poskusi najti komunikacijsko postavko, ki predstavlja najboljše ujemanje za ime naprave APPC in ime načina.

Komunikacijska postavka podaja, kateri profil uporabnika bo uporabil sistem za zahteve SECURITY(NONE). Sledi zgled komunikacijske postavke v opisu podsistema:

```
                      Prikaz komunikacijskih postavk

Opis podsistema:      QCMN           Status:   ACTIVE

                       Opis                          Privzeti      Največ
Naprava      Način     Opravila      Knjižnica       uporabnik     aktivnih
*ALL         *ANY      *USRPRF                       *SYS          *NOMAX
*ALL         QPCSUPP   *USRPRF                       *NONE         *NOMAX
```

Tabela 20 kaže možne vrednosti za parameter privzetega uporabnika v komunikacijski postavki:

Tabela 20. Možne vrednosti za parameter privzetega uporabnika

Vrednost	Rezultat
***NONE**	Na voljo ni noben privzeti uporabnik. Če izvorni sistem v zahtevi ne poda ID-ja uporabnika, se opravilo ne bo izvedlo.
***SYS**	Zagnali se bodo samo IBM-ovi programi (sistemska opravila). Zagnala se ne bo nobena uporabniška aplikacija.
ime-uporabnika	Če izvorni sistem ne pošlje ID-ja uporabnika, se bo opravilo zagnalo pod tem profilom uporabnika.

S pomočjo ukaza PRTSBSDAUT (Natisni opis podsistema) lahko natisnete seznam vseh podsistemov, ki imajo komunikacijske postavke s profilom privzetega uporabnika.

Možnosti prehoda zaslonske postaje

Prehod zaslonske postaje je zgled aplikacije, ki uporablja komunikacije APPC. Prehod zaslonske postaje lahko prijavite za prijavo v drug sistem, ki je z vašim sistemom povezan prek omrežja.

Tabela 21 kaže zglede zahtev za prehod (ukaz STRPASTHR) in kako jih obravnava ciljni sistem. Za prehod zaslonske postaje uporablja sistem osnovne elemente komunikacij APPC in sistemsko vrednost oddaljene prijave (QRMTSIGN).

Opomba: Zahteve za prehod zaslonske postaje niso več usmerjene prek podsistemov QCMN ali QBASE. Od izdaje V4R1 naprej niso več usmerjene prek podsistema QSYSWRK. Pred izdajo V4R1 ste lahko sklepali, da v primeru, da podsistem QCMD ali QBASE ni zagnan, prehod zaslonske postaje ne bo deloval. Vendar to ni več res. Prehod zaslonske postaje lahko prisilite prek QCMN (ali QBASE, če je aktiven), tako da spremenite sistemsko vrednost QPASTHRSVR v 0.

Tabela 21. Vzorčne zahteve za prijavo v prehod

Vrednosti v ukazu STRPASTHR		**Ciljni sistem**		
ID uporabnika	**Geslo**	**Vrednost SECURELOC**	**Vrednost QRMTSIGN**	**Rezultat**
*NONE	*NONE	Any	Any	Uporabnik se mora prijaviti v ciljni sistem.
Ime profila uporabnika	Ni vneseno	Any	Any	Zahteva ne uspe
*CURRENT	Ni vneseno	*NO	Any	Zahteva ne uspe
		*YES	*SAMEPRF	Interaktivno opravilo se zažene z istim imenom profila uporabnika kot profil uporabnika v izvornem sistemu. Oddaljenemu sistemu ni posredovano nobeno geslo.V ciljnem sistemu mora obstajati ime profila uporabnika.
			*VERIFY	
			*FRCSIGNON	Uporabnik se mora prijaviti v ciljni sistem.
		*VFYENCPWD	*SAMEPRF	Interaktivno opravilo se zažene z istim imenom profila uporabnika kot profil uporabnika v izvornem sistemu. Izvorni sistem pridobi geslo uporabnika in ga pošlje oddaljenemu sistemu. V ciljnem sistemu mora obstajati ime profila uporabnika.
			*VERIFY	
			*FRCSIGNON	Uporabnik se mora prijaviti v ciljni sistem.
*CURRENT (ali ime trenutnega profila uporabnika za opravilo)	Vneseno	Any	*SAMEPRF	Interaktivno opravilo se zažene z istim imenom profila uporabnika kot profil uporabnika v izvornem sistemu. Geslo *je* poslano oddaljenemu sistemu. V ciljnem sistemu mora obstajati ime profila uporabnika.
			*VERIFY	
			*FRCSIGNON	Uporabnik se mora prijaviti v ciljni sistem.

Tabela 21. Vzorčne zahteve za prijavo v prehod (nadaljevanje)

Vrednosti v ukazu STRPASTHR		Ciljni sistem		
ID uporabnika	**Geslo**	**Vrednost SECURELOC**	**Vrednost QRMTSIGN**	**Rezultat**
Ime profila uporabnika (ime, ki se razlikuje od trenutnega profila uporabnika za opravilo)	Vneseno	Any	*SAMEPRF	Zahteva ne uspe
			*VERIFY	Interaktivno opravilo se zažene z istim imenom profila uporabnika kot profil uporabnika v izvornem sistemu. Geslo *je* poslano oddaljenemu sistemu. V ciljnem sistemu mora obstajati ime profila uporabnika.
			*FRCSIGNON	Interaktivno opravilo se zažene s podanim imenom profila uporabnika. Geslo je poslano v ciljni sistem. Ime profila uporabnika mora obstajati v ciljnem sistemu.

Izognitev nepričakovanim dodelitvam naprav

Če pride do aktivni napravi do napake, jo poskusi sistem popraviti. V nekaterih primerih, ko pride do prekinitve povezave, lahko drug uporabnik nenamerno znova vzpostavi sejo, v kateri je prišlo do napake. Denimo, da je uporabnik USERA izklopil delovno postajo, ne da bi se odjavil. USERB lahko vklopi delovno postajo in znova zažene sejo USERA, ne da bi se prijavil.

Da bi preprečili to možnost, nastavite sistemsko vrednost QDEVRCYACN (Dejanje pri V/I napaki naprave) na *DSCMSG. Če pride do napake na napravi, bo sistem zaustavil opravilo uporabnika.

Krmiljenje oddaljenih ukazov in paketnih opravil

Kot pomoč pri nadzorovanju oddaljenih ukazov in opravil, ki se izvajajo v sistemu, so na voljo številne možnosti, vključno z naslednjim:

- Če v sistemu uporabljate DDM, lahko omejite dostop do datotek DDM, da uporabnikom preprečite uporabo ukaza SBMRMTCMD (Predloži oddaljeni ukaz) iz drugega sistema. Za uporabo SBMRMTCMD mora uporabnik odpreti datoteko DDM. Omejiti morate tudi zmožnost za izdelavo datotek DDM.
- Za sistemsko vrednost DDMACC (Dostop do zahtev DDM) lahko podate izhodni program. V izhodnem programu lahko preverite vse zahteve DDM, preden jih dovolite.
- S pomočjo omrežnega atributa JOBACN (Dejanje omrežnega opravila) lahko preprečite predložitev omrežnih opravil in njihovo samodejno izvajanje.
- Katere programske zahteve se lahko izvajajo v komunikacijskem okolju, lahko izrecno podate, če odstranite usmerjevalno postavko PGMEVOKE iz opisov podsistemov. Usmerjevalna postavka PGMEVOKE omogoča, da zahtevnik poda program, ki se izvaja. če odstranite to usmerjevalno postavko iz opisov podsistemov, kot je na primer opis podsistema QCMN, morate dodati usmerjevalne postavke za komunikacijske zahteve, ki se morajo uspešno izvesti.

  “Zahteve TPN-jev arhitekture” na strani 82 navaja imena programov za komunikacijske zahteve, ki jih zahtevajo IBM-ove aplikacije. Za vsako zahtevo, ki jo želite dovoliti, lahko dodate usmerjevalno postavko s primerjalno vrednostjo in z imenom programa, ki sta enaka imenu programa.

Če uporabite ta način, morate razumeti okolje za upravljanje dela v sistemu in vrste komunikacijskih zahtev, ki se izvajajo v sistemu. Če je mogoče, po spremembi usmerjevalnih postavk preizkusite vse vrste komunikacijskih in zagotovite, da pravilno delujejo. Če komunikacijska zahteva ne najde razpoložljive usmerjevalne postavke, se prikaže sporočilo CPF1269. Druga možnost (ki je manj občutljiva na napake, toda morda nekoliko manj učinkovita) je, da nastavite javno pooblastilo za transakcijske programe, ki jih ne želite izvajati v sistemu, na *EXCLUDE.

Opomba: V knjigi *Work Management* boste našli podrobnejše informacije o usmerjevalnih postavkah in o tem, kako sistem obravnava zahteva za zagon programov.

Vrednotenje konfiguracije APPC

S pomočjo ukaza PRTCMNSEC (Natisni zaščito komunikacij) ali menijskih možnosti lahko natisnete vrednosti, povezane z zaščito v konfiguraciji APPC. Teme, ki sledijo, opisujejo informacije na poročilih.

Ustrezni parametri za naprave APPC

Slika 9 kaže zgled poročila s komunikacijskimi informacijami za opise naprav. Slika 10 kaže zgled poročila za konfiguracijske sezname. Za poročili sledijo razlage polj na poročilih.

```
                          Komunikacijske informacije (celotno poročilo)
                                                                                SYSTEM4
Tip objekta  . . . . . . . . . :   *DEVD

                                                                                    Vnaprej       Zagon
Ime             Tip             Kategorija      Zaščiteno   Geslo       Zmožen za     Ena       vzpostavljena  programa
objekta         objekta         naprave         mesto       mesta        APPN         seja        seja         SNUF

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

Slika 9. Opisi naprav APPC - vzorčno poročilo

```
                  Prikaz konfiguracijskega seznama                Stran    1
                            SYSTEM4  12/17/95  07:24:36
Konfiguracijski seznam . . . . . :   QAPPNRMT
Tip konfiguracijskega seznama. . :   *APPNRMT
Besedilo . . . . . . . . . . . . :
-----------------Oddaljena mesta APPN------------------
          ID                  Oddaljena Omr. ID
Oddaljeno oddalj.   Lokalno   krmilna   krmilne   Zaščiteno
mesto     omrežja   mesto     točka     točke      mesto
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
-------------------------Oddaljena mesta APPN--------------------------
          ID                                        Lokalna    Vnaprej
Oddalj.   oddalj.    Lokalno    Ena       Število     krmilna  vzpostavljena
mesto     omrežja    mesto     seja      pogovorov     točka     seja
SYSTEM36  APPN      SYSTEM4    *NO             10      *NO        *NO
SYSTEM32  APPN      SYSTEM4    *NO             10      *NO        *NO
```

Slika 10. Poročilo konfiguracijskega seznama - zgled

Polje varnega mesta

Polje Varno mesto (SECURELOC) podaja, ali bo lokalni sistem zaupal oddaljenemu sistemu, ki bo izvajal preverjanje veljavnosti gesel namesto lokalnega sistema. Polje SECURELOC velja samo za aplikacije, ki uporabljajo vrednost SECURITY(SAME), kot so DDM in aplikacije, ki uporabljajo API komunikacij CPI.

Vrednost SECURELOC(*YES) poveča ranljivost lokalnega sistema zaradi možnih slabosti v oddaljenem sistemu. Vsi uporabniki, ki obstajajo v obeh sistemih, lahko pokličejo programe v lokalnem sistemu. To je še posebej nevarno, ker obstaja profil uporabnika QSECOFR (skrbnik za zaščito) v vseh sistemih iSeries in ima posebno pooblastilo *ALLOBJ. Če sistem v omrežju ne ščiti dobro gesla QSECOFR, so v nevarnosti drugi sistemi, ki obravnavajo ta sistem kot varno mesto.

Če uporabite SECURELOC(*VFYENCPWD), je sistem manj izpostavljen zaradi drugih sistemov, ki gesel ne ščitijo ustrezno. Uporabnik, ki zahteva aplikacijo, ki uporablja SECURITY(SAME), mora imeti enak ID uporabnika in geslo v obeh sistemih. SECURELOC(*VFYENCPWD) zahteva načela za upravljanje gesel v celotnem omrežju, tako da imajo uporabniki enako geslo v vseh sistemih.

Opomba: Vrednost SECURELOC(*VFYENCPWD) je podprta samo v sistemih, v katerih se izvaja V3R2, V3R7 ali V4R1. Če poda ciljni sistem SECURELOC(*VFYENCPWD) in izvorni sistem ne podpira te funkcije, je zahteva obravnavana kot SECURITY(NONE).

Če poda sistem SECURELOC(*NO), bodo potrebovale aplikacije, ki uporabljajo SECURITY(SAME), privzetega uporabnika za izvajanje programov. Privzeti uporabnik je odvisen od opisa naprave in načina, ki sta povezana z zahtevo. (Preglejte razdelek “Dodelitev ciljnega sistema za profile uporabnikov opravil” na strani 101.)

Polje gesla mesta

Polje z geslom mesto določa, ali bosta dva sistema izmenjala gesla, in preverila, da zahtevni sistem ni lažni sistem. V razdelku“Zgled: osnovna seja APPC” na strani 98 boste našli podrobnejše informacije o geslih mest.

Polje z zmožnostjo za

APPN

Polje Zmožen za APPN (APPN) podaja, ali lahko nudi oddaljeni sistem podporo za zahtevnejše funkcije omrežja ali je omejen na povezave z enim preskokom. APPN(*YES) pomeni naslednje:

- Če je oddaljeni sistem omrežno vozlišče, lahko oddaljeni sistem poveže lokalni sistem z drugimi sistemi. To se imenuje **usmerjanje prek vmesnega vozlišča**. To pomeni, da lahko uporabniki v vašem sistemu uporabijo oddaljeni sistem na poti do večjega omrežja.
- Če je lokalni sistem omreženo vozlišče, ga lahko uporabi oddaljeni sistem za povezavo z drugimi sistemi. Uporabniki v oddaljenem omrežju lahko uporabijo vaš sistem na poti do večjega omrežja.

  Opomba: Za določitev, ali je sistem omrežno vozlišče ali končno vozlišče, lahko uporabite ukaz DSPNETA.

Polje ene seje

Polje ene seje (SNGSSN) podaja, ali lahko oddaljeni sistem z uporabo istega opisa naprave APPC sočasno izvaja več kot eno sejo. Običajno se uporablja SNGSSN(*NO), ker ni potrebno izdelati več opisov naprav za oddaljeni sistem. Uporabnik PC-ja na primer pogosto

zahteva več kot eno emulacijsko sejo 5250 in seje za funkcije datotečnega in tiskalnega strežnika. Če podate SNGSSN(*NO), lahko omogočite to funkcijo z enim opisom naprave za PC v oddaljenem sistemu iSeries.

SNGSSN(*NO) pomeni, da se morate zanesti na operacijske postopke uporabnikov PC in drugih uporabnikov APPC, ki upoštevajo zaščito. Vaš sistem je izpostavljen nekomu v oddaljenemu sistemu, ki zažene nepooblaščeno sejo, ki uporablja isti opis naprave kot obstoječa seja. (Ta postopek se včasih imenuje **priklop**.)

Polje vnaprej vzpostavljene seje

Polje vnaprej vzpostavljene seje (PREESTSSN) za napravo z eno sejo nadzoruje, ali zažene lokalni sistem sejo z oddaljenim sistemom, ko oddaljeni sistem prvič stopi v stik z lokalnim sistemom. PREESTSSN(*NO) pomeni, da lokalni sistem ne vzpostavi seje, dokler aplikacija ne zahteva seje s sistemom. Nastavitev PREESTSSN(*YES) je koristna za zmanjšanje časa, potrebnega, da uporabniški program dokonča povezavo.

Nastavitev PREESTSSN(*YES) preprečuje, da bi sistem prekinil naročniško (klicno) linijo, ki ni več v uporabi. Aplikacija ali uporabnik morata linijo izrecno izključiti. PREESTSSN(*YES) lahko poveča čas, ko je lokalni sistem ranljiv za priklop nekoga na sejo.

Polje zagona programa SNUF

Polje zagona programa SNUF podaja, ali lahko oddaljeni sistem zažene programe v oddaljenem sistemu. *YES pomeni, da morate v lokalnem sistemu uporabljati ustrezno shemo objektnih pooblastil, ki ščiti objekte, ko uporabniki v oddaljenem sistemu zaženejo opravila in programe v lokalnem sistemu.

Parametri za krmilnike APPC

Slika 11 kaže zgled poročila komunikacijskih informacij za opise krmilnikov. Za poročili boste našli opise polj poročil.

```
                    Komunikacijske informacije (celotno poročilo)
                                                                                SYSTEM4
Tip objekta  . . . . . . . . . . :   *CTLD

Ime       Tip       Kategorija  Samodejna  Naročniški    Smer      Zmožen za   Seje     Časomer      Sekunde   Ime
objekta   objekta   krmilnika    izdelava   krmilnik     klica      APPN        CP      prekinitve   brisanja  naprave
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. Opisi krmilnikov APPC - vzorčno poročilo

Polje samodejne izdelave

Polje samodejne izdelave (AUTOCRTCTL) v opisu linije podaja, ali bo lokalni sistem samodejno izdelal opis krmilnika, če vhodna zahteva ne more najti ustreznega opisa krmilnika. Polje samodejne izdelave (AUTOCRTDEV) v opisu krmilnika podaja, ali bo lokalni sistem samodejno izdelal opis naprave, če vhodna zahteva ne more najti ustreznega opisa naprave.

Za krmilnike z zmožnostjo za APPN polje samodejne izdelave ne velja. Sistem samodejno izdela opise naprav po potrebi, ne glede na to, kako nastavite polje samodejne izdelave.

Če podate za opis linije *YES, se lahko z vašim sistemom poveže vsakdo z dostopom do linije. To vključuje tudi mesta, ki so povezana z mostiči in usmerjevalniki.

Polje sej krmilne točke

Za krmilnike z zmožnostjo za APPN nadzoruje polje sej krmilne točke (CPSSN) ali bo sistem samodejno vzpostavil povezavo APPC z oddaljenim sistemom. Sistem izmenja omrežne

informacije in status z oddaljenim sistemom s pomočjo seje CP. Izmenjava najnovejših informacij med omrežnimi vozlišči APPN je še posebej pomembna za neovirano delovanje omrežja.

Če podate *YES, se mirujoča naročniška linija ne prekine samodejno. Zaradi tega je vaš sistem bolj ranljiv na priklop nekoga na sejo.

Polje časomera prekinitve

Za krmilnike APPC podaja polje časomera prekinitve kako dolga mora biti krmilnik neuporabljen (brez aktivnih sej), preden sistem prekine linijo z oddaljenim sistemom. To polje ima dve vrednosti. Prva vrednost podaja, kako dolgo bo ostal krmilnik aktiven od prve vzpostavitve povezave. Druga vrednost podaja, kako dolgo bo sistem počakal po dokončanju zadnje seje krmilnika, preden bo prekinil povezavo.

Sistem uporabi časomer prekinitve samo, če je polje prekinitve naročniške linije (SWTDSC) nastavljeno na *YES.

Če uporabite za to nastavitev velike vrednosti, bo vaš sistem bolj ranljiv za priklop na seje.

Parametri za opise linij

Slika 12 kaže zgled poročila komunikacijskih informacij za opise lini.j Za poročili boste našli opise polj poročil.

```
                    Komunikacijske informacije (celotno poročilo)

Tip objekta  . . . . . . . . . . :   *LIND
Ime
samodejnega    Tip           Kategorija     Samodejna  Sekunde     Samodejni  Samodejno
objekta        objekta       linije         izdelava   brisanja    odgovor    klicanje
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. Opisi linij APPC - vzorčno poročilo

Polje samodejnega odgovora

Polje samodejnega odgovora (AUTOANS) podaja, ali bo sprejela naročniška linija vhodne klice brez posega operaterja.

Če podate *YES, bo vaš sistem manj zaščiten, ker je dostop do njega preprostejši. Če želite zmanjšati luknjo v zaščiti, če podate *YES, izklopite linijo, kadar je ne potrebujete.

Polje samodejnega klicanja

Polje samodejnega klicanja (AUTODIAL) podaja, ali lahko izvaja naročniška linija izhodne klice brez posega operaterja. Če podate *YES, omogočite, da se lokalni uporabniki, ki nimajo fizičnega dostopa do komunikacijskih linij in modemov, povežejo z drugimi sistemi.

Poglavje 14. Zaščitene komunikacije TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) je splošen način, ki ga uporabljajo računalniki vseh vrst za medsebojno komuniciranje. Aplikacije TCP/IP so dobro znane in veliko uporabljane v "informacijski poti".

V tem poglavju boste našli nasvete za naslednje:

- Preprečevanja izvajanja aplikacij TCP/IP v sistemu.
- Zaščita sistemskih sredstev, če omogočite izvajanje aplikacij TCP/IP v sistemu.

Na spletni strani iSeries Informacijski center—>Delo z omrežjem—>TCP/IP boste našli popolne informacije o vseh aplikacijah TCP/IP. *SecureWay: iSeries in Internet* (iSeries Informacijski center—>Zaščita—>SecureWay opisuje problematiko zaščite, če povežete strežnik iSeries v internet (zelo veliko omrežje TCP/IP) ali intranet. V razdelku "Predpogoji in s tem povezane informacije" na strani xii boste našli informacije o dostopu do Informacijskega centra iSeries.

Ne pozabite, da podpirajo strežniki iSeries številne možne aplikacije TCP/IP. Če se odločite, da boste v sistemu omogočili eno aplikacijo TCP/IP, lahko omogočite tudi druge. Kot skrbnik za zaščito morate poznati območje aplikacij TCP/IP in vpliv na zaščito, ki ga imajo te aplikacije.

Preprečevanje obdelave TCP/IP

Opravila strežnika TCP/IP se izvajajo v podsistemu QSYSWRK. Z ukazom STRTCP (Zaženi TCP/IP) zaženete TCP/IP v sistemu. Če ne želite, da se izvede kakršnakoli obdelava ali aplikacija TCP/IP, ne uporabite ukaza STRTCP. Sistem je naložen tako, da je javno pooblastilo za ukaz STRTCP nastavljeno na *EXCLUDE.

Če sumite, da kdo z dostopom do ukaza izvaja TCP/IP (na primer izven uradnih ur), lahko za ukaz STRTCP nastavite objektno beleženje. Sistem bo zapisal postavko beleženja vsakič, ko uporabnik zažene ukaz.

Komponente zaščite TCP/IP

Uporabljate lahko številne komponente zaščite TCP/IP, ki bodo izboljšale omrežno zaščito in dodale prožnost. Čeprav lahko nekatere od teh tehnologij najdete tudi v izdelkih požarnih zidov, namen teh komponent za zaščito TCP/IP za OS/400 ni, da bi jih uporabljali kot požarni zid. Vendar pa boste nekatere od teh komponent v določenih primerih lahko uporabili namesto ločenega izdelka požarnega zidu. Te komponente TCP/IP vam bodo nudile tudi dodatno zaščito v okoljih, kjer že uporabljate požarni zid.

S pomočjo naslednjih komponent lahko izboljšate zaščito TCP/IP:

- Pravila paketov
- Strežnik Proxy HTTP
- VPN (delo z navideznim zasebnim omrežjem)
- SSL (plast zaščitenih vtičnic)

Uporaba pravil paketov za zaščito prometa TCP/IP

Pravila paketov, ki so kombinacija filtriranja IP in prevoda omrežnega naslova (NAT), delujejo kot požarni zid, ki ščiti notranje omrežje pred napadalci. Filtriranje IP omogoča

nadzor nad prometom IP, ki lahko vstopa v omrežje in potuje iz njega. V bistvu ščiti omrežje s filtriranjem paketov na osnovi pravil, ki jih definirate. Po drugi strani pa NAT omogoča, da skrijete neregistrirane zasebne naslove IP za niz registriranih naslovov IP. S tem zaščitite notranje omrežje pred zunanjimi omrežji. NAT tudi pomaga pri zmanjšanju težav zaradi izčrpanosti naslovov IP, ker lahko veliko zasebnih naslovov predstavite z majhnim nizom registriranih naslovov. Podrobnejše informacije boste našli v Informacijskem centru iSeries.

Strežnik HTTP proxy

Strežnik HTTP proxy je del strežnika IBM HTTP za strežnik iSeries. Strežnik HTTP je del OS/400. Strežnik proxy sprejema zahteve HTTP spletnih brskalnikov in jih pošilja spletnim strežnikom. Spletni strežniki, ki sprejmejo zahteve, poznajo samo naslov IP strežnika proxy in ne morejo določiti imen ali naslov PC-jev, s katerih izvirajo zahteve. Strežnik proxy lahko obravnava zahteve URL za HTTP, FTP, Gopher in WAIS.

Strežnik proxy shrani v predpomnilnik vrnjene spletne strani zahtev, ki jih izdajo vsi uporabniki strežnika proxy. Če uporabniki torej zahtevajo stran, strežnik proxy preveri, ali je v predpomnilniku. Če je, jo strežnik proxy vrne. Z uporabo strani iz predpomnilnika lahko strežnik proxy hitreje streže spletne strani, s čimer odstrani dolgotrajne zahteve za spletne strežnike.

Strežnik proxy lahko tudi zabeleži vse zahteve URL v namen sledenja. S pomočjo dnevnikov lahko nato nadzorujete uporabo in napačno uporabo omrežnih sredstev.

Podporo za HTTP lahko uporabite na strežniku IBM HTTP za ojačanje dostopa do spletnih strani. Naslovi odjemalcev PC-ce so skriti pred spletnimi strežniki, do katerih dostopajo; ti strežniki poznajo samo naslov IP strežnika proxy. Uporaba shranjevanja strani v predpomnilnik lahko tudi zmanjša zahteve za komunikacijsko pasovno širino in obremenitev požarnega zidu. Poiščite domačo stran IBM HTTP Server for iSeries, kjer boste našli podrobnejše informacije. Naslov je naslednji: http://www-1.ibm.com/servers/eserver/iseries/software/http/index.html

Delo z navideznim zasebnim omrežjem (VPN)

Navidezno zasebno omrežje (VPN) omogoča, da v podjetju varno razširite zasebni intranet prek obstoječega ogrodja javnega omrežja kot je internet. S pomočjo VPN lahko v podjetju nadzorujete promet in nudite pomembni komponenti zaščite kot sta overjanje in zasebnost podatkov.

OS/400 VPN je komponenta Navigatorja iSeries, grafičnega uporabniškega vmesnika (GUI) za OS/400, ki jo je mogoče namestiti po želji. Omogoča vam, da izdelate zaščiteno pot med kakršnokoli kombinacijo gostitelja in prehoda. OS/400 VPN uporablja metode overjanja, algoritme šifriranja in druge varnostne ukrepe, s pomočjo katerih zagotovi, da so podatki, ki se pošiljajo med dvema končnima točkama povezave, zaščiteni.

VPN se izvaja v omrežni plasti modela komunikacijskega sklada TCP/IP. VPN uporablja odprto ogrodje arhitekture IPSec (IP Security). IPSec nudi osnovne zaščitne funkcije za internet, kot tudi prožne gradnike, na osnovi katerih lahko izdelate robustna, zaščitena navidezna zasebna omrežja.

VPN podpira tudi rešitve VPN L2TP (Layer 2 Tunnel Protocol). Povezave L2TP, ki se imenujejo tudi navidezne linije, nudijo oddaljenim uporabnikom stroškovno sprejemljiv dostop, saj omogočajo, da združen omrežni strežnik upravlja naslove IP, dodeljene njegovim oddaljenim uporabnikom. Poleg tega nudijo povezave L2TP zaščiten dostop do sistema ali omrežja, če jih zaščitite z IPSec.

Pomembno je, da razumete vpliv, ki ga ima VPN na vaše celotno omrežje. Bistvenega pomena za uspešno delovanje sta pravilno načrtovanje in izvedba. Preberite temo Informacijskega centra iSeries z naslovom VPN, da boste razumeli, kako deluje VPN in kako ga lahko uporabite. Podrobnejše informacije boste našli v Informacijskem centru iSeries —>Zaščita—>Delo z navideznim zasebnim omrežjem. V razdelku “Predpogoji in s tem povezane informacije” na strani xii boste našli informacije o dostopu do Informacijskega centra iSeries.

Plast zaščitenih vtičnic (SSL)

Plast zaščitenih vtičnic (SSL) je postala industrijski standard za omogočanje aplikacij za zaščitene komunikacijske seje prek nezaščitenega omrežja kot je internet. Protokol SSL vzpostavi zaščiteno povezavo med odjemalskimi in strežniškimi aplikacijami, kar omogoči overjanje ene ali obeh zaključnih točk komunikacijske seje. SSL nudi tudi zasebnost in integriteto podatkov, ki jih izmenjajo odjemalske in strežniške aplikacije. Podrobnejše informacije lahko najdete v Informacijskem centru iSeries –>Zaščita—>Plast zaščitenih vtičnic (SSL). V razdelku “Predpogoji in s tem povezane informacije” na strani xii boste našli podrobnejše informacije o dostopu do Informacijskega centra iSeries.

Zaščita okolja TCP/IP

V tej temi boste našli splošne predloge za korake, ki jih lahko opravite, da zmanjšate luknje v zaščiti okolja TCP/IP v sistemu. Ti nasveti se nanašajo na celotno okolje TPC/IP in ne na specifične aplikacije, ki so razložene v nadaljnjih temah.

- Pri pisanju aplikacije za vrata TCP/IP morate paziti, da je aplikacija ustrezno zaščitena. Zavedati se morate, da lahko poskusi napadalec dostopiti do te aplikacije prek teh vrat. Izkušen napadalec lahko poskusi dostopiti do te aplikacije z uporabo TELNET-a.
- Nadzorujte uporabo vrat TCP/IP v sistemu. Uporabniška aplikacija, ki je povezana z vrati TCP/IP, lahko nudi vhod prek “zadnjih vrat” v sistem brez ID-ja uporabnika in gesla. Nekdo z zadostnim pooblastilom v sistemu lahko poveže aplikacijo z vrati TCP ali UDP.
- Kot skrbnik za zaščito morate tehniko, imenovano *lažno predstavljanje IP*, ki jo uporabljajo hekerji. Vsak sistem v omrežju TCP/IP ima naslov IP. Nekdo, ki uporablja lažno predstavljanje IP, nastavi sistem (običajno PC) tako, da se pretvarja, da je obstoječ naslov IP ali overjen naslov IP. Lažen sistem se tako pretvarja, da je sistem, s katerim se običajno povežete, in vzpostavi povezavo z vašim sistemom.

  Če v sistemu izvajate TCP/IP in sistem sodeluje v omrežju, ki ni fizično zaščiteno (vse nenaročniške linije in vnaprej definirane povezave), niste zaščiteni pred lažnim predstavljanjem IP. Da bi sistem zaščitili pred škodo, ki jo lahko povzroči “slepar”, začnite s predlogi v tem poglavju kot sta zaščita prijave in zaščita objektov. Zagotoviti morate tudi, da ima sistem nastavljene ustrezne omejitve pomožnega pomnilnika. S tem preprečite lažnemu sistemu, da bi vaš sistem preobremenil s pošto ali vmesnimi datotekami v tolikšni meri, da sistem ne bi mogel več delovati.

  Prav tako morate tudi redno nadzorovati dejavnost TCP/IP v sistemu. Če odkrijete lažno predstavljanje IP, lahko poskusite odkriti slabe točke v nastavitvi TCP/IP in opraviti prilagoditve.
- Za intranet (omrežje sistemov, ki ne potrebujejo neposredno izhodne povezave) uporabite naslove IP, ki jih je mogoče znova uporabiti. Naslovi, ki jih je mogoče znova uporabiti, so namenjeni za uporabo znotraj zasebnega omrežja. Hrbtenica interneta ne usmerja paketov z naslovi IP, ki jih je mogoče znova uporabiti. Zato nudijo naslovi, ki jih je mogoče znova uporabiti, dodatno plast zaščite znotraj požarnega zidu.

  Na spletni strani iSeries Informacijski center—>Delo z omrežjem—>TCP/IP boste našli podrobnejše informacije o dodeljevanju naslovov IP in o območjih naslovov IP, kot tudi o zaščitnih informacijah TCP/IP.

- Če nameravate povezati sistem v internet ali intranet, preglejte informacije o zaščiti na *SecureWay: iSeries in internet* (Informacijski center iSeries —>Zaščita—>SecureWay). V razdelku“Predpogoji in s tem povezane informacije” na strani xii lahko najdete informacije o dostopu do Informacijskega centra iSeries.

Krmiljenje, kateri strežniki TCP/IP se zaženejo samodejno

Kot skrbnik za zaščito morate nadzorovati, katere aplikacije TCP/IP se samodejno zaženejo pri zagonu TCP/IP. Za zagon TCP/IP sta na voljo dva ukaza. Za vsak ukaz uporabi sistem drug način za določitev, katere aplikacije (strežnike) bo zagnal.

Tabela 22 kaže dva ukaza in priporočila za zaščito, povezana z njima. Tabela 23 kaže privzete vrednosti samodejnega zagona za strežnike. Če želite spremeniti vrednost samodejnega zagona za strežnik, uporabite ukaz CHGxxxA (Spremeni atribute xxx) za strežnik. Ukaz za TELNET je na primer CHGTELNA.

Tabela 22. Kako TCP/IP določi, katere strežnike zagnati

Ukaz	Kateri strežniki se zaženejo	Priporočila za zaščito
Zaženi TCP/IP (STRTCP)	Sistem zažene vse strežnike, ki imajo podano vrednost AUTOSTART(*YES). Tabela 23 kaže naloženo vrednost za vsak strežnik TCP/IP.	• Pri dodelitvi posebnega pooblastila *IOSYSCFG bodite previdni, saj boste tako lahko nadzorovali, kdo lahko spreminja nastavitve samodejnega zagona. • Natančno nadzorujte, kdo ima pooblastilo za uporabo ukaza STRTCP. Privzeto javno pooblastilo za ukaz je *EXCLUDE. • Nastavite beleženje objektov za ukaze Spremeni atribute *ime-strežnika* (kot je CHGTELNA), da boste nadzorovali uporabnike, ki poskušajo spremeniti vrednost AUTOSTART za strežnik.
Zaženi strežnik TCP/IP (STRTCPSVR)	Za podajanje, katere strežnike zagnati, uporabite parameter. Privzeta vrednost tega ukaza je zagon vseh strežnikov.	• S pomočjo ukaza CHGCMDDFT (Spremeni privzetek ukaza) nastavite ukaz STRTCPSVR tako, da bo zagnal samo določen strežnik. S tem uporabnikom ne preprečite zagona drugih strežnikov, toda če spremenite privzeto vrednost ukaza, bo manj verjetno, da bodo uporabniki po nesreči zagnali vse strežnike. Naslednji ukaz lahko na primer uporabite za nastavitev privzete vrednosti, ki podaja zagon samo strežnika TELNET: CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*TELNET)') **Opomba:** Če spremenite privzeto vrednost, lahko podate samo en strežnik. Izberite strežnik, ki ga redno uporabljate ali strežnik, za katerega je manjša verjetnost, da bo povzročal luknje v zaščiti (kot je TFTP). • Natančno nadzorujte, kdo ima pooblastilo za uporabo ukaza STRTCPSVR. Privzeto javno pooblastilo za ukaz je *EXCLUDE.

Naslednja tabela vsebuje vrednosti samodejnega zagona za strežnike TCP/IP. Podrobnejše informacije za te strežnike lahko najdete v Informacijskem centru iSeries (**Delo z omrežjem—>TCP/IP**). V razdelku“Predpogoji in s tem povezane informacije” na strani xii lahko najdete podrobnejše informacije o dostopu do Informacijskega centra iSeries.

Tabela 23. Vrednosti samodejnega zagona za strežnike TCP/IP

Strežnik	Privzeta vrednost	Vaša vrednost
TELNET	AUTOSTART(*YES)	
FTP (file transfer protocol)	AUTOSTART(*YES)	
BOOTP (Bootstrap Protocol)	AUTOSTART(*NO)	
TFTP (trivial file transfer protocol)	AUTOSTART(*NO)	

Tabela 23. Vrednosti samodejnega zagona za strežnike TCP/IP (nadaljevanje)

Strežnik	Privzeta vrednost	Vaša vrednost
REXEC (strežnik za oddaljeno izvedbo)	AUTOSTART(*NO)	
RouteD (Demon usmerjanja)	AUTOSTART(*NO)	
SMTP (simple mail transfer protocol)	AUTOSTART(*YES)	
POP (Post Office Protocol)	AUTOSTART(*NO)	
HTTP (Hypertext Transfer Protocol) [1]	AUTOSTART(*NO)	
ICS (Internet Connection Server)[1]	AUTOSTART(*NO)	
LPD (demon vrstičnega tiskalnika)	AUTOSTART(*YES)	
SNMP (Simple Network Management Protocol (SNMP))	AUTOSTART(*YES)	
DNS (imenski sistem domen)	AUTOSTART(*NO)	
DDM	AUTOSTART(*NO)	
DHCP (dynamic host configuration protocol)	AUTOSTART(*NO)	
NSMI	AUTOSTART(*NO)	
INETD	AUTOSTART(*NO)	

Opombe:

1. S strežnikom IBM HTTP za strežnik iSeries uporabite za nastavitev vrednosti AUTOSTART ukaz CHGHTTPA.

Problematika zaščite pri uporabi SLIP

Podpora TCP/IP za strežnik iSeries vključuje Serial Interface Line Protocol (SLIP). SLIP nudi povezljivost od točke do točke z nizkimi stroški. Uporabnik SLIP lahko vzpostavi povezavo z omrežjem LAN ali WAN z vzpostavitvijo povezave od točke do točke s sistemom, ki je del omrežja LAN ali WAN.

SLIP se izvaja prek asinhrone povezave. Uporabite ga lahko za klicno povezavo na strežnike iSeries in z njih. S pomočjo protokola SLIP lahko na primer pokličete sistem iSeries s PC-ja. Ko je povezava vzpostavljena, se lahko s pomočjo aplikacije TELNET na PC-ju povežete s strežnikom TELNET iSeries ali pa z aplikacijo FTP prenesete datoteke med dvema sistemoma.

Ko dobite sistem, v njem ne obstaja konfiguracija SLIP. Če torej ne želite, da se SLIP (in klicni dostop TCP/IP) izvaja v sistemu, ne konfigurirajte nobenih konfiguracijskih profilov za SLIP. Za izdelavo konfiguracij SLIP uporabite ukaz WRKTCPPTP (Delo s TCP/IP od točke do točke). Za uporabo ukaza WRKTCPPTP potrebujete posebno pooblastilo *IOSYSCFG.

Če želite, da se SLIP izvaja v sistemu, izdelajte enega ali več konfiguracijskih profilov SLIP (od točke do točke). Konfiguracijske profile lahko izdelate v naslednjih operacijskih načinih:
- vhodno klicanje (*ANS)
- izhodno klicanje (*DIAL)

V temah, ki sledijo, bomo razložili, kako lahko nastavite zaščito za konfiguracijske profile SLIP.

Opomba: **Profil uporabnika** je objekt strežnika iSeries, ki omogoča prijavo. Za vsako opravilo strežnika iSeries se mora izvajati profil uporabnika. **Konfiguracijski profil** shranjuje informacije, ki se uporabljajo za vzpostavitev povezave SLIP s

sistemom iSeries. Ko zaženete povezavo SLIP s strežniki iSeries, preprosto vzpostavite povezavo. S tem se še ne prijavite in zaženete opravila strežnika iSeries. Zato za zagon povezave SLIP s strežniki iSeries ni nujno potreben profil uporabnika. Toda kot boste videli kasneje v razlagi, bo lahko zahteval profil konfiguracije SLIP profil uporabnika za določitev, ali naj dovoli povezavo.

Nadzorovanje vhodnih klicnih povezav SLIP

Preden lahko nekdo vzpostavi vhodno klicno povezavo z vašim sistemom s pomočjo SLIP, morate zagnati konfiguracijski profil *ANS SLIP. Za izdelavo ali spremembo konfiguracijskega profila SLIP uporabite ukaz WRKTCPPTP (Delo s TCP/IP od točke do točke). Za zagon konfiguracijskega profila uporabite ukaz STRTCPPTP (Zaženi TCP/IP od točke do točke) ali možnost z zaslona WRKTCPPTP. Ko dobite sistem, je javno pooblastilo za ukaza STRTCPPTP in ENDTCPPTP nastavljeno na *EXCLUDE. Možnosti za dodajanje, spreminjanje in brisanje konfiguracijskih profilov SLIP so na voljo samo, če imate posebno pooblastilo *IOSYSCFG. Kot skrbnik za zaščito lahko s pomočjo pooblastil za ukaze in posebnih pooblastil določite, kdo lahko nastavi sistem, tako da bo omogočal vhodne klicne povezave.

Zaščita vhodne klicne povezave SLIP

Če želite preveriti veljavnost sistemov, ki kličejo vaš sistem, morajo poslati zahtevni sistemi ID uporabnika in geslo. Vaš sistem nato preveri njuno veljavnost. Če ID uporabnika in geslo nista veljavna, lahko sistem zavrne zahtevo za vzpostavitev seje.

Preverjanje veljavnosti vhodnih klicev nastavite takole:

__ Korak 1. Izdelajte profil uporabnika, ki ga lahko uporabi zahtevni sistem za vzpostavitev povezave. ID uporabnika in geslo, ki ju pošlje zahtevnik, se morata ujemati s tem imenom profila uporabnika in geslom.

Opomba: Da bi lahko sistem preverjal veljavnost gesel, mora biti sistemska vrednost QSECURITY nastavljena na 20 ali več.

Kot dodatno zaščito boste najbrž izdelali profile uporabnikov, namenjene posebej za vzpostavljanje povezav SLIP. Profili uporabnikov naj imajo omejeno pooblastilo v sistemu. Če nameravate uporabljati profile samo za vzpostavljanje povezav SLIP, lahko v profilih uporabnikov nastavite naslednje vrednosti:

- INLMNU (začetni meni) *SIGNOFF
- INLPGM (začetni program) *NONE.
- LMTCPB (omeji zmožnosti) *YES

Te vrednosti preprečujejo, da bi se kdorkoli prijavil interaktivno s profilom uporabnika.

__ Korak 2. Izdelajte pooblastitveni seznam, da bo sistem preverjal, kdaj poskusi zahtevnik vzpostaviti povezavo SLIP.

Opomba: Ta pooblastitveni seznam podate v polju *Pooblastitveni seznam za dostop do sistema*, ko izdelate ali spremenite profil SLIP. (Glejte korak 4.)

__ Korak 3. S pomočjo ukaza ADDAUTLE (Dodaj pooblastitveno postavko) dodajte na pooblastitveni seznam profil uporabnika, ki ste ga izdelali v koraku 1. Za vsak konfiguracijski profil od točke do točke lahko izdelate unikaten pooblastitveni seznam ali izdelate pooblastitveni seznam, ki ga souporablja več konfiguracijskih profilov.

__ Korak 4. S pomočjo ukaza WRKTCPPTP nastavite profil *ANS TCP/IP od točke do točke, ki ima naslednje značilnosti:

- Konfiguracijski profil mora uporabljati skript povezovalnega pogovornega okna, ki vključuje funkcijo preverjanja veljavnosti uporabnikov. Preverjanje veljavnosti uporabnikov vključuje sprejem ID-jev uporabnikov in gesel zahtevnikov in preverjanje njihove veljavnosti. Sistem vključuje številne vzorčne skripte pogovornih oken, ki nudijo to funkcijo.
- Konfiguracijski profil mora podajati ime pooblastitvenega seznama, ki ste ga izdelali v koraku 2. ID uporabnika, ki ga prejme skript povezovalnega pogovornega okna, mora biti na pooblastitvenem seznamu.

Ne pozabite, da vplivajo na vrednost nastavitve zaščite za vhodne klice varnostni postopki in zmožnosti sistemov, ki kličejo v omrežje. Če zahtevate ID uporabnika in geslo, mora skript povezovalnega pogovornega okna v sistemu zahtevnika poslati ta ID uporabnika in geslo. Nekateri sistemi, kot so strežniki iSeries, nudijo varen način za shranjevanje ID-jev uporabnikov in gesel. (Ta način opisuje “Zaščita in seje izhodnih klicev”.) Drugi sistemi shranijo ID uporabnika in geslo v skriptu, do katerega lahko dostopi kdorkoli, ki ve, kje v sistemu najti skript.

Zaradi različnih varnostnih postopkov in zmožnosti partnerjev, s katerimi komunicirate, lahko izdelate različne konfiguracijske profile za različna okolja zahtevnikov. S pomočjo ukaza STRTCPPTP lahko nastavite sistem tako, da sprejme sejo za določen konfiguracijski profil. Seje za nekatere konfiguracijske profile je na primer mogoče zagnati samo ob določenih urah. Za beleženje dejavnosti povezanih profilov uporabnikov lahko uporabite beleženje zaščite.

Preprečevanje dostopa uporabnikom vhodnih klicev do drugih sistemov

Od konfiguracije vašega sistema in omrežja je odvisno, ali bo lahko uporabnik, ki zažene povezavo SLIP, dostopil do drugega sistema v omrežju, ne da bi se prijavil v vaš sistem. Uporabnik lahko na primer vzpostavi povezavo SLIP z vašim sistemom, nato pa vzpostavi povezavo FTP z drugim sistemom v omrežju, ki ne dopušča vhodnih klicev.

Če želite preprečiti uporabnikom SLIP dostop do drugih sistemov v omrežju, podajte v polju konfiguracijske profila *Omogoči odpošiljanje datagramov IP* vrednost N (Ne). S tem preprečite, da bi uporabnik dostopil do omrežja, preden se prijavi v sistem. Toda ko se uporabnik uspešno prijavi v sistem, vrednost za odpošiljanje datagramov ne deluje več. Vrednost ne omeji zmožnosti uporabnika za uporabo aplikacije TCP/IP v sistemu iSeries (kot je FTP ali TELNET) za vzpostavitev povezave z drugim sistemom v omrežju.

Krmiljenje sej izhodnih povezav

Preden lahko nekdo s pomočjo SLIP vzpostavi izhodno povezavo iz vašega sistema, morate zagnati konfiguracijski profil SLIP *DIAL. Za izdelavo ali spremembo konfiguracijskega profila SLIP uporabite ukaz WRKTCPPTP. Za zagon konfiguracijskega profila uporabite ukaz STRTCPPTP (Zaženi TCP/IP od točke do točke) ali možnost z zaslona WRKTCPPTP. Ko dobite sistem, je javno pooblastilo za ukaza STRTCPPTP in ENDTCPPTP nastavljeno na *EXCLUDE. Možnosti za dodajanje, spreminjanje in brisanje konfiguracijskih profilov SLIP so na voljo samo, če imate posebno pooblastilo *IOSYSCFG. Kot skrbnik za zaščito lahko s pomočjo pooblastil za ukaze in posebnih pooblastil določite, kdo lahko nastavi sistem, tako da bo omogočal izhodne klicne povezave.

Zaščita in seje izhodnih klicev

Uporabniki v vašem sistemu iSeries lahko vzpostavijo izhodne povezave s sistemi, ki zahtevajo preverjanje veljavnosti uporabnikov. Skript povezovalnega pogovornega okna na strežniku iSeries mora poslati oddaljenemu sistemu ID uporabnika in geslo. Strežniki iSeries nudijo varen način za shranitev tega gesla. Geslo ni nujno shranjeno v skriptu povezovalnega pogovornega okna.

Opombe:

1. Čeprav shrani sistem geslo povezave v šifrirani obliki, ga pred pošiljanjem dešifrira. Gesla SLIP, podobno kot gesla FTP in TELNET, so poslana nešifrirana ("v čistem besedilu"). Toda za razliko od gesel FTP in TELNET so gesla SLIP poslana, preden sistem vzpostavi način TCP/IP.

   Ker uporablja SLIP povezavo od točke do točke v asinhronem načinu, se izpostavitev v zaščiti pri nešifriranih geslih razlikuje od izpostavitve v geslih FTP in TELNET. Nešifrirana gesla FTP in TELNET so lahko poslana kot promet IP v omrežju in zato niso zaščitena pred elektronskim vohljanjem. Prenos gesla SLIP je varen v tolikšni meri kot telefonska povezava med dvema sistemoma.
2. Privzeta datoteka za shranjevanje skriptov povezovalnih pogovornih oken SLIP je QUSRSYS/QATOCPPSCR. Privzeto pooblastilo za to datoteko je *USE, ki uporabnikom preprečuje spreminjanje privzetih skriptov povezovalnih pogovornih oken.

Ko izdelate profil povezave za oddaljeno sejo, ki zahteva preverjanje veljavnosti, naredite naslednje:

__ Korak 1. Zagotovite, da je sistemska vrednost QRETSVRSEC (Ohrani podatke o zaščiti strežnika) nastavljena na 1 (Da). Ta sistemska vrednost določa, ali boste omogočili shranjevanje gesel, ki jih je mogoče dešifrirati, v zaščitenem področju sistema.

__ Korak 2. S pomočjo ukaza WRKTCPPTP izdelajte konfiguracijski profil, ki ima naslednje značilnosti:

- Za način konfiguracijskega profila podajte *DIAL.
- Za *Ime dostopa do oddaljene storitve* podajte ID uporabnika, ki ga pričakuje oddaljeni sistem. Če se na primer povezujete z drugim strežnikom iSeries, podajte ime profila uporabnika na tem strežniku iSeries.
- Za *Geslo dostopa do oddaljene storitve* podajte geslo, ki ga pričakuje oddaljeni sistem za ta ID uporabnika. To geslo je shranjeno na strežniku iSeries v zaščitenem področju v obliki, ki jo je mogoče dešifrirati. Imena in gesla, ki jih dodelite konfiguracijskim profilom, so povezana s profilom uporabnika QTCP. Do imen in gesel ni mogoče dostopiti z uporabniškimi ukazi ali vmesniki. Do informacij o geslih lahko dostopijo samo registrirani sistemski programi.

  Opomba: Ne pozabite, da se gesla za profile povezav ne shranijo pri shranitvi konfiguracijskih datotek TCP/IP. Za shranitev gesel SLIP morate uporabiti ukaz SAVSECDTA (Shrani podatke o zaščiti), s katerim shranite profil uporabnika QTCP.
- Za skript povezovalnega pogovornega okna podajte skript, ki pošlje ID uporabnika in geslo. Sistem vključuje številne vzorčne skripte pogovornih oken, ki nudijo to funkcijo. Ko sistem zažene skript, pridobi geslo, ga dešifrira in ga pošlje oddaljenemu sistemu.

Problematika zaščite za protokol od točke do točke

Protokol od točke do točke (PPP) je na voljo kot del TCP/IP. PPP je industrijski standard za povezave od točke do točke, ki nudijo poleg funkcij, ki so na voljo v SLIP, še dodatne funkcije.

S pomočjo PPP lahko vzpostavi strežnik iSeries povezave z visoko hitrostjo neposredno s ponudnikom internetnih storitev ali z drugimi sistemi v intranetu ali ekstranetu. Oddaljena lokalna omrežja lahko izvajajo vhodne klicne povezave na strežnik iSeries.

Ne pozabite, da nudi PPP, podobno kot SLIP, omrežno povezavo s strežnikom iSeries. Povezava PPP v bistvu pripelje zahtevnika pred vrata vašega sistema. Zahtevnik še vedno potrebuje za vhod v sistem in povezavo s strežnikom TCP/IP kot je TELTNET ali FTP, ID uporabnika in geslo. V nadaljevanju sledi problematika zaščite, ki jo omogoča ta nova povezovalna zmožnost:

Opomba: PPP lahko konfigurirate s pomočjo Navigatorja iSeries na delovni postaji IBM iSeries Access za Windows.

- PPP nudi zmožnost vzpostavitve namenskih povezav (kjer ima en uporabnik vedno isti naslov IP). Če uporabljate namenski naslov, se poveča možnost lažnega predstavljanja IP (lažni sistem, ki se predstavlja kot overjeni sistem z znanim naslovom IP). Toda izboljšanje zmožnosti overjanja, ki jih nudi PPP, pomagajo pri zaščiti pred lažnim predstavljanjem IP.
- Podobno kot s protokolom SLIP izdelate tudi s PPP profile povezav, ki imajo ime uporabnika in z njim povezano geslo. Toda za razliko od SLIP ni nujno, da ima uporabnik veljaven profil uporabnika in geslo. Ime uporabnika in geslo nista povezana s profilom uporabnika. Za overjanje PPP so namesto tega uporabljeni seznami za preverjanje veljavnosti. PPP poleg tega ne zahteva povezovalnega skripta. Overjanje (izmenjava imena uporabnika in gesla) je del arhitekture PPP in se izvaja na nižji ravni kot s SLIP.
- PPP nudi možnost za uporabo protokola CHAP (challenge handshake authentication protocol). Če ga uporabite, vam ne bo več treba skrbeti, da bi prisluškovalci vohljali po vaših geslih, ker CHAP šifrira imena uporabnikov in gesla.

  Povezava PPP uporabi CHAP samo, če je na obeh straneh omogočena podpora za CHAP. Med izmenjalnimi signali za nastavitev komunikacij med dvema modemoma se izvajajo pogajanja dveh sistemov. Če na primer SYSTEMA podpira CHAP, SYSTEMB pa ne, lahko SYSTEMA zavrne sejo ali pa se strinja, da bo uporabil nešifrirano ime uporabnika in geslo. Strinjanje z uporabo nešifriranega imena uporabnika in gesla se imenuje pogajanje v smeri navzdol. Odločitev za pogajanje v smeri navzdol je konfiguracijska možnost. V intranetu, kjer veste, da imajo vsi sistemi zmožnost za CHAP, konfigurirajte profil povezave, tako da ne bo dopuščal pogajanj v smeri navzdol. Za javno povezavo, kjer vaš sistem kliče iz omrežja, boste najbrž dopustili pogajanje v smeri navzdol.

  Profil povezave za PPP nudi zmožnost podajanja veljavnih naslovov IP. Določite lahko na primer, da pričakujete od določenega uporabnika določen naslov ali območje naslovov. Ta zmožnost skupaj z zmožnostjo šifriranja gesel nudi nadaljnjo zaščito pred lažnim predstavljanjem.

  Kot dodatno zaščito pred lažnim predstavljanjem ali priklapljanjem na aktivno sejo lahko konfigurirate PPP tako, da izvaja pozive ob določenih intervalih. Ko je seja PPP aktivna, lahko strežnik iSeries na primer pozove drug sistem, da poda uporabnika in geslo. To naredi vsakih 15 minut in zagotovi, da gre za isti profil povezave. (Končni uporabnik se ne bo zavedal te dejavnosti vnovičnega pozivanja. Sistem namreč izmenja imena in gesla pod ravnijo, ki je vidna končnemu uporabniku.)

  Če uporabljate PPP, je realistično pričakovati, da bodo oddaljena lokalna omrežja vzpostavila vhodne klicne povezave z vašim strežnikom iSeries in s podaljšanim omrežjem. V tem okolju je skoraj nujno, da vključite odpošiljanje IP. Z odpošiljanjem IP je povezana možnost vdora v vaše omrežje, toda PPP uporablja močnejšo zaščito (kot je šifriranje gesel in preverjanje veljavnosti naslovov IP). Zaradi tega je možnost, da bi vdiralec vzpostavil omrežno povezavo, veliko manjša.

Podrobnejše informacije o PPP lahko najdete v Informacijskem centru iSeries.

Problematika zaščite pri uporabi strežnika Bootstrap Protocol

Bootstrap Protocol (BOOTP) nudi dinamičen način za povezovanje delovnih postaj s strežniki in dodeljevanje naslovov IP delovnih postaj in izvorov za nalaganje začetnega programa (IPL).

BOOTP je protokol TCP/IP, ki omogoča, da zahteva delovna postaja brez nosilca (odjemalec) datoteko z omrežnega strežnika, ki vsebuje začetno kodo. Strežnik BOOTP posluša na znanih vratih strežnika BOOTP 67. Ko prejme zahtevo odjemalca, poišče naslov IP, definiran za odjemalca, in vrne odjemalcu odgovor z naslovom IP odjemalca in z imenom datoteke za nalaganje. Odjemalec nato inicializira zahtevo TFTP za strežnik, v kateri zahteva datoteko za nalaganje. Preslikava med strojnim naslovom odjemalca in naslovom IP je shranjena v tabeli BOOTP na strežniku iSeries.

Preprečevanje dostopa BOOTP

Če v omrežju nimate nobenega odjemalca z zmanjšano namestitvijo, v sistemu ni potrebno izvajati strežnika BOOTP. Uporabite ga lahko za druge naprave, toda boljša rešitev za te naprave je uporaba DHCP. Izvajanje strežnika BOOTP preprečite takole:

__ Korak 1. Če želite preprečiti, da bi se opravila strežnika BOOTP samodejno zagnala pri zagonu TCP/IP, vpišite naslednje:

```
CHGBPA AUTOSTART(*NO)
```

Opombe:

a. AUTOSTART(*NO) je privzeta vrednost.

b. V razdelku“Krmiljenje, kateri strežniki TCP/IP se zaženejo samodejno” na strani 112 boste našli podrobnejše informacije o nadzorovanju, kateri strežniki TCP/IP se samodejno zaženejo.

__ Korak 2. Če želite preprečiti, da bi nekdo povezal uporabniško aplikacijo, kot je aplikacija vtičnice, z vrati, ki jih sistem običajno uporablja za BOOTP, naredite naslednje:

Opomba: Ker uporabljata DHCP in BOOTP isto številko vrat, s tem prepoveste tudi vrata, ki jih uporablja DHCP. Če želite uporabljati DHCP, ne omejite vrat.

__ Korak a. Vpišite GO CFGTCP, da boste prikazali meni Konfiguriranje TCP/IP.

__ Korak b. Izberite možnost 4 (Delo z omejitvami vrat TCP/IP).

__ Korak c. Na zaslonu Delo z omejitvami vrat TCP/IP podajte možnost 1 (Dodaj).

__ Korak d. Za območje nižjih vrat podajte 67.

__ Korak e. Za območje višjih vrat podajte *ONLY.

Opombe:

1) Omejitve vrat stopijo v veljavo pri naslednjem zagonu TCP/IP. Če je pri nastavitvi omejitve vrat TCP/IP aktiven, ga zaustavite in nato znova zaženite.

2) V RFC1700 boste našli podrobnejše informacije o splošnih dodelitvah številk vrat.

__ Korak f. Za protokol podajte *UDP.

__ Korak g. Za polje profila uporabnika podajte ime profila uporabnika, ki je v sistemu zaščiten. (Zaščiten profil uporabnika je tisti, ki ni lastnik programov, ki prevzamejo pooblastilo in njegovega gesla ne poznajo drugi uporabniki.) Če omejite vrata na določenega uporabnika, samodejno izključite vse ostale uporabnike.

Zaščita strežnika BOOTP

Strežnik BOOTP ne omogoča neposrednega dostopa do sistema iSeries in tako predstavlja manjšo luknjo v zaščiti. Glavna skrb skrbnika za zaščito je zagotoviti povezavo pravilnih

informacij s pravilnim odjemalcem z zmanjšano namestitvijo. To pomeni, da lahko napadalec spremeni tabelo BOOTP in povzroči, napačno delovanje odjemalcev z zmanjšano namestitvijo ali celo nedelovanje.

Za upravljanje strežnika BOOTP in tabele BOOTP potrebujete posebno pooblastilo *IOSYSCFG. Profile uporabnikov, ki imajo posebno pooblastilo *IOSYSCFG v sistemu, morate natančno nadzorovati.

Problematika zaščite pri uporabi strežnika DHCP

Dynamic host configuration protocol (DHCP) nudi ogrodje za posredovanje konfiguracijskih informacij gostiteljem v omrežju TCP/IP. Za odjemalske postaje lahko nudi DHCP funkcijo, ki je podobna samodejnemu konfiguriranju. Program na odjemalski delovni postaji, omogočen za DHCP, razpošlje zahtevo za konfiguracijske informacije. Če se na strežniku iSeries izvaja strežnik DCHP, se odzove na zahtevo, tako da pošlje informacije, ki jih potrebuje odjemalska delovna postaja za pravilno konfiguriranje TCP/IP.

DHCP lahko uporabite, da za uporabnike poenostavite prvo povezavo s strežnikom iSeries. Razlog za to je, da uporabniku ni potrebno vnesti konfiguracijskih informacij TCP/IP. DHCP lahko uporabite tudi za zmanjšanje števila notranjih naslovov TCP/IP, potrebnih v podmreži. Strežnik DHCP lahko začasno dodeli naslove IP aktivnim uporabnikom (iz področja naslovov IP).

Za odjemalce z zmanjšano namestitvijo lahko uporabite DHCP namesto BOOTP. DHCP nudi več funkcij kot BOOTP in lahko nudi tudi podporo za dinamično konfiguriranje odjemalcev z zmanjšano namestitvijo in PC-jev.

Preprečevanje dostopa DHCP

Če *ne* želite, da bi kdorkoli uporabljal DHCP v vašem sistemu, naredite naslednje:

1. Če želite preprečiti, da bi se opravila strežnika DHCP samodejno zagnala pri zagonu TCP/IP, vpišite naslednje:

   ```
   CHGDHCPA AUTOSTART(*NO)
   ```

   Opombe:

   a. AUTOSTART(*NO) je privzeta vrednost.

   b. V razdelku“Krmiljenje, kateri strežniki TCP/IP se zaženejo samodejno” na strani 112 boste našli podrobnejše informacije o nadzorovanju, kateri strežniki TCP/IP se samodejno zaženejo.

2. Če želite preprečiti, da bi nekdo povezal uporabniško aplikacijo, kot je aplikacija vtičnice, z vrati, ki jih sistem običajno uporablja za DHCP, naredite naslednje:

   a. Vpišite GO CFGTCP, da boste prikazali meni Konfiguriranje TCP/IP.

   b. Izberite možnost 4 (Delo z omejitvami vrat TCP/IP).

   c. Na zaslonu Delo z omejitvami vrat TCP/IP podajte možnost 1 (Dodaj).

   d. Za območje nižjih vrat podajte 67.

   e. Za območje višjih vrat podajte 68.

      Opombe:

      1) Omejitve vrat stopijo v veljavo pri naslednjem zagonu TCP/IP. Če je pri nastavitvi omejitve vrat TCP/IP aktiven, ga zaustavite in nato znova zaženite.

      2) V RFC1700 boste našli podrobnejše informacije o splošnih dodelitvah številk vrat.

   f. Za protokol podajte *UDP.

g. Za polje profila uporabnika podajte ime profila uporabnika, ki je v sistemu zaščiten. (Zaščiten profil uporabnika je tisti, ki ni lastnik programov, ki prevzamejo pooblastilo in njegovega gesla ne poznajo drugi uporabniki.) Če omejite vrata na določenega uporabnika, samodejno izključite vse ostale uporabnike.

Zaščita strežnika DHCP

Sledi problematika zaščite, če izberete izvajanje DHCP v sistemu iSeries:

- Omejite število uporabnikov, ki imajo pooblastilo za upravljanje DHCP. Za upravljanje DHCP sta potrebni naslednji pooblastili:
  - posebno pooblastilo *IOSYSCFG
  - pooblastilo *RW za naslednje datoteke:

    ```
    /QIBM/UserData/OS400/DHCP/dhcpsd.cfg
    /QIBM/UserData/OS400/DHCP/dhcprd.cfg
    ```
- Ocenite, kolikšna je možnost fizičnega dostopa do lokalnega omrežja. Ali lahko zunanji uporabnik preprosto pride na vaše mesto s prenosnim računalnikom in ga fizično poveže v vaše lokalno omrežje? Če ugotovite, da gre za luknjo v zaščiti, lahko DHCP izdela seznam odjemalcev (strojnih naslovov), ki jih bo konfiguriral strežnik DHCP. Če uporabite to možnost, odstranite nekaj storilnostnih prednosti, ki jih nudi DHCP za skrbnike omrežij, toda sistemu tudi preprečite, da bi konfiguriral neznane delovne postaje.
- Če je mogoče, uporabite področje naslovov IP, ki jih je mogoče znova uporabiti (ki niso oblikovani za internet). S tem preprečite, da bi delovna postaja, ki ni v vašem omrežju, pridobila koristne konfiguracijske informacije s strežnika.
- Če potrebujete dodatno zaščito, uporabite izhodne točke DHCP. Sledi pregled izhodnih točk in njihovih zmožnosti. Knjiga *iSeries System API Reference* opisuje uporabo teh izhodnih točk.

  Vhod prek vrat
  Sistem pokliče izhodni program vsakič, ko prebere podatkovni paket na vratih 67 (vrata DHCP). Izhodni program sprejme celoten podatkovni paket in se lahko odloči, ali naj sistem paket obdela ali ga zavrže. To izhodno točko lahko uporabite, če obstoječe funkcije zaščite DHCP ne zadostujejo vašim potrebam.

  Dodelitev naslova
  Sistem pokliče izhodni program, vsakič ko DHCP formali dodeli naslov odjemalcu.

  Sprostitev naslova
  Sistem pokliče izhodni program, vsakič ko DHCP formalno sprosti naslov in ga vrne v področje naslovov.

Problematika zaščite pri uporabi strežnika TFTP

Trivial file transfer protocol (TFTP) nudi osnoven prenos datotek brez overjanja uporabnikov. TFTP deluje z bodisi Bootstrap Protocol (BOOTP) ali Dynamic Host Configuration Protocol (DHCP).

Odjemalec se sprva poveže bodisi s strežnikom BOOTP ali s strežnikom DHCP. Strežnik BOOTP ali DHCP odgovori z naslovom IP odjemalca in z imenom datoteke za nalaganje. Odjemalec nato inicializira zahtevo TFTP za strežnik, v kateri zahteva datoteko za nalaganje. Ko odjemalec konča s snemanjem datoteke za nalaganje, konča sejo TFTP.

Preprečevanje dostopa TFTP

Če v omrežju nimate nobenega odjemalca z zmanjšano namestitvijo, v sistemu najbrž ni potrebno izvajati strežnika TFTP. Izvajanje strežnika TFTP preprečite takole:

__ Korak 1. Če želite preprečiti, da bi se opravila strežnika TFTP samodejno zagnala pri zagonu TCP/IP, vpišite naslednje:

```
CHGTFTPA AUTOSTART(*NO)
```

Opombe:

a. AUTOSTART(*NO) je privzeta vrednost.

b. V razdelku“Krmiljenje, kateri strežniki TCP/IP se zaženejo samodejno” na strani 112 boste našli podrobnejše informacije o nadzorovanju, kateri strežniki TCP/IP se samodejno zaženejo.

__ Korak 2. Če želite preprečiti, da bi nekdo povezal uporabniško aplikacijo, kot je aplikacija vtičnice, z vrati, ki jih sistem običajno uporablja za TFTP, naredite naslednje:

__ Korak a. Vpišite GO CFGTCP, da boste prikazali meni Konfiguriranje TCP/IP.

__ Korak b. Izberite možnost 4 (Delo z omejitvami vrat TCP/IP).

__ Korak c. Na zaslonu Delo z omejitvami vrat TCP/IP podajte možnost 1 (Dodaj).

__ Korak d. Za območje nižjih vrat podajte 69.

__ Korak e. Za območje višjih vrat podajte *ONLY.

Opombe:

1) Omejitve vrat stopijo v veljavo pri naslednjem zagonu TCP/IP. Če je pri nastavitvi omejitve vrat TCP/IP aktiven, ga zaustavite in nato znova zaženite.

2) V RFC1700 boste našli podrobnejše informacije o splošnih dodelitvah številk vrat.

__ Korak f. Za protokol podajte *UDP.

__ Korak g. Za polje profila uporabnika podajte ime profila uporabnika, ki je v sistemu zaščiten. (Zaščiten profil uporabnika je tisti, ki ni lastnik programov, ki prevzamejo pooblastilo in njegovega gesla ne poznajo drugi uporabniki.) Če omejite vrata na določenega uporabnika, samodejno izključite vse ostale uporabnike.

Zaščita strežnika TFTP

Po privzetku nudi strežnik TFTP zelo omejen dostop do sistema iSeries. Posebej je konfiguriran zato, da nudi začetno kodo za odjemalce z zmanjšano namestitvijo. Kot skrbnik za zaščito morate poznati naslednje značilnosti strežnika TFTP:

- Strežnik TFTP ne zahteva overjanja (ID uporabnika in geslo). Vsa opravila TFTP se izvajajo pod profilom uporabnika QTFTP. Profil uporabnika QTFTP nima gesla in zato ni na voljo za interaktivno prijavo. Profil uporabnika QTFTP nima nobenih posebnih pooblastil, niti ni izrecno pooblaščen za sistemska sredstva. Za dostop do sredstev, ki jih potrebuje za odjemalce z zmanjšano namestitvijo, uporablja javno pooblastilo.
- Ko dobite strežnik TFTP, je konfiguriran tako, da dostopi do imenika, ki vsebuje informacije o odjemalcu z zmanjšano namestitvijo. Za branje iz tega imenika ali pisanje vanj potrebujete pooblastilo *PUBLIC ali QTFTP. Za pisanje v imenik potrebujete pooblastilo *CREATE, podano v parametru ″Omogoči pisanje v datoteko″ ukaza CHGTFTPA. Za pisanje v obstoječo datoteko potrebujete pooblastilo *REPLACE, podano v parametru ″Omogoči pisanje v datoteko″ ukaza CHGTFTPA. *CREATE omogoča zamenjavo obstoječih datotek ali izdelavo novih datotek. *REPLACE omogoča samo zamenjavo obstoječih datotek.

  Odjemalec TFTP ne more dostopiti do nobenega drugega imenika, razen če imenik izrecno definirate z ukazom Spremeni atribute TFTP (CHGTFTPA). Če torej poskusi lokalni ali

oddaljeni uporabnik zagnati sejo TFTP z vašim sistemom, je njegova zmožnost za dostop do informacij ali povzročitev škode zelo omejena.

- Če konfigurirate strežnik TFTP tako, da nudi poleg obravnavanja odjemalcev z zmanjšano namestitvijo tudi druge storitve, lahko definirate izhodni program, ki oceni in pooblasti vsako zahtevo TFTP. Strežnik TFTP nudi izhod za preverjanje veljavnosti zahteve, podoben izhodu, ki je na voljo za strežnik FTP. Podrobnejše informacije lahko najdete v Informacijskem centru iSeries —>Delo z omrežjem—>TCP/IP—>TFTP. V razdelku“Predpogoji in s tem povezane informacije” na strani xii lahko najdete informacije o dostopu do Informacijskega centra iSeries.

Problematika zaščite pri uporabi strežnika REXEC

Strežnik za oddaljeno izvedbo (REXEC) sprejme in izvaja ukaze, ki jih pošlje odjemalec REXEC. Odjemalec REXEC je običajno aplikacija za PC ali UNIX, ki podpira pošiljanje ukazov REXEC. Podpora, ki jo nudi ta strežnik, je podobna zmožnosti, ki je na voljo pri uporabi podukaza RCMD (Oddaljen ukaz) za strežnik FTP.

Preprečevanje dostopa REXEC

Če ne želite, da strežnik iSeries sprejema ukaze odjemalca REXEC, takole preprečite izvajanje strežnika REXEC:

__ Korak 1. Če želite preprečiti, da bi se opravila strežnika REXEC samodejno zagnala pri zagonu TCP/IP, vpišite naslednje:

```
CHGRXCA AUTOSTART(*NO)
```

Opombe:

a. AUTOSTART(*NO) je privzeta vrednost.

b. V razdelku“Krmiljenje, kateri strežniki TCP/IP se zaženejo samodejno” na strani 112 boste našli podrobnejše informacije o nadzorovanju, kateri strežniki TCP/IP se samodejno zaženejo.

__ Korak 2. Če želite preprečiti, da bi nekdo povezal uporabniško aplikacijo, kot je aplikacija vtičnice, z vrati, ki jih sistem običajno uporablja za REXEC, naredite naslednje:

__ Korak a. Vpišite GO CFGTCP, da boste prikazali meni Konfiguriranje TCP/IP.

__ Korak b. Izberite možnost 4 (Delo z omejitvami vrat TCP/IP).

__ Korak c. Na zaslonu Delo z omejitvami vrat TCP/IP podajte možnost 1 (Dodaj).

__ Korak d. Za območje nižjih vrat podajte 512.

__ Korak e. Za območje višjih vrat podajte *ONLY.

__ Korak f. Za protokol podajte *TCP.

__ Korak g. Za polje profila uporabnika podajte ime profila uporabnika, ki je v sistemu zaščiten. (Zaščiten profil uporabnika je tisti, ki ni lastnik programov, ki prevzamejo pooblastilo in njegovega gesla ne poznajo drugi uporabniki.) Če omejite vrata na določenega uporabnika, samodejno izključite vse ostale uporabnike.

Opombe:

a. Omejitve vrat stopijo v veljavo pri naslednjem zagonu TCP/IP. Če je pri nastavitvi omejitve vrat TCP/IP aktiven, ga zaustavite in nato znova zaženite.

b. V RFC1700 boste našli podrobnejše informacije o splošnih dodelitvah številk vrat.

Zaščita strežnika REXEC

Sledi problematika, povezana z izbiro strežnika za oddaljeno izvedbo v sistemu:

- Zahteva REXCD vključuje ID uporabnika, geslo in ukaz za izvedbo. Uporablja se običajno overjanje strežnika iSeries in preverjanje pooblastil:
  - Kombinacija profila uporabnika in gesla mora biti veljavna.
  - Sistem uveljavi vrednost *Omeji zmožnosti* (LMTCPB) za profil uporabnika.
  - Uporabnik mora imeti pooblastilo za ukaz in za vsa sredstva, ki jih uporablja ukaz.
- Strežnik REXEC nudi izhodne točke, podobne izhodnim točkam, ki so na voljo za strežnik FTP. Za ocenitev ukaza lahko uporabite izhodno točko Validation in se odločite, ali ga boste dopustili. Podrobnejše informacije lahko najdete v Informacijskem centru iSeries —>Delo z omrežjem—>TCP/IP—>REXEC. V razdelku"Predpogoji in s tem povezane informacije" na strani xii lahko najdete informacije o dostopu do Informacijskega centra iSeries.
- Če izberete izvajanje strežnika REXEC, poteka izvajanje izven vsega krmiljenja menijskega dostopa, ki ga uporabljate v sistemu. Za zaščito sredstev morate zagotoviti uporabo ustrezne sheme za objektna pooblastila.

Problematika zaščite pri uporabi RouteD

Strežnik demona usmeritve (RouteD) nudi podporo za protokol RIP (Routing Information Protocol na strežnikih iSeries. RIP je eden izmed najpogosteje uporabljanih protokolov usmerjevanja. To je Interior Gateway Protocol, ki pomaga TCP/IP pri usmerjevanju paketov IP znotraj avtonomnih sistemov.

RouteD je namenjen povečanju učinkovitosti omrežnega prometa, saj da omogoči sistemom znotraj overjenega omrežja medsebojno ažuriranje s pomočjo trenutnih informacij o smereh. Ko zaženete RouteD, lahko vaš sistem prejme popravke iz drugih sodelujočih sistemov o načinu usmeritve prenosov (paketov). Če torej lahko do strežnika RouteD dostopi heker, ga lahko uporabi za preusmeritev paketov prek sistema, ki lahko pregleda ali spremeni te pakete. Sledi nekaj predlogov za zaščito RouteD:

- Strežniki iSeries uporabljajo RIPv1, ki ne nudi nobenega načina za overjanje usmerjevalnikov. Namenjen je za uporabo znotraj overjenega omrežja. Če je vaš sistem v omrežju z drugimi sistemi, ki jim ne zaupate, ne zaženite strežnika RouteD. Če želite preprečiti samodejni zagon strežnika RouteD, vpišite naslednje:

  ```
  CHGRTDA AUTOSTART(*NO)
  ```

  Opombe:

  1. AUTOSTART(*NO) je privzeta vrednost.
  2. V razdelku"Krmiljenje, kateri strežniki TCP/IP se zaženejo samodejno" na strani 112 boste našli podrobnejše informacije o nadzorovanju, kateri strežniki TCP/IP se samodejno zaženejo.
- Natančno morate nadzorovati, kdo lahko spreminja konfiguracijo RouteD, ki zahteva posebno pooblastilo *IOSYSCFG.
- Če sodeluje vaš sistem v več kot enem omrežju (na primer v intranetu in internetu), lahko konfigurirate strežnik RouteD tako, da izvaja pošiljanje in sprejemanje popravkov samo z zaščitenim omrežjem.

Problematika zaščite pri uporabi strežnika DNS

Strežnik Imenski sistem domen (DNS) nudi prevode imen gostiteljev v naslove IP in obratno. Namen strežnika DNS na strežnikih iSeries je nuditi prevode naslovov za notranje, zaščiteno omrežje (intranet).

Preprečevanje dostopa DNS

Če *ne* želite, da bi kdorkoli v vašem sistemu uporabljal DNS, naredite naslednje:

1. Če želite preprečiti, da bi se opravila strežnika DNS samodejno zagnala pri zagonu TCP/IP, vpišite naslednje:

   ```
   CHGDNSA AUTOSTART(*NO)
   ```

   Opombe:

   a. AUTOSTART(*NO) je privzeta vrednost.

   b. V razdelku“Krmiljenje, kateri strežniki TCP/IP se zaženejo samodejno” na strani 112 boste našli podrobnejše informacije o nadzorovanju, kateri strežniki TCP/IP se samodejno zaženejo.

2. Če želite preprečiti, da bi nekdo povezal uporabniško aplikacijo, kot je aplikacija vtičnice, z vrati, ki jih sistem običajno uporablja za DNS, naredite naslednje:

   a. Vpišite GO CFGTCP, da boste prikazali meni Konfiguriranje TCP/IP.

   b. Izberite možnost 4 (Delo z omejitvami vrat TCP/IP).

   c. Na zaslonu Delo z omejitvami vrat TCP/IP podajte možnost 1 (Dodaj).

   d. Za območje nižjih vrat podajte 53.

   e. Za območje višjih vrat podajte *ONLY.

      Opombe:

      1) Omejitve vrat stopijo v veljavo pri naslednjem zagonu TCP/IP. Če je pri nastavitvi omejitve vrat TCP/IP aktiven, ga zaustavite in nato znova zaženite.

      2) V RFC1700 boste našli podrobnejše informacije o splošnih dodelitvah številk vrat.

   f. Za protokol podajte *TCP.

   g. Za polje profila uporabnika podajte ime profila uporabnika, ki je v sistemu zaščiten. (Zaščiten profil uporabnika je tisti, ki ni lastnik programov, ki prevzamejo pooblastilo in njegovega gesla ne poznajo drugi uporabniki.) Če omejite vrata na določenega uporabnika, samodejno izključite vse ostale uporabnike.

   h. Ponovite korake od 2c do 2g za protokol *UDP (uporabniški datagram).

Zaščita strežnika DNS

Sledi problematika zaščite, če izberete izvajanje DNS v sistemu iSeries:

- Funkcija, ki jo nudi strežnik DNS, je prevod naslovov IP in prevod imen. Strežnik DNS ne nudi nobenega dostopa do objektov v sistemu iSeries. Tveganje, ki ste mu izpostavljeni, če zunanji uporabnik dostopi do strežnika DNS, je, da nudi strežnik preprost način za ogled topologije omrežja. Strežnik DNS lahko prihrani hekerju kar nekaj truda pri določanju naslovov možnih ciljev. Toda DNS ne nudi informacij, ki bi pomagale pri vdoru v te ciljne sisteme.
- Strežnik DNS iSeries se običajno uporablja za intranet, zato najbrž ne bo potrebno omejiti zmožnosti za poizvedovanje na strežniku DNS. Toda znotraj intraneta imate lahko več podomrežij in ne želite, da bi uporabniki iz drugih podomrežij izvajali poizvedbe DNS na strežniku iSeries. Možnost zaščite DNS omogoča, da omejite dostop na primarno domeno. S pomočjo Navigatorja iSeries podajte naslove IP, na katere naj se odziva strežnik DNS.

  Druga možnost zaščite omogoča, da podate, kateri sekundarni strežniki lahko prekopirajo informacije s primarnega strežnika DNS. Če uporabite to možnost, bo sprejel strežnik zahteve za conski prenos (zahteva za kopiranje informacij) samo od sekundarnih strežnikov, ki jih izrecno navedete.
- Pazite, da boste previdno omejili zmožnost za spreminjanje konfiguracijskih informacij za strežnik DNS. Nekdo z zlobnimi nameni lahko na primer spremeni datoteko DNS, tako da

kaže na naslov IP izven omrežja. Prav tako lahko simulira strežnik v vašem omrežju in morda celo pridobi dostop do zaupnih informacij od uporabnikov, ki obiščejo strežnik.

Problematika zaščite pri uporabi strežnika HTTP za iSeries

Strežnik HTTP nudi odjemalcem spletnega brskalnika dostop do večpredstavnih objektov strežnika iSeries kot so dokumenti HTML (Hypertext Markup Language). Prav tako podpira tudi specifikacijo *Common Gateway Interface (CGI)*. Programerji aplikacij lahko napišejo programe CGI, s katerimi razširijo funkcionalnost strežnika.

Skrbnik lahko s pomočjo Internet Connection Server ali strežnika IBM HTTP za iSeries sočasno izvaja več strežnikov na enem strežniku iSeries. Vsak strežnik, ki se izvaja, se imenuje **primerek strežnika**. Vsak primerek strežnika ima unikatno ime. Skrbniki nadzorujejo, kateri primerki so zagnani in kaj lahko posamezni primerki naredijo.

Opomba: Pri uporabi spletnega brskalnika za konfiguriranje ali upravljanje naslednjega se mora izvajati primerek *ADMIN strežnika HTTP:

- Požarni zid za iSeries
- Internet Connection Server
- Internet Connection Secure Server
- IBM-ov strežnik HTTP za iSeries

Uporabnik (obiskovalec spletne strani) nikoli ne vidi zaslona za prijavo na strežnik iSeries. Toda skrbnik strežnika iSeries mora izrecno pooblastiti vse dokumente HTML in programe CGI, tako da jih definira v smernicah HTTP. Poleg tega lahko skrbnik nastavi zaščito sredstev in overjanje uporabnikov (ID uporabnika in geslo) za nekatere ali vse zahteve.

Napad hekerja lahko na spletnem strežniku povzroči zavrnitev storitve. Strežnik lahko odkrije napad z zavrnitvijo storitve tako, da meri čakalni čas zahtev določenih odjemalcev. Če strežnik ne prejme zahteve odjemalca, določi, da poteka napad z zavrnitvijo storitve. Do tega pride pri začetni povezavi odjemalca s strežnikom. Strežnik po privzetku izvaja odkrivanje napadov in kaznovanje.

Preprečevanje dostopa HTTP

Če *ne* želite, da bi kdorkoli uporabljal program za dostop do vašega sistema, preprečite izvajanje strežnika HTTP. Naredite naslednje:

__ Korak 1. Če želite preprečiti, da bi se opravila strežnika HTTP samodejno zagnala pri zagonu TCP/IP, vpišite naslednje:

```
CHGHTTPA AUTOSTART(*NO)
```

Opombe:

a. AUTOSTART(*NO) je privzeta vrednost.

b. V razdelku“Krmiljenje, kateri strežniki TCP/IP se zaženejo samodejno” na strani 112 boste našli podrobnejše informacije o nadzorovanju, kateri strežniki TCP/IP se samodejno zaženejo.

__ Korak 2. Po privzetku uporablja opravilo strežnika HTTP profil uporabnika QTMHHTTP. Če želite preprečiti zagon strežnika HTTP, nastavite status profila uporabnika QTMHHTTP na *DISABLED.

Krmiljenje dostopa do strežnika HTTP

Osnovni namen izvajanja strežnika HTTP je nudenje dostopa obiskovalcem spletne strani v vašem sistemu iSeries. Na obiskovalca vaše spletne strani lahko gledate podobno kot na nekoga, ki si ogleduje oglas v prodajnem časopisu. Obiskovalec ne pozna strojne in

programske opreme, ki izvajata vašo spletno stran, kot je na primer tip strežnika, ki ga uporabljate in kje fizično se nahaja strežnik. Običajno ne boste želeli med možnega obiskovalca in spletno stran postaviti nobene omejitve (kot je prijavni zaslon). Vendar pa boste gotovo želeli omejiti dostop do nekaterih dokumentov ali programov CGI, ki jih nudi spletna stran.

Morda boste želeli tudi, da en sistem iSeries nudi več logičnih spletnih strani. Sistem iSeries lahko podpira različne dejavnosti vašega podjetja, ki imajo različne skupine strank. Za vsako od teh dejavnosti podjetja izdelajte unikatno spletno stran, ki je obiskovalcu prikazana povsem neodvisno. Poleg tega lahko nudite tudi notranje spletne strani (intranet) z zaupnimi informacijami o vašem podjetju.

Kot skrbnik za zaščito morate zaščititi vsebino spletne strani, pri tem pa tudi zagotoviti, da dejavnosti, povezane z zaščito, ne bodo negativno vplivale na vrednost spletne strani. Zagotoviti morate tudi, da dejavnost strežnika HTTP ne spravi v nevarnost integritete sistema ali omrežja. V temah, ki sledijo, boste našli predloge za zaščito pri uporabi programa.

Problematika upravljanja

V nadaljevanju sledi problematika zaščite, povezana z upravljanjem internetnega strežnika.

- Funkcije namestitve in konfiguriranja izvajate s pomočjo spletnega brskalnika in primerka *ADMIN. Za nekatere funkcije, kot je izdelava dodatnih primerkov na strežniku, *morate* uporabiti strežnik *ADMIN.
- Privzeti URL za domačo stran upravljanja (domača stran za strežnik *ADMIN) je objavljen v dokumentaciji za izdelke, ki nudijo funkcijo za upravljanje brskalnikov. Zato bodo za privzeti URL najverjetneje izvedeli hekerji in bo objavljen v hekerskih forumih, tako kot so poznana in objavljena tudi gesla za IBM-ove uporabniške profile. Pred to luknjo se lahko zaščitite na več načinov:
  - Če morate izvesti funkcije upravljanja, zaženite samo primerek *ADMIN strežnika HTTP. Primerek *ADMIN naj se ne izvaja ves čas.
  - Aktivirajte podporo za SSL za primerek *ADMIN (s pomočjo Upravljalnika digitalnih potrdil). Primerek *ADMIN zahteva ID uporabnika in geslo z uporabo smernic za zaščito HTTP. Če uporabite SSL, sta ID uporabnika in geslo šifrirana (skupaj z vsemi drugimi informacijami o konfiguraciji, prikazani na obrazcih za upravljanje).
  - S pomočjo požarnega zidu preprečite dostop do strežnika *ADMIN prek interneta in za skritje sistema in imen domen, ki so del URL-ja.
- Pri izvajanju funkcij upravljanja se morate prijaviti s profilom uporabnika, ki ima posebno pooblastilo *IOSYSCFG. Morda boste potrebovali tudi pooblastilo za specifične objekte v sistemu, kot so naslednji:
  - Knjižnice ali imeniki, ki vsebujejo dokumente HTML in programe CGI.
  - Vsi profili uporabnikov, ki jih nameravate izmenjati znotraj smernic za strežnik.
  - Seznami za nadzorovanje dostopa (ACL-ji) za vse imenike, ki jih uporabljajo smernice.
  - Objekt seznama za preverjanje veljavnosti za izdelavo in vzdrževanje ID-jev uporabnikov in gesel.

  Če uporabljate strežnik *ADMIN in TELNET, lahko izvajate funkcije upravljanja oddaljeno, in sicer prek internetne povezave. Če izvajate upravljanje prek javne povezave (internet), se morate zavedati, da izpostavite močan ID uporabnika in geslo vohljanju. ″Vohljač″ lahko s tem ID-jem uporabnika in geslom poskusi dostopiti do sistema, tako da uporabi na primer TELNET ali FTP.

  Opombe:

  1. Če uporabite TELNET, je obravnavan prijavni zaslon tako kot vsak drug zaslon. Čeprav geslo pri vpisu ni prikazano, ga sistem prenese, ne da bi ga šifriral ali kodiral.

2. Če uporabite strežnik *ADMIN, je geslo kodirano in ne šifrirano. Kodirna shema je industrijski standard in je torej hekerjem dobro znana. Priložnostni ″vohljači″ ne morejo ravno preprosto razumeti kodiranja, toda prebrisani vohljači imajo gotovo na voljo orodja, s pomočjo katerih poskusijo dekodirati geslo.

Nasvet za zaščito

Če izvajate oddaljeno upravljanje prek interneta, uporabite primerek *ADMIN s SSL, tako da bodo prenosi šifrirani. Ne uporabljajte nezaščitenih aplikacij kot je različica TELNET pred V4R4 (TELNET nudi podporo za SSL od V4R4 naprej). Če uporabljate strežnik *ADMIN prek intraneta *overjenih* uporabnikov, lahko ta način najbrž varno uporabljate za upravljanje.

- Smernice HTTP nudijo osnovo za vse dejavnosti strežnika. Naložena konfiguracija nudi zmožnost za streženje privzete naslovne strani. Odjemalec si razen naslovne strani ne more ogledati nobenih drugih dokumentov, dokler skrbnik strežnika ne definira smernic za strežnik. Za definiranje smernic uporabite spletni brskalnik in strežnik *ADMIN ali ukaz Delo s konfiguracijo HTTP (WRKHTTPCFG). Oba načina zahtevata posebno pooblastilo *IOSYSCFG. Če povežete strežnik iSeries z internetom, postaneta ocenitev in nadzorovanje števila uporabnikov v podjetju, ki imajo posebno pooblastilo *IOSYSCFG, še bolj pomembna.

Zaščita sredstev

Strežnik IBM HTTP za iSeries vključuje smernice HTTP, ki lahko natančno nadzorujejo informacijska sredstva, ki jih uporablja strežnik. Smernice lahko uporabite za nadzorovanje, iz katerih imenikov streže spletni strežnik URL-je za datoteke HTML in programe CGI, za zamenjavo v druge profile uporabnikov in za zahtevanje overjanja za nekatera sredstva.

Opomba: Dokumentacija v Informacijskem centru pod temo ″Spletno streženje″ nudi celoten opis razpoložljivih smernic HTTP in razlago za njihovo uporabo. Sledi nekaj predlogov in problematike za uporabo te podpore:

- Strežnik HTTP začne z osnovo ″izrecnega pooblastila.″ Strežnik ne sprejme zahteve, če ni izrecno definirana v smernicah. Ali povedano z drugimi besedami, strežnik takoj zavrne vse zahteve za URL, če ta URL ni definiran v smernicah (z imenom ali splošno).
- Smernice za zaščito lahko uporabite za zahtevo ID-ja uporabnika in gesla, preden sprejmete zahtevo za nekatera ali vsa sredstva.
  - Če uporabnik (odjemalec) zahteva zaščiteno sredstvo, strežnik pozove brskalnik na vnos ID-ja uporabnika in gesla. Brskalnik pozove uporabnika, da vnese ID uporabnika in geslo, in te informacije nato pošlje strežniku. Nekateri brskalniki shranijo ID uporabnika in geslo in ga nato samodejno pošljejo z nadaljnjimi zahtevami. Na ta način uporabniku ni potrebno pri vsaki zahtevi na novo vnesti ID-ja uporabnika in gesla.

    Ker nekateri brskalniki shranijo ID uporabnika in geslo, morate opraviti isto nalogo poučevanja uporabnikov, kot če vnesejo uporabniki sistem prek prijavnika zaslona strežnika iSeries ali prek usmerjevalnika. Nenadzorovana seja brskalnika predstavlja možno luknjo v zaščiti.
  - Za način, na katerega sistem obravnava ID-je uporabnikov in gesel, so na voljo tri možnosti (podane v smernicah za zaščito):
    1. Uporabite lahko običajen profil uporabnika strežnika iSeries in preverjanje veljavnosti gesla. Ta način se najpogosteje uporablja za zaščito sredstev v intranetu (zaščiteno omrežje).
    2. Izdelate lahko ″internetne uporabnike″; to so uporabniki, za katere je mogoče preveriti veljavnost, vendar na strežniku iSeries nimajo profila uporabnika. Internetni uporabniki se izvajajo prek objekta strežnika iSeries, imenovanega

″seznam za preverjanje veljavnosti″. Objekti seznama za preverjanje veljavnosti vsebujejo seznam uporabnikov in gesel, ki so posebej definirani za uporabo z določeno aplikacijo.

Vaša odločitev je, kako bodo podani ID-ji in gesla internetnih uporabnikov (kot na primer prek aplikacije ali tako, da jih bo podal skrbnik kot odziv na zahtevo elektronske pošte), kot tudi, kako boste upravljali internetne uporabnike. Pri tej nastavitvi uporabite vmesnik, temelječ na brskalniku strežnika HTTP.

Za nezaščitena omrežja (internet) nudi uporaba internetnih uporabnikov boljšo splošno zaščito kot uporaba običajnih profilov uporabnikov in gesel. Unikaten niz ID-jev uporabnikov in gesel izdela vgrajeno omejitev za to, kaj lahko naredijo tej uporabniki. ID-ji uporabnikov in gesla niso na voljo za običajno prijavo (na primer s TELNETOM ali s FTP). Poleg tega običajnih ID-jev uporabnikov in gesel ne izpostavite vohljanju.

3. LDAP (Lightweight directory access protocol) je protokol imeniške storitve, ki nudi dostop do imenika prek TCP (Transmission Control Protocol). Omogoča, da shranite informacije v tej imeniški storitve in zanjo izvedete poizvedbo. LDAP je zdaj podprt kot možnost za overjanje uporabnikov.

Opombe:

1. Ko pošlje brskalnik ID uporabnika in geslo (za profil uporabnika ali za internetnega uporabnika), sta kodirana in ne šifrirana. Kodirna shema je industrijski standard in je torej hekerjem dobro znana. Priložnostni ″vohljači″ ne morejo ravno preprosto razumeti kodiranja, toda prebrisani vohljači imajo gotovo na voljo orodja, s pomočjo katerih poskusijo dekodirati te informacije.
2. Strežnik iSeries shrani objekt za preverjanje veljavnosti v zaščitenem sistemskem področju. Do njega lahko dostopite samo z definiranimi sistemskimi vmesniki (API-ji) in s pravilnim pooblastilom.

– S pomočjo Upravljalnika digitalnih potrdil (DCM) lahko izdelate lastno intranetno službo za pooblastila. Digitalno potrdilo samodejno poveže potrdila s profilom uporabnika lastnika. Potrdilo ima ista pooblastila in dovoljenja kot povezan profil.

- Ko strežnik sprejme zahtevo, začne veljati običajna zaščita sredstev strežnika iSeries. Profil uporabnika, ki zahteva sredstvo, mora imeti pooblastilo zanj (kot je mapa ali izvorna fizična datoteka, ki vsebuje dokument HTML). Po privzetku se izvaja opravilo pod profilom uporabnika QTMHHTTP. Za zamenjavo v drug profil uporabnika lahko uporabite smernico. Sistem nato uporabi za dostop do objektov pooblastilo tega profila uporabnika. Sledi problematika, povezana s to podporo:
  – Zamenjava profilov uporabnikov je lahko posebej koristna, če nudi vaš strežnik več kot eno logično spletno stran. Različne profile uporabnikov lahko povežete s smernicami za vsako spletno stran in tako uporabite običajno zaščito sredstev strežnika iSeries za zaščito dokumentov za vsako stran.
  – Zmožnost za zamenjavo profilov uporabnikov lahko uporabite v kombinaciji z objektom za preverjanje veljavnosti. Strežnik oceni začetno zahtevo z uporabo unikatnega ID-ja uporabnika in gesla (ki sta ločena od običajnega ID-ja uporabnika in gesla). Ko strežnik overi uporabnika, sistem preklopi v drug profil uporabnika in tako izkoristi prednosti zaščite sredstev. Uporabnik tako ne pozna pravega imena profila uporabnika in ga ne more uporabiti na druge načine (kot je FTP):
- Nekatere zahteve strežnika HTTP morajo zagnati program na strežniku HTTP. Program lahko na primer dostopi do podatkov v sistemu. Preden se lahko program zažene, mora skrbnik strežnika preslikati zahtevo (URL) v določen uporabniško definiran program, ki ustreza standardom uporabniškega vmesnika CGI. Sledi problematika, povezana s programi CGI:
  – Smernice za zaščito programov CGI lahko uporabljate na enak način kot za dokumente HTML. Tako lahko pred izvedbo programa zahtevate ID uporabnika in geslo.

– Po privzetku se izvajajo programi CGI pod profilom uporabnika QTMHHTP1. Preden zaženete program, lahko preklopite v drug profil uporabnika. Zato lahko nastavite običajno zaščito sredstev strežnika iSeries za sredstva, do katerih dostopajo programi CGI.

– Kot skrbnik za zaščito morate pregledati zaščito, preden dovolite uporabo kateregakoli programa CGI v sistemu. Vedeti morate, od kje izvira sistem in katere funkcije izvaja. Nadzorovati morate tudi zmožnosti profilov uporabnikov, pod katerimi izvajate programe CGI. S programi CGI morate izvesti tudi preizkuse, da na primer določite, ali je mogoče pridobiti dostop do ukazne vrstice. S programi CGI morate biti ravno tako previdni kot s programi, ki prevzamejo pooblastilo.

– Poleg tega morate oceniti, ali imajo občutljivi objekti morda neustrezno javno pooblastilo. Slabo oblikovan program CGI lahko v nekaterih primerih omogoči izkušenemu in zlonamernemu uporabniku gostovanje v sistemu.

– Vse programe CGI shranite v določeni uporabniški knjižnici, kot je na primer CGILIB. S pomočjo objektnega pooblastila določite, kdo lahko v to knjižnico shranjuje nove objekte in kdo lahko izvaja programe v tej knjižnici. S smernicami omejite strežnik HTTP na izvajanje programov CGI v tej knjižnici.

Opomba: Če nudi vaš strežnik več logičnih spletnih strani, lahko nastavite ločeno knjižnico za programe CGI za vsako spletno stran.

Druga problematika zaščite

Sledi dodatna problematika zaščite:

- HTTP nudi za vaš sistem iSeries dostop, ki je samo za branje. Zahteve strežnika HTTP ne morejo neposredno ažurirati ali brisati podatkov v vašem sistemu. Toda uporabite lahko programe CGI, ki ažurirajo podatke. Poleg tega lahko omogočite program CGI Net.Data, ki dostopi do baze podatkov strežnika iSeries. Strežnik s pomočjo skripta (ki je podoben izhodnemu programu) oceni zahteve za program Net.Data. Zato lahko skrbnik sistema nadzoruje, katera dejanja lahko izvaja program Net.Data.
- Strežnik HTTP nudi dnevnik dostopa, s pomočjo katerega lahko nadzorujete dostope in poskuse dostopov prek strežnika.

Problematika zaščite pri uporabi SSL s strežnikom IBM HTTP za iSeries

Strežnik IBM HTTP za iSeries lahko nudi zaščitene spletne povezave s strežnikom iSeries. **Zaščitena spletna stran** pomeni, da so prenosi med odjemalcem in strežnikom (v obeh smereh) šifrirani. Ti šifrirani prenosi so zaščiteni pred vohljači in pred tistimi, ki poskušajo zajeti ali spremeniti prenose.

Opomba: Ne pozabite, da se nanaša zaščitena spletna stran zgolj na zaščito informacij, ki potujejo med odjemalcem in strežnikom. Namen te zaščite ni zmanjšati ranljivosti strežnika pred napadi hekerjev. Toda v vsakem primeru omeji informacije, ki bi jih dobil možen heker s pomočjo vohljanja.

V temah Informacijskega centra o SSL in spletnem streženju (HTTP) boste našli popolne informacije o namestitvi, konfiguriranju in upravljanju postopka šifriranja. Te teme nudijo pregled možnosti strežnika in problematiko uporabe strežnika.

Strežnik za povezavo z internetom nudi podporo za HTTP in HTTPS, če namestite enega od naslednjih licenčnih programov:

- 5722–NC1
- 5722–NCE

Če namestite ti možnosti, se izdelek imenuje zaščiteni strežnik za povezavo z internetom.

Strežnik IBM HTTP za iSeries (5722–DG1) nudi podporo za http in https. Če želite omogočiti SSL, morate namestiti enega od naslednjih šifrirnih izdelkov:

- 5722–AC2
- 5722–AC3

Zaščita, ki je odvisna od šifriranja, ima več zahtev:

- Pošiljatelj in prejemnik (strežnik in odjemalec) morate ″razumeti″ mehanizem šifriranja in imeti zmožnost za izvedbo šifriranja in dešifriranja. Strežnik HTTP zahteva odjemalca, omogočenega za SSL. (Večina priljubljenih spletnih brskalnikov je omogočenih za SSL.). Licenčni programi za šifriranje iSeries podpirajo številne načine šifriranja po industrijskem standardu. Ko poskusi odjemalec vzpostaviti zaščiteno sejo, pride do pogajanj strežnika in odjemalca, ki poiščeta najvarnejši način šifriranja, ki ga podpirata oba.
- Prenos mora biti takšen, da ga prisluškovalec ne more dešifrirati. Načini šifriranja tako zahtevajo, da uporabljata obe strani **zasebni ključ** šifriranja/dešifriranja, ki je znan samo njima. Če želite vzpostaviti zaščiteno *zunanjo* spletno stran, uporabite neodvisno službo za pooblastila (CA), ki bo izdelovala in izdajala digitalna potrdila za uporabnike in strežnike. Služba za pooblastila je overjena stranka.

S šifriranjem zaščitite tajnost prenesenih informacij. Toda za občutljive informacije, kot so na primer finančne informacije, želite poleg tajnosti zagotoviti tudi integriteto in pristnost. Odjemalec in (izbirno) tudi strežnik morata zaupati stranki na drugem koncu (prek neodvisne reference) in biti gotovi, da prenos ni bil spremenjen. Ta zagotovila za pristnost in integriteto nudi digitalni podpis, ki ga izda služba za pooblastila (CA). Protokol SSL nudi overjanje s preverjanjem digitalnega podpisa potrdila strežnika (in po izbiri tudi potrdila odjemalca).

Šifriranje in dešifriranje zahtevata določen čas obdelave in vplivata na zmogljivost prenosov. Zato nudijo strežniki iSeries zmožnost za sočasno izvajanje programov za zaščiteno in nezaščiteno streženje. Za streženje dokumentov, ki ne zahtevajo zaščite, kot je na primer katalog izdelkov, lahko uporabite nezaščiten strežnik HTTP. Ti dokumenti bodo imeli URL, ki se začne s http://. Zaščiten strežnik HTTP lahko uporabite za občutljive informacije, kot so na primer obrazci, na katere vnesejo stranke informacije o kreditni kartici. Program lahko streže dokumente, katerih URL se začne s http:// ali s https://.

Opomnik

Nepisan internetni zakon je, da svoje odjemalce obvestite, kdaj so prenosi zaščiteni in kdaj ne, še posebej, če vaša spletna stran uporablja za nekatere dokumente samo zaščiten strežnik.

Ne pozabite, da zahteva šifriranje zaščito odjemalca in zaščito strežnika. Zaščiteni brskalniki (odjemalci HTTP) so zdaj že kar precej pogosti.

Problematika zaščite za LDAP

Možnosti zaščite LDAP (Lightweight Directory Access Protocol) vključujejo plast zaščitenih vtičnic (SSL), sezname za nadzor dostopa in šifriranje gesel CRAM-MD5. V V5R1 smo za izboljšanje zaščite LDAP dodali podporo za povezave Kerberos in beleženje zaščite.

Podrobnejše informacije o teh temah lahko najdete v Informacijskem centru iSeries —>Delo z omrežjem–>TCP/IP–>Imeniške storitve (LDAP). V razdelku “Predpogoji in s tem povezane informacije” na strani xii poiščite informacije o dostopu do Informacijskega centra iSeries.

Problematika zaščite za LPD

LPD (demon vrstičnega tiskalnika) nudi zmožnost za porazdelitev izhodnih podatkov tiskalnika v sistem. Sistem za LPD ne izvaja nobene prijavne obdelave.

Preprečevanje dostopa LPD

Če *ne* želite, da bi kdorkoli uporabljal dostop LPD do vašega sistema, preprečite izvajanje strežnika LPD. Naredite naslednje:

__ Korak 1. Če želite preprečiti, da bi se opravila strežnika LPD samodejno zagnala pri zagonu TCP/IP, vpišite naslednje:

```
CHGLPDA AUTOSTART(*NO)
```

Opombe:

a. AUTOSTART(*YES) je privzeta vrednost.

b. V razdelku“Krmiljenje, kateri strežniki TCP/IP se zaženejo samodejno” na strani 112 boste našli podrobnejše informacije o nadzorovanju, kateri strežniki TCP/IP se samodejno zaženejo.

__ Korak 2. Če želite preprečiti, da bi nekdo povezal uporabniško aplikacijo, kot je aplikacija vtičnice, z vrati, ki jih sistem običajno uporablja za LPD, naredite naslednje:

__ Korak a. Vpišite GO CFGTCP, da boste prikazali meni Konfiguriranje TCP/IP.

__ Korak b. Izberite možnost 4 (Delo z omejitvami vrat TCP/IP).

__ Korak c. Na zaslonu Delo z omejitvami vrat TCP/IP podajte možnost 1 (Dodaj).

__ Korak d. Za območje nižjih vrat podajte 515.

__ Korak e. Za območje višjih vrat podajte *ONLY.

Opombe:

1) Omejitve vrat stopijo v veljavo pri naslednjem zagonu TCP/IP. Če je pri nastavitvi omejitve vrat TCP/IP aktiven, ga zaustavite in nato znova zaženite.

2) V RFC1700 boste našli podrobnejše informacije o splošnih dodelitvah številk vrat.

__ Korak f. Za protokol podajte *TCP.

__ Korak g. Za polje profila uporabnika podajte ime profila uporabnika, ki je v sistemu zaščiten. (Zaščiten profil uporabnika je tisti, ki ni lastnik programov, ki prevzamejo pooblastilo in njegovega gesla ne poznajo drugi uporabniki.) Če omejite vrata na določenega uporabnika, samodejno izključite vse ostale uporabnike.

__ Korak h. Ponovite korake od 2c do 2g še za protokol *UDP.

Krmiljenje dostopa LPD

Če želite odjemalcem LPD omogočiti dostop do sistema, morate upoštevati naslednja vprašanja, povezana z zaščito:

- Če želite uporabnikom preprečiti, da bi sistem preobremenili z neželenimi objekti, morate nastaviti ustrezne omejitve praga za pomožne pomnilniške prostore (ASP-je). Pragove za ASP-je lahko prikažete in nastavite s sistemskimi servisnimi orodji (SST) ali z namenskimi servisnimi orodji (DST). Podrobnejše informacije o pragovih ASP lahko najdete v knjigi *Backup and Recovery*.

- Za omejitev, kdo lahko pošilja vmesne datoteke v vaš sistem, lahko uporabite pooblastilo za izhodne čakalne vrste. Uporabniki LPD brez ID-ja uporabnika uporabljajo profil uporabnika QTMPLPD. Temu profilu uporabnika lahko dodelite dostop samo za nekaj izhodnih čakalnih vrst.

Problematika zaščite za SNMP

Strežnik iSeries lahko deluje v omrežju kot posrednik SNMP (simple network management protocol). SNMP nudi sredstva za upravljanje prehodov, usmerjevalnikov in gostiteljev v omrežnem okolju. Posrednik SNMP zbira informacije o sistemu in izvaja funkcije, ki jih zahtevajo oddaljeni upravljalniki omrežja SNMP.

Preprečevanje dostopa SNMP

Če *ne* želite, da bi kdorkoli uporabljal dostop SNMP do vašega sistema, preprečite izvajanje strežnika SNMP. Naredite naslednje:

__ Korak 1. Če želite preprečiti, da bi se opravila strežnika SNMP samodejno zagnala pri zagonu TCP/IP, vpišite naslednje:

```
CHGSNMPA AUTOSTART(*NO)
```

Opombe:

a. AUTOSTART(*YES) je privzeta vrednost.

b. V razdelku“Krmiljenje, kateri strežniki TCP/IP se zaženejo samodejno” na strani 112 boste našli podrobnejše informacije o nadzorovanju, kateri strežniki TCP/IP se samodejno zaženejo.

__ Korak 2. Če želite preprečiti, da bi nekdo povezal uporabniško aplikacijo, kot je aplikacija vtičnice, z vrati, ki jih sistem običajno uporablja za SNMP, naredite naslednje:

__ Korak a. Vpišite GO CFGTCP, da boste prikazali meni Konfiguriranje TCP/IP.

__ Korak b. Izberite možnost 4 (Delo z omejitvami vrat TCP/IP).

__ Korak c. Na zaslonu Delo z omejitvami vrat TCP/IP podajte možnost 1 (Dodaj).

__ Korak d. Za območje nižjih vrat podajte 161.

__ Korak e. Za območje višjih vrat podajte *ONLY.

Opombe:

1) Omejitve vrat stopijo v veljavo pri naslednjem zagonu TCP/IP. Če je pri nastavitvi omejitve vrat TCP/IP aktiven, ga zaustavite in nato znova zaženite.

2) V RFC1700 boste našli podrobnejše informacije o splošnih dodelitvah številk vrat.

__ Korak f. Za protokol podajte *TCP.

__ Korak g. Za polje profila uporabnika podajte ime profila uporabnika, ki je v sistemu zaščiten. (Zaščiten profil uporabnika je tisti, ki ni lastnik programov, ki prevzamejo pooblastilo in njegovega gesla ne poznajo drugi uporabniki.) Če omejite vrata na določenega uporabnika, samodejno izključite vse ostale uporabnike.

__ Korak h. Ponovite korake od 2c do 2g še za protokol *UDP.

Krmiljenje dostopa SNMP

Če želite upravljalnikom SNMP omogočiti dostop do sistema, morate upoštevati naslednja vprašanja, povezana z zaščito:

- Nekdo, ki lahko dostopi do vašega omrežja s SNMP, lahko zbere informacije o vašem omrežju. Informacije, ki jih skrijete s pomočjo vzdevkov in imenskega strežnika domen, postanejo prek SNMP na voljo možnemu vdiralcu. Vdiralec lahko z uporabo SNMP tudi spremeni konfiguracijo omrežja in prekine komunikacije.
- SNMP uporablja za dostop skupno ime. Konceptualno gledano je skupno ime podobno geslu, vendar skupno ime ni šifrirano. Zato je v njem mogoče vohljanje. S pomočjo ukaza ADDCOMSNMP (Dodaj skupno ime za SNMP) nastavite parameter internetnega naslova upravljalnika (INTNETADR) namesto na *ANY na enega ali več specifičnih naslovov IP. Parameter OBJACC ukaza ADDCOMSNMP ali CHGCOMSNMP lahko nastavite tudi na *NONE in preprečite, da bi upravljalniki v skupini dostopali do objektov MIB. To naredite samo začasno, da zavrnete dostop upravljalnikov v skupini, ne da bi odstranili skupino.

Problematika zaščite za strežnik INETD

Za razliko od drugih strežnikov TCP/IP strežnik INETD ne nudi odjemalcem ene storitve, pač pa različne mešane storitve, ki jih skrbniki lahko prilagodijo. Zaradi tega se strežnik INETD včasih imenuje ″super strežnik″. Strežnik INETD vključuje naslednje vgrajene storitve:

- čas
- dan
- ponovitev
- izvrženje
- sprememba

Te storitve so podprte za TCP in UDP. Za UDP sprejmejo storitve ponovitve, časa, dneva in spremembe pakete UDP, ki jih nato pošljejo nazaj tvorcu. Strežnik ponovitev vrne pakete, ki jih prejme, strežniki časa in dneva ustvarijo čas v specifični obliki in ga pošljejo nazaj, strežnik sprememb pa ustvari paket natisljivih znakov ASCII, ki ga pošlje nazaj.

Zaradi narave teh storitev UDP je sistem dostopen za napad z zavrnitvijo storitev. Denimo, da imate dva strežnika iSeries: SYSTEMA in SYSTEMB. Zlonameren programer lahko ponaredi oglavje IP in oglavje UDP z izvornim naslovom SYSTEMA in s številko vrat UDP časovnega strežnika. Ta paket lahko nato pošlje časovnemu strežniku v SYSTEMB, ki bo poslal čas v SYSTEMA, ki bo nato odgovoril SYSTEMB in tako naprej. To povzroči nepretrgano zanko, ki porablja sredstva CPU v obeh sistemih, kot tudi omrežno pasovno širino.

Zato morate v sistemu iSeries upoštevati tveganje za takšen napad in uporabljati te storitve samo v zaščitenem omrežju. Strežnik INETD je naložen tako, da se pri zagonu TCP/IP ne zažene samodejno. Konfigurirate lahko, ali želite pri zagonu INETD zagnati storitve ali ne. Po privzetku se časovna strežnika in strežnika dneva TCP in UDP zaženeta, ko zaženete strežnik INETD.

Za strežnik INETD obstajata dve konfiguracijski datoteki:

```
/QIBM/UserData/OS400/inetd/inetd.conf
/QIBM/ProdData/OS400/inetd/inetd.conf
```

Ti datoteki določata, kateri programi se zaženejo pri zagonu strežnika INETD. Določata tudi, pod katerim profilom uporabnika se izvajajo ti programi, ko jih zažene INETD.

Opomba: Konfiguricajske datoteke v proddata nikoli ne spreminjajte. Vsakič, ko na novo naložite sistem, je zamenjana. Konfiguracijske spremembe stranke je potrebno opraviti v datoteki v drevesu imenikov uporabniških podatkov, saj ta datoteka **ni** ažurirana med nadgraditvijo izdaje.

Če pridobi zlonamerni programer dostop do teh datotek, jih lahko konfigurira tako, da pri zagonu INETD zaženejo katerikoli program. Zato je zelo pomembno, da so te datoteke

zaščitene. Po privzetku zahtevajo za izvajanje sprememb pooblastilo QSECOFR. Priporočamo, da za dostop do njih ne zmanjšate zahtevanega pooblastila.

Opomba: Konfiguracijske datoteke v imeniku ProdData ne spreminjajte. Ta datoteka je zamenjana vsakič, ko na novo naložite sistem. Konfiguracijske spremembe stranke je potrebno opraviti v datoteki v drevesu imenikov uporabniških podatkov, ker ta datoteka med nadgraditvami izdaj ni ažurirana.

Problematika zaščite pri omejitvi gostovanja TCP/IP

Če je vaš sistem povezan v omrežje, lahko omejite zmožnost uporabnikov za gostovanje v omrežju z aplikacijami TCP/IP. Eden izmed načinov, na katerega lahko to naredite, je z omejitvijo dostopa do naslednjih ukazov TCP/IP odjemalcev:

Opomba: Ti ukazi lahko obstajajo v več knjižnicah v sistemu, ali pa vsaj v knjižnicah QSYS in QTCP. Ne pozabite poiskati in zaščititi vseh primerov.

- STRTCPFTP
- FTP
- STRTCPTELN
- TELNET
- LPR
- SNDTCPSPLF
- RUNRMTCMD (odjemalec REXEC)

Možni cilji uporabnikov so določeni z naslednjim:

- Vnosi v tabeli gostiteljev TCP/IP.
- Postavka *DFTROUTE v usmerjevalni tabeli TCP/IP. To uporabnikom omogoča, da vnesejo naslov IP sistema naslednjega preskoka, če je njihov cilj neznano omrežje. Uporabnik lahko doseže oddaljeno omrežje ali stopi v stik z njim z uporabo privzete smeri.
- Konfiguracija oddaljenega imenskega strežnika. Ta podpora omogoča, da drug strežnik v omrežju poišče imena gostiteljev za vaše uporabnike.
- Oddaljena sistemska tabela.

Natančno morate nadzorovati, kdo lahko dodaja postavke v te tabele in spremeni vašo konfiguracijo. Razumeti morate tudi vpliv postavk tabele in vaše konfiguracije.

Zavedati se morate, da lahko izkušen uporabnik z dostopom do prevajalnika ILE C izdela program vtičnice, ki se lahko priključi na vrata TCP ali UDP. To lahko otežite z omejitvijo dostopa do naslednjih datotek vmesnikov vtičnic v knjižnici QSYSINC:

- SYS
- NETINET
- H
- ARPA
- vtičnice in SSL

Za servisne programe lahko omejite uporabo že prevedenih aplikacij vtičnic in SSL, tako da omejite uporabo naslednjih servisnih programov:

- QSOSRV1
- QSOSRV2
- QSOSKIT(SSL)
- QSOSSLSR(SSL)

Storitveni programi so naloženi z javnim pooblastilom *USE, vendar lahko spremenite pooblastilo v *EXCLUDE (ali po potrebi v kakšno drugo vrednost).

Poglavje 15. Varen dostop do delovne postaje

Številni uporabniki vašega sistema imajo osebne računalnike (PC-je), ki jih uporabljajo kot delovne postaje. Uporabljajo orodja, ki se izvajajo na PC-ju in se s pomočjo PC-ja povežejo s strežnikom iSeries.

Večina načinov povezovanja PC-ja s strežniki iSeries nudi več funkcij kot emulacija delovne postaje. iSeries vidi PC kot zaslon in nudi uporabniku interaktivne prijavne seje. Poleg tega lahko vidijo strežniki iSeries PC kot drug računalnik in mu nudijo funkcije kot so prenos datotek in klic oddaljeni proceduri.

Kot skrbnik za zaščito strežnika iSeries morate upoštevati naslednje:

- Funkcije, ki so na voljo uporabnikom PC-jev, ki so povezani z vašim sistemom.
- Sredstva strežnika iSeries, do katerih lahko dostopijo uporabniki PC.

Če vaša shema zaščite za strežnik iSeries še ni pripravljena za zahtevnejše funkcije PC (kot sta prenos datotek in klic oddaljeni proceduri), jih lahko preprečite. Toda vaš cilj je najbrž omogočiti zahtevnejše funkcije PC in kljub temu zaščititi informacije v sistemu. Teme, ki sledijo, razlagajo nekaj vprašanj glede zaščite, ki so povezana z dostopom PC.

Preprečevanje virusov na delovni postaji

V naslednjih informacijah predlagamo nekaj načinov, ki jih lahko uporabijo skrbniki za zaščito pred virusi na PC-jih.

Zaščita dostopa do podatkov na delovni postaji

Določena programska oprema odjemalcev PC shranjuje informacije na strežnik s pomočjo map v skupni rabi. Za dostop do datotek baz podatkov iSeries ima uporabnik na voljo omejen, dobro definiran niz vmesnikov. S pomočjo zmožnosti prenosa datotek, ki je del večine odjemalsko/strežniške programske opreme, lahko uporabnik PC-ja prekopira datoteke med strežnikom in PC-jem. Z uporabo zmožnosti dostopa do baze podatkov, kot so datoteka DDM, oddaljeni SQL ali gonilnik ODBC, lahko dostopi uporabnik PC do podatkov na strežniku.

V tem okolju lahko izdelate programe, ki bodo prestrezali in ocenjevali zahteve uporabnikov PC za dostop do sredstev strežnika. Če uporabljajo zahteve datoteko DDM, podate izhodni program v omrežnem atributu dostopa do upravljanja do porazdeljenih podatkov (DDMACC). Za nekatere načine prenosa datotek PC lahko podate izhodni program v omrežnem atributu dostopa odjemalske zahteve (PCSACC). Namesto tega lahko podate PCSACC (*REGFAC) za uporabo registracijske funkcije. Če uporabijo zahteve za dostop do podatkov druge strežniške funkcije, lahko s pomočjo ukaza WRKREGINF registrirate izhodne programe za te strežniške funkcije.

Toda izhodne programe je težko oblikovati in redko se izkažejo kot popolnoma varni. Izhodni programi niso zamenjava za objektno pooblastilo, ki je oblikovano za zaščito objektov pred nepooblaščenim dostopom iz kateregakoli vira.

Določena programska oprema odjemalcev, kot je IBM iSeries Access za Windows, shranjuje podatke na strežnike iSeries in dostopa do njih s pomočjo integriranega datotečnega sistema. Če uporabite integrirani datotečni sistem, je dostop do strežnika za uporabnike PC veliko preprostejši. Pomen objektnega pooblastila se še poveča. Prek integriranega datotečnega sistema si lahko ogleda uporabnik z ustreznim pooblastilom knjižnico strežnika kot bi bila

imenik PC. Preprosta ukaza kopiranja in lepljenja lahko takoj preneseta podatke iz knjižnice strežnika iSeries v imenik PC ali obratno. Sistem samodejno opravi ustrezne spremembe v formatu podatkov.

Opombe:

1. Za nadzor nad uporabo objektov v datotečnem sistemu QSYS.LIB lahko uporabite pooblastitveni seznam. Podrobnejše informacije poiščite v “Omejitev dostopa do datotečnega sistema QSYS.LIB” na strani 92.
2. V razdelkuPoglavje 12, “Uporaba integriranega datotečnega sistema za zaščito datotek”, na strani 87 boste našli podrobnejše informacije o vprašanjih zaščite v povezavi z integriranim datotečnim sistemom.

Moč integriranega datotečnega sistema je v njegovi preprostosti uporabe za uporabnike in razvijalce. Uporabnik lahko prek enega vmesnika dela z objekti v več okoljih. Uporabnik PC ne potrebuje za dostop do objektov nobene posebne programske opreme ali API-jev. Namesto tega lahko uporabi znane ukaze PC ali način “postavitve in klika” za neposredno delo z objekti.

Za vse sisteme, na katere so priključeni PC-ji, toda še posebej za sisteme z odjemalsko programsko opremo, ki uporablja integrirani datotečni sistem, je zelo pomembna dobra shema objektnih pooblastil. Ker je zaščita vgrajena v izdelek OS/400, morajo vse zahteve za dostop do podatkov opraviti postopek preverjanja pooblastil. Preverjanje pooblastil se izvaja za zahteve iz kateregakoli izvora in za dostop do podatkov na kakršenkoli način.

Objektno pooblastilo z dostopom do delovne postaje

Pri nastavitvi pooblastila za objekte morate oceniti, kaj to pooblastilo omogoča uporabniku PC. Če ima uporabnik na primer pooblastilo *USE za datoteko, si lahko datoteko ogleda ali jo natisne, ne more pa spremeniti informacij v njej ali datoteke zbrisati. Za uporabnika PC je ogled enakovreden “branju”, ki nudi zadostno pooblastilo za izdelavo kopije datoteke na PC-ju. Toda tega morda niste nameravali.

Za nekatere pomembne datoteke boste morda morali nastaviti javno pooblastilo na *EXCLUDE, da boste preprečili snemanje. “Ogled” datoteke na strežniku lahko omogočite na kakšen drug način kot je z uporabo menija ali programov, ki prevzamejo pooblastilo.

Snemanje lahko preprečite tudi z uporabo izhodnega programa, ki se zažene vsakič, ko uporabnik PC zažene funkcijo strežnika (razen interaktivne prijave). Izhodni program lahko podate v omrežnem atributu PCSACC s pomočjo ukaza CHGNETA (Spremeni omrežni atribut) ali registrirate izhodne programe s pomočjo ukaza WRKREGINF (Delo z registracijskimi informacijami). Način, ki ga uporabite, je odvisen od tega, kako dostopajo PC-ji do podatkov v sistemu in katere odjemalske programe uporabljajo. Izhodni program (QIBM_QPWFS_FILE_SERV) velja za dostop programoviSeries Access in Net Server do IFS, ne preprečuje pa dostopa s PC-ja z drugimi načini kot sta FTP ali ODBC.

Programska oprema PC običajno nudi tudi zmožnost odlaganja, da lahko uporabnik prekopira podatke s PC-ja v datoteko baze podatkov strežnika. Če niste pravilno nastavili pooblastitvene sheme, lahko uporabnik PC prekrije vse podatke v datoteki s podatki PC-ja. Pri dodelitvi pooblastila *CHANGE morate biti zelo previdni. V dodatku D knjige *iSeries Security Reference* preberite, katero pooblastilo je potrebno za datotečne operacije.

Informacijski center iSeries nudi podrobnejše informacije o pooblastilu za funkcije PC in o uporabi izhodnih programov. Podrobnosti poiščitev razdelku“Predpogoji in s tem povezane informacije” na strani xii.

Upravljanje aplikacij

Upravljanje aplikacij je izbirna namestitvena komponenta Navigatorja iSeries, grafičnega uporabniškega vmesnika (GUI) za strežnik iSeries. Upravljanje aplikacij omogoča skrbnikom nadzor nad funkcijami ali aplikacijami, ki so na voljo za uporabnike in skupine na določenem strežniku. To vključuje tudi nadzor nad funkcijami, ki so na voljo za uporabnike, ki dostopajo do strežnika prek odjemalcev. Tu moramo poudariti, da pri dostopu do strežnika iz odjemalcev Windows določa funkcije, ki so na voljo za upravljanje, uporabnik strežnika iSeries in ne uporabnik Windows.

Celotno dokumentacijo o Upravljanju aplikacij Navigatorja iSeries, najdete v razdelku iSeries Informacijski center–>Povezava z iSeries—>Možna sredstva povezave —>Navigator iSeries (../html/as400/v5r2/ic2924/info/rzaj3/rzaj3overview.htm).

Upravljanje načel

Načela so orodje, ki ga lahko uporabijo skrbniki pri konfiguriranju programske opreme na odjemalskih PC-jih. Načela lahko omejijo, do katerih funkcij in aplikacij lahko dostopi uporabnik na PC-ju. Načela lahko tudi predlagajo ali obvezujejo uporabo konfiguracij za določene uporabnike ali PC-je.

Opomba: Načela ne nudijo nadzora nad sredstvi strežnika in niso zamenjava za zaščito strežnika. Načela lahko vplivajo na način, na katerega lahko iSeries Access dostopi do strežnika z določenega PC-ja z določenim uporabnikom. Vendar pa ne spremenijo načina dostopa do sredstev strežnika s pomočjo drugih načinov.

Načela so shranjena na datotečnem strežniku. Vsakič, ko se uporabnik prijavi na delovno postajo Windows, so načela, ki veljajo za tega uporabnika Windows, presneta z datotečnega strežnika. Načela se uveljavijo v registru, preden uporabnik na delovni postaji opravi kakršnokoli dejanje.

Načela **Microsoft v primerjavi z upravljanjem aplikacij**

iSeries Access Express podpira dve različni strategiji za izvedbo upravnega nadzora znotraj vašega omrežja: Sistemska pravila Microsoft in Upravljanje aplikacij Navigatorja iSeries. Pri odločanju, kateri način je najprimernejši za vas, razmislite o naslednjem.

Sistemska načela **Microsoft**

Načela so vodena na PC-ju in niso odvisna od določenih izdaj OS/400. Načela lahko uveljavite za PC-je, kot tudi za uporabnike Windows. To pomeni, da se sklicujejo uporabniki za profil uporabnika Windows in ne na profil uporabnika strežnika. Načela lahko uporabite za ″konfiguriranje″ kot tudi za omejevanje. V primerjavi z upravljanjem aplikacij nudijo večjo zrnatost in več funkcij. Razlog za to je, da za določitev, ali lahko uporabnik uporabi funkcijo ali ne, ni potrebna povezava s strežnikom. Izvedba načel je v primerjavi v izvedbo upravljanja aplikacij bolj zapletena, ker je potrebna uporaba urejevalnika sistemskih načel Microsoft in konfigurirati je potrebno posamezne PC-je za snemanje načel.

Upravljanje aplikacij Navigatorja **iSeries**

Upravljanje aplikacij poveže podatke s profilom uporabnika in ne s profilom Windows, s katerim se povežejo sistemska načela Microsoft. Za uporabo upravljanja aplikacij so potrebni strežniki iSeries, na katerih se izvaja izdaja OS/400 V4R3 ali novejša, toda nekatere funkcije so na voljo samo v izdaji V4R4 ali novejši. Upravljanje aplikacij izvaja upravljanje s pomočjo grafičnega uporabniškega vmesnika Navigatorja iSeries, katerega uporaba je v primerjavi z urejevalnikom načel veliko preprostejša. Upravljanje aplikacij velja za uporabnika ne glede na to, s katerega PC-ja se prijavi. Določene funkcije znotraj Navigatorja iSeries lahko omejite.

Uporabo upravljanja aplikacij priporočamo, če so vse funkcije, ki jih želite omejiti, omogočene za upravljanje aplikacij, in če različica OS/400, ki jo uporabljate, podpira upravljanje aplikacij.

Uporaba SSL z iSeries Access za Windows

Informacije o uporabi programa iSeries Access Express z SSL, preglejte Informacijski center iSeries teme *Upravljanje plasti zaščitenih vtičnic, Zaščita iSeries Access Express in Navigatorja iSeries, iSeries Developer Kit za Javo , in iSeries Java Toolbox*, v glavni temiJava. Te informacije si lahko ogledate tudi na zgoščenki, ki ste jo dobili s sistemom.

Zaščita Navigatorja iSeries

Navigator iSeries nudi preprost vmesnik za strežnik uporabnikom, ki imajo iSeries Access. Z vsako novo izdajo izdelka OS/400 je prek Navigatorja iSeries na voljo več funkcij strežnika. Preprost vmesnik nudi številne prednosti, ki vključujejo tudi zmanjšane stroške za tehnično pomoč in izboljšano sliko sistema. Poleg tega pa predstavlja tudi izziv za zaščito.

Kot skrbnik za zaščito se za ščitenje sredstev ne morete več zanašati na nevednost svojih uporabnikov. Številne funkcije v Navigatorju iSeries so preproste in vidne za uporabnike. Paziti morate, da oblikujete in izvršite zaščitna načela za profile uporabnikov in za zaščito objektov, tako da ustrezajo vašim zahtevam za zaščito.

IBM e(logo)server iSeries Access za Windows različice V4R4 in novejših različic nudi naslednje načine za nadzor nad funkcijami, ki jih lahko izvajajo uporabniki prek Navigatorja iSeries:

- Izbirna namestitev
- Upravljanje aplikacij
- Podpora za sistemska načela Windows NT

Navigator iSeries je razdeljen v več komponent, ki jih lahko namestite ločeno. To omogoča, da namestite samo funkcije, ki jih potrebujete. Upravljanje aplikacij omogoča, da skrbnik nadzoruje funkcije, do katerih lahko dostopata uporabnik ali skupina prek Navigatorja iSeries. Upravljanje aplikacij uredi aplikacije v naslednje kategorije:

Navigator iSeries
Vključuje Navigator iSeries in vse dodatke.

Odjemalske aplikacije
Zajema vse druge odjemalske aplikacije, vključujoč iSeries Access, ki nudijo funkcije odjemalcem, upravljanim prek Upravljanja aplikacij.

Gostiteljske aplikacije
Vključuje vse aplikacije, ki so v celoti shranjene na strežniku in nudijo funkcije, ki so vodene prek upravljanja aplikacij.

Za omejitev funkcij Navigatorja iSeries, do katerih lahko dostopi uporabnik, lahko uporabite izbirno namestitev, upravljanje aplikacij in načela. Toda nobenega izmed teh načinov ne uporabite za zaščito sredstev.

Od izdaje V4R4 naprej podpira IBM e(logo)server iSeries Access za Windows tudi uporabo urejevalnika sistemskih načel Windows NT, ki nadzoruje, katere funkcije je mogoče izvajati z določenega odjemalca PC ne glede na to, kdo uporablja ta PC.

Dodatne informacije o izbirni namestitvi, upravljanju aplikacij in upravljanju načel poiščite v Informacijskem centru iSeries. Razlago o upravljanju aplikacij boste našli tudi v razdelku “Funkcija omejitve dostopa do programa” na strani 5 te knjige.

Preprečevanje dostopa do ODBC

Open database connectivity (ODBC) je orodje, ki ga lahko uporabijo aplikacije za PC za dostop do podatkov iSeries, kot če bi šlo za podatke PC. Programer v ODBC lahko nastavi fizično mesto podatkov tako, da so transparenti za uporabnika aplikacije za PC. Podrobnejše informacije o problematiki zaščite, povezani z ODBC, lahko najdete v informacijah ″Zaščita ODBC iSeries Access za Windows″ (/rzaii/rzaiiodbc09.HTM) v Informacijskem centru iSeries.

Problematika zaščite za gesla seje delovne postaje

Ko uporabnik PC-ja zažene povezovalno programsko opremo, kot je na primer iSeries Access, običajno samo enkrat vpiše ID uporabnika in geslo strežnika. Geslo je šifrirano in shranjeno v pomnilniku PC. Vsakič, ko vzpostavi uporabnik novo sejo z istim strežnikom, pošlje PC geslo in ID uporabnika samodejno.

Določena odjemalsko/strežniška programska oprema nudi tudi možnost zaobitja prijavnega zaslona za interaktivne seje. Programska oprema pošlje ID uporabnika in šifrirano geslo, ko zažene uporabnik interaktivno sejo (emulacija 5250). Če želite uporabiti podporo za to možnost, mora biti nastavljena sistemska vrednost QRMTSIGN na strežniku na *VERIFY.

Če izberete zaobitje prijavnega zaslona, morate razmisliti o vplivu tega dejanja na zaščito.

Luknja v zaščiti: Za emulacijo 5250 ali katerokoli drugo vrsto interaktivne seje je prijavni zaslon enak kot katerikoli drugi zaslon. Čeprav geslo pri vpisu ni prikazano na zaslonu, je poslano prek povezave v nešifrirani obliki kot vsa druga podatkovna polja. V nekaterih vrstah povezav je to priložnost, ko lahko možni vdiralec nadzoruje povezavo in odkrije ID uporabnika in geslo. Nadzorovanje povezave z uporabo elektronske opreme se pogosto imenuje **vohljanje**. Od V4R4 naprej, lahko z uporabo plasti zaščitenih vtičnic (SSL) šifrirate komunikacije med iSeries Access in strežnikom iSeries. S tem zaščitite podatke, vključno z gesli, pred vohljanjem.

Če izberete možnost zaobitja prijavnega zaslona, PC šifrira geslo preden ga pošlje. Šifriranje prepreči možnost kraje gesla z vohljanjem. Toda zagotoviti morate, da izvajajo uporabniki PC operacijsko zaščito. PC, na katerem ne dela nihče, vendar je na njem aktivna seja s sistemom iSeries, je priložnost, da nekdo zažene drugo sejo, ne da bi poznal ID uporabnika in geslo. PC-ji morajo biti nastavljeni tako, da se zaklenejo, če sistem določen čas ni aktiven, in morajo za obnovitev seje zahtevati geslo.

Tudi če ne izberete zaobitja prijavnega zaslona predstavlja PC, na katerem ne dela nihče, vendar ima aktivno sejo, luknjo v zaščiti. S programsko opremo PC lahko nekdo zažene strežniško sejo in dostopi do podatkov, ne da bi poznal ID uporabnika in geslo. Nevarnost v emulaciji 5250 je nekoliko večja, ker zahteva manj znanja za zagon seje in začetek dostopa do podatkov.

Uporabnike morate podučiti o posledicah prekinitve seje iSeries Access. Številni uporabniki menijo (logično, toda nepravilno), da možnost prekinitve povezave v celoti zaustavi povezavo s strežnikom. Toda ko uporabnik izbere prekinitev povezave, strežnik omogoči sejo uporabnika (licenco) za drugega uporabnika, vendar je povezava odjemalca s strežnikom še vedno odprta. Na ta način lahko kakšen drug uporabnik pristopi k nezaščitenemu PC-ju in dostopi do sredstev strežnika, ne da bi vnesel ID uporabnika in geslo.

Za uporabnike, ki morajo prekiniti svoje seje, lahko predlagate dve možnosti:

- Zagotovite, da je na PC-jih nastavljena funkcija zaklepanja, ki zahteva geslo. S tem postane nezaščiten PC nerazpoložljiv za vsakogar, ki ne pozna gesla.

- Za popolno prekinitev seje se je potrebno odjaviti iz Windows ali znova zagnati PC. S tem zaustavite sejo z iSeries.

Uporabnike morate podučiti tudi o možni luknji v zaščiti pri uporabi iSeries Access za Windows. Če uporabnik poda UNC (univerzalno pravilo o poimenovanju) za določitev sredstva iSeries, izdela odjemalec Win95 ali NT omrežno povezavo s strežnikom. Ker uporabnik poda UNC, uporabnik tega ne vidi kot preslikanega omrežnega pogona. Uporabnik se pogosto celo ne zaveda obstoja omrežne povezave. Toda ta omrežna povezava predstavlja luknjo v zaščiti na PC-jih, na katerih ne dela nihče, ker je strežnik na PC-ju prikazan v imeniškem drevesu. Če ima seja uporabnika močan profil uporabnika, so lahko sredstva strežnika na nezaščitenem PC-ju izpostavljena. Enako kot za prejšnji zgled velja tudi tu, da boste najlažje zagotovili varnost, če bodo uporabniki razumeli možno luknjo v zaščiti in uporabljali funkcijo zaklepanja PC-jev.

Zaščita strežnika pred oddaljenimi ukazi in procedurami

Podučen uporabnik PC, ki uporablja programsko opremo, kot je iSeries, lahko izvaja ukaze na strežniku, ne da bi uporabil prijavni zaslon. Sledijo številni načini, ki so na voljo uporabnikom PC za izvajanje strežniških ukazov. Odjemalsko/strežniška programska oprema določa načine, ki so na voljo za uporabnike PC.

- Uporabnik lahko odpre datoteko DDM in izvede ukaz s pomočjo funkcije oddaljenega ukaza.
- Določena programska oprema, kot so optimizirani odjemalci za iSeries, nudi funkcijo oddaljenega ukaza prek API-jev za klic porazdeljenemu programu (DPC) brez uporabe DDM.
- Določena programska oprema, kot je oddaljeni SQL in ODBC, nudi funkcijo oddaljenega ukaza brez DDM ali DPC.

Za odjemalsko/strežniško programsko opremo, ki nudi podporo za oddaljeni ukaz s pomočjo DDM, lahko v celoti preprečite oddaljene ukaze z omrežnim atributom. DDMACC. Za odjemalsko/strežniško programsko opremo, ki uporablja drugo strežniško podporo, lahko registrirate izhodne programe za strežnik. Če želite omogočiti oddaljene ukaze, morate zagotoviti, da shema objektnih pooblastil ustrezno ščiti vaše podatke. Zmožnost oddaljenega ukaza je enakovredna dodelitvi ukazne vrstice uporabniku. Če prejme iSeries oddaljeni ukaz prek DDM, sistem ne uveljavi nastavitve profilov uporabnikov LMTCPB (Omejena zmožnost).

Zaščita delovnih postaj pred oddaljenimi ukazi in procedurami

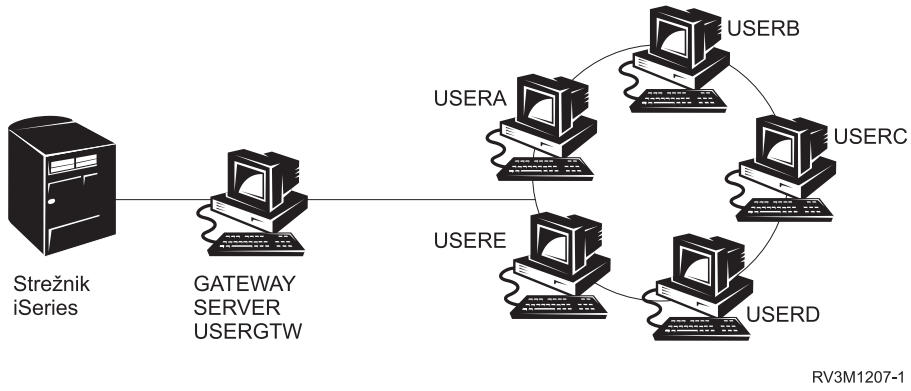
IBM iSeries Access za Windows nudi zmožnost sprejema oddaljenih ukazov na PC-ju. Za izvajanje procedure na nezaščitenem PC-ju lahko uporabite ukaz RUNRMTCMD (Zaženi oddaljeni ukaz). Funkcija RUNRMTCMD je koristno orodje za skrbnike sistemov in osebje v službi pomoči. Toda po drugi strani nudi tudi možnost za okvaro podatkov na PC-ju, pa naj bo namerno ali po nesreči.

PC-ji nimajo istih funkcij objektnih pooblastil kot strežniki iSeries. Najboljša zaščita pred težavami, ki jih povzroča ukaz RUNRMTCMD, je temeljita omejitev sistemskih uporabnikov z dostopom do ukaza. IBM iSeries Access za Windows nudi zmožnost registriranja uporabnikov, ki lahko izvajajo oddaljene ukaze na določenem PC-ju. Če je vzpostavljena povezava prek TCP/IP, lahko za nadzor dostopa do oddaljenih ukazov uporabite nadzorno ploščo lastnosti. Uporabnike lahko pooblastite z ID-jem uporabnike ali z imenom oddaljenega sistema. Če je vzpostavljena povezava prek SNA, nudi določena odjemalska programska oprema zmožnost nastavitve zaščite pogovora. V drugi odjemalski programski opremi pa preprosto izberete, ali želite nastaviti zmožnost vhodnega ukaza ali ne.

Za vsako kombinacijo odjemalske programske opreme in vrste povezave (kot sta TCP/IP ali SNA), morate razmisliti o možnosti vhodnih ukazov za priključene PC-je. Preglejte tudi dokumentacijo, ki ste jo dobili z odjemalcem; v nje poiščite “vhodni ukaz” ali “RUNRMTCMD”. Pripravljeni bodite, da boste uporabnikom PC-jev in skrbnikom omrežja svetovali pravilen (varen) način za konfigurriranje odjemalcev, ki bo omogočila ali preprečila to zmožnost.

Strežniki prehoda

Vaš sistem je morda povezan v omrežje, v katerem deluje med sistemom iSeries in PC-ji vmesni strežnik ali strežnik prehoda. Denimo, da je vaš sistem iSeries priključen v LAN s strežnikom PC, ki ima PC-je, povezane s strežnikom. Težave, povezane z zaščito v tej situaciji, so odvisne od zmožnosti programske opreme, ki se izvaja na strežniku prehoda. Slika 13 kaže zgled konfiguracije strežnika prehoda:



Slika 13. Sistem iSeries s strežnikom prehoda

Določena programska oprema sistemu iSeries ne dopušča, da bi zaznal uporabnike (kot sta USERA ali USERC), ki so v smeri navzdol od strežnika prehoda. Strežnik se bo prijavil v sistem kot samostojen uporabnik (USERGTW). Za obravnavo vseh zahtev uporabnikov v smeri navzdol bo uporabil ID uporabnika USERGTW. Strežnik bo videl zahtevo iz USERA kot zahtevo uporabnika USERGTW.

V tem primeru se morate za uveljavitev zaščite zanesti na strežnik prehoda. Razumeti in upravljati morate njegove zmožnosti zaščite. S stališča strežnika iSeries imajo vsi uporabniki isto pooblastilo kot ID uporabnika, ki ga uporablja strežnik prehoda za zagon seje. To je skoraj enakovredno izvajanju programa, ki prevzame pooblastilo in nudi ukazno vrstico.

V drugi programski opremi posreduje strežnik prehoda zahteve posameznih uporabnikov strežnikom iSeries. Strežnik iSeries ve, da USERA zahteva dostop do določenega objekta. Prehod je skoraj transparenten za sistem.

Če je vaš sistem v omrežju, v katerem delujejo strežniki prehoda, morate oceniti, katera pooblastila boste dodelili ID-jem uporabnikov, ki jih uporabljajo strežniki prehoda. Razumeti pa morate tudi naslednje:
- Mehanizme zaščite, ki jih uveljavijo strežniki prehoda
- Kako vidi sistem iSeries uporabnike v smeri navzdol.

Brezžične komunikacije LAN

Nekateri odjemalci lahko z uporabo brezžičnega lokalnega omrežja iSeries komunicirajo z vašim omrežjem brez žic. Brezžično lokalno omrežje iSeries uporablja tehnologijo radio-frekvenčnih komunikacij. Kot skrbnik za zaščito se morate zavedati naslednjih značilnosti izdelkov brezžičnih lokalnega omrežja iSeries, povezanih z zaščito:

- Ti izdelki brezžičnega lokalnega omrežja uporabljajo tehnologijo razpršenega spektra. To tehnologijo je v preteklosti uporabljala vlada za zaščito radijskih prenosov. Nekdo, ki poskuša elektronsko nadzorovati prenos podatkov, sliši zvok.
- Brezžična povezava ima tri konfiguracijske parametre, povezane z zaščito:
  - Stopnja prenosa podatkov (dve možni stopnji prenosa podatkov)
  - Frekvenca (pet možnih frekvenc)
  - Identifikator sistema (8 milijonov možnih identifikatorjev)

  Kombinacija teh konfiguracijskih elementov nudi 80 milijonov mogočih konfiguracij, zato je možnost, da bi heker uganil pravilno konfiguracijo, zelo majhna.
- Podobno kot pri drugih načinih komuniciranja vpliva tudi na zaščito brezžičnih komunikacij zaščita odjemalske naprave. Informacije o ID-ju sistema in drugi konfiguracijski parametri so v datoteki na odjemalski napravi in jih je potrebno zaščititi.
- Če brezžično napravo izgubite ali jo kdo ukrade, nudijo običajne mere za zaščito strežnika, kot sta zaščita prijave in objektov, zaščito pred poskusi nepooblaščenih uporabnikov za uporabo izgubljene ali ukradene enote za dostop do sistema.
- Če izgubite brezžično odjemalsko enoto ali vam jo ukradejo, je najbolje, da spremenite informacije o ID-ju sistema za vse uporabnike, dostopne točke in sisteme. Podobno bi ravnali, če bi izgubili ključe in bi zamenjali ključavnice na vratih.
- Strežnik lahko razdelite na skupine odjemalcev, ki imajo unikatne sistemske ID-je. S tem omejite vpliv, če enoto izgubite ali vam jo ukradejo. Ta način deluje samo, če omejite skupino uporabnikov na določen del namestitve.
- Za razliko od tehnologije LAN veljajo za tehnologijo brezžičnega LAN lastninske pravice. Zato za te izdelke brezžičnega LAN niso na voljo nobeni javno razpoložljivi vohljači. Vohljač je elektronska naprava, ki izvaja nepooblaščeno nadzorovanje prenosa.

Poglavje 16. Izhodni programi zaščite

Nekatere funkcije strežnika iSeries nudijo izhod, da se lahko v vašem sistemu izvaja uporabniško izdelan program, ki izvaja dodatno pregledovanje in preverjanje veljavnosti. Tako lahko na primer nastavite sistem tako, da bo zagnal izhodni program vsakič, ko bo v sistemu nekdo poskusil odpreti datoteko DDM (porazdeljeno upravljanje podatkov). Za podajanje izhodnih programov, ki se izvajajo pod določenimi pogoji, lahko uporabite funkcijo registracije.

Številne publikacije za iSeries vsebujejo zglede izhodnih programov, ki izvajajo funkcije zaščite. V tabeliTabela 24 boste našli seznam teh izhodnih programov in vzorčne programe v izvorni obliki.

Tabela 24. Izvorna oblika za vzorčne izhodne programe

Tip izhodnega programa	**Namen**	**Kje najti zglede**
Preverjanje veljavnosti gesla	Sistemska vrednost QPWDVLDPGM lahko podaja ime programa ali kaže, da bodo za preverjanje novega gesla za dodatne zahteve, ki jih ne obravnavajo sistemske vrednosti QPWDxxx, uporabljeni programi za preverjanje veljavnosti, registrirani za izhodno točko QIBM_QSY_VLD_PASSWRD. Uporabo tega programa je potrebno natančno nadzorovati, ker sprejema nešifrirana gesla. Ta program **naj ne** hrani gesel v datoteki ali jih posreduje drugemu programu.	• *An Implementation Guide for iSeries Security and Auditing, GG24–4200* • *iSeries Security Reference*, SC41-5302-07
PC Support/400 ali dostop Client Access[1]	Ime tega programa lahko podate v parametru PCSACC (Dostop odjemalskih zahtev) omrežnih atributov, da krmili naslednje funkcije: • Funkcija navideznega tiskalnika • Funkcija prenosa datotek • Funkcija map v skupni rabi tipa 2 • Funkcija sporočil dostopa odjemalcev • Podatkovne čakalne vrste • Funkcija oddaljenega SQL	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
Dostop do DDM (porazdeljeno upravljanje podatkov)	Ime tega programa lahko podate v parametru DDMACC (Dostop do zahtev DDM) omrežnih atributov, da krmili naslednje funkcije: • Funkcija map v skupni rabi tipa 0 in 1 • Funkcija predložitve oddaljenega ukaza	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
Oddaljena prijava	Program lahko podate v sistemski vrednosti QRMTSIGN, da krmili, kateri uporabniki se lahko samodejno prijavijo in s katerih mest (prehod).	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*

Tabela 24. Izvorna oblika za vzorčne izhodne programe (nadaljevanje)

Tip izhodnega programa	Namen	Kje najti zglede
Open Database Connectivity (ODBC) z iSeries Access[1]	Nadzoruje naslednje funkcije ODBC: • Ali je ODBC sploh dovoljen • Katere funkcije so dovoljene za datoteke baz podatkov iSeries • Kateri stavki SQL so dovoljeni • Katere informacije o objektih strežnika baz podatkov je mogoče pridobiti • Katere funkcije katalogiziranja SQL so na voljo	Ni na voljo.
Program za obravnavanje prekinitev QSYSMSG	Izdelate lahko program, ki bo nadzoroval čakalno vrsto sporočil QSYSMSG in opravil ustrezno dejanje (na primer poslal opozorilo skrbniku za zaščito) glede na tip sporočila.	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
TCP/IP	Številni strežniki TCP/IP (kot so FTP, TFTP, TELNET in REXEC) nudijo izhodne točke. Dodate lahko izhodne programe, ki bodo obravnavali prijavo in preverjali veljavnost zahtev uporabnikov, kot so na primer zahteve za pridobitev ali shranitev določene datoteke. Te izhodne programe lahko uporabite tudi za omogočanje anonimnega FTP v sistemu.	"Uporabniški izhodi TCP/IP v knjigi *iSeries System API Reference* "
Spremembe v profilih uporabnikov	Izdelate lahko izhodne programe za naslednje ukaze profilov uporabnikov: CHGUSRPRF CRTUSRPRF DLTUSRPRF RSTUSRPRF	• *iSeries Security Reference*, SC41-5302-07 • "Uporabniški izhodi TCP/IP v knjigi *iSeries System API Reference* "

Opombe:

1. Dodatne informacije o tej temi lahko najdete v Informacijskem centru iSeries. Za podrobnosti preglejte razdelek "Predpogoji in s tem povezane informacije" na strani xii.

Poglavje 17. Problematika zaščite za internetne brskalnike

Številni uporabniki PC-jev v vašem podjetju imajo na svojih delovnih postajah nameščene brskalnike in se lahko povezujejo v internet. Povežejo se lahko tudi z vašim strežnikom. Sledi opis problematike, povezane z zaščito, za PC-je in strežnik.

Tveganje: okvara delovne postaje

S spletno stranjo, ki jo obišče uporabnik, je lahko povezan ″program,″ kot je programček Java, krmilni element Active-X ali kakšna druga vrsta dodatka. Če to vrsto ″programa″ zaženete na PC-ju, lahko v nekaterih, čeprav redkih primerih, povzroči škodo v informacijah na PC-ju. Kot skrbnik za zaščito morate za zaščito PC-jev v podjetju razmisliti o naslednjem:

- Razumeti morate možnosti zaščite različnih brskalnikov, ki jih imajo uporabniki. Nekateri brskalniki na primer nadzorujejo dostop, ki ga imajo programčki Java izven brskalnika (omejeno operacijsko okolje Java se imenuje *predal*). S tem lahko preprečite, da bi programčki poškodovali podatke na PC-ju.

  Opomba: Koncept predala in z njim povezane omejitve zaščite ne obstajajo za Active-X in druge dodatke.
- Uporabnikom priporočite nastavitve brskalnikov. Najbrž nimate na voljo dovolj časa niti sredstev, da bi preverjali, ali uporabniki upoštevajo vaša priporočila, zato jih morate podučiti o možnih tveganjih, ki jih povzročijo nepravilne nastavitve.
- Razmislite o standardizaciji spletnih brskalnikov, ki nudijo potrebne možnosti zaščite.
- Uporabnikom dajte navodila, naj vas obvestijo o vsakem nenavadnem vedenju ali simptomih, ki so lahko povezani z določenimi spletnimi stranmi.

Tveganje: dostop do imenikov iSeries prek preslikanih pogonov

Denimo, da je PC povezan s strežnikom s sejo IBM iSeries Access za Windows. Ta seja je nastavila preslikane pogone za povezavo z integriranim datotečnim sistemom iSeries. Tako se lahko na primer pogon **G** na PC-ju preslika v integrirani datotečni sistem strežnika SYSTEM1 v omrežju.

Zdaj denimo, da ima isti uporabnik PC-ja brskalnik in lahko dostopi do interneta. Uporabnik zahteva spletno stran, na kateri se izvaja kvaren ″program″, kot je programček Java ali krmilni element Active-X. Program lahko poskusi zbrisati vse podatke na pogonu G PC-ja.

Pred škodo na preslikanih pogonih se lahko zaščitite na več načinov:

- Najpomembnejša zaščita je zaščita sredstev na strežniku. Strežnik vidi programček Java ali krmilni element Active-X kot uporabnika, ki vzpostavi sejo PC. Pri uporabnikih, ki imajo pooblastila za strežnik, morate biti previdni.
- Uporabnikom PC-jev svetujte, naj nastavijo svoje brskalnike tako, da bodo preprečili poskuse dostopa do preslikanih pogonov. To deluje za programčke Java, ne pa za krmilne elemente Active-X, ki nimajo koncepta predala.
- Uporabnike podučite o nevarnostih povezave s strežnikom in internetom v isti seji. Zagotovite tudi, da bodo uporabniki PC-jev (na primer z odjemalci Windows 95) razumeli, da ostanejo pogoni preslikani tudi, če se zdi, da je seja iSeries končana.

Tveganje: overjeni podpisani programčki

Uporabniki so morda upoštevali vaše nasvete in nastavili brskalnike tako, da preprečujejo programčkom zapisovanj na pogone PC. Vendar pa se morajo uporabniki PC-jev zavedati, da lahko *podpisan programček* nadomesti nastavitev brskalnika.

Podpisan programček vsebuje povezan digitalni podpis, ki vzpostavi njegovo pristnost. Ko uporabnik dostopi do spletne strani, ki vsebuje podpisan programček, se mu prikaže sporočilo. Sporočilo navaja podpis programčka (kdo ga je podpisal in kdaj). Ko uporabnik sprejme programček, mu dovoli, da prepiše nastavitve zaščite za brskalnik. Podpisan programček lahko piše na lokalne pogone PC-ja, čeprav privzeta nastavitev brskalnika to preprečuje. Podpisan programček lahko piše tudi na preslikane pogone strežnika, saj jih vidi PC kot lokalne pogone.

Za lastne programčke Java, ki izhajajo z vašega strežnika, boste morda morali uporabiti podpisane programčke. Vendar pa uporabnike na splošno podučite, naj ne sprejemajo podpisanih programčkov iz neznanih virov.

Poglavje 18. S tem povezane informacije

Priročniki

- *APPC Programming*, SC41-5443-00 opisuje podporo za zahtevnejše komuniciranje programa s programom (APPC), ki je na voljo za sistem iSeries. To knjigo uporabite kot vodilo v razvijanju uporabniških programov, ki uporabljajo APPC, in definiranju komunikacijskega okolja za komunikacije APPC. Knjiga vključuje problematiko, povezano z uporabniškimi programi, konfiguracijske zahteve in ukaze, upravljanje težav za APPC in splošno problematiko, povezano z delom v omrežju. Preglejte CD-ROM Informacijskega centraiSeries.
- *Internetna zaščita AS/400: Zaščita vašega AS/400 pred nevarnostmi na internetu* Redbook, SG24-4929 opisuje težave z zaščito in tveganja, povezana s povezovanjem vašega iSeries z internetom. V njej boste našli zglede, priporočila, nasvete in tehnike za aplikacije TCP/IP.
- *Backup and Recovery*, SC41-5304-07 nudi informacije o načrtovanju strategije varnostnega kopiranja in obnavljanja, shranjevanju informacij iz sistema in obnavljanju sistema. Oglejte si Informacijski centeriSeries. Dodatne informacije o tej temi lahko najdete tudi v Informacijskem centru iSeries. Za podrobnosti preglejte razdelek “Predpogoji in s tem povezane informacije” na strani xii.
- *CL Programming*, SC41-5721-06 nudi podroben opis kodiranja specifikacij z opisi podatkov (DDS) za datoteke, ki jih je mogoče opisati zunanje. Te datoteke so fizične, logične, prikazne, tiskalne ter datoteke s funkcijo komuniciranja med sistemi (ICF). Oglejte si Informacijski centeriSeries.
- Tema CL v Informacijskem centru (za podrobnosti preglejte razdelek “Predpogoji in s tem povezane informacije” na strani xii) nudi opis vseh ukazov iSeries krmilnega jezika (CL) in njegovih ukazov OS/400. Ukazi OS/400 so v rabi za zahtevanje funkcij licenčnega programa (5722-SS1)zaOperating System/400. Vsi drugi ukazi CL, ki niso za OS/400 - tisti, ki so povezani z drugimi licenčnimi programi, vključno z različnimi jeziki in pomožnimi programi - so opisani v drugih knjigah, ki podpirajo te licenčne programe.
- *Implementing iSeries Security, 3rd Edition* by Wayne Madden and Carol Woodbury. Loveland, Colorado: 29th Street Press, a division of Duke Communications International, 1998. V tej knjigi boste našli vodila in praktične nasvete za načrtovanje, nastavitev in upravljanje zaščite iSeries.

  Številka naročila ISBN:

  1-882419-78-2
- Podrobnejše informacije o strežniku HTTP lahko najdete na naslednjem URL-ju:

  `http://www.ibm.com/eserver/iseries/software/http/docs/doc.htm`
- *iSeries Security Reference*, SC41-5302-07 nudi popolne informacije o sistemskih vrednostih za zaščito, profilih uporabnikov, zaščiti sredstev in beleženju zaščite. Ta priročnik ne opisuje zaščite za specifične licenčne programe, jezike in pomožne programe. Oglejte si Informacijski centeriSeries.
- Tema Informacijskega centra z naslovom ″Osnovne operacije sistema″ nudi informacije o nekaterih ključnih konceptih in nalogah, potrebnih za osnovne operacije iSeries. Za podrobnosti poglejte “Predpogoji in s tem povezane informacije” na strani xii.
- Informacijski center opisuje, kako uporabiti in konfigurirati TCP/IP in številne aplikacije za TCP/IP kot so FTP, SMTP in TELNET. Za podrobnosti preglejte razdelek “Predpogoji in s tem povezane informacije” na strani xii.
- *Podpora datotečnega strežnika TCP/IP za OS/400 Installation and User’s Guide*, SC41-0125 nudi uvodne informacije, navodila za namestitev in postopke namestitve za

paket licenčnega programa Podpora za datotečni strežnik. Razlaga funkcije, ki so na voljo z izdelkom in vključuje zglede in nasvete za njihovo uporabo z drugimi sistemi.

- *Trusted Computer Systems Evaluation Criteria* DoD 5200.28.STD, opisuje kriterij za ravni zaupanja računalniškim sistemom. TCSEC je publikacija ameriške vlade. Njen izvod lahko dobite na naslednjem naslovu:

  Office of Standards and Products
  National Computer Security Center
  Fort Meade, Maryland 20755-6000 USA
  Attention: Chief, Computer Security Standards
- Informacijski center vsebuje številne teme povezane z upravljanjem sistema in delav razdelkuiSeries. Nekatere teme vključujejo zbirko podatkov zmogljivosti, upravljanje sistemskih vrednosti in upravljanje pomnilnika. Podrobnosti o dostopu do Informacijskega centra poiščitev razdelku“Predpogoji in s tem povezane informacije” na strani xii. Work Management, SC41-5306-03, nudi informacije o izdelavi in upravljanju okolja za upravljanje dela. Oglejte si Informacijski centeriSeries.

Poleg teh tem Informacijskega centra in dodatnih priročnikov lahko kot pomoč uporabite tudi naslednje vire:

- **IBM SecureWay**
  IBM SecureWay predstavlja skupni imenovalec IBM-ove pestre ponudbe sredstev za zaščito; strojno in programsko zaščito ter posvetovanje in servise, s pomočjo katerih stranke kar najbolje zaščitijo svoj IT. Naj bo to reševanje individualne težave ali pa izdelava celotne rešitve za podjetja, IBM SecureWay vam nudi vso strokovnost, potrebno za planiranje, načrtovanje, uvedbo in rokovanje z rešitvami za zaščito v poslovanju. Več informacij o ponudbi IBM SecureWay najdete na domači strani IBM SecureWay:
  `http://www.ibm.com/secureway`
- **Paketi storitev**
  Namestitev nove strojne ali programske opreme lahko gotovo pripomore k izboljšanju učinkovitosti in poslovnih operacij. Toda predstavlja tudi grožnjo za prekinitev poslovanja in vpliva na pomembna notranja sredstva. IBM Global Services nudi storitve, povezane z zaščito iSeries. Na naslednji spletni strani si lahko ogledate celoten izpis storitev za iSeries:
  `http://www.as.ibm.com/asus`

Opombe

Te informacije smo razvili za izdelke in storitve, ki jih nudimo v ZDA.

IBM v drugih državah morda ne bo nudil izdelkov, storitev ali možnosti, opisanih v tem dokumentu. Informacije o izdelkih in storitvah, ki so trenutno na voljo pri vas, lahko dobite pri lokalnem IBM-ovem tržnem predstavniku. Nobena referenca na IBM-ov izdelek, program ali storitev ne pomeni, da lahko uporabite samo ta IBM-ov izdelek, program ali storitev. Namesto njih lahko uporabite katerikoli enakovreden izdelek, program ali storitev, ki ne krši IBM-ovih pravic do intelektualne lastnine. Dolžnost uporabnika je, da preveri in oceni ustreznost delovanja izdelkov, programov ali storitev, ki niso izdelek IBM-a.

IBM ima lahko patente ali patentne aplikacije, ki pokrivajo predmet tega dokumenta. Posedovanje tega dokumenta vam ne daje licence za te patente. Pisna vprašanja v zvezi z licencami lahko pošljete na naslednji naslov:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
ZDA

Če imate vprašanja v zvezi z dvobajtnim naborom znakov (DBCS), se obrnite na IBM-ov oddelek za intelektualno lastnino v vaši državi ali pa pošljite pisno poizvedbo na naslednji naslov:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

Naslednji odstavek ne velja za Veliko Britanijo ali katerokoli drugo državo, v kateri takšni pogoji niso v skladu z lokalnim zakonom: PODJETJE INTERNATIONAL BUSINESS MACHINES ZAGOTAVLJA, DA JE TA PUBLIKACIJA “TAKŠNA KOT JE” IN SICER BREZ VSAKRŠNEGA JAMSTVA, PA NAJ BO IZRECNO ALI VKLJUČENO, KAR BREZ OMEJITVE VKLJUČUJE TUDI VKLJUČENA JAMSTVA ZA TRŽNOST ALI PRIMERNOST ZA DOLOČEN NAMEN. V nekaterih državah ne dopuščajo zavrnitve izrecnih ali vključenih jamstev, zato ta stavek morda ne velja za vas.

Te informacije lahko vsebujejo tehnične netočnosti ali tipografske napake. Informacije iz tega dokumenta občasno spremenimo; te spremembe bodo vključene v nove izdaje te publikacije. IBM lahko brez vnaprejšnjega obvestila izboljša in/ali spremeni izdelek(ke) in/ali program(e), opisane v tej publikaciji.

Spletne strani, ki niso last podjetja IBM, so omenjene le zaradi pripravnosti in na noben način ne pomenijo, da so potrjene. Gradivo na teh spletnih straneh ni del gradiva za ta IBM-ov izdelek in te spletne strani uporabljate na lastno odgovornost.

IBM lahko vaše informacije posreduje naprej na katerikoli način, za katerega meni, da je primeren, ne da bi si s tem naprtil kakršnekoli obveznosti do vas.

Imetniki licenc za ta program, ki želijo informacije, da bi omogočili: (i) izmenjavo informacij med neodvisno izdelanimi programi in drugimi programi (vključno s tem) in (ii) skupno rabo izmenjanih informacij, naj se obrnejo na:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
ZDA

Takšne informacije bodo na voljo v skladu z ustreznimi določbami in pogoji, ki lahko v določenih primerih zajemajo tudi plačilo.

Licenčni program, opisan v teh informacijah, in vse licenčno gradivo, ki je na voljo zanj, nudi IBM pod pogoji IBM-ove licence s strankamiIBM-ove mednarodne pogodbe za licenčne programe ali enakovredne pogodbe med nami.

Vse podatke o zmogljivosti, opisane v tem dokumentu, smo določili v nadzorovanem okolju. Zato se lahko rezultati, ki jih boste dobili v drugih operacijskih okoljih, precej razlikujejo. Nekatere meritve so bile opravljene v sistemih na razvojni stopnji in zato ne dajemo nobenega jamstva, da bodo te meritve enake tudi v splošno razpoložljivih sistemih. Prav tako so bile nekatere meritve pridobljene z ocenitvijo. Dejanski rezultati so lahko drugačni. Uporabniki tega dokumenta naj preverijo ustrezne podatke za svoje specifično okolje.

Informacije o izdelkih, ki niso IBM-ovi, smo pridobili pri dobaviteljih teh izdelkov, iz njihovih natisnjenih objav ali drugih javno razpoložljivih virov. IBM teh izdelkov ni preizkusil in ne more potrditi natančnosti glede zmogljivosti, združljivosti in drugih zahtev, povezanih z izdelki, ki niso IBM-ovi. Vprašanja v zvezi z zmogljivostjo izdelkov, ki niso IBM-ovi, naslovite na njihove dobavitelje.

Vse izjave glede IBM-ove bodoče usmeritve lahko spremenimo ali umaknemo brez vsakega obvestila, in predstavljajo zgolj namene in cilje.

Te informacije so namenjene zgolj za načrtovanje. Preden boste lahko kupili izdelke, opisane v tem dokumentu, lahko te informacije spremenimo.

Te informacije vsebujejo vzorce podatkov in poročil, uporabljenih v dnevnih poslovnih dejavnostih. Da bi bili zgledi čim bolj nazorni, vključujejo imena posameznikov, podjetij, znamk in izdelkov. Vsa ta imena so izmišljena in vsaka podobnost z uporabljenimi imeni in naslovi dejanskih podjetij je zgolj naključna.

LICENCA ZA AVTORSKE PRAVICE:

Informacije vsebujejo vzorčne uporabniške programe v izvorni kodi, ki prikazujejo tehnike programiranja na različnih operacijskih platformah. Te vzorčne programe lahko brez nadomestila IBM-u kopirate, popravljate in razdeljujete za namene razvijanja, uporabe, trženja ali razdeljevanja uporabniških programov, ki ustrezajo aplikacijskemu programerskemu vmesniku za operacijsko platformo, za katero so vzorčni programi napisani. Teh zgledov nismo natančno preizkusili v vseh pogojih. Zato IBM ne more jamčiti zanesljivosti, uporabnosti ali delovanja teh programov. Te vzročne programe lahko brez nadomestila IBM-u kopirate, popravljate in razdeljujete za namene razvijanja, uporabe, trženja ali razdeljevanja uporabniških programov, ki ustrezajo IBM-ovim aplikacijskim programerskim vmesnikom.

Če te informacije berete kot zaslonsko publikacijo, morda ne boste videli fotografij in barvnih ilustracij.

Blagovne znamke

Naslednji izrazi so prodajne znamke podjetja International Business Machines Corporation v Združenih državah Amerike, v drugih državah ali v oboljih:

Advanced Peer-to-Peer Networking
APPN
AS/400
DB2
DRDA
e (logotip)
IBM
iSeries
Net.Data
Operating System/400
OS/400
PowerPC
SecureWay
System/36
System/38
400

ActionMedia, LANDesk, MMX, Pentium in ProShare so prodajne znamke ali zaščitene prodajne znamke družbe Intel Corporation v ZDA, v drugih državah, ali v oboljih.

Microsoft, Windows, Windows NT in logotip Windows so prodajne znamke družbe Microsoft Corporation v ZDA, drugih državah, ali v oboljih.

Java in vse prodajne znamke, ki temeljijo na Javi, so prodajne znamke Sun Microsystems, Inc. v ZDA, drugih državah, ali v oboljih.

UNIX je zaščitena prodajna znamka The Open Group v ZDA in drugih državah.

Ostala imena podjetij, izdelkov ali storitev so lahko prodajne ali storitvene znamke drugih.

Stvarno kazalo

Posebni znaki

A

B

C

Č

D

E

F

G

I

J

K

L

M

N

O

P

Q

R

S

Š

T

U

V

Z

Pripombe bralcev

iSeries
Nasveti in orodja za zaščito iSeries
Različica 5

Številka publikacije SA12-6308-07

Zelo cenimo vaše komentarje o tej publikaciji. Vaš komentar se lahko nanaša na določene napake ali pomanjkljivosti, na točnost, organizacijo, predmet ali popolnost te knjige. Komentarji, ki jih pošiljate, naj se nanašajo le na informacije iz tega priročnika in način, kako so te informacije predstavljene.

Za tehnična vprašanja in informacije o izdelkih in cenah se, prosimo, obrnite na svojo podružnico IBM-a, na IBM-ovega poslovnega partnerja oziroma na svojega pooblaščenega prodajalca.

Za splošna vprašanja pokličite ″Halo IBM″ (telefonska številka 0180 3 313233).

S tem, da svoje komentarje pošljete IBM-u, mu dajete tudi neizključno pravico do uporabe ali distribucije vaših komentarjev na katerikoli način, za katerega meni, da je primeren, brez vsake obveznosti do Vas.

Komentarji

Zahvaljujemo se Vam za pomoč.

Za predložitev Vaših komentarjev:
- Pošljite svoje komentarje na naslov, ki je na hrbtni strani tega obrazca.
- Pošljite faks na naslednjo številko: Združene države Amerike in Kanada: 1-800-937-3430
- Pošljite svoje komentarje po elektronski pošti na: RCHCLERK@us.ibm.com

Če bi želeli odgovor od IBM-a, prosimo vpišite naslednje informacije:

Ime	Naslov
Podjetje	
Telefonska številka	Naslov elektronske pošte:

IBM

IBM CORPORATION
ATTN DEPT 542 IDCLERK
3605 Highway 52 N
ROCHESTER MN

Natisnjeno na Danskem

SA12-6308-07