IBM

eserver

iSeries

Sugestii pentru securizarea iSeries

Versiunea 5

SA12-7296-07

IBM

@server

iSeries

Sugestii pentru securizarea iSeries

Versiunea 5

SA12-7296-07

Notă

Înainte de a folosi aceste informaţii şi produsul pe care îl suportă, citiţi informaţiile din “Observaţii” la pagina 155.

Ediţia a opta (aprilie 2004)

Această ediţie se aplică la versiunea 5, ediţia 3, modificarea 0 a IBM Operating System/400 (număr produs 5722-SS1) şi la toate ediţiile şi modificările ulterioare, până când nu se specifică altfel în noua ediţie. Această versiune nu rulează pe toate modelele RISC şi nu rulează pe modelele CISC.

Această ediţie înlocuieşte SC41-5300-06.

Cuprins

Figuri

Tabele

Despre Sugestii şi unelte pentru securizarea iSeries (SC41-5300-07)

Rolul calculatoarelor în organizaţii se modifică rapid. Managerii IT, furnizorii de software, administratorii de securitate şi auditorii trebuie să îşi înnoiască imaginea despre multe aspecte pe care până acum le-au acceptat aşa cum erau. Securitatea iSeries ar trebui să fie în această listă.

Sistemele furnizează multe funcţii noi care sunt în mod substanţial diferite de aplicaţiile contabile tradiţionale. Utilizatorii intră în sisteme în noi moduri: LAN-uri, linii comutate (apel telefonic), conexiune necablată, reţele de toate tipurile. Deseori, utilizatorii nu văd un ecran pentru conectare. Multe organizaţii se extind pentru a deveni "întreprinderi extinse", fie prin reţele proprietare, fie prin Internet.

Deodată, sistemele par să aibă un set nou de uşi şi ferestre. Managerii de sistem şi administratorii de securitate sunt în mod justificat preocupaţi de modul de protejare a avantajelor informaţiilor în acest mediu aflat în schimbare rapidă.

Aceste informaţii furnizează un set de sugestii practice pentru folosirea opţiunilor de securitate ale iSeries şi pentru stabilirea procedurilor de operare care ţin de securitate. Recomandările din aceste informaţii se aplică la o instalare cu expuneri şi cerinţe de securitate medii. Aceste informaţii nu furnizează o descriere completă a opţiunilor de securitate disponile pentru iSeries. Dacă doriţi să citiţi despre opţiuni suplimentare sau aveţi nevoie de mai multe informaţii de fundal, consultaţi publicaţiile care sunt descrise în Capitolul 17, "Informaţii înrudite", la pagina 153.

Aceste informaţii descriu de asemenea cum să setaţi şi să folosiţi uneltele de securitate care sunt parte din OS/400. Capitolul 4, "Configurarea iSeries pentru a folosi Unelte de securitate", la pagina 25 şi "Comenzi şi meniuri pentru comenzile de securitate" la pagina 26 furnizează informaţii de referinţă despre uneltele de securitate. Aceste informaţii furnizează exemple pentru utilizarea uneltelor.

Cine trebuie să citească această carte

Un **responsabil cu securitatea** sau **administrator de securitate** răspunde de securitatea unui sistem. Această responsabilitate include de obicei următoarele sarcini:

- Configurarea şi administrarea profilurilor de utilizator
- Configurarea variabilelor globale ale sistemului care afectează securitatea
- Administrarea autorizărilor pe obiecte
- Impunerea şi urmărirea politicilor de securitate

Dacă sunteţi responsabil cu administrarea securităţii pentru unul sau mai multe sisteme iSeries , aceste informaţii vă sunt necesare. Instrucţiunile din aceste informaţii asumă următoarele:

- Sunteţi familiarizat cu procedurile de operare de bază ale iSeries, cum ar fi conectarea şi folosirea comenzilor.
- Sunteţi familiarizat cu elementele de bază ale securităţii iSeries: niveluri de securitate, valorile sistemului de securitate, profiluri de utilizator şi securitatea obiectelor.

  Notă: Capitolul 1, "Elemente de bază ale securităţii iSeries", la pagina 3 oferă o trecere în revistă a acestor elemente. dacă aceste elemente de bază vă sunt noi, citiţi apoi

subiectul *Securitate de bază şi planificare* din Centru de informare iSeries. Vezi "Condiţii prealabile şi informaţii conexe" pentru mai multe detalii.

- Aţi activat securitatea în sistemul dumneavoastră setând variabila de sistem nivel de securitate (QSECURITY) la cel puţin 30.

IBM îmbunătăţeşte continuu capabilităţile de securitate ale iSeries. Pentru a beneficia de aceste îmbunătăţiri, ar trebui să cercetaţi în mod regulat pachetul de fixuri cumulative care este disponibil pentru distribuţia dumneavoastră. Vedeţi dacă conţine corecţii care sunt relevante pentru securitate.

Cum să folosiţi aceste informaţii

Dacă nu aţi setat sistemul dumneavoastră pentru a folosi instrumente de securitate sau dacă aţi instalat Set de instrumente de securitate pentru OS/400 pentru o versiune anterioară, faceţi următoarele:

1. Începeţi cu Capitolul 2, "Vrăjitor securitate iSeries şi eServer Security Planner", la pagina 9. Acesta descrie modul de utilizare al acestor caracteristici pentru a selecta care dintre unelte de securitate sunt recomandate şi modul de a începe lucrul cu ele.
2. Pentru mai multe informaţii de bază despre securitate, puteţi revedea informaţiile Referinţe de securitate, localizate în iSeries Centru informaţii.

Notă

Aceste informaţii au *multe* indicii pentru securizarea iSeries. Sistemul dumneavoastră poate solicita protecţie numai în anumite zone. Folosiţi aceste informaţii pentru a vă informa despre problemele de securitate posibile şi remediile lor. Apoi concentraţi-vă eforturile asupra zonelor cele mai critice pentru sistemul dumneavoastră.

Condiţii prealabile şi informaţii conexe

Utilizaţi Centru de informare iSeries ca punct de plecare pentru căutarea informaţiilor tehnice iSeries.

Puteţi accesa Centru informaţii în 2 moduri:

- De pe umătorul Web site:

  `http://www.ibm.com/eserver/iseries/infocenter`
- De pe CD_ROM-ul *Centru de informare iSeries*, SK3T-4091-04. Acest CD-ROM se livrează cu comanda de hardware iSeries nou sau cu modernizarea software-ului IBM Operating System/400. Puteţi de asemenea ordona CD-ROM-ul din IBM Publications Center:

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

Centru de informare iSeries conţine informaţii iSeries noi şi actualizate cum ar fi instalarea hardware şi software, Linux, WebSphere, Java, înalta disponibilitate, baza de date, partiţii logice, comenzi CL şi API-uri. În plus, oferă consilieri şi programe de căutare care vă ajută la planificarea, depanarea şi configurarea hardware şi software pentru iSeries.

Cu fiecare echipament nou comandat veţi primi *iSeries Setup and Operations CD-ROM*, SK3T-4098-02. Acest CD-ROM conţine produsele IBM @server IBM e(logo)server iSeries Access pentru Windows şi vrăjitorul EZ-Setup. iSeries Access Family oferă un set puternic de capabilităţi client şi server pentru conectarea PC-urilor la serverele iSeries. Vrăjitorul EZ-Setup automatizează multe din operaţiile de setare pentru iSeries.

Cum să trimiteţi comentariile dumneavoastră

Comentariile dumneavoastră sunt importante pentru a ne ajuta să furnizăm informaţia cea mai exactă şi superioară calitativ. Dacă aveţi ceva de comentat despre cartea aceasta sau despre altă documentaţie iSeries, scrieţi în comentariul cititorilor de la sfârşitul cărţii.

- Dacă preferaţi să trimiteţi comentariile prin poştă, folosiţi formularul pentru comentarii din partea cititorului cu adresa care este tipărită pe verso. Dacă trimiteţi un formular de comentariu al unui cititor dintr-o ţară alta decât SUA, îi puteţi da formularul oficiului local IBM sau reprezentanţei IBM pentru poştă plătită.
- Dacă preferaţi să trimiteţi comentariile prin fax, folosiţi unul din următoarele numere:
  - Statele Unite, Canada şi Porto Rico: 1-800-937-3430
  - Alte ţări: 1-507-2 53-5192
- Dacă preferaţi să trimiteţi comentariile pe cale electronică, folosiţi una dintre aceste adrese de poştă electronică:
  - Comentarii asupra cărţilor:

    RCHCLERK@us.ibm.com
  - Comentarii despre Centru de informare iSeries:

    RCHINFOC@us.ibm.com

Nu uitaţi să includeţi următoarele:

- Numele cărţii sau subiectul Centrului de informare iSeries.
- Numărul de publicaţie al unei cărţi.
- Numărul paginii sau subiectul cărţii cărora li se aplică comentariul dumneavoastră.

Partea 1. Securitate iSeries de bază

Capitolul 1. Elemente de bază ale securităţii iSeries

Acest capitol furnizează o scurtă trecere în revistă a elementelor de bază ce conlucrează pentru a asigura securitatea iSeries. În alte părţi ale acestei cărţi trecem dincolo de elementele de bază pentru a furniza sfaturi în utilizarea acestor elemente de securitate pentru a întruni cerinţele organizaţiei dumneavoastră.

Nivele de securitate

Puteţi folosi câtă securitate doriţi în sistem pentru a impune prin setări valoarea de sistem a nivelului de securitate (QSECURITY). Sistemul oferă cinci niveluri de securitate:

Nivel 10:

Sistemul nu impune nici o securitate. Nu este necesară parola. Dacă profilul de utilizator specificat nu există în sistem când cineva se semnează, sistemul creează un profil.

ATENŢIE:

Începând cu V4R3 şi versiunile viitoare, nu puteţi seta variabila de sistem QSECURITY la 10. Dacă sistemul este în acest moment la nivelul de securitate 10, va rămâne la nivelul 10 când instalaţi V4R3. Dacă modificaţi nivelul de securitate la o altă valoare, nu îl veţi mai putea aduce înapoi la nivelul 10. Deoarece nivelul 10 nu furnizează protecţie de securitate, acest nivel nu este recomandat IBM. **IBM nu va furniza suport pentru nici o problemă care apare la nivelul 10 de securitate exceptând cazul în care problema apare la un nivel mai mare de securitate.**

Nivel 20:

Sistemul cere un ID de utilizator şi o parolă pentru semnare. Nivelul de securitate 20 este deseori numit **securitate semnare**. Implicit, toţi utilizatorii au acces la toate obiectele pentru că toţi utilizatorii au autorizarea specială *ALLOBJ.

Nivel 30:

Sistemul cere un ID de utilizator şi o parolă pentru semnare. Utilizatorii trebuie să aibă autorizarea de a folosi obiecte deoarece utilizatorii nu au nici o autorizare implicită. Aceasta este numită **securitatea resurselor**.

Nivel 40:

Sistemul cere un ID de utilizator şi o parolă pentru semnare. În plus faţă de securitatea resurselor, sistemul furnizează funcţii pentru **protecţia integrităţii**. Funcţiile de protecţie a integrităţii, cum ar fi validarea parametrilor pentru interfeţele la sistemul de operare, sunt necesare pentru a proteja atât sistemul dumneavoastră cât şi obiectele din sistemul dumneavoastră la acţiunile utilizatorilor sistemului. Pentru cele mai multe instalări, nivelul de securitate recomandat este nivelul 40. Când primiţi un nou sistem iSeries cu V4R5 sau o versiune mai nouă, nivelul de securitate este setat la 40.

Nivel 50:

Sistemul cere un ID de utilizator şi o parolă pentru semnare. Sistemul impune atât securitatea resurselor, cât şi protecţia integrităţii nivelului 40, dar adaugă **protecţie îmbunătăţită a integrităţii**, cum ar fi restricţia de tratare a mesajelor între programele de stare sistem şi programele de stare utilizator. Nivelul de securitate 50 este destinat sistemelor iSeries cu cerinţe înalte de securitate.

Notă: Nivelul 50 este nivelul solicitat pentru certificare C2 (şi certificare FIPS-140).

Capitolul 2 al cărţii *Referinţă securitate iSeries* furnizează mai multe informaţii despre nivelurile de securitate şi descrie modul de deplasare de la un nivel de securitate la altul.

Setări globale

Sistemul dumneavoastră are setări globale care afectează modul în care funcţionează sistemul şi cum apare sistemul altor utilizatori ai sistemului. Aceste setări includ următoarele:

Valorile de securitate ale sistemului:
Valorile de securitate ale sistemului sunt folosite penru a controla securitate în sistemul dumneavoastră. Aceste variabile sunt împărţite în patru grupuri:
- Variabile de sistem pentru securitate generală
- Alte variabile de sistem referitoare la securitate
- Variabile de sistem care controlează parole
- Variabile de sistem care controlează auditing

Mai multe subiecte din carte abordează implicaţiile de securitate ale anumitor variabile de sistem. Capitolul 3 din cartea *Referinţă securitate iSeries* descrie toate variabilele de sistem relevante pentru securitate.

Atributele reţelei:
Atributele reţelei controlează cum participă sistemul (sau alege să nu participe) într-o reţea cu alte sisteme. Puteţi citi mai multe despre atributele reţelei în cartea *Control funcţionare*.

Descrierea subsistemelor şi a altor elemente de administrare a activităţii:
Elementele administrării activităţii determină cum intră activităţile în sistem şi în ce mediu rulează activităţile. Mai multe subiecte din această informaţie descriu implicaţiile de securitate ale unor valori de gestiune a funcţionării. Cartea *Control funcţionare* furnizează informaţii complete.

Configurarea comunicaţiilor:
Configurarea comunicaţiilor afectează şi cum intră activităţile în sistem. Mai multe subiecte din această informaţie furnizează sugestii pentru protejarea sistemului dumneavoastră când acesta face parte dintr-o reţea.

Profiluri utilizator

Orice utilizator al sistemului **trebuie** să aibe un profil utilizator. Trebuie să creaţi un profil utilizator înainte ca un utilizator să se poată înregistra. Profilurile utilizator pot fi de asemenea utilizate pentru a controla accesul la uneltele de service cum ar fi DASD şi dump-urile de memorie principală. Vezi “Gestionarea uneltelor de service” la pagina 58 pentru mai multe informaţii.

Profilul de utilizator este un instrument puternic şi flexibil. Controlează ce poate face utilizatorul şi particularizează modul în care sistemul apare utilizatorului. Cartea *Referinţă securitate iSeries* descrie toţi parametrii din profilul de utilizator.

Profiluri de grup

Un profil de grup este un tip special de profil de utilizator. Puteţi folosi un profil de grup pentru a defini autorizări pentru un grup de utilizatori, decât să daţi autorizări fiecărui utilizator în mod individual. Puteţi de asemenea folosi un profil de grup ca model când creaţi profiluri utilizator individuale folosind funcţia copiere-profil sau dacă folosiţi Navigator iSeries puteţi utiliza meniul politicilor de securitate pentru editarea autorizărilor utilizator.

Capitolul 5 şi capitolul 7 din cartea *Referinţă securitate iSeries* furnizează mai multe informaţii despre planificarea şi folosirea profilurilor de grup.

Securitatea resurselor

Securitatea resurselor din sistem vă permite să definiţi cine poate folosi obiectele şi cum pot fi folosite aceste obiecte. Capacitatea de a accesa un obiect este numită **autorizare**. Atunci când setaţi autorizarea obiect, ar trebui să fiţi atenţi să acordaţi utilizatorilor autorizare îndeajuns pentru a îşi efectua lucrul, fără a le oferi autorizări pentru a răsfoi şi a modifica sistemul. Autorizarea obiect oferă utilizatorului permisiunea pentru un anumit obiect şi poate specifica ce îi este permis utilizatorului să facă cu obiectul. Resursele unui obiect pot fi limitate prin anumite autorizări utilizator detaliate, cum ar fi adăugarea înregistrărilor sau modificarea înregistrărilor. Resursele sistem pot fi folosite pentru a oferi acces utilizatorului spre anumite subseturi de autorizări definite de sistem: *ALL, *CHANGE, *USE şi *EXCLUDE.

Fişierele, programele, bibliotecile şi directoarele sunt cele mai comune obiecte ce necesită protecţie de securitate, dar puteţi specifica autorizări pentru orice obiect individual din sistem.

Capitolul 5, “Protejarea informaţiilor cu autorizare obiect” tratează importanţa stabilirii autorizării obiectelor din sistem. Capitolul 5 al cărţii *Referinţă securitate iSeries* descrie opţiunile pentru stabilirea securităţii resurselor.

Funcţia de limitare a acesului la program

Funcţia de limitare a accesului la program vă permite să furnizaţi securitate pentru program când nu aveţi un obiectiSeries pentru siguranţa programului. Înainte de adăugarea suportului pentru accesul limitat la funcţiile programului în V4R3, puteţi realiza acest lucru creând o listă de autorizări sau un alt obiect şi verificând autorizarea pentru obiect pentru a controla accesul la funcţiile programului. Acum puteţi utiliza limitarea accesului la funcţiile program pentru a controla mai uşor accesul la o aplicaţie, la părţi dintr-o aplicaţie sau la funcţii dintr-un program.

Sunt două metode pe care le puteţi folosi pentru a gestiona accesul utilizatorului la funcţiile aplicaţiei prin Navigator iSeries. Prima foloseşte suportul pentru Administrare aplicaţii:

1. Faceţi clic dreapta pe sistemul care conţine funcţia ale cărei setări de acces doriţi să le modificaţi.
2. Selectaţi **Administrare aplicaţii**.
3. Dacă sunteţi într-un sistem de administrare, selectaţi**Setări locale**. Altfel, continuaţi cu pasul următor.
4. Selectaţi o funcţie de administrare.
5. Selectaţi **Acces implicit**, dacă se poate aplica. Prin selectarea acesteia, permiteţi tuturor utilizatorilor să acceseze funcţia în mod implicit.
6. Selectaţi **Acces la toate obiectele**, dacă este aplicabilă. Prin selectarea acesteia, permiteţi tuturor utilizatorilor cu privilegii la toate obiectele sistem să acceseze această funcţie.
7. Selectaţi **Personalizare**, dacă se poate aplica. Folosiţi butoanele **Adăugare** şi **Înlăturare** din dialogul **Personalizare acces** pentru a adăuga sau înlătura utilizatori sau grupuri din listele **Acces permis** şi **Acces interzis**.
8. Selectaţi **Înlăturare personalizare**, dacă este aplicabilă. Prin selectarea acesteia, ştergeţi orice acces personalizat pentru funcţia selectată.
9. Faceţi clic pe **OK** pentru a închide dialogul**Administrare aplicaţii**.

A doua metodă de gestionare a accesului utilizatorilor implică suportul Navigator iSeries pentru Utilizatori şi grupuri:

1. În Navigator iSeries, expandaţi **Utilizatori şi grupuri**.
2. Selectaţi **Toţi utilizatorii**, **Grupuri**, sau **Utilizatori care nu sunt într-un grup** pentru a afişa o listă a utilizatorilor şi a grupurilor.
3. Faceţi clic dreapta pe un utilizator sau grup şi selectaţi**Proprietăţi**.
4. Faceţi clic pe **Posibilităţi**.
5. Faceţi clic pe fişa **Aplicaţii**.
6. Folosiţi această pagină pentru a modifica setarea accesului pentru un utilizator sau grup.
7. Faceţi clic pe **OK** de două ori pentru a închide dialogul **Proprietăţi**.

Consultaţi “Securitate Navigator iSeries” la pagina 144 pentru mai multe informaţii despre problemele de securitate Navigator iSeries.

Dacă sunteţi dezvoltator de aplicaţii, puteţi utiliza API-urile de limitare acces la funcţii program pentru a realiza următoarele:

- Înregistrarea unei funcţii
- Recuperarea informaţiilor despre funcţie
- Definirea celor care pot şi a celor care nu pot să folosească funcţia
- Verifică dacă utilizatorului îi este permis să folosească funcţia

Notă: Acest suport **nu** este un înlocuitor pentru securitatea resurselor. Funcţia de limitare a accesului la program nu împiedică utilizatorii să acceseze o resursă (cum ar fi un fişier sau program) dintr-o altă interfaţă.

Pentru a folosi acest suport într-o aplicaţie, furnizorul aplicaţiei trebuie să înregistreze funcţiile când este instalată aplicaţia. Funcţia înregistrată corespunde unui bloc de cod pentru anumite funcţii din aplicaţie. Când aplicaţia este rulată de către utilizator, aplicaţia apelează API înainte să invoce blocul de cod. API apelează verificarea folosirii API pentru a vedea dacă utilizatorului îi este permis să folosească funcţia. Dacă utilizatorul are permisiunea de a folosi funcţia înregistrată, blocul de cod este rulat. Dacă utilizatorul nu are permisiunea de a folosi funcţia, utilizatorul este împiedicat să ruleze codul.

Notă: API-urile implică înregistrarea unui ID funcţie de 30 de caractere în baza de date de înregistrări (WRKREGINF). Deşi nu există puncte de ieşire referitoare la ID-urile funcţilor utilizate de limitarea accesului la funcţiile API, este necesar să existe puncte de ieşire. Pentru a înregistra ceva în registry, **trebuie** să furnizaţi un nume în format punct de ieşire. Pentru a face aceasta API-ul de înregistrare funcţii creează un nume de format machetă şi foloseşte acest nume de format machetă pentru toate funcţiile care sunt înregistrate. Deoarece acesta este un nume format dummy, nu este apelat niciodată vreun program punct de ieşire.

Administratorul de sistem specifică cui i se permite şi cui i se interzice accesul la o funcţie. Administratorul poate fie să folosească API-ul pentru a gestiona accesul la funcţia program fie să folosească interfaţa cu utilizatorul de administrare aplicaţii din Navigator iSeries. Cartea *iSeries server API Reference* furnizează informaţii despre API-urile care îndeplinesc funcţia de limitare a accesului la program. Pentru informaţii suplimentare despre controlul accesului la funcţii, consultaţi “Securitate Navigator iSeries” la pagina 144

Auditare de securitate

Verificarea securităţii sistemului se efectuează din mai multe motive:

- Pentru a evalua dacă planul de securitate este complet.
- Pentru a se asigura dacă, controalele de securitate planificată funcţionează . Acesta tip de verificare este utilizat frecvent de ofiţerul de securitate ca parte a procesului de

administrare zilnică a securităţii. De asemenea, este efectuat, câteodată, mai detaliat, ca parte a procesului de trecere în vedere periodică a securităţii de către revizorii interni sau externi.

- Pentru a se asigura faptul că securitatea sistemului nu este influenţată de modificările din mediul sistem. Câteva exemple de modificări care afectează securitatea :
  - Obiecte nou create de către utilizatorii sistemului
  - Utilizatori noi admişi în sistem
  - Modificarea proprietăţii obiectelor (autorizare neajustată)
  - Modificarea responsabilităţilor (grup de utilizatori modificat)
  - Autoritate temporară (fără oportunitate de revocare)
  - Noi produse instalate
- Pentru pregătirea unui viitor eveniment, ca de exemplu instalarea unei noi aplicaţii, mutarea la un nivel mai mare de securitate, sau setarea unei reţele de comunicaţii.

Tehnicile descrise aici sunt potrivite pentru toate aceste situaţii. Componenta verificată şi cât de des depinde de mărimea şi nevoile de securitate ale sistemului.

Auditarea securităţii implică folosirea comenzilor pe sistemul dumneavoastră şi accesarea informaţiilor de jurnal şi înregistrare. Puteţi crea un profi utilizator special pentru a fi folosit de către cineva care face o auditare de securitate a sistemului dumneavoastră. Profilul auditorului are nevoie de autorizarea specială *AUDIT pentru a modifica caracteristicile de auditare ale sistemului. Anumite sarcini de verificare amintite în acest capitol necesită un profil de utilizator cu autorizare specială *ALLOBJ şi *SECADM. Setaţi parola pentru profilul auditorului la *NONE când perioada de auditare s-a terminat.

Pentru mai multe detalii privind auditarea securităţii, vezi Capitolul 9, al cărţii *Referinţe de securitate*.

Exemplu: Raportarea atributelor de securitate a sistemului

Figura 1 evidenţiază un exemplu de ieşire din comanda Tipărire atribute de securitate sistem (PRTSYSSECA). Raportul evidenţiază setările pentru valorile relevante ale sistemului de securitate şi atributele de reţea recomandate pentru sisteme cu cereri de securitate obişnuite. Evidenţiază, de asemenea, setările curente din sistem.

Notă: Coloana*Valori curente* din raport evidenţiază setările curente din sistem. Pentru detectarea expunerilor de securitate comparaţi aceste valori cu cele recomandate.

```
Atribute de securitate a sistemului

Valoare sistem
Nume             Valoare curentă        Valoare recomandată
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
```

Figura 1. Prezentarea atributelor de securitate a sistemului - Exemplu (Partea 1 din 4)

```
QAUTOCFG         0                    0
QAUTORMT         1                    0
QAUTOVRT         9999                 0
QCMNRCYLMT       0 0                  0 0
QCRTAUT          *CHANGE              Control la nivel bibliotecă.
QCRTOBJAUD       *NONE                Control la nivel bibliotecă.
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
```

Figura 1. Prezentarea atributelor de securitate a sistemului - Exemplu (Partea 2 din 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
```

Figura 1. Prezentarea atributelor de securitate a sistemului - Exemplu (Partea 3 din 4)

```
Atribute de securitate a sistemului

Atribute reţea
Nume             Valoare curentă      Valoare recomandată
DDMACC           *OBJAUT              *REJECT
JOBACN           *FILE                *REJECT
PCSACC           *OBJAUT              *REJECT
```

Figura 1. Prezentarea atributelor de securitate a sistemului - Exemplu (Partea 4 din 4)

Capitolul 2. Vrăjitor securitate iSeries şi eServer Security Planner

Uneltele Vrăjitor de securitate pentru serverul iSeries şi eServer Security Planner vă pot ajuta să decideţi ce valori de securitate să devină efective pe serverul iSeries. Folosind Vrăjitorul de securitate server iSeries în Navigator iSeries veţi produce rapoarte care reflectă necesităţile de securitate, bazate pe răspunsurile selectate. Puteţi apoi utiliza aceasta pentru a configura securitatea sistemului dumneavoastră.

Folosiţi vrăjitorul de securitate iSeries sau eServer Security Planner pentru a vă ajuta în planificarea unei politici de bază pentru securitate şi la implementarea ei la serverele iSeries. Scopul ambelor unelte este să vă uşureze implementarea şi gestionarea securităţii pe sistemele dumneavoastră. Vrăjitorul, care este disponibil ca parte dinOS/400, vă pune mai multe întrebări de nivel înalt despre mediul serverului dumneavoastră şi pe baza răspunsurilor dumneavoastră, vă furnizează un set de recomandări pe care vrăjitorul le poate aplica sistemului dumneavoastră în continuare.

eServer Security Planner este versiunea on-line a Vrăjitorului de securitate. Vă permite să selectaţi alegerile dumneavoastră bazat pe nevoile dumneavoastră de securitate şi apoi vă livrează un raport care vă sugerează ce caracteristici sunt necesare pentru a vă securiza locaţia.

eServer Security Planner este o versiune a vrăjitorului bazată pe Internet. Acesta furnizează recomandări pentru implementarea securităţii pe sistemul dumneavoastră, în acelaşi mod ca şi vrăjitorul. Dar, consilierul nu poate aplica recomandările. Mai degrabă, acesta afişează o listă de valori de securitate sistem şi alte atribute pe care ar trebui să le aplicaţi pe serverul dumneavoastră, pe baza răspunsurilor dumneavoastră la întrebările consilierului.

Vrăjitor de securitate

Deciderea valorilor de securitate pentru sistemul iSeries care trebuiesc folosite pentru afacerea dumneavoastră poate fi complicată. Dacă sunteţi la începutul implementărilor de securitate pe serverele iSeries, sau mediul în care rulaţi serverul dumneavoastră iSeries a fost modificat recent, Vrăjitorul de securitate vă poate ajuta cu decizii.

Ce este un vrăjitor?

- Un vrăjitor este o unealtă proiectată pentru a fi rulată de către un utilizator începător pentru a instala sau a configura ceva într-un sistem.
- Vrăjitorul cere utilizatorului informaţii punând întrebări. Răspunsul la fiecare întrebare decide întrebarea care este pusă în continuare.
- După ce assitentul termină interogarea, utilizatorul este prezentat cu o căsuţă de dialog de încheiere. Utilizatorul va selecta apoi butonul **Încheiere** pentru instalarea şi configurarea articolului .

Scopurile Vrăjitorului de securitate

Scopul Vrăjitorului de securitate este să configureze, pe baza răspunsurilor utilizatorului următoarele.

- Valori de sistem legate de securitate şi atribute de reţea.
- Rapoarte de securitate pentru monitorizarea sistemului.
- Pentru a genera un Raport de informaţii de administrare şi un Raport de informaţii utilizator:

  - Raportul informaţii administrator conţine setările de securitate recomandate şi orice procedură ce ar trebui să fie realizată înainte de implementarea recomandărilor.
  - Raportul informaţii utilizator conţine informaţii care pot fi folosite pentru politica de securitate a afacerii. De exemplu, sunt incluse în acest raport regulile de compunere a parolei.
- Pentru furnizarea setărilor recomandate pentru diferite elemente de securitate din sistem.

Obiectivele Vrăjitorului de securitate

- Obiectivele Vrăjitorului de securitate sunt:
  - Pentru determinarea setărilor de securitate necesare sistemului, bazată pe răspunsurile utilizatorului la întrebările vrăjitorului şi implementarea acestor setări la momentul oportun.
  - Vrăjitorul produce rapoarte cu informaţii detaliate incluzând următoarele.
    - Raport care explică recomandările Vrăjitorului.
    - Raport care detaliază procedurile care trebuie urmate înaintea implementării.
    - Raport care listează informaţii relevante pentru a fi distribuite utilizatorilor din sistem.
- Aceste elemente implementează politica de securitate de bază în sistemul dumneavoastră
- Vrăjitorul recomandă rapoarte jurnal auditare pe care ar trebui să le planificaţi să fie rulate periodic. Atunci când sunt planificate, aceste rapoarte ajută la următoarele:
  - Asigurarea urmării politicilor de securitate.
  - Asigurarea faptului că politicile de securitate se modifică numai cu permisiunea dumneavoastră
  - Planificarea rapoartelor care să monitorizeze evenimentele legate de securitate din sistem
- Vrăjitorul vă permite să salvaţi recomandările sau să aplicaţi unele sau toate recomandările pentru sistemul dumneavoastră.

Notă: Vrăjitorul de securitate poate fi utilizat mai mult decât o dată pe acelaşi sistem pentru a permite utilizatorilor care pot avea o instalare mai veche să îşi reexamineze securitatea lor curentă. Vrăjitorul de securitate poate fi folosit începând de cu sistemele V3R7 (când a fost introdus Navigator iSeries).

Pentru a folosi Navigator iSeries, trebuie să aveţi produsul IBM iSeries Access pentru Windows instalat pe PC-ul dumneavoastră Windows 95/NT şi să aveţi o conexiune la serverul iSeries de la acest PC. Utilizatorul Vrăjitorului trebuie să fie conectat la un server iSeries. Utilizatorul trebuie să aibe un ID utilizator care are autorizări speciale *ALLOBJ, *SECADM, *AUDIT şi *IOSYSCFG. Pentru ajutor în conectarea PC-ului dumneavoastră Windows 95/NT la sistemul iSeries, consultaţi subiectul IBM iSeries Access pentru Windows din Centru informaţii (urmăriţi“Condiţii prealabile şi informaţii conexe” la pagina xii pentru detalii).

Pentru a accesa Vrăjitorul de securitate, efectuaţi următoarele:

1. În Navigator iSeries, expandaţi serverul dumneavoastră.
2. Faceţi clic dreapta pe **Securitate** şi selectaţi **Configurare**.
   - Când un utilizator porneşte opţiunea **Securitate** din Navigator iSeries este trimisă o cerere la serverul iSeries pentru a verifica autorizarea specială a utilizatorului.
   - În cazul în care utilizatorul nu dispune de toate autorizările speciale solicitate (*ALLOBJ, *AUDIT, *IOSYSCFG, *SECADM) aceştia nu vor putea vizualiza opţiunea **Configurare** şi nu vor putea accesa Vrăjitorul de securitate.
3. Se presupune că utilizatorul dispune de autorizarea solicitată:
   - Răspunsuri ale vrăjitorului anterioare sunt recuperate.
   - Setările de securitate curente sunt recuperate.

Vrăjitorul securitate vă va primi cu unul din cele trei ecrane de întâmpinare. Ecranul prezentat depinde de existenţa uneia dintre situaţiile următoare:

- Vrăjitorul nu a fost niciodată rulat pentru serverul destinaţieiSeries.
- Vrăjitorul a mai fost rulat şi modificările de securitate au fost amânate.
- Vrăjitorul a mai fost rulat şi modificările de securitate au fost implementate.

Dacă nu folosiţi Navigator iSeries, puteţi încă să obţineţi ajutor în planificarea nevoilor dumneavoastră de securitate. eServer Security Planner este versiunea on-line a vrăjitorului de securitate, cu o diferenţă. Consilierul nu va configura automat sistemul dumneavoastră. Totuşi, el va genera un raport al opţiunilor de securitate recomandate, pe baza răspunsurilor dumneavoastră. Pentru a accesa eServer Security Planner, mergeţi la Centrul de informare eServer:

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

eServer Security Planner

eServer Security Planner este versiunea on-line a Vrăjitorului de securitate. El pune aceleaşi întrebări ca şi Vrăjitorul de securitate şi, pe baza răspunsurilor dumneavoastră, generează aceleaşi recomandări. Principalele deosebiri dintre cele două instrumente sunt:

- eServer Security Planner **nu**—
  - Produce rapoarte.
  - Compară setările curente cu setările recomandate.
  - Setează automat vreo variabilă de sistem.
- Nu puteţi aplica recomandările din eServer Security Planner.

eServer Security Planner generează un program CL pe care puteţi edita pentru propriul dumneavoastră uz în scopul automatizării configurarea de securitate. Vă puteţi de asemenea lega direct din eServer Security Planner la documentaţia serverului iSeries. Aceasta furnizează informaţii despre valorile de sistem sau rapoartele care vă ajută să determinaţi dacă această configurare este corespunzătoare mediului dumneavoastră.

Pentru a accesa eServer Security Planner, indicaţi browser-ului Internet următorul URL:

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

Capitolul 3. Controlul semnării interactive

Când vă gândiţi să restricţionaţi intrarea în sistemul dumneavoastră, porniţi, bineînţeles, cu ecranul Semnare. În continuare sunt opţiuni pe care le puteţi utiliza pentru a împiedica pe cineva să deschidă o sesiune pe sistemul dumneavoastră folosind ecranul Semnare.

Setare reguli parolă

Pentru securizarea semnării pe sistemul dumneavoastră, faceţi următoarele:
- Setaţi o politică care determină că parolele trebuie să nu fie banale şi partajate.
- Setaţi variabilele de sistem pentru a vă ajuta cu restricţiile. Tabela 1 arată recomandările setărilor variabilelor de sistem.

Combinaţia de valori din Tabela 1 este destul de restrictivă şi presupune reducerea semnificativă a probabilităţii parolelor banale. Totuşi, utilizatorii dumneavoastră pot considera dificilă şi frustrantă găsirea unei parole care să respecte aceste restricţii.

Furnizaţi utilizatorilor următoarele:
1. O listă de criterii pentru parole.
2. Exemple de parole care sunt şi care nu sunt valide.
3. Sugestii despre cum să vă gândiţi la o parolă bună.

Rulaţi comanda CFGSYSSEC (Configure System Security - Configurare securitate sistem) pentru seta aceste valori. Folosiţi comanda PRTSYSSECA (Print System Security Attributes - Imprimare atribute de securitate sistem) pentru a tipări setările curente ale acestor variabile de sistem.

Capitolul 3 al cărţii *Referinţă securitate iSeries*. “Valorile setate de comanda Configurare securitate sistem” la pagina 34 oferă mai multe informaţii desprecomanda CFGSYSSEC.

Tabela 1. Variabile de sistem pentru parole

Nume valoare sistem	Descriere	Valoare recomandată
QPWDEXPITV	Cât de des, de regulă, utilizatorii trebuie să schimbe parolele lor. Puteţi specifica o valoare diferită pentru utilizatori individuali în profilul utilizator.	60 (zile)
QPWDLMTAJC	Dacă sistemul împiedică folosirea a două caractere identice alăturate.	1 (da)
QPWDLMTCHR	Caractere care nu pot fi utilizate în parole.[2]	AEIOU#$@
QPWDLMTREP	Dacă sistemul împiedică folosirea aceluiaşi caracter de mai multe ori într-o parolă.	2 (nu este permis consecutiv)
QPWDLVL	În caz că parolele utilizator sunt limitate la 10, maxim 128 caractere.	0[3]
QPWDMAXLEN	Numărul maxim de caractere dintr-o parolă.	8
QPWDMINLEN	Numărul minim de caractere dintr-o parolă.	6
QPWDPOSDIF	Dacă fiecare caracter dintr-o parolă trebuie să fie diferit de caracterul din aceeaşi poziţie al parolei precedente.	1 (da)
QPWDRQDDGT	Dacă parola trebuie să aibă cel puţin un caracter numeric.	1 (da)
QPWDRQDDIF	Cât de mult poate aştepta utilizatorul până să folosească aceeaşi parolă, din nou. [2]	5 sau mai puţin (intervale de expirare) [1]
QPWDVLDPGM	Ce program de ieşire este apelat pentru a valida o nouă parolă asociată.	*NONE

Tabela 1. Variabile de sistem pentru parole (continuare)

Nume valoare sistem	Descriere	Valoare recomandată

Note:

1. Variabila de sistem QPWDEXPITV specifică cum trebuie să schimbaţi, de regulă, parola dumneavoastră, cum ar fi la fiecare 60 de zile. Acesta este **intervalul de expirare**. Variabila de sistem QPWDRQDDIF specifică câte intervale de expirare trebuie să treacă înainte de a putea folosi aceeaşi parolă din nou. Capitolul 3 al cărţii *Referinţă securitate iSeries* furnizează mai multe informaţii despre cum lucrează aceste variabile de sistem împreună.
2. QPWDLMTCHR nu este impusă la nivelurile 2 şi 3 de parolare. Vezi “Nivele de parole” pentru detalii.
3. Vedeţi “Planificarea modificărilor nivelului de parole” pentru a determina nivelul de parolare necesar.

Nivele de parole

Începând cu V5E1 a sistemului de operare, valoarea sistem QPWDLVL oferă o securitate a parolelor mai mare. În celelalte ediţii, utilizatorii erau limitaţi la utilizarea de parole de maxim 10 caractere, dintr-un număr limitat de caractere. Acum, utilizatorii pot selecta o parolă (o frază) de maxim 128 caractere, depinzând de nivelul de parolare la care este configurat sistemul. Nivelele de parole sunt:

- **Nivelul 0:** Sistemele sunt livrate la acest nivel. La nivelul 0, parolele sunt de maxim 10 caractere, conţinând numai A-Z, 0–9, #, @, $ şi caracterul _ . Parola de nivel 0 este mai puţin sigură decât cele de nivel superior.
- **Nivelul 1:** Aceleaşi reguli ca la nivelul 0 de parole, dar parolele pentru suportul iSeries pentru Windows Network Neighborhood (referit mai târziu ca NetServer iSeries) nu sunt salvate.
- **Nivelul 2:** Parolele sunt sigure la acest nivel. Acest nivel poate fi folosit în scopul testării. Parolele sunt salvate pentru utilizatori pe nivelul 0 sau 1 dacă au o lungime de 10 caractere sau mai mică şi folosesc setul de caractere pentru nivelul de parole 0 sau 1. Parolele (sau expresiile de trecere) de la acest nivel au următoarele caracteristici:
  - maxim 128 caractere.
  - oric fel de caracter.
  - nu pot fi formate numai din blancuri; blancurile de la sfârşit sunt înlăturate.
  - ţin cont de tipul caracterului (mare sau mic).
- **Nivelul 3:** Parolele de la acest nivel sunt cele mai sigure şi folosesc cei mai avansaţi algoritmi de criptare disponibili. Parolele de la acest nivel au aceleaşi caracteristici ca cele de la nivelul 2. Parolele pentru NetServer iSeries nu sunt salvate la acest nivel.

Ar trebui să folosiţi numai nivelurile de parole 2 şi 3 dacă fiecare sistem din reţeaua dumneavoastră îndeplineşte aceste criterii:

- Sistemul de operare este V5E1 sau mai vechi
- Nivelul de parole este setat la 2 sau 3

La fel, utilizatorii trebuie să intre în sesiune, folosind acelaşi nivel de parolare. Nivelele de parole sunt globale; utilizatorii nu pot alege nivelul la care doresc ca parolele lor să fie securizate.

Planificarea modificărilor nivelului de parole

Schimbarea nivelurilor de parolare trebuie planificată cu grijă. Operaţiunile cu alte sisteme pot eşua sau utilizatorii nu vor putea accesa sistemul, dacă programarea schimbului de parole nu s-a făcut cum trebuie. Înainte de a schimba valoarea de sistem QPWDLVL asiguraţi-vă că aţi salvat datele de securitate, folosind comenzile SAVSECDTA or SAVSYS. Dacă doriţi să

vă reântoarceţi la un nivel inferior de parolare, puteţi şterge parolele din profilul tuturor utilizatorilor, asigurându-vă mai întâi cu un backup nou.

Produsele pe care le folosiţi în sistem şi pe clienţii cu care sistemul interfaţează, pot avea probleme când valoara sistem (QPWDLVL) a nivelului de parole este setată la 2 sau 3. Orice produs sau client care trimite parole sistemului într-o formă criptată, mai degrabă decât în text clar pe care utilizatorul îl introduce într-un ecran de semnare, trebuie actualizat astfel încât să lucreze cu noile reguli de criptare a parolelor pentru QPWDLVL 2 sau 3. Trimiterea parolei criptate este cunoscută ca **substituirea parolei**.

Substituirea parolei este folosită pentru a preveni capturarea parolei la transmitera printr-o reţea. Parolele substituite generate de clienţi mai vechi care nu suportă noul algoritm pentru QPWDLVL 2 sau 3, chiar dacă secvenţa de caractere este corectă, nu vor fi acceptate. Aceasta se aplică de asemenea la orice acces pereche iSeries la iSeries care utilizează valorile criptate pentru autentificare de pe un sistem pe altul.

Problema este compusă din faptul că unele produse afectate (cum ar fi Setul de unelteJava) sunt furnizate cu grad mediu de siguranţă. Un produs de la un terţ, care încorporează o versiune anterioară a acestor produse, nu va lucra corect, până nu se va trece pe versiunea nouă de middleware.

Luând în considerare aceasta şi altele, este uşor a vedea necesitatea planificării cu grijă, înainte de a schimba valoarea de sistem QPWDLVL.

Consideraţii asupra schimbării QPWDLVL de la 0 la 1

Nivelul 1 de parole permite unui sistem, care nu are nevoie să comunice cu Suportul clientWindows 95/98/ME AS/400pentru produsulWindows Network Neighborhood (NetServer iSeries), să aibă parolele NetServer iSeries eliminate din sistem. Eliminarea parolelor encriptate, fără a fi necesar, măreşte securitatea sistemului.

La QPWDLVL 1, toate mecanismele de autentificare, toate substituirile de parole, curente şi pre-V5R1, vor continua să lucreze. Pierderile sunt foarte puţin probabile cu excepţia funcţiilor şi serviciilor care necesită parola NetServer iSeries.

Consideraţii asupra schimbării QPWDLVL de la 0 la 2

Nivelul 2 de parolare introduce luarea în considerare a dimensiunii caracterului (mare sau mic), lungimea de până la 128 caractere şi oferă abilitatea maximă de revenire la QPWDLVL 0 sau 1.

Indiferent de nivelul de parolare al sistemului, nivelurile 2 şi 3, sunt create oridecâte ori se schimbă o parolă sau un user se conectează la sistem. Având parole de nivel 2 şi 3 în timp ce sistemul este încă la nivelul 0 sau 1, ajută la trecerea pe nivel 2 sau 3.

Înainte de a modifica QPWDLVL la 2, ar trebui să folosiţi comenzileDSPAUTUSR sau PRTUSRPRF TYPE(*PWDINFO) pentru a localiza toate profilurile utilizator care nu au o parolă care poate fi folosită la nivelul de parole 2. În funcţie de ce profiluri utilizator localizează aceste comenzi, veţi dori probabil să folosiţi unul din următoarele mecanisme pentru a avea un nivel de parole 2 sau 3 adăugat la profiluri.

- Schimbă parola din profilul utilizator, folosind comanda CHGUSRPRF sau CHGPWD CL sau QSYCHGPW API. Aceasta va conduce la schimbarea nivelului parolei la nivelul 0 şi 1; sistemul va crea, de asemenea, două parole sensibile la caracter (mare şi mic), care sunt utilizabile pentru nivelurile 2 şi 3. Toate variantele de caractere mari şi mici sunt utilizate pentru folosirea parolei pe nivel 2 sau 3.

  De exemplu, schimbând parola în C4D2RB4Y sistemul va genera C4D2RB4Y şi c4d2rb4y - parole de nivel 2.

- Conectarea la sistem prin mecanismul prezentării parolei în clar (când nu se utilizează substituirea parolei). Dacă parola e validă şi profilul de user nu are o parolă utilizabilă pe nivelul 2 şi 3, sistemul creează două parole sensibile la tipul caracterului (mare sau mic), care sunt utilizabile pentru nivelurile 2 şi 3. Se creează două parole - una cu caractere mari şi alta cu toate caracterele, mici, pentru a fi utilizate ca parole de nivel 2 sau 3.

Absenţa unei parole utilizabilă în nivelul 2 sau 3, poate fi o problemă ori de câte ori profilul utilizatorului nu are o parolă utilizabilă în nivelul 0 şi 1 sau când utilizatorul încearcă să se conecteze cu un produs prin substituţia de parolă. În aceste cazuri, utilizatorul nu va putea să se conecteze, când nivelul de parolare se schimbă pe 2.

Dacă un profil utilizator nu are o parolă utilizabilă pe nivelurile 2 şi 3, profilul utilizatorului are o parolă utilizabilă pe nivelurile 0 şi 1 şi utilizatorul se conectează printr-un produs care trimite parola în clar, atunci sistemul validează utilizatorul conform nivelului 0 şi creează două parole de nivel 2 (ca mai sus), pentru profilul acestui utilizator. Următoarele conectări se vor face pe parolă de nivel 2.

Orice client / serviciu care foloseste substituţia de parolă, nu va lucra corect pe QPWDLVL 2 dacă nu a fost adus la schema de substituire a parolei. Administratorul va verifica dacă clientul / serviciul care nu a fost adus la zi cu substituţia de parolă , este cerut.

Clienţii / serviciile care utilizează substituţia de parolă, includ:

- TELNET
- iSeries Access
- iSeries Host Servers
- QFileSrv.400
- Suportul de imprimare NetServer iSeries
- DDM
- DRDA
- SNA LU6.2

Este strict recomandat ca datele de securitate să fie salvate înainte de a face schimbarea la QPWDLVL 2. Aceasta poate folosi la revenirea la QPWDLVL 0 sau 1, mai uşor, dacă va fi necesar.

Se recomandă ca celelalte valori ale sistemului de parolare, ca QPWDMINLEN şi QPWDMAXLEN să nu fie schimbate decât după câteva teste la QPWDLVL 2. Aceasta va permite o revenire mai uşoară la QPWDLVL 1 sau 0, dacă e necesar. Totuşi, sistemul de valori QPWDVLDPGM trebuie să specifice *REGFAC sau *NONE înainte ca sistemul să permită schimbarea lui QPWDLVL în 2. De aceea, dacă utilizaţi programul de validare a parolei, veţi putea dori scrierea unuia nou care să fie înregistrat pentru QIBM_QSY_VLD_PASSWRD exit point, folosind comanda ADDEXITPGM.

Parolele NetServer iSeries mai sunt suportate la QPWDLVL 2, aşa că orice funcţie/serviciu care necesită o parolă NetServer iSeries va funcţiona în continuare.

Odată ce administratorul s-a obişnuit să folosească sistemul la QPWDLVL 2, el poate începe schimbarea valorilor sistem pentru exploatarea parolelor mai lungi. Totuşi, administratorul trebuie să ţină cont că parolele mai lungi pot avea următoarele efecte:

- Dacă parolele sunt mai lungi de 10 caractere, nivelurile 0 şi 1 de parolare sunt şterse. Acest profil utilizator nu va putea să se conecteze dacă sistemul se reîntoarce la nivelul de parolare 0 sau 1.

- Dacă parolele conţin caractere speciale sau nu urmează reguluile de compunere pentru numele obiectelor simple (excluzând dependenţa de dimensiunea caracterului), cuvântul de paro lă, de nivel 0 şi 1 e şters.
- Dacă sunt specificate parole mai lungi de 14 caractere, parola NetServer iSeries pentru profilul utilizator este ştearsă.
- Valorile sistem pentru parole se aplică numai la valoarea 2 a noului nivel de parole şi nu se aplică la nivelurile de parole 0 şi 1 generate de sistem sau valorile de parole NetServer iSeries (dacă sunt generate).

Consideraţii asupra schimbării QPWDLVL de la 2 la 3

După ce s-a folosit sistemul cu QPWDLVL 2, pentru mai mult timp, administratorul poate tr ece la QPWDLVL 3, pentru a maximiza sistemul de securitate prin parole.

La QPWDLVL 3, toate parolele NetServer iSeries sunt şterse astfel încât un sistem să nu trebuiască trecut la QPWDLVL 3 până când nu este nevoie să fie utilizate parolele NetServer iSeries.

La QPWDLVL 3, toate parolele de nivel 0 şi 1 sunt şterse. Administratorul poate utiliza comenzile DSPAUTUSR sau PRTUSRPRF pentru a localiza profilul de utilizator care nu au parole de nivel 2 sau 3 asociate.

Modificarea la un nivel de parole mai scăzut

Revenirea la o valoare inferioară pentru QPWDLVL, cu toate că e posibilă, nu este o treabă uşoară. În general, această operaţie trebuie văzută într-un singur sens - de la un QPWDLVL mai mic la lo valoare mai mare pentru QPWDLVL. Totuşi, pot exista cazuri când se cere revenirea la un QPWDLVL mai mic.

În continuare se va prezenta trecerea la un nivel inferior dwe parolare.

Consideraţii asupra trecerii QPWDLVL de la 3 la 2: Această schimbare e relativ uşoară. O dată ce QPWDLVL este setat la 2, administratorul trebuie să determine daca vreun profil utilizator trebuie să conţină parole NetServer iSeries sau parole din nivelurile de parole 0 sau 1 şi, dacă este aşa, să modifice parola profilului utilizator la o valoare permisă.

Suplimentar, valorile sistem ale parolelor ar putea necesită să fie modificate înapoi la valori compatibile cu NetServer iSeries şi parole din nivelurile de parole 0 sau 1, dacă aceste parole sunt necesare.

Consideraţii asupra trecerii QPWDLVL de la 3 la 1: Deoarece există un potenţial crescut de a fi provocate probleme sistemului (nici un utilizator nu se poate conecta, deoarece toate parolele de nivel 0 şi 1 au fost şterse), această schimbare nu se face direct. Pentru a trece de la QPWDLVL 3 la 1 sau 0, sistemul trebuie să trecă mai întâi prin QPWDLVL 2.

Consideraţii asupra trecerii QPWDLVL de la 2 la 1: Înainte de a schimba QPWDLVL în 1, administratorul trebuie să utilizeze comanda DSPAUTUSR sau PRTUSRPRF TYPE(*PWDINFO), pentru a localiza profilurile de utilizator care nu au nive l de parolare 0 sau 1. Dacă profilul utilizator va cere o parolă după ce QPWDLVL e schimbat, administratorul trebuie să asigure un nivel 0 şi 1 pentru acest profil, utilizând unul din următoarele mecanisme:

- Schimbă parola din profilul utilizator, folosind comanda CHGUSRPRF sau CHGPWD CL sau QSYCHGPW API. Aceasta va conduce la schimbarea nivelului parolei la nivelul 2 şi 3; sistemul va crea, o parolă caractere mari, care este utilizabilă pentru nivelurile 0 şi 1. Siste mul poate crea niveluri de parolare 0 şi 1 dacă sunt îndeplinite următoarele condiţii:
  - Parola este de 10 caractere sau mai puţin.
  - Parola poate fi convertită în caractere mari EBCDIC: A-Z, 0-9, @, #, $ şi underscore.

– Parola nu începe cu un număr sau caracterul underscore.

De exemplu, schimbând parola în RainyDay sistemul va genera parole de nivel 0 şi 1 RAINYDAY. Dar, schimbând parola în Rainy Days In April va face ca sistemul să şteargă parola de nivel 0 şi 1 (pentru că parola e prea lungă şi conţine blancuri).

Nu apare nici un mesaj care să arate că nu pot fi create parole de nivel 0 sau 1.

- Conectarea la sistem prin mecanismul prezentării parolei în clar (când nu se utilizează substituirea parolei). Dacă parola e validă şi profilul de user nu are o parolă utilizabilă pe nivelul 0 şi 1, sistemul creează o parolă sensibile la caracter mare, care este utilizabilă pentru nivelurile 0 şi 1. Sistemul poate crea parolă de nivel 0 şi 1, dacă sunt îndeplinite condiţiile de mai jos:

Administratorul poate apoi modifica QPWDLVL la 1. Toate parolele NetServer iSeries sunt şterse când modificarea la QPWDLVL 1 are loc (următorul IPL).

Consideraţii asupra trecerii QPWDLVL de la 2 la 0: Specificaţiile sunt aceleaşi ca şi în cazul modificării QPWDLVL de la 2 la 1 cu excepţia că toate parolele NetServer iSeries sunt reţinute când se produce modificarea.

Consideraţii asupra trecerii QPWDLVL de la 1 la 0: După modificarea QPWDLVL la 0, administratorul ar trebui să folosească comenzile DSPAUTUSR sau PRTUSRPRF pentru a localiza orice profil utilizator care nu are o parolă NetServer iSeries. Dacă profilul utilizator necesită o parolă NetServer iSeries, aceasta poate fi creată prin modificarea parolei utilizatorului sau prin semnarea printr-un mecanism care prezintă parola în text clar.

Administratorul poate apoi schimba QPWDLVL în 0.

Modificarea parolelor cunoscute

Faceţi următoarele pentru a închide unele intrări bine cunoscute în serverul iSeries care ar putea exista în sistemul dumneavoastră.

__ Pasul 1. Asiguraţi-vă că nici un profil utilizator nu mai are parole implicite (aceleaşi cu numele profil utilizator). Puteţi folosi comanda Analizare parole implicite (Analyze Default Passwords - ANZDFTPWD). (Vedeţi “Evitarea parolelor implicite” la pagina 23)

__ Pasul 2. Încercaţi să deschideţi o sesiune la sistemul dumneavoastră cu combinaţiile dintre profilurile utilizator şi parolele care se găsesc în Tabela 2 la pagina 19. Aceste parole sunt publicate şi sunt prima alegere pentru oricine încearcă să pătrundă în sistemul dumneavoastră. Dacă puteţi să vă semnaţi, folosiţi comanda Modificare profil utilizator (Change User Profile - CHGUSRPRF) pentru a modifica parola la valoarea recomandată.

__ Pasul 3. Porniţi Uneltele service dedicate (DST) şi încercaţi să vă înregistraţi cu parolele care sunt afişate în Tabela 2 la pagina 19. Faceţi referire la iSeries Centrul de informare—>Securitate—>Unelte de service. Consultaţi“Condiţii prealabile şi informaţii conexe” la pagina xii pentru informaţii despre accesarea Centrului de informareiSeries.

__ Pasul 4. Dacă vă puteţi înregistra la DST cu oricare din aceste parole, ar trebui să modificaţi parolele. Centrul de informare iSeries —>Securitate—>Unelte de service furnizează instrucţiuni detaliate despre cum să modificaţi ID-urile utilizator şi parolele pentru uneltele de service. Consultaţi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru informaţii despre accesarea Centrului de informare iSeries.

__ Pasul 5. În cele din urmă, asiguraţi-vă că nu vă puteţi semna apăsând doar tasta Enter la ecranul de semnare fără introducerea unui ID utilizator şi a unei parole.

Încercaţi mai multe ecrane diferite. Dacă puteţi să semnaţi fără a introduce informaţii la ecranul Semnare, faceţi următoarele:

- Modificaţi nivelul de securitate la 40 sau 50 (variabila de sistem QSECURITY).

  Notă: Aplicaţiile dumneavoastră ar trebui să ruleze diferit când măriţi nivelul de securitate la 40 sau 50.
- Modificaţi toate intrările staţie de lucru pentru subsisteme interactive pentru a indica descrierea de job care specifică USER(*RQD).

Tabela 2. Parole pentru profilurile furnizate deIBM

ID utilizator	Parolă	Valoare recomandată
QSECOFR	QSECOFR[1]	O valoare nebanală cunoscută doar de administratorul de securitate. **Notaţi parola pe care aţi selectat-o şi stocaţi-o într-un loc sigur.**
QSYSOPR	QSYSOPR	*NONE[2]
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2, 3]
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

Note:

1. Sistemul este livrat cu valoarea *Setare parolă să expire* pentru QSECOFR setată la *YES. Prima dată când deschideţi o sesiune pe un sistem nou, trebuie să schimbaţi parola QSECOFR.
2. Sistemul necesită aceste profiluri utilizator pentru funcţiile sistem, dar trebuie să nu permiteţi utilizatorilor să deschidă sesiuni cu aceste profiluri. Pentru noile sisteme instalate cu V3R1 sau versiuni mai noi, această parolă este livrată ca *NONE.

   Când rulaţi comanda CFGSYSSEC, sistemul setează aceste parole la *NONE.
3. Pentru a rulaiSeries Access pentru Windows folosind TCP/IP, profilul utilizator QUSER trebuie activat.

Tabela 3. Parole pentru unelte de service dedicate

Nivel DST	ID utilizator[1]	Parolă	Valoare recomandată
Facilităţi de bază	11111111	11111111	O valoare nebanală cunoscută doar de administratorul de securitate.[2]
Facilităţi complete	22222222	22222222[3]	O valoare nebanală cunoscută doar de administratorul de securitate.[2]
Facilităţi de securitate	QSECOFR	QSECOFR[3]	O valoare nebanală cunoscută doar de administratorul de securitate.[2]
Posibilităţi de Service	QSRV	QSRV[3]	O valoare nebanală cunoscută doar de administratorul de securitate.[2]

Note:

1. Un ID utilizator este necesar numai pentru ediţiilePowerPC AS (RISC) ale sistemului de operare.
2. Dacă reprezentantul dumneavoastră de service hardware trebuie să deschidă o sesiune cu aceste ID utilizator şi parolă, modificaţi parola la o nouă valoare după ce reprezentantul de service hardware o părăseşte.
3. Profilul utilizator al uneltelor de service va expira după prima utilizare.

Notă: Parolele DST pot fi doar schimbate de un dispozitiv de autentificare. Aceasta e valabil pentru toate parolele şi profilurile utilizator care sunt identice. Pentru informaţii suplimentare despre dispozitivele autentificate, consultaţi informaţiile de setare ale Consolei de operaţii din Centrul de informare iSeries.

Setarea valorilor de semnare

Tabela 4 arată mai multe valori pe care le puteţi seta pentru a face mai dificilă semnarea de către o persoană neautorizată la sistemul dumneavoastră. Dacă rulaţi comanda CFGSYSSEC, setaţi aceste variabile de sistem la valorile recomandate. Puteţi citi mai multe despre aceste variabile de sistem în capitolul 3 al cărţii *Referinţă securitate iSeries*.

Tabela 4. Valori sistem de semnare

Nume valoare sistem	Descriere	Setare recomandată
QAUTOCFG	Dacă sistemul configurează automat noi dispozitive.	0 (Nu)
QAUTOVRT	Numărul de descrieri de dispozitive virtuale pe care sistemul le va crea automat dacă nu există dispozitive disponibile pentru utilizare.	0
QDEVRCYACN	Ce face sistemul când un dispozitiv este reconectat după o eroare.[1]	*DSCMSG
QDSCJOBITV	Cât aşteaptă sistemul înainte de a termina un job deconectat.	120
QDSPSGNINF	Dacă sistemul afişează informaţii despre activitatea de semnare anterioară când un utilizator se semnează.	1 (Da)
QINACTITV	Cât aşteaptă sistemul înainte de a acţiona când un job interactiv este inactiv.	60
QINACTMSGQ	Ce face sistemul când atinge intervalul de expirare QINACTITV.	*ENDJOB
QLMTDEVSSN	Dacă sistemul împiedică un utilizator să deschidă o sesiune de la mai multe staţii de lucru în acelaşi timp.	1 (Da)
QLMTSECOFR	Dacă utilizatorii cu autorizarea specială *ALLOBJ sau *SERVICE pot deschide sesiuni doar la staţii de lucru specifice.	1 (Da)[2]
QMAXSIGN	Maxim consecutiv, încercări semnare incorectă (profilul utilizator sau parola este incorectă).	3
QMAXSGNACN	Ce face sistemul când atinge limita QMAXSIGN.	3 (Dezactivează profilul utilizator şi dispozitivul)

Note:

1. Sistemul poate deconecta şi reconecta sesiunile TELNET când descrierea dispozitiv pentru sesiune este asociată explicit.
2. Dacă setaţi variabila de sistem pe 1 (Da), va trebui să autorizaţi explicit utilizatorii cu autorizările speciale *ALLOBJ sau *SERVICE la dispozitive. Cel mai simplu mod de a face aceasta este de a da profilului utilizator QSECOFR autorizarea *CHANGE pentru dispozitivul specific.

Modificarea mesajelor de eroare la semnare

Hacker-ii doresc să ştie când fac progrese în spargerea unui sistem. Când un mesaj de eroare la ecranul Semnare spune Parolă incorectă, hacker-ul poate şti că ID utilizator este corect. Puteţi frustra hacker-ul folosind comanda Modificare descriere mesaje (Change Message Description - CHGMSGD) pentru a schimba textul celor două mesaje de eroare semnare. Tabela 5 arată textul recomandat.

Tabela 5. Mesaje de eroare la semnare

ID mesaj	Text livrat	Text recomandat
CPF1107	CPF1107 – Parolă incorectă pentru profilul utilizator.	Informaţiile semnare incorecte **Notă:** Nu includeţi ID-ul mesajului în textul mesaj.

Tabela 5. Mesaje de eroare la semnare (continuare)

ID mesaj	Text livrat	Text recomandat
CPF1120	CPF1120 – Utilizatorul XXXXX nu există.	Informaţiile semnare incorecte **Notă:** Nu includeţi ID-ul mesajului în textul mesaj.

Planificarea disponibilităţii profilurilor utilizator

Puteţi dori ca unele profiluri utilizator să fie disponibile pentru semnarea în anumite momente ale zilei sau anumite zile ale săptămânii. De exemplu, dacă aveţi un profil utilizator setat pentru un auditor de securitate, puteţi dori să activaţi acel profil utilizator în timpul orelor în care auditorul este programat să lucreze. Puteţi dori, de asemenea, ca profilurile utilizator cu autorizările speciale *ALLOBJ (inclusiv profilul utilizator QSECOFR) să fie dezactivate în timpul orelor libere.

Puteţi utiliza comanda CHGACTSCDE (Change Activation Schedule Entry - Modificare intrare planificare activare) pentru a seta profilurile utilizator să fie disponibile şi nedisponibile automat. Pentru fiecare profil utilizator pe care îl programaţi, creaţi o intrare care defineşte planificarea profilului utilizator.

De exemplu, dacă doriţi ca profilul QSECOFR să fie disponibil doar între 7 dimineaţa şi 10 seara, trebuie să introduceţi următoarele la ecranul CHGACTSCDE:

```
             Modificare intrare planificare activare (CHGACTSCDE)

Introduceţi opţiunea şi apoi apăsaţi Enter.

Profil utilizator. . . . . . . . > QSECOFR       Nume
Oră activare . . . . . . . . . . > '7:00'       Oră, *NONE
Oră dezactivare. . . . . . . . . > '22:00'      Oră, *NONE
Zile . . . . . . . . . . . . . . > *MON         *ALL, *MON, *TUE, *WED...
                                 > *TUE
                                 > *WED
                                 > *THU
               + pentru mai multe valori > *FRI
```

Figura 2. Ecran de planificare a activării profilului – Exemplu

De fapt, aţi putea dori să aveţi disponibil profilul QSECOFR doar pentru un număr limitat de ore pe zi. Puteţi folosi alt profil utilizator cu clasa *SECOFR pentru a realiza cele mai multe funcţii sistem. Astfel, împiedicaţi apariţia problemelor la încercările unui hacking pentru profilurile utilizator cunoscute.

Puteţi folosi comanda Afişare intrări jurnal auditare (DSPAUDJRNE) regulat pentru a tipări intrări CP în jurnal auditare (Change Profile - Modificare profil). Folosiţi aceste intrări pentru a verifica dacă sistemul activează şi dezactivează profilurile utilizator conform cu planul dumneavoastră de programări.

Altă metodă de verificare pentru a vă asigura că profilurile utilizator au fost dezactivate din planul dumneavoastră de programări este de a folosi comanda Tipărire profiluri utilizator (PRTUSRPRF). Când specificaţi *PWDINFO pentru tipul de raport raportul include starea fiecărui profil utilizator selectat. Dacă, de exemplu, activaţi regulat toate profilurile utilizator cu autorizarea specială *ALLOBJ, puteţi programa următoarea comandă să ruleze imediat după dezactivarea profilurilor:

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

Înlăturarea profilurilor utilizator inactive

Sistemul dumneavoastră trebuie să conţină doar profilurile utilizator necesare. Dacă nu mai aveţi nevoie de un profil utilizator deoarece fie utilizatorul a plecat fie a luat alt job în cadrul organizaţiei, înlăturaţi profilul utilizator. Dacă cineva pleacă din organizaţie pentru o perioadă mai mare de timp, dezactivaţi profilul utilizatorului. Un profil utilizator care nu mai este necesar poate furniza intrări neautorizate pe sistemul dumneavoastră.

Dezactivarea automată a profilurilor utilizator

Puteţi utiliza comanda Analiză activitate profil (ANZPRFACT) pentru a dezactiva regulat profilurile utilizator care au fost inactive pentru un număr specific de zile. Când folosiţi comanda ANZPRFACT, specificaţi numărul de zile de inactivitate pe care le caută sistemul. Sistemul caută data ultimei utilizări, data de restaurare şi data de creare pentru profilul utilizator.

Odată ce aţi specificat o valoare pentru comanda ANZPRFACT, sistemul programează un job pentru a rula în fiecare săptămână la 1 a.m. (începând cu prima zi de la specificarea valorii). Jobul analizează toate profilurile şi le dezactivează pe cele inactive. Nu trebuie să folosiţi comanda ANZPRFACT din nou decât dacă doriţi să modificaţi numărul de zile de inactivitate.

Puteţi folosi comanda Modificare listă profiluri active (Change Active Profile List - CHGACTPRFL) pentru a excepta unele profiluri de la procesarea ANZPRFACT. Comanda CHGACTPRFL creează o listă de profiluri utilizator pe care comanda ANZPRFACT nu le va dezactiva, indiferent de cât de mult aceste profiluri au fost inactive.

Când sistemul rulează comanda ANZPRFACT, scrie o intrare CP în jurnalul auditare pentru fiecare profil utilizator care este dezactivat. Puteţi utiliza comanda DSPAUDJRNE pentru a lista profilurile utilizator care sunt recent disponibilizate.

Notă: Sistemul scrie intrări auditare doar dacă valoarea QAUDCTL specifică *AUDLVL şi variabila de sistem QAUDLVL specifică *SECURITY.

Altă metodă de verificare pentru a vă asigura că profilurile utilizator au fost dezactivate din planul dumneavoastră de programări este de a folosi comanda Tipărire profiluri utilizator (PRTUSRPRF). Când specificaţi *PWDINFO pentru tipul de raport, raportul include starea fiecărui profil utilizator specificat.

Înlăturarea automată a profilurilor utilizator

Puteţi utiliza comanda Modificare intrare programare expirare (Change Expiration Schedule Entry - CHGEXPSCDE) pentru a administra înlăturarea sau dezactivarea profilurilor utilizator. Dacă ştiţi că un utilizator pleacă pentru o lungă durată, puteţi programa înlăturarea sau dezactivarea profilurilor utilizator.

Prima dată când utilizaţi comanda CHGEXPSCDE, se creează o intrare planificare joburi ce rulează la 1 minut după miezul nopţii în fiecare zi. Jobul verifică fişierul QASECEXP pentru a determina dacă vreun profil de utilizator este setat să expire în acea zi.

Cu comanda CHGEXPSCDE, dezactivaţi sau ştergeţi un profil de utilizator. Dacă alegeţi să ştergeţi un profil de utilizator, trebuie să specificaţi ce va face sistemul cu obiectele pe care utilizatorul le deţine. Înainte de a planifica un profil de utilizator pentru ştergere, trebuie să cercetaţi obiectele pe care le deţine utilizatorul. De exemplu, dacă utilizatorul deţine programe care adoptă autorizare, doriţi ca aceste programe să adopte proprietatea noului proprietar? Sau noul proprietar are mai multă autorizare decât este necesar (cum ar fi autorizarea specială)?

Probabil, trebuie să creaţi un profil de utilizator nou cu autorizări specifice pentru a deţine programele care au nevoie să adopte autorizare.

Aveţi de asemenea nevoie să verificaţi dacă va apărea vreo problemă în aplicaţie dacă ştergeţi profilul utilizatorului. De exemplu, vreo descriere de job specifică profilul utilizatorului ca utilizator implicit?

Puteţi utiliza comanda Afişare planificare expirare (Display Expiration Schedule - DSPEXPSCD) pentru a afişa lista profilurilor care sunt planificate pentru dezactivare sau înlăturare.

Puteţi folosi comanda Afişare utilizatori autorizaţi (Display Authorized Users - DSPAUTUSR) pentru a lista toate profilurile de utilizatori din sistem. Folosiţi comanda Ştergere profil utilizator (Delete User Profile - DLTUSRPRF) pentru a şterge profilurile ieşite din uz.

Notă de securitate:: Dezactivaţi un profil de utilizator prin configurarea stării pe *DISABLED. Când dezactivaţi un profil de utilizator, îl faceţi indisponibil pentru folosire interactivă. Nu puteţi semna sau modifica jobul cu un profil de utilizator dezactivat. Joburile batch pot rula sub un profil de utilizator dezactivat.

Evitarea parolelor implicite

Când creaţi un profil nou de utilizator, implicit înseamnă să faceţi parola la fel cu numele profilului utilizatorului. Aceasta furnizează o oportunitate pentru cineva să intre în sistem, dacă cineva vă cunoaşte politica de asociere a numelui de profil şi ştie că o nouă persoană a intrat în organizaţia dumneavoastră.

Când creaţi noi profiluri de utilizatori, luaţi în considerare asocierea unei parole unice care nu este banală, în locul parolei implicite. Spuneţi-i noului utilizator parola confidenţial, cum ar fi într-o scrisoare “Bine aţi venit în sistem” care conturează politicile dumneavoastră de securitate. Solicitaţi utilizatorului să schimbe parola prima dată când se semnează prin configurarea profilului utilizatorului pe PWDEXP(*YES).

Puteţi folosi comanda Analiză parole implicite (Analyze Default Passwords - ANZDFTPWD) pentru a verifica toate profilurile de utilizator dacă cumva au parolă implicită. Când tipăriţi raportul, aveţi opţiunea de a specifica dacă sistemul trebuie să întreprindă vreo acţiune (cum ar fi dezactivarea profilului utilizatorului) în cazul în care parola este la fel cu numele profilului. Comanda ANZDFTPWD tipăreşte o listă a profilurilor care sunt găsite şi orice acţiune care se întreprinde.

Notă: Parolele sunt stocate în sistem într-o formă criptată într-un singur sens. Ele nu pot fi decriptate. Sistemul criptează parola specificată şi o compară cu parola stocată ca şi cum ar verifica parola când deschideţi o sesiune în sistem. Dacă auditaţi greşala de autentificare (*AUTFAIL), sistemul va scrie o intrare într-un jurnal de auditare PW pentru fiecare profil de utilizator care nu *are* o parolă iniţială (pentru sistemul care merge V4R1 sau o variantă mai de început). Începând cu V4R2, sistemul nu scrie intrări PW în jurnalul de auditare când rulaţi comanda ANZDFTPWD.

Monitorizarea activităţii parolei şi înregistrării

Dacă sunteţi îngrijorat de încercările neautorizate de intrare în sistem, puteţi folosi comanda PRTUSRPRF pentru a vă ajuta să monitorizaţi activitatea de semnare şi a parolei.

Următoarele sunt câteva sugestii pentru utilizarea acestui raport:

- Determinaţi dacă intervalul de expirare a parolei pentru unele profiluri de utilizator este mai mare decât variabila de sistem şi dacă intervalul de expirare mai lung este justificat. De exemplu, în raport, USERY are un interval de expirare a parolei de 120 de zile.
- Rulaţi raportul periodic pentru a monitoriza încercările eşuate de semnare. Cineva care încearcă să pătrundă în sistem poate fi conştient de faptul că sistemul întreprinde o acţiune după un anumit număr de încercări eşuate. În fiecare noapte, aşa-zisul intrus poate încerca de mai puţine ori decât variabila QMAXSIGN pentru a evita să vă alerteze. Totuşi, dacă rulaţi acest raport în fiecare dimineaţă devreme şi observaţi că anumite profiluri au avut deseori încercări nereuşite de semnare, s-ar putea să suspectaţi că aveţi o problemă.
- Identificaţi profilurile de utilizator care nu au fost folosite de mult timp sau ale căror parole nu au fost schimbate de mult timp.

Memorarea informaţiilor despre parolă

Pentru a suporta unele funcţii de reţea şi cerinţe de comunicaţii, serverele iSeries furnizează o metodă de securitate pentru stocarea parolelor care pot fi decriptate. Sistemul dumneavoastră foloseşte aceste parole, de exemplu, pentru a stabili o conexiune SLIP cu alte sisteme. (“Securitate şi sesiuni dial-out” la pagina 120 descrie această folosire a parolelor stocate.)

Serverele iSeries memorează aceste parole speciale într-o zonă sigură care nu este accesibilă oricăror programe utilizator sau interfeţe. Doar funcţiile sistem autorizate explicit pot seta aceste parole şi recupera.

De exemplu, când folosiţi parole stocate pentru dial-out conexiuni SLIP, setaţi parola cu comanda sistem care creează profilul de configurare (WRKTCPPTP). Trebuie să aveţi *IOSYSCFG pentru a utiliza comanda. Un script conexiune codat special recuperează parola şi o decriptează în timpul procedurii dial-out. Parola decriptată nu este vizibilă de utilizator sau în nici un istoric de joburi.

Ca administrator de securitate, trebuie să decideţi dacă veţi permite parolelor care pot fi decriptate să fie stocate pe sistemul dumneavoastră. Folosiţi variabila sistem Păstrare date securitate server (Retain Server Security Data - QRETSVRSEC) pentru a specifica aceasta. Cea implicită este 0 (Nu). De aceea, sistemul dumneavoastră nu va stoca parolele care pot fi decriptate până când nu setaţi explicit această variabilă de sistem.

Dacă aveţi cerinţe de reţea sau comunicaţii pentru parolele stocate, trebuie să setaţi politicile potrivite şi să înţelegeţi politicile şi practicile partenerilor dumneavoastră de comunicaţii. De exemplu, când folosiţi SLIP pentru a comunica cu alt server iSeries, ambele sisteme ar trebui să seteze profilurile utilizator speciale pentru stabilirea sesiunilor. Profilurile speciale trebuie să aibă autorizări limitate pe sistem. Aceasta limitează impactul asupra sistemului dumneavoastră dacă o parolă stocată este compromisă pe un sistem partener.

Capitolul 4. Configurarea iSeries pentru a folosi Unelte de securitate

Aceste informaţii descriu cum să setaţi sistemul dumneavoastră pentru a folosi unelte de securitate care sunt parte din OS/400. Când instalaţi OS/400, unelte de securitate sunt gata pentru a fi folosite. Subiectele ce urmează oferă sugestii pentru procedurile de operare cu unelte de securitate.

Operare Unelte de securitate în siguranţă

Când instalaţi OS/400, obiectele care sunt asociate cu unelte de securitate sunt securizate. Pentru a folosi unelte de securitate în siguranţă, evitaţi realizarea de modificări de autorizare la vreun obiect de tip unealtă de securitate.

Mai jos sunt setări de securitate şi cerinţe pentru obiectele unealtă de securitate:

- Programele şi comenzile unealtă de securitate sunt în biblioteca de produse QSYS. Comenzile şi programele sunt furnizate cu autorizare publică *EXCLUDE. Multe din comenzile unealtă de securitate creează fişiere în biblioteca QUSRSYS. Când sistemul creează aceste fişiere, autorizarea publică pentru fişiere este *EXCLUDE.

  Fişierele ce conţin informaţii pentru realizarea de rapoarte modificate au nume ce încep cu QSEC. Fişierele ce conţin informaţii pentru administrarea profilurilor utilizator au nume ce încep cu QASEC. Aceste fişiere conţin informaţii confidenţiale despre sistem. De aceea, nu ar trebui să modificaţi autorizarea fişierelor.
- unelte de securitate foloseşte configurarea normală a sistemului pentru direcţionarea ieşirii tipărite. Aceste fişiere conţin informaţii confidenţiale despre sistem. Pentru a direcţiona ieşirea către o coadă de ieşire protejată, faceţi modificările corespunzătoare în profilul utilizatorului sau în descrierea de job pentru utilizatorii care vor rula unelte de securitate.
- Datorită funcţiilor lor de securitate şi deoarece ei accesează multe obiecte din sistem, comenzile unealtă de securitate necesită autorizarea specială *ALLOBJ. Unele din comenzi necesită şi autorizările speciale *SECADM, *AUDIT sau *IOSYSCFG. Pentru a asigura că aceste comenzi sunt rulate cu succes, trebuie să deschideţi o sesiune ca responsabil când folosiţi unelte de securitate. De aceea, nu aveţi nevoie să acordaţi autorizare privată nici unei comenzi unealtă de securitate.

Evitarea conflictelor de fişiere

Multe din comenzile de raportare unealtă de securitate creează un fişier bază de date pe care îl folosiţi ca să tipăriţi versiunea modificată a raportului. “Comenzi şi meniuri pentru comenzile de securitate” la pagina 26 arată numele fişierului pentru fiecare comandă. La un moment dat, puteţi executa doar o comandă dintr-un job. Majoritatea comenzilor au verificări care determină acest lucru. Dacă executaţi o comandă a cărei execuţie nu s-a terminat în alt job, veţi primi un mesaj de eroare.

Multe joburi de tipărire durează mult. Trebuie să fiţi atenţi pentru a evita conflictele între fişiere când lansaţi rapoarte în batch sau le adăugaţi la un planificator de joburi. De exemplu, s-ar putea să doriţi să tipăriţi două versiuni ale raportului PRTUSRPRF cu criterii de selecţie diferite. Dacă lansaţi rapoartele în batch, trebuie să folosiţi o coadă de joburi care rulează numai un job o dată pentru a asigura că joburile cu rapoartele rulează succesiv.

Dacă folosiţi un planificator de joburi, trebuie să planificaţi două joburi suficient de depărtate în timp unul de celălalt astfel încât prima versiune să se termine înainte de a începe al doilea job.

Salvare Unelte de securitate

Salvaţi programele unealtă de securitate ori de câte ori rulaţi comanda Salvare sistem (Save System - SAVSYS) sau o opţiune din meniul Salvare ce rulează comanda SAVSYS.

Fişierele unealtă de securitate sunt în biblioteca QUSRSYS. Ar trebui să salvaţi deja această bibliotecă ca o parte din procedurile normale de operare. Biblioteca QUSRSYS conţine date pentru multe programe licenţiate din sistem. Vezi Centru de informare pentru mai multe detalii privind comenzile şi opţiunile folosite pentru salvarea bibliotecii QUSRSYS.

Comenzi şi meniuri pentru comenzile de securitate

Această secţiune descrie comenzile şi meniurile pentru instrumentele de securitate. Exemple despre cum să folosiţi comenzile sunt incluse în aceste informaţii.

Două meniuri sunt disponibile pentru instrumente de securitate:

- Meniul SECTOOLS (Security Tools - Unelte de securitate) rulează comenzi interactive.
- Meniul SECBATCH (Submit or Schedule Security Reports to Batch - Lansare sau planificare rapoarte de securitate în batch) pentru a rula comenzi de raportare în batch. Meniul SECBATCH are două părţi. Prima parte a meniului foloseşte comanda Lansare job (Submit Job - SBMJOB) pentru a lansa rapoarte pentru prelucrare imediată în batch.

  A doua parte a meniului foloseşte comanda Adăugare intrare planificare job (Add Job Schedule Entry - ADDJOBSCDE). Este folosită pentru a planifica rapoartele de securitate să fie realizate periodic într-o anumită zi şi la o anumită oră.

Opţiunile meniu Unelte de securitate

Tabela 6 descrie aceste opţiuni din meniu şi comenzile asociate:

Tabela 6. Comenzi unelte pentru profilurile utilizator

Opţiunea de meniu[1]	**Nume comandă**	**Descriere**	**Fişier bază de date utilizat**
1	ANZDFTPWD	Folosiţi comanda Analiză parole implicite (Analyze Default Passwords) pentru a raporta şi a realiza acţiunile corespunzătoare profilurilor de utilizator ce au parola egală cu numele profilului utilizatorului.	QASECPWD[2]
2	DSPACTPRFL	Folosiţi comanda Afişare listă profiluri active (Display Active Profile List) pentru a afişa sau tipări lista cu profilurile utilizatorilor exceptaţi de la prelucrarea ANZPRFACT.	QASECIDL[2]
3	CHGACTPRFL	Folosiţi comanda Modificare listă profiluri active (Change Active Profile List) pentru a adăuga sau înlătura profilurile utilizatorilor din lista de exceptări pentru comanda ANZPRFACT. Un profil de utilizator ce este în lista de profiluri active este activ permanent (până când îl înlăturaţi din această listă). Comanda ANZPRFACT nu dezactivează un profil care este în lista profiluri active, indiferent cât de mult a fost inactiv profilul.	QASECIDL[2]

Tabela 6. Comenzi unelte pentru profilurile utilizator (continuare)

Opţiunea de meniu[1]	Nume comandă	Descriere	Fişier bază de date utilizat
4	ANZPRFACT	Folosiţi comanda Analiză activitate profil (Analyze Profile Activity) pentru a dezactiva profilurile de utilizator ce nu au fost folosite de un număr specificat de zile. După ce folosiţi comanda ANZPRFACT pentru a specifica numărul de zile, sistemul rulează jobul de noapte ANZPRFACT. Puteţi utiliza comanda CHGACTPRFL pentru a excepta profilurile de utilizator de la dezactivare.	QASECIDL[2]
5	DSPACTSCD	Folosiţi comanda Afişare planificare activare profil (Display Profile Activation Schedule) pentru a afişa sau tipări informaţii despre planificarea pentru dezactivarea şi activarea profilurilor de utilizator. Creaţi planificarea cu comanda CHGACTSCDE.	QASECACT[2]
6	CHGACTSCDE	Folosiţi comanda Modificare intrare planificare activare (Change Activation Schedule Entry) pentru a face profilul utilizatorului disponibil pentru a se semna în anumite momente ale zilei sau ale săptămânii. Pentru fiecare profil de utilizator pe care l-aţi planificat, sistemul creează intrări în planificarea joburilor pentru momentele de dezactivare şi activare.	QASECACT[2]
7	DSPEXPSCD	Folosiţi comanda Afişare planificare expirare (Display Expiration Schedule) pentru a afişa sau tipări lista profilurilor de utilizator care sunt planificate să fie dezactivate sau să fie înlăturate din sistem în viitor. Folosiţi comanda CHGEXPSCDE pentru a seta un profil de utilizator pentru expirare.	QASECEXP[2]
8	CHGEXPSCDE	Folosiţi comanda Modificare intrare planificare expirare (Change Expiration Schedule Entry) pentru a planifica un profil de utilizator pentru înlăturare. Îl puteţi înlătura temporar (dezactivându-l) sau îl puteţi şterge din sistem. Această comandă foloseşte o intrare în planificatorul de joburi ce rulează în fiecare zi la 00:01 (1 minut după miezul nopţii). Jobul verifică fişierul QASECEXP pentru a determina dacă vreun profil de utilizator este setat să expire în acea zi. Folosiţi comanda DSPEXPSCD pentru a afişa profilurile utilizatorilor care sunt planificate pentru expirare.	QASECEXP[2]
9	PRTPRFINT	Folosiţi comanda Tipărire conţinut profil (Print Profile Internals) pentru a tipări un raport ce conţine informaţii despre numărul de intrări dintr-un profil de utilizator. Numărul de intrări determină dimensiunea profilului utilizatorului.	

Note:

1. Opţiunile sunt din meniul SECTOOLS.
2. Acest fişier este în biblioteca QUSRSYS.

Puteţi derula în jos meniul pentru a vedea opţiuni suplimentare. Tabela 7 descrie opţiunile din meniu şi comenzile asociate pentru auditarea securităţii:

Tabela 7. Comenzi unealtă pentru securitat audit

Opţiunea demeniu[1]	Nume comandă	Descriere	Fişier bază de date utilizat
10	CHGSECAUD	Folosiţi comanda Modificare auditare securitate (Change Security Auditing) pentru a seta auditarea securităţii şi pentru a modifica variabilele de sistem ce controlează auditarea securităţii. Când rulaţi comanda CHGSECAUD, sistemul creează jurnalul auditare de securitate (QAUDJRN) dacă acesta nu există deja. Comanda CHGSECAUD furnizează opţiuni ce simplifică configurarea variabilei de sistem QAUDLVL (nivel audit). Puteţi specifica *ALL pentru a activa toate setările posibile de nivel auditare. Sau puteţi specifica *DFTSET pentru a activa setările cele mai des folosite (*AUTFAIL, *CREATE, *DELETE, *SECURITY şi *SAVRST). **Notă:** Dacă folosiţi instrumente de securitate pentru a seta auditarea, planificaţi gestiunea receptorilor jurnalului de auditare. Altfel s-ar putea să aveţi repede probleme cu utilizarea discului.	
11	DSPSECAUD	Folosiţi comanda Afişare auditare securitate (Display Security Auditing) pentru a afişa informaţii despre jurnalul de auditare al securităţii şi despre variabilele de sistem ce controlează auditarea securităţii.	

Note:

1. Opţiunile sunt din meniul SECTOOLS.

Folosirea meniului Batch securitate

În continuare este prima parte a meniului SECBATCH:

```
SECBATCH         Lansare sau planificare rapoarte de securitate în batch
                                                                  Sistem:
Selectaţi una din următoarele:

  Lansare rapoarte în batch
     1. Adoptare obiecte (Adopting objects)
     2. Intrări jurnal auditare (Audit journal entries)
     3. Autorizări listă autorizare (Authorization list authorities)
     4. Autorizare comandă (Command authority)
     5. Autorizări private comandă (Command private authorities)
     6. Securitate comunicaţii (Communications security)
     7. Autorizare director (Directory authority)
     8. Autorizare privată director (Directory private authority)
     9. Autorizare document (Document authority)
    10. Autorizare privată document (Document private authority)
    11. Autorizare fişier (File authority)
    12. Autorizare privată fişier (File private authority)
    13. Autorizare folder (Folder authority)
```

Când selectaţi o opţiune din acest meniu, vedeţi ecranul SBMJOB (Submit Job - Lansare job). Dacă doriţi să modificaţi opţiunile implicite pentru comandă, puteţi apăsa F4 (Prompt) în linia *Comandă de executat*.

Pentru a vedea Planificare rapoarte batch (Schedule Batch Reports), rulaţi în jos meniul SECBATCH. Folosind opţiunile din această parte a meniului, puteţi, de exemplu, să setaţi sistemul să ruleze periodic versiuni modificate ale rapoartelor. Puteţi rula în jos pentru opţiuni suplimentare. Când selectaţi o opţiune din această parte a meniului, vedeţi ecranul ADDJOBSCDE (Add Job Schedule Entry - Adăugare intrare planificare job).

Puteţi poziţiona cursorul pe linia *Comandă de executat* şi apăsaţi F4 (Prompt) pentru a alege setări diferite pentru raport. Ar trebui să asociaţi un nume de job semnificativ astfel încât să recunoaşteţi intrarea când afişaţi intrările planificare job.

Opţiunile meniu Securitate batch

Tabela 8 descrie opţiunile din meniu şi comenzile asociate pentru rapoartele de securitate.

Când rulaţi rapoarte de securitate, sistemul tipăreşte numai informaţiile ce îndeplinesc atât criteriile de selecţie pe care le-aţi specificat cât şi criteriile de selecţie pentru utilitar. De exemplu, descrierile jobului care specifică numele profilului de utilizator sunt relevante pentru securitate. De aceea, Raportul descriere job (PRTJOBDAUT) tipăreşte descrierile joburilor în biblioteca specificată numai dacă autorizarea publică pentru descrierea de job nu este *EXCLUDE *şi* dacă descrierea de job specifică un nume de profil de utilizator în parametrul USER.

În mod similar, când tipăriţi informaţii despre subsistem (comanda PRTSBSDAUT), sistemul tipăreşte informaţii despre un subsistem numai când descrierea subsistemului are o intrare de comunicaţii care specifică un profil de utilizator.

Dacă un anumit raport tipăreşte mai puţine informaţii decât vă aşteptaţi, consultaţi ajutorul online pentru a găsi criteriile de selecţie pentru raport.

Tabela 8. Comenzi pentru rapoarte de securitate

Opţiunea demeniu[1]	**Nume comandă**	**Descriere**	**Fişier bază de date utilizat**
1, 40	PRTADPOBJ	Folosiţi comanda Tipărire obiecte care adoptă (Print Adopting Objects) pentru a tipări o listă de obiecte ce adoptă autorizarea profilului de utilizator specificat. Puteţi specifica un singur profil, un nume generic de profil (cum ar fi toate profilurile ce încep cu Q) sau toate profilurile de utilizator din sistem. Acest raport are două versiuni. Raportul complet listează toate obiectele adoptate ce corespund criteriilor de selecţie. Raportul modificări listează diferenţele dintre obiectele adoptate care sunt în acel moment în sistem si obiectele adoptate care erau în sistem ultima dată când s-a realizat raportul.	QSECADPOLD[2]
2, 41	DSPAUDJRNE	Folosiţi comanda Afişare intrări jurnal auditare (Display Audit Journal Entries) pentru a afişa sau pentru a tipări informaţii despre intrări în jurnalul auditarea de securitate. Puteţi selecta anumite tipuri de intrări, anumiţi utilizatori şi o perioadă de timp.	QASYxxJ4[3]

Tabela 8. Comenzi pentru rapoarte de securitate (continuare)

Opţiunea demeniu[1]	**Nume comandă**	**Descriere**	**Fişier bază de date utilizat**
3, 42	PRTPVTAUT *AUTL	Când folosiţi comanda Tipărire autorizări private (Print Private Authorities) pentru obiectele *AUTL, recepţionaţi o listă a tuturor listelor de autorizare din sistem. Raportul include utilizatorii ce sunt autorizaţi pentru fiecare listă şi ce autorizare au utilizatorii pentru listă. Folosiţi aceste informaţii pentru a vă ajuta să analizaţi sursele autorizării obiectelor din sistem. Acest raport are trei versiuni. Raportul complet listează toate listele de autorizare din sistem. Raportul modificări listează adăugările şi modificările autorizărilor de la ultima realizare a raportului. Raportul ştergere listează utilizatorii ale căror autorizări la lista de autorizări le-au fost şterse de la ultima rulare a raportului. Când tipăriţi un raport complet, aveţi opţiunea de a tipări o listă a obiectelor pe care fiecare listă de autorizare le protejează. Sistemul va crea un raport separat pentru fiecare listă de autorizare.	QSECATLOLD[2]
6, 45	PRTCMNSEC	Folosiţi comanda Tipărire securitate comunicaţii (Print Communications Security) pentru a tipări setările relevante de securitate pentru obiectele ce afectează comunicaţiile sistemului. Aceste setări influenţează modul în care pot intra utilizatorii şi joburile în sistem. Această comandă produce două rapoarte: un raport ce afişează setările pentru listele de configurare ale sistemului şi un raport ce listează parametrii relevanţi pentru securitate ale descrierilor de linie, controlerelor şi ale descrierilor de dispozitive. Fiecare din aceste rapoarte are o versiune completă şi o versiune cu modificări.	QSECCMNOLD[2]
15, 54	PRTJOBDAUT	Folosiţi comanda Tipărire autorizare descriere job (Print Job Description Authority) pentru a tipări o listă a descrierilor de joburi ce specifică un profil de utilizator şi au autorizare publică ce nu este *EXCLUDE. Raportul arată autorizările speciale ale profilului de utilizator care este specificat în descrierea de job. Acest raport are două versiuni. Raportul complet listează toate obiectele de descriere de job ce corespund criteriilor de selecţie. Raportul modificări listează diferenţele dintre obiectele descriere de job care sunt în acel moment în sistem si obiectele descriere de job care erau în sistem ultima dată când s-a realizat raportul.	QSECJBDOLD[2]

Tabela 8. Comenzi pentru rapoarte de securitate (continuare)

Opţiunea demeniu[1]	Nume comandă	Descriere	Fişier bază de date utilizat
Vezi nota 4	PRTPUBAUT	Folosiţi comanda Tipărire obiecte autorizate public (Print Publicly Authorized Objects) pentru a tipări o listă a obiectelor a căror autorizare publică nu este *EXCLUDE. Când rulaţi comanda, specificaţi tipul de obiect şi biblioteca sau bibliotecile pentru raport. Folosiţi comanda PRTPUBAUT pentru a tipări informaţii despre obiectele pe care orice utilizator din sistem le poate accesa. Acest raport are două versiuni. Raportul complet listează toate obiectele ce corespund criteriilor de selecţie. Raportul modificări listează diferenţele dintre obiectele care sunt în acel moment în sistem şi obiectele (de acelaşi tip şi din aceeaşi bibliotecă) care erau în sistem ultima dată când s-a realizat raportul.	QPBxxxxxx[5]
Vezi nota 5.	PRTPVTAUT	Folosiţi comanda Tipărire autorizări private (Print Private Authorities) pentru a tipări o listă a autorizărilor private la obiecte de tipul specificat din biblioteca specificată. Folosiţi acest raport pentru a vă ajuta să determinaţi sursa autorizării obiectelor. Acest raport are trei versiuni. Raportul complet listează toate obiectele ce corespund criteriilor de selecţie. Raportul modificări listează diferenţele dintre obiectele care sunt în acel moment în sistem şi obiectele (de acelaşi tip şi din aceeaşi bibliotecă) care erau în sistem ultima dată când s-a realizat raportul. Raportul ştergere listează utilizatorii ale căror autorizări la un obiect le-au fost şterse de la ultima tipărire a raportului.	QPVxxxxxx[5]
24, 63	PRTQAUT	Folosiţi Tipărire raport cozi (Print Queue Report) pentru a tipări setările de securitate pentru cozile de ieşire şi pentru cozile de job din sistem. Aceste setări controlează cine poate vizualiza şi modifica intrările în coada de ieşire sau în coada de joburi. Acest raport are două versiuni. Raportul complet listează toate obiectele coadă de ieşire şi coadă de joburi ce corespund criteriilor de selecţie. Raportul modificări listează diferenţele dintre obiectele coadă ieşire şi coadă job care sunt în acel moment în sistem şi obiectele coadă ieşire şi coadă job care erau în sistem ultima dată când s-a realizat raportul.	QSECQOLD[2]

Tabela 8. Comenzi pentru rapoarte de securitate (continuare)

Opţiunea demeniu[1]	Nume comandă	Descriere	Fişier bază de date utilizat
25, 64	PRTSBSDAUT	Folosiţi comanda Tipărire descriere subsistem (Print Subsystem Description) pentru a tipări intrările de comunicaţii relevante de securitate pentru descrierile subsistemelor din sistem. Aceste setări controlează cum pot activităţile să intre în sistem şi cum rulează joburile. Raportul tipăreşte o descriere de subsistem numai dacă are intrări de comunicaţii care specifică un nume de profil de utilizator. Acest raport are două versiuni. Raportul complet listează toate obiectele descriere de subsistem ce corespund criteriilor de selecţie. Raportul modificări listează diferenţele dintre obiectele descriere de subsistem care sunt în acel moment în sistem şi obiectele descriere de subsistem care erau în sistem ultima dată când s-a realizat raportul.	QSECSBDOLD[2]
26, 65	PRTSYSSECA	Folosiţi comanda Tipărire atribute securitate sistem (Print System Security Attributes) pentru a tipări o listă a variabilelor de sistem şi atributele reţelei relevante pentru securitate. Raportul arată valorile curente şi valorile recomandate.	
27, 66	PRTTRGPGM	Folosiţi comanda Tipărire programe declanşatoare (Print Trigger Programs) pentru a tipări o listă a programelor declanşator ce sunt asociate cu fişierele bazei de date în sistem. Acest raport are două versiuni. Raportul complet listează fiecare program declanşator care este alocat şi corespunde cu criteriile de selecţie. Raportul modificare listează programele declanşator ce au fost alocate de la ultima rulare a raportului.	QSECTRGOLD[2]
28, 67	PRTUSROBJ	Folosiţi comanda Imprimare obiecte utilizator pentru a imprima o listă a obiectelor utilizator (obiecte nelivrate deIBM) care sunt într-o bibliotecă. Aţi putea folosi acest raport pentru a tipări o listă a obiectelor de utilizator ce sunt într-o bibliotecă (cum ar fi QSYS) care este în porţiunea de sistem a listei de biblioteci. Acest raport are două versiuni. Raportul complet listează toate obiectele de utilizator ce corespund criteriilor de selecţie. Raportul modificări listează diferenţele dintre obiectele de utilizator care sunt în acel moment în sistem si obiectele de utilizator care erau în sistem ultima dată când s-a realizat raportul.	QSECPUOLD[2]
29, 68	PRTUSRPRF	Folosiţi comanda Tipărire profil utilizator (Print User Profile) pentru a analiza profilurile de utilizator ce corespund criteriilor de selecţie. Puteţi selecta profiluri de utilizatori bazate pe autorizări speciale, clase de utilizatori sau o diferenţă între autorizările speciale şi clasa utilizator. Puteţi tipări informaţii privind autorizarea, mediul, parola, sau nivelul de parolă.	
30, 69	PRTPRFINT	Folosiţi comanda Tipărire conţinut profil (Print Profile Internals) pentru a tipări un raport ce conţine informaţii despre numărul de intrări.	

Tabela 8. Comenzi pentru rapoarte de securitate (continuare)

Opţiunea demeniu[1]	Nume comandă	Descriere	Fişier bază de date utilizat
31, 70	CHKOBJITG	Folosiţi comanda Verificare integritate obiect (Check Object Integrity) pentru a determina dacă obiectele cu care se poate opera (cum ar fi programele) au fost modificate fără folosirea unui compilator. Această comandă vă poate ajuta să detectaţi încercările de a introduce un program virus în sistem sau de a modifica un program pentru a realiza instrucţiuni neautorizate. Cartea *Referinţă securitate iSeries* furnizează mai multe informaţii despre comanda CHKOBJITG.	

Note:

1. Opţiunile sunt din meniul SECBATCH.
2. Acest fişier este în biblioteca QUSRSYS.
3. xx este un tip de intrare de două caractere în jurnal. De exemplu, fişierul de ieşire model pentru intrările jurnal AE este QSYS/QASYAEJ4. Fişierele de ieşire model sunt descrise în Anexa F a cărţii *Referinţă securitate iSeries*.
4. Meniul SECBATCH conţine opţiuni pentru tipurile de obiecte ce intră, de obicei, în preocupările administratorilor de securitate. De exemplu, folosiţi opţiunile 11 sau 50 pentru a rula comanda PRTPUBAUT pentru obiectele *FILE. Folosiţi opţiunile generale (18 şi 57) pentru a specifica tipul obiectului.
5. Meniul SECBATCH conţine opţiuni pentru tipurile de obiecte ce intră, de obicei, în preocupările administratorilor de securitate. De exemplu, opţiunile 12 sau 51 rulează comanda PRTPVTAUT pentru obiectele *FILE. Folosiţi opţiunile generale (19 şi 58) pentru a specifica tipul obiectului.
6. xxxxxx în numele unui fişier este tipul obiectului. De exemplu, fişierul pentru obiectele program este numit QPBPGM pentru autorizările publice şi QPVPGM pentru autorizările private. Fişierele sunt în biblioteca QUSRSYS.

   Fişierul conţine un membru pentru fiecare bibliotecă pentru care aţi tipărit raportul. Numele membrului este acelaşi cu cel al bibliotecii.

Comenzi pentru personalizarea securităţii

Tabela 9 descrie comenzile pe care le puteţi folosi pentru a particulariza securitatea sistemului. Aceste comenzi sunt în meniul SECTOOLS.

Tabela 9. Comenzi pentru personalizarea sistemului dumneavoastră

Opţiunea demeniu[1]	Nume comandă	Descriere	Fişier bază de date utilizat
60	CFGSYSSEC	Folosiţi comanda Configurare securitate sistem (Configure System Security) pentru a seta variabilele de sistem relevante pentru securitate la setările recomandate. Comanda setează şi auditarea securităţii din sistem. “Valorile setate de comanda Configurare securitate sistem” la pagina 34 descrie ce face comanda. **Notă:** Pentru a obţine recomandări de securitate personalizate pentru situaţia dumneavoastră, rulaţi Vrăjitorul de securitate iSeries sau Consilierul de securitateiSeries în loc să rulaţi această comandă. Consultaţi Capitolul 2, “Vrăjitor securitate iSeries şi eServer Security Planner”, la pagina 9 pentru informaţii despre aceste instrumente.	
61	RVKPUBAUT	Folosiţi comanda Revocare autorizare publică (Revoke Public Authority) pentru a seta autorizarea publică pe *EXCLUDE pentru un set de comenzi sensibile la securitate din sistem. “Funcţii ale comenzii Revocare autorizare publică” la pagina 36 listează acţiunile pe care le realizează comanda RVKPUBAUT.	

Tabela 9. Comenzi pentru personalizarea sistemului dumneavoastră (continuare)

Opţiunea demeniu[1]	Nume comandă	Descriere	Fişier bază de date utilizat
Note: 1. Opţiunile sunt din meniul SECTOOLS.			

Valorile setate de comanda Configurare securitate sistem

Tabela 10 listează variabilele de sistem care sunt setate atunci când rulaţi comanda CFGSYSSEC. Comanda CFGSYSSEC rulează un program numit QSYS/QSECCFGS.

Tabela 10. Valorile setate de comanda CFGSYSSEC

Nume valoare sistem	Configurare	Descriere valoare sistem
QALWOBJRST	*NONE	Dacă programele stare-sistem şi programele care adoptă autorizarea pot fi restaurate
QAUTOCFG	0 (Nu)	Configurare automată a noilor dispozitive
QAUTOVRT	0	Numărul de descrieri de dispozitive virtuale pe care sistemul le va crea automat dacă nu există dispozitive disponibile pentru utilizare.
QDEVRCYACN	*DSCMSG (Deconectare cu mesaj)	Acţiunea sistemului când comunicaţiile sunt restabilite
QDSCJOBITV	120	Perioada de timp înainte ca sistemul să execute o acţiune asupra unui job deconectat
QDSPSGNINF	1 (Da)	Dacă utilizatorii văd ecranul cu informaţii despre semnare
QINACTITV	60	Perioada de timp înainte ca sistemul să execute o acţiune asupra unui job interactiv inactiv
QINACTMSGQ	*ENDJOB	Acţiunea pe care sistemul trebuie să o efectueze asupra unui job inactiv
QLMTDEVSSN	1 (Da)	Dacă utilizatorii sunt limitaţi să deschidă sesiunea de la un singur dispozitiv la un moment dat
QLMTSECOFR	1 (Da)	Dacă utilizatorii *ALLOBJ şi *SERVICE sunt limitaţi la anumite dispozitive
QMAXSIGN	3	Câte încercări nereuşite de semnare consecutive sunt permise
QMAXSGNACN	3 (Ambele)	Dacă sistemul dezactivează staţia de lucru sau profilul de utilizator când limita QMAXSIGN este atinsă.
QRMTSIGN	*FRCSIGNON	Cum administrează sistemul o încercare de semnare (pass-through sau TELNET).
QRMTSVRATR	0 (închis)	Permite sistemului să fie analizat de la distanţă.
QSECURITY [1 la pagina 35]	50	Nivelul de securitate impus
QVFYOBJRST	3 (Verifică semnătura la restaurare)	Verificare obiect la restaurare
QPWDEXPITV	60	Cât de des utilizatorii trebuie să-şi schimbe parolele
QPWDMINLEN	6	Lungimea minimă a parolei
QPWDMAXLEN	8	Lungimea maximă a parolei
QPWDPOSDIF	1 (Da)	Dacă fiecare poziţie din noua parolă trebuie să difere de aceeaşi poziţie din vechea parolă
QPWDLMTCHR	Vezi nota 2 la pagina 35	Caracterele care nu sunt permise în parolă
QPWDLMTAJC	1 (Da)	Dacă sunt interzise numere adiacente în parolă

Tabela 10. Valorile setate de comanda CFGSYSSEC (continuare)

Nume valoare sistem	Configurare	Descriere valoare sistem
QPWDLMTREP	2 (Nu pot fi repetate consecutiv)	Dacă repetarea caracterelor este interzisă în parolă
QPWDRQDDGT	1 (Da)	Dacă parolele trebuie să conţină cel puţin un număr
QPWDRQDDIF	1 (32 de parole unice)	Câte parole unice sunt cerute înainte ca o parolă să se repete
QPWDVLDPGM	*NONE	Programul de ieşire al utilizatorului pe care sistemul îl apelează pentru a valida parola

Note:

1. Dacă rulaţi în prezent cu valoarea 40 sau mai puţin a parametrului QSECURITY, asiguraţi-vă că aţi revăzut informaţiile din Capitolul 2 din cartea *Referinţă securitate iSeries* înainte de a trece la un nivel de securitate mai ridicat.
2. Caracterele nepermise sunt stocate în mesajul ID CPXB302 din fişierul de mesaje QSYS/QCPFMSG. Sunt livrate ca AEIOU@$#. Puteţi utiliza comanda Modificare descriere mesaj (Change Message Description - CHGMSGD) pentru a modifica caracterele nepermise. Valoarea sistemului QPWDLMTCHR nu este forţată la nivelurile parolă 2 sau 3.

Comanda CFGSYSSEC setează şi parola pe *NONE pentru următoarele profiluri de utilizator furnizate de IBM:

QSYSOPR

QPGMR

QUSER

QSRV

QSRVBAS

Comanda CFGSYSSEC setează auditarea securităţii utilizând comanda Schimbare auditare securitate (Change Security Auditing - CHGSECAUD). Comanda CFGSYSSEC activează auditarea acţiunilor şi obiectelor şi, de asemenea, specifică setul de acţiuni implicite de auditat cu comanda CHGSECAUD.

Personalizarea programului

Dacă unele dintre aceste setări nu sunt potrivite pentru instalarea dumneavoastră, puteţi crea propria versiune de program care prelucrează comanda. Faceţi următoarele:

__ Pasul 1. Utilizaţi comanda Recuperare sursă CL (Retrieve CL Source - RTVCLSRC) pentru a copia sursa programului care rulează când utilizaţi comanda CFGSYSSEC. Programul de recuperat este QSYS/QSECCFGS. Când îl recuperaţi, daţi-i un *nume diferit*.

__ Pasul 2. Editaţi programul pentru a face modificări. Apoi compilaţi-l. Când îl compilaţi, asiguraţi-vă că *nu* aţi înlocuit programul QSYS/QSECCFGS furnizat de IBM. Programul dumneavoastră trebuie să aibă un nume diferit.

__ Pasul 3. Utilizaţi comanda Modificare comandă (Change Command - CHGCMD) pentru a modifica parametrul (PGM) program prelucrare comandă pentru comanda CFGSYSSEC. Setaţi valoarea PGM pe numele programului dumneavoastră. De exemplu, în cazul în care creaţi un program în biblioteca QGPL numit MYSECCFG, veţi introduce următoarele:

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

Notă: Dacă schimbaţi programul QSYS/QSECCFGS , IBM nu poate garanta sau sugera siguranţa, durabilitatea, performanţa sau funcţionarea unui program. Se renunţă la garanţiile comerciale şi de potrivire pentru un anumit scop implicit.

Funcţii ale comenzii Revocare autorizare publică

Puteţi utiliza comanda Revocare autorizare publică (Revoke Public Authority - RVKPUBAUT) pentru a seta autorizarea publică pe *EXCLUDE pentru un set de comenzi şi programe. Comanda RVKPUBAUT rulează un program numit QSYS/QSECRVKP. Aşa cum este livrat, QSECRVKP revocă autorizarea publică (setând autorizarea publică pe *EXCLUDE) pentru comenzile care sunt listate în Tabela 11 şi API-urile listate în Tabela 12. Când sistemul dumneavoastră soseşte, aceste comenzi şi API au autorizarea lor publică setată pe *USE.

Comenzile care sunt listate în Tabela 11 şi API care sunt listate în Tabela 12 execută funcţii pe sistem care pot oferi o şansă pentru cei rău intenţionaţi. În calitate de administrator de securitate, trebuie mai degrabă să autorizaţi în mod explicit utilizatorii care rulează aceste comenzi şi programe, decât să le faceţi disponibile tuturor utilizatorilor din sistem.

Când rulaţi comanda RVKPUBAUT, specificaţi biblioteca ce conţine comenzile. Biblioteca implicită este QSYS. Dacă aveţi mai mult de o limbă naţională, nu trebuie să rulaţi comanda pentru fiecare bibliotecă QSYSxxx.

Tabela 11. Comenzi ale căror autorizare publică este setată de comanda 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 din Tabela 12 sunt toate în biblioteca QSYS:

Tabela 12. Programe ale căror autorizare publică este setată de comanda RVKPUBAUT

%FPALANDRIVER02%
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

Când rulaţi comanda RVKPUBAUT, sistemul setează autorizarea publică pentru directorul root la *USE (doar dacă este deja *USE sau mai mică).

Personalizarea programului

Dacă unele dintre aceste setări nu sunt potrivite pentru instalarea dumneavoastră, puteţi crea propria versiune de program care prelucrează comanda. Faceţi următoarele:

__ Pasul 1. Utilizaţi comanda Recuperare sursă CL (Retrieve CL Source - RTVCLSRC) pentru a copia sursa programului care rulează când utilizaţi comanda RVKPUBAUT. Programul de recuperat este QSYS/QSECRVKP. Când îl recuperaţi, daţi-i un *nume diferit*.

__ Pasul 2. Editaţi programul pentru a face modificări. Apoi compilaţi-l. Când îl compilaţi, asiguraţi-vă că *nu* aţi înlocuit programul QSYS/QSECRVKP furnizat de IBM. Programul dumneavoastră trebuie să aibă un nume diferit.

__ Pasul 3. Utilizaţi comanda Modificare comandă (Change Command - CHGCMD) pentru a modifica parametrul (PGM) program prelucrare comandă pentru comanda RVKPUBAUT. Setaţi valoarea PGM pe numele programului dumneavoastră. De exemplu, în cazul în care creaţi un program în biblioteca QGPL numit MYRVKPGM, veţi introduce următoarele:

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

Notă: Dacă schimbaţi programul QSYS/QSECRVKP , IBM nu poate garanta sau sugera siguranţa, durabilitatea, performanţa sau funcţionarea unui program. Se renunţă la garanţiile comerciale şi de potrivire pentru un anumit scop implicit.

Partea 2. Securitate iSeries avansată

Capitolul 5. Protejarea informaţiilor cu autorizare obiect

Sarcina dumneavoastră ca administrator de securitate este de a proteja informaţiile organizaţiei fără a frustra utilizatorii sistemului dumneavoastră. Trebuie să fiţi siguri că utilizatorii au autorizare suficientă pentru a executa joburile lor fără a le da autorizarea să umble în sistemul dumneavoastră şi să facă modificări neautorizate.

Indiciu pentru securitate

Autoritatea prea rigidă poate reacţiona. Utilizatorii reacţionează uneori la restricţiile autorizărilor prea slabe prin împărţirea între ei a parolelor.

Sistemul de operare OS/400 furnizează securitate de obiect integrată. Utilizatori trebuie să utilizeze interfeţele pe care le furnizează sistemul pentru a accesa obiectele. De exemplu, dacă doriţi să accesaţi un fişier bază de date, trebuie să folosiţi comenzile sau programele care realizează accesul la baze de date. Nu puteţi folosi o comandă care realizează accesul la o coadă de mesaje sau la un istoric de joburi.

Oricând utilizaţi o interfaţă sistem pentru a accesa un obiect, sistemul verifică dacă aveţi autorizarea cerută pentru obiectul care este cerut de acea interfaţă. Autorizarea obiect este un instrument puternic şi flexibil pentru a proteja datele sistemului dumneavoastră. Scopul dumneavoastră ca administrator de securitate este să setaţi o schemă de securitate obiect efectivă pe care o puteţi gestiona şi întreţine.

Forţarea autorizării obiect

Ori de câte ori încercaţi să accesaţi un obiect, sistemul de operare verifică autorizarea dumneavoastră la acel obiect. Totuşi, dacă nivelul de securitate al sistemului dumneavoastră (variabila de sistem QSECURITY) este setat la 10 sau 20, toţi utilizatorii au automat autorizarea de a accesa orice obiect deoarece toate profilurile utilizator au autorizarea specială *ALLOBJ.

Indiciu de autorizare obiect: Dacă nu sunteţi sigur dacă folosiţi securitatea obiectelor, verificaţi valoarea sistem QSECURITY (nivel de securitate). Dacă QSECURITY este 10 sau 20, fără utilizarea obiectelor de securitate.

Trebuie să vă pregătiţi înainte de a modifica nivelul de securitate la 30 sau mai mult. Altfel, utilizatorii dumneavoastră ar putea să nu reuşească să acceseze informaţiile de care au nevoie.

Subiectul **Planificare şi securitate sistem de bază** din Centru informaţii furnizează o metodă pentru analiza aplicaţiilor dumneavoastră şi pentru a decide cum ar trebui să setaţi securitatea obiect. Dacă nu utilizaţi încă securitatea obiect sau schema dumneavoastră de securitate obiect este expirată şi complicată, citiţi acest subiect pentru a vă ajuta cum să începeţi.

Meniul securitate

Serverul iSeries a fost proiectat iniţial ca un produs pentru continuareaS/36 şi S/38. Multe instalări server iSeries au fost, la un moment dat, instalări S/36 sau instalări S/38. Pentru a decide care din utilizatori pot fi, administratori de securitate în aceste sisteme, s-a utilizat destul de des o tehnică cunoscută ca **securitate meniu** sau **control acces meniu**.

Meniul de control acces înseamnă că atunci când un utilizator se înregistrează, utilizatorul vede un meniu. Utilizatorul nu poate realiza decât funcţiile din meniu. Utilizatorul nu poate trece la o linie de comandă a sistemului pentru a executa funcţii ce nu există în meniu. Teoretic, administratorul de securitate nu trebuie să se îngrijoreze de autorizarea obiectelor deoarece meniurile şi programele controlează ce pot face utilizatorii.

Serverul iSeries furnizează mai multe opţiuni pentru profilul utilizator pentru a ajuta cu meniul de control al accesului, puteţi folosi:

- **Meniul iniţial** Parametrul (INLMNU) pentru a controla care meniu este văzut primul de utilizator după ce se conectează.
- **Programul iniţial** Parametrul (INLPGM) pentru a rula un program de configurare înainte ca utilizatorul să vadă un meniu. Sau, puteţi folosi parametrul INLPGM pentru a restricţiona utilizatorul la rularea unui singur program.
- **Limitare capabilităţi** Parametrul (LMTCPB) pentru a restricţiona un utilizator la un set limitat de comenzi. Împiedică, de asemenea, utilizatorul să specifice un alt program sau meniu iniţial în ecranul de semnare (Parametrul LMTCPB limitează doar comenzile care se introduc de la linia de comandă).

Limitări ale meniului de control al accesului

Calculatoarele şi utilizatorii de calculatoare s-au schimbat foarte mult în ultimii ani. Multe instrumente, cum ar fi programe de interogare şi foi de calcul, sunt disponibile astfel că utilizatorii pot face propriile lor programe în departamente IS off-load. Anumite instrumente, cum ar fi SQL sau ODBC, furnizează posibilitatea vizualizării informaţiilor şi modificării lor. Pentru a activa aceste instrumente într-o structură de meniu este foarte dificil.

Staţiile de lucru cu ecrane verzi (“green-screen”) au fost înlocuite rapid cu calculatoare personale şi reţele calculator-la-calculator. Dacă sistemul dumneavoastră face parte dintr-o reţea, utilizatorii pot accesa sistemul dumneavoastră fără măcar să vadă un ecran sau un meniu de semnare.

Ca administrator de securitate care încearcă să impună control acces meniu, aveţi două probleme de bază:

- Dacă aţi limitat cu succes utilizatorii la meniu, utilizatorii dumneavoastră pot fi nefericiţi deoarece posibilităţile lor de a utiliza instrumente moderne sunt limitate.
- Dacă utilizatorii nu sunt limitaţi în acţiunile lor, vă expuneţi datele, informaţiile confidenţiale pe care control acces meniu ar fi trebuit să le protejeze. Când sistemul dumneavoastră face parte dintr-o reţea, posibilitatea de a impune control acces meniu scade. De exemplu, parametrul LMTCPB se aplică doar comenzilor introduse de la linia de comandă dintr-o sesiune interactivă. Parametrul LMTCPB nu afectează cererile sesiunilor de comunicare cum ar fi transfer de fişiere PC, FTP sau comenzi de la distanţă.

Îmbunătăţirea meniului de control al accesului cu securitate obiect

Cu multe din noile opţiuni care sunt disponibile pentru conectarea la sisteme, o schemă de securitate viabilă a serverului iSeries pentru viitor nu se poate baza numai pe meniul de control al accesului. Aceste subiecte oferă sugestii pentru adăugarea de securitate obiecte pentru a completa controlul accesului la meniuri.

Subiectul *Securitatea sistemului de bază şi planificare* din Centru informaţii descrie o tehnică de analiză a aplicaţiilor pe care trebuie să le aibă utilizatorii pentru obiecte în vederea rulării aplicaţiilor curente. Apoi asociaţi utilizatorii grupurilor şi daţi grupurilor autorizarea corespunzătoare. Această abordare este rezonabilă şi logică. Totuşi, dacă sistemul dumneavoastră a funcţionat mulţi ani şi are multe aplicaţii, procesul de analiză a aplicaţiilor şi configurarea autorizării obiect pare, probabil, copleşitor.

Indiciu de autorizare obiect: Meniurile dumneavoastră curente combinate cu programe care adoptă autorizarea proprietarilor de program poate furniza o tranziţie mai avansată decât meniul de control al accesului. Asiguraţi-vă că protejaţi atât programele care adoptă autorizare, cât şi profilurile utilizator cărora le aparţin.

Puteţi utiliza meniurile dumneavoastră curente pentru a vă ajuta să setaţi un mediu de tranziţie atâta timp cât analizaţi gradual aplicaţiile şi obiectele dumneavoastră. În continuare este un exemplu care foloseşte meniul OEMENU (Order Entry - ordonare intrare) şi fişierele şi programele asociate.

Exemplu: Setarea unui mediu de tranziţie

Acest exemplu porneşte cu următoarele ipoteze şi cereri:

- Toate fişierele sunt în biblioteca ORDERLIB.
- Nu cunoaşteţi numele tuturor fişierelor. Nu cunoaşteţi, de asemenea, ce autorizări cer opţiunile meniului pentru diferite fişiere.
- Meniul şi toate programele pe care le apelează se găsesc în biblioteca intitulată ORDERPGM.
- Doriţi ca oricine care se conectează la sistemul dumneavoastră să poată vizualiza toate fişierele comandă, fişiere clienţi şi fişiere obiect (cu interogări sau foi de calcul, de exemplu).
- Doar utilizatorii al căror meniu de conectare este OEMENU ar trebui să poată modifica fişierele. Şi trebuie să utilizeze programele din meniu pentru a face aceasta.
- Utilizatorii de sistem alţii decât administratorii de securitate nu au autorizăriile speciale *ALLOBJ sau *SECADM.

Realizaţi paşii următori pentru a modifica acest mediu al meniului de control al accesului pentru rezolva şi necesitatea de interogări:

__ Pasul 1. Faceţi o listă a utilizatorilor al căror meniu iniţial este OEMENU.

Puteţi utiliza comanda Tipărire profil utilizator (PRTUSRPRF *ENVINFO) pentru a lista mediul tuturor profilurilor utilizator de pe sistemul dumneavoastră. Raportul include meniul iniţial, programul iniţial şi biblioteca curentă. Figura 7 la pagina 58 vă arată un exemplu de raport.

__ Pasul 2. Asiguraţi-vă că obiectul OEMENU (poate fi un obiect *PGM sau un obiect *MENU) este proprietatea unui profil utilizator care nu este folosit pentru conectare. Profilul utilizator trebuie să fie dezactivat sau să aibă o parolă *NONE. Pentru acest exemplu, asiguraţi-vă că OEOWNER conţine obiectul program OEMENU.

__ Pasul 3. Asiguraţi-vă că profilul utilizator căruia îi aparţine obiectul program OEMENU nu este un profil de grup. Puteţi folosi următoarea comandă:

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

__ Pasul 4. Modificaţi programul OEMENU pentru a adopta autorizarea profilului utilizator OEOWNER (Folosiţi comanda CHGPGM pentru a modifica parametrul USRPRF la *OWNER).

Notă: Obiectele *MENU nu pot adopta autorizare. Dacă OEMENU este un obiect *MENU, puteţi adapta acest exemplu făcând următoarele:

- Creaţi un program pentru a afişa meniul.
- Folosiţi autorizări adoptate pentru programele care rulează când utilizatorii selectează opţiunile meniului OEMENU.

__ Pasul 5. Setaţi autorizarea publică a tuturor fişierelor din ORDERLIB la *USE introducând următoarele două comenzi:

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

Amintiţi-vă că dacă selectaţi autorizarea *USE, utilizatorii pot copia fişierul utilizând transferul de fişiere PC sau FTP.

__ Pasul 6. Daţi profilului proprietar al programului meniu autorizarea *ALL pentru fişiere, introducând următoarele:

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

Pentru cele mai multe aplicaţii, autorizarea *CHANGE a fişierelor este suficientă. Totuşi, aplicaţiile dumneavoastră pot executa funcţii, cum ar fi ştergerea membrilor fişier fizic, care cer autorizare mai mare decât *CHANGE. Eventual, trebuie să analizaţi aplicaţiile dumneavoastră şi să furnizaţi doar minimum de autorizare necesară aplicaţiei. Totuşi, în timpul tranziţiei, prin adoptarea autorizării *ALL, împiedicaţi eşuarea aplicaţiilor care ar putea fi cauzată de autorizare insuficientă.

__ Pasul 7. Restricţionaţi autorizarea programelor din bibliotecă introducând următoarele:

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

__ Pasul 8. Daţi profilului OEOWNER autorizare la programele din bibliotecă, introducând următoarele:

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

__ Pasul 9. Daţi utilizatorilor pe care i-aţi identificat în pasul 1 autorizarea programului meniu introducând pentru fiecare utilizator următoarele:

```
GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM)
     USER(nume profil utilizator) AUT(*USE)
```

Când aţi terminat aceşti paşi, toţi utilizatorii sistem care nu sunt excluşi explicit vor putea accesa (dar nu modifica) fişierele din biblioteca ORDERLIB. Utilizatorii care au autorizare pentru programul OEMENU vor putea folosi programele ce sunt în meniu pentru a actualiza fişierele din biblioteca ORDERLIB. Doar utilizatorii care au autorizare pentru programul OEMENU vor putea modifica fişierele din această bibliotecă. O combinaţie de securitate obiect şi control acces meniu protejează fişierele.

Când terminaţi paşii similar pentru toate bibliotecile care conţin date utilizator, aţi creat o schemă simplă pentru controlul actualizărilor bazelor de date. Această metodă împiedică utilizatorii sistem să actualizeze fişierele baze de date cu excepţia când folosesc meniurile şi programele aprobate. În acelaşi timp, aţi disponibilizat fişierele baze de date pentru vizualizare, analizare şi copiere pentru utilizatorii cu instrumente de suport decizie sau cu legătură de la alt sistem sau de la un PC.

Indiciu de autorizare obiect: Când sistemul dumneavoastră face parte dintr-o reţea, autorizarea *USE poate furniza o autorizare mai mare decât vă aşteptaţi. De exemplu, cu FTP, puteţi face o copie a unui fişier de pe alt sistem (inclusiv un PC) dacă aveţi autorizarea *USE pentru fişier.

Folosirea securităţii bibliotecii pentru complementarea securităţii meniului

Pentru a accesa un obiect dintr-o bibliotecă, trebuie să aveţi autorizare atât pentru bibliotecă cât şi pentru obiect. Cele mai multe operaţii cer fie autorizarea *EXECUTE, fie *USE pentru bibliotecă.

În funcţie de situaţie, puteţi folosi autorizarea bibliotecă ca cel mai simplu mod de a securiza obiectele. De exemplu, presupuneţi că pentru exemplul de meniu Introducere comenzi, oricine are autorizarea pentru meniul Introducere comenzi poate utiliza toate programele din biblioteca ORDERPGM. Mai bine decât să securizaţi programele individual, puteţi seta autorizarea publică pentru biblioteca ORDERPGM la *EXCLUDE. Puteţi apoi acorda autorizarea *USE pentru biblioteci anumitor profiluri de utilizator, fapt ce le va permite să folosească programele din bibliotecă (Aceasta presupune ca autorizarea publică pentru programe este *USE sau mai mare).

Autorizarea bibliotecă poate fi o metodă simplă şi eficientă pentru administrarea autorizării obiect. Totuşi, trebuie să vă asiguraţi că cunoaşteţi conţinutul bibliotecilor pe care le securizaţi astfel ca să nu furnizaţi neintenţionat accesul la obiecte.

Configurarea dreptului de proprietate a obiectului

Proprietatea obiectelor sistemului dumneavoastră este o parte importantă a schemei dumneavoastră de autorizare obiect. Implicit, proprietarul unui obiect are autorizarea *ALL pentru obiect. Capitolul 5 al cărţii *Referinţă securitate iSeries* furnizează recomandări şi exemple pentru planificarea proprietarilor obiectelor. Următoarele sunt câteva sfaturi:

- În general, profilurile grup trebuie să nu aibă obiecte în proprietate. Dacă un profil grup are un obiect în proprietate, toţi membrii de grup au autorizarea *ALL pentru obiect, atâta timp cât membrul nu este exclus explicit.
- Dacă folosiţi autorizare adoptată, determinaţi dacă profilurile utilizator care au obiecte trebuie, de asemenea, să aibă obiecte aplicaţie, cum ar fi fişiere. Puteţi să nu doriţi ca utilizatorii care rulează programe ce adoptă autorizare să aibă autorizarea *ALL pentru fişiere.

Dacă folosiţi Navigator iSeries, aceasta poate fi realizată efectuând modificările folosind funcţia de **politici** de securitate. Pentru mai multe informaţii, recurgeţi la Centru de informare iSeries (vezi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru detalii).

Autorizare obiect la programele şi comenzile sistem

Următoarele sunt câteva sugestii când restricţionaţi autorizarea pentru obiectele furnizate de IBM:

- Dacă aveţi mai mult de o limbă naţională pe sistemul dumneavoastră, sistemul dumneavoastră are mai mult de o bibliotecă sistem (QSYS). Sistemul dumneavoastră are câte o bibliotecă QSYSxxxx pentru fiecare limbă naţională de pe sistemul dumneavoastră. Dacă folosiţi autorizare obiect pentru a controla accesul la comenzile sistem, amintiţi-vă să securizaţi comenzile în biblioteca QSYS şi în fiecare bibliotecă QSYSxxx de pe sistemul dumneavoastră.
- Biblioteca System/38 furnizează câteodată o comandă cu funcţie care este echivalentă cu comenzile pe care doriţi să restricţionaţi. Fiţi sigur că restricţionaţi comanda echivalentă din biblioteca QSYS38.
- Dacă aveţi mediul System/36, trebuie să restricţionaţi programele suplimentare. De exemplu, programul QY2FTML furnizează fişierulSystem/36 de transfer.

Funcţii de auditare securitate

Acest capitol descrie tehnici de verificare a eficienţei securităţii din sistem. Auditarea securităţii sistemului se efectuează din mai multe motive:

- Pentru a evalua dacă planul de securitate este complet.
- Pentru a se asigura dacă, controalele de securitate planificată funcţionează . Acesta tip de auditare este utilizat frecvent de responsabilul de securitate ca parte a procesului de

administrare zilnică a securităţii. De asemenea, este efectuat, câteodată, mai detaliat, ca parte a procesului de trecere în vedere periodică a securităţii de către auditorii interni sau externi.

- Pentru a se asigura faptul că securitatea sistemului nu este influenţată de modificările din mediul sistem. Câteva exemple de modificări care afectează securitatea :
  - Obiecte nou create de către utilizatorii sistemului
  - Utilizatori noi admişi în sistem
  - Modificarea proprietarilor obiectelor (autorizare neajustată)
  - Modificarea responsabilităţilor (grup de utilizatori modificat)
  - Autoritate temporară (fără oportunitate de revocare)
  - Noi produse instalate
- Pentru pregătirea unui viitor eveniment, ca de exemplu instalarea unei noi aplicaţii, mutarea la un nivel mai mare de securitate sau setarea unei reţele de comunicaţii.

Tehnicile descrise aici sunt potrivite pentru toate aceste situaţii. Componenta verificată şi cât de des depinde de mărimea şi nevoile de securitate ale sistemului. Scopul acestui capitol este de a evidenţia informaţiile disponibile, modul de obţinere a acestora, de ce sunt necesare, mai degrabă decât să să ofere informaţii despre frecvenţa verificărilor.

Această informaţie are trei părţi:

- Lista de verificare a articolelor de securitate ce pot fi planificate şi auditate.
- Informaţii privind setarea şi utilizarea jurnalului de auditare oferit de sistem.
- Alte tehnici disponibile pentru obţinerea de informaţii de securitate din sistem.

Verificarea securităţii presupune utilizarea comenzilor în iSeries sistem şi accesarea informaţiilor de jurnal şi semnare în sistem. Puteţi crea un profil special de utilizator pentru a fi utilizat de cei care efectuează auditarea securităţii sistemului. Profilul de auditor va avea nevoie de autorizare specială *AUDIT pentru a putea modifica caracteristicile de auditare ale sistemului. Anumite sarcini de auditare amintite în acest capitol necesită un profil de utilizator cu autorizare specială *ALLOBJ şi *SECADM. Amintiţi-vă să setaţi parola pentru profilul de auditor la *NONE după încheierea perioadei de auditare.

Pentru mai multe detalii privind auditarea securităţii, vezi Capitolul 9, al cărţii *Referinţe de securitate*.

Analiza profilurilor utilizator

Puteţi afişa sau tipări o listă completă a tuturor utilizatorilor de pe sistemul dumneavoastră cu comanda DSPAUTUSR. Lista poate fi secvenţiată după numele profilului sau după numele grupului. Urmează un exemplu a secvenţei de profil de grup:

```
                          Afişare utilizatori autorizaţi

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

Tipărirea profilurilor utilizator selectate

Puteţi folosi comanda DSPUSRPRF pentru a crea un fişier de ieşire, pe care puteţi să-l procesaţi folosint o unealtă de interogare.

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

Puteţi folosi o unealtă de chestionare pentru a crea o varietate de rapoarte de analiză a fişierului dumneavoastră de ieşire, precum:

- O listă a tuturor utilizatorilor care au autorizările speciale *ALLOBJ şi *SPLCTL.
- O listă a tuturor utilizatorilor, secvenţiaţi după un câmp profil utilizator, precum programul iniţial sau clasa utilizator.

Puteţi crea programe de chestionare pentru a porduce rapoarte diferite din fişierul dumneavoastră de ieşire. De exemplu:

- Afişaţi profilurile tuturor utilizatorilor care au vreo autorizare specială prin selectarea înregistrărilor unde câmpul UPSPAU nu este *NONE.
- Afişarea tuturor utilizatorilor cărora le este permis să introducă comenzi prin selectarea înregistrărilor unde câmpul *Capacităţi limită* (numit UPLTCP în fişierul de ieşire model bază de date) este egal cu *NO au *PARTIAL.
- Afişarea tuturor utilizatorilor care au un meniu sau program initial.
- Aişarea utilizatorilor inactivi prin vizionarea câmpului ultimei date de intrare

Examinarea profilurilor utilizator mari

Profilurile utilizator cu număr mare de autorizări, care par să fie împărţiţi în mod aleator peste tot sistemul, pot reflecta o lipsă de planificare a securităţii. Urmează o metodă pentru localizarea şi evaluarea profilurilor utilizator:

1. Folosirea comenzii DSPOBJD pentru a crea un fişier de ieşire ce conţine aproape toate profilurile utilizator de pe sistem:

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

2. Creaţi un program de chestionare pentru a lista numele şi mărimea fiecărui profil utilizator, în secventă descrescătoare în funcţie de mărime.

3. Afişaţi informaţii detaliate despre cele mai mari profiluri utilizator şi evaluaţi autorizările şi obiectele avute pentru a vedea dacă sunt potrivite:

   ```
   DSPUSRPRF USRPRF(numele-profil-utilizator) +
             TYPE(*OBJAUT) OUTPUT(*PRINT)
   DSPUSRPRF USRPRF(numele-profil-utilizator) +
             TYPE(*OBJOWN) OUTPUT(*PRINT)
   ```

   Anumite profiluri utilizator furnizate de IBM sunt foarte mari din cauza numărului de obiecte pe care le au. Listarea şi analizarea lor nu este de obicei necesară. Oricum, ar trebui să căutaţi programe care acceptă autorizarea profilurilor utilizator furnizate de IBM care au autorizarea specială *ALLOBJ, precum QSECOFR şi QSYS.

Pentru mai multe detalii despre auditarea de securitate, vazi Capitolul 9, din cartea *Referinţe de securitate*.

Analiza autorizărilor obiect

Puteţi folosi următoarea metodă pentru a determina cine are autorizare la bibliotecile de pe sistem:

1. Folosiţi comanda DSPOBJD pentru a afişa toate bibliotecile de pe sistem:

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

   Notă: Biblioteci din pool-uri de stocare auxiliare independente care nu sunt în stare AVAILABLE nu vor afişate de această comandă.

2. Folosiţi comanda DSPOBJAUT pentru a afişa autorizările unei biblioteci specifice:

   ```
   DSPOBJAUT OBJ(QSYS/library-name) OBJTYPE(*LIB) +
             ASPDEV(nume-dispozitiv-asp) OUTPUT(*PRINT)
   ```

3. Folosiţi comanda DSPLIB pentru a afişa obiectele din bibliotecă:

   ```
   DSPLIB LIB(QSYS/nume-bibliotecă) ASPDEV(nume-dispozitiv-asp) OUTPUT(*PRINT)
   ```

Folosind aceste rapoarte, puteţi determina care este într-o bibliotecă şi cine are acces la bibliotecă. Dacă este necesar, puteţi folosi comanda DSPOBJAUT pentru a vedea de asemenea autorizările pentru obiectele selectate din bibliotecă.

Verificarea obiectelor alterate

Puteţi folosi comanda CHKOBJITG pentru a căuta obiecte care au fost alterate. Un obiect alterat este de obicei indicaţia că cineva încearcă să umble la sistemul dumneavoastră. S-ar putea să doriţi să rulaţi această comandă după ce cineva:

- A restaurat programe pe sistemul dumneavoastră
- A folosit unelte de service dedicate (DST)

Când rulaţi comanda, sistemul creează un fişier bază de date conţinând informaţii despre orice probleme potenţiale de integritate. Puteţi verifica aceste obiecte avute de profilul cuiva, de câteva profiluri diferite sau de toate profilurile. Puteţi căuta obiecte ale căror domenii au fost alterate. Puteţi de asemenea recalcula valorile de validare program pentru a căuta obiecte de tipul *PGM, *SRVPGM, *MODULE şi *SQLPKG care au fost alterate.

Rularea programului CHKOBJITG necesită autorizarea specială *AUDIT. Comanda poate lua un timp mai lung pentru a rula, din cauza scanărilor şi calculelor pe care le efectuează. Ar trebui să-l rulaţi de fiecare dată când sistemul dumneavoastră nu este ocupat.

Notă: Profilurile care posedă mai multe obiecte cu multe autorizări private, pot deveni foarte mari. Mărimea unui profil de proprietar afectează performanţa când afişaţi şi lucraţi cu autorizarea la obiectelor deţinute şi când salvaţi sau restauraţi profilurile. Operaţiile de sistem pot fi de asemenea afectate. Pentru a preveni afectarea performaţelor sau

operaţiilor sistem, distribuiţi porprietatea asupra obiectelor către mai multe profiluri. **Nu acordaţi toate (sau aproape toate) obiectele unui singur profil utilizator.**

Analiza programelor care adoptă autorizare

Programe care adoptă autoritare unui utilizator cu autorizarea specială *ALLOBJ reprezintă o expunere de securitate. Metoda următoare poate fi folosită pentru a găsi şi a inspecta aceste programe:

1. Pentru fiecare utilizator cu autorizarea specială *ALLOBJ, folosiţi comanda DSPPGMADP (Afişare Programe Care Adoptă) pentru a lista programele care adoptă autorizarea utilizatorilor:

   ```
   DSPPGMADP USRPRF(nume-profil-utilizator) +
             OUTPUT(*PRINT)
   ```

   Notă: Subiectul “Tipărirea profilurilor utilizator selectate” la pagina 47 arată cum să afişaţi utilizatori cu autorizare *ALLOBJ.

2. Folosiţi comanda DSPOBJAUT pentru a determina cine este autorizat pentru folosirea fiecărui program care adoptă şi ceea ce este autorizarea publică pentru program:

   ```
   DSPOBJAUT OBJ(nume-bibliotecă/nume-program) +
             OBJTYPE(*PGM) ASPDEV(nume-bibliotecă/nume-program) +
             OUTPUT(*PRINT)
   ```

3. Inspectaţi codul sursă şi descrierea programului pentru a evalua:
   - Dacă utilizatorul programului este privat de funcţia de ieşire, precum folosirea unei linii de comandă, când rulează sub profilul adoptat.
   - Dacă programul adoptă nivelul minim de autorizare necesar pentru funcţia intenţionată. Aplicaţii care folosesc căderi de program pot fi proiectate folosind acelaşi proprietar de profil pentru obiecte şi programe. Când autorizarea proprietarului programului este adoptată, utilizatorul are toată (*ALL) autorizarea pentru obiectele aplicaţie. În multe cazuri, profilul proprietar nu are nevoie de nici o autorizare specială.

4. Verificaţi când programul a fost schimbat ultima dată, folosind comanda DSPOBJD:

   ```
   DSPOBJD OBJ(nume-bibliotecă/nume-program) +
           OBJTYPE(*PGM) ASPDEV(nume-bibliotecă/nume-program) +
           DETAIL(*FULL)
   ```

Gestionarea jurnalului de auditare şi receptorilor jurnal

Jurnalul de auditare, QSYS/QAUDJRN, aşa cum este intenţionat doar pentru auditări de securitate. Obiectele nu trebuie să fie înregistrate în jurnalul de auditare. Controlul obligaţiilor nu trebuie să folosească jurnalul de auditare. Intrările utilizator nu trebuie să fie trimise la acest jurnal folosind comanda Trimitere Intrare Jurnal (Send Journal Entry (SNDJRNE)) sau API-ul Trimitere Intrare Jurnal(Send Journal Entry (QJOSJRNE)).

Sunt folosite protecţii speciale de blocare pentru asigurarea că sistemul poate scrie intrări de auditare în jurnalul de auditare. Când auditarea este activă (valoarea sistem QAUDCTL nu este *NONE), sarcina de arbitrare sistem (QSYSARB) ţine o blocare pe jurnalul QSYS/QAUDJRN. Nu puteţi efectua anumite operaţii pe jurnalul de auditare când auditarea este activă, precum:

- comanda DLTJRN
- comanda ENDJRNxxx
- comanda APYJRNCHG
- comanda RMVJRNCHG
- comanda DMPOBJ sau DMPSYSOBJ
- Mutarea jurnalului
- Restaurarea jurnalului

- Operaţii care lucrează cu autorizarea, precum comanda GRTOBJAUT
- comanda WRKJRN

Informaţia înregistrată în intrările de securitate în jurnal este descrisă în cartea *Referinţe de securitate*. Toate intrările de securitate din jurnalul de auditare au codul de jurnal T. În plus la intrările de securitate, intrările sistem apar de asemenea în jurnalul QAUDJRN. Acestea sunt intrările cu codul de jurnal J, care se referă la încărcarea iniţială a programului (initial program load (IPL)) şi la operaţiile generale efectuate pe destinatarii jurnalului (de exemplu, salvarea destinatarului).

Dacă apare vreo stricăciune la jurnal sau la destinatarul său curent în aşa fel încât intrările de auditare nu mai pot fi înregistrate, valoarea de sistem QAUDENDACN determină ce acţiuni urmează sistemul. Recuperarea dintr-un jurnal sau destinatar de jurnal afectat este aceeaşi ca pentru alte jurnale.

Este posibil să doriţi ca sistemul să conducă schimbarea destinatarilor jurnalului. Specificaţi MNGRCV(*SYSTEM) când creaţi jurnalul QAUDJRN, sau când schimbaţi jurnalul la acea valoare. Dacă specificaţi MNGRCV(*SYSTEM), sistemul detaşează automat destinatarul când ajunge la mărimea coşului de gunoi şi creează şi ataşează un nou destinatar al jurnalului. Aceasta este numită **Gestiune modificare-jurnal sistem**. ConsultaţiiSeries Centrul de informare—>Gestiune sisteme–> Gestiune jurnal–>Gestiune jurnal local–>Gestiune jurnale pentru informaţii suplimentare. Consultaţi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru informaţii despre accesarea Centrului de informare iSeries.

Capitolul 6. Gestiunea autorizării

Un set de rapoarte de securitate sunt disponibile pentru a vă ajuta să urmăriţi cum este setată autorizarea pe sistemul dumneavoastră. Când rulaţi aceste rapoarte iniţial, puteţi tipări orice (autorizarea pentru toate fişierele şi programele, de exemplu).

După ce aţi stabilit baza dumneavoastră de informaţii, puteţi rula cu regularitate rapoartele cu modificări. Rapoartele cu modificări vă ajută să identificaţi modificările relevante de securitate de pe sistemul dumneavoastră care necesită atenţia dumneavoastră. De exemplu, puteţi rula raportul care arată autorizarea publică pentru fişiere în fiecare săptămână. Puteţi solicita doar versiunea cu modificări a raportului. Vă va arăta atât noile fişiere de pe sistem care sunt disponibile oricui, cât şi fişierele existente ale căror autorizări publice s-au modificat de la ultimul raport.

Două meniuri sunt disponibile pentru a rula instrumentele de securitate:

- Folosiţi meniul SECTOOLS pentru a rula programele interactiv.
- Folosiţi meniul SECBATCH pentru a rula programele în batch. Meniul SECBATCH are două părţi: una pentru a lansa joburi în coada de joburi imediat şi cealaltă pentru a plasa joburile în planificatorul de joburi.

Dacă folosiţi Navigator iSeries, urmaţi aceşti paşi pentru a rula uneltele de securitate:

1. În Navigator iSeries, expandaţi serverul dumneavoastră—>**Securitate**.
2. Faceţi clic dreapta pe **Politici** şi selectaţi **Explorare** pentru a afişa o listă de politici pe care le puteţi crea şi gestiona.

Monitorizarea autorizării publice a obiectelor

Atât pentru simplitate, cât şi pentru performanţă, cele mai multe sisteme sunt setate asfel încât cele mai multe obiecte sunt disponibile pentru majoritatea utilizatorilor. Utilizatorii au mai degrabă explicit accesul interzis pentru anumite obiecte confidenţiale, sensibile la securitate, decât să fie autorizaţi explicit pentru a folosi fiecare obiect. Puţine sisteme, care au cerinţe mari de securitate, au o abordare opusă şi autorizează obiectele pe baza nevoilor de cunoştinţe. Pe aceste sisteme, cele mai multe obiecte sunt create cu autorizarea publică setată la *EXCLUDE.

iSeries este un sistem bazat pe obiecte cu diferite tipuri de obiecte. Cele mai multe tipuri de obiecte nu conţin informaţii sensibile sau nu îndeplinesc funcţii relevante de securitate. Ca administrator de securitate pe un sistem iSeries cu necesităţi tipice de securitate, probabil doriţi să vă concentraţi atenţia asupra obiectelor care cer protecţie, cum ar fi fişiere baze de date şi programe. Pentru alte tipuri de obiecte, doar setaţi autorizarea publică, care este suficientă pentru aplicaţiile dumneavoastră, care pentru cele mai multe tipuri de obiecte este autorizarea *USE.

Puteţi utiliza comanda Tipărire autorizări publice (PRTPUBAUT) pentru a tipări informaţiile despre obiectele pe care le pot accesa utilizatorii publici (Un **utilizator public** este oricine deţine autorizare de semnare şi care nu are autorizare explicită pentru un obiect). Când folosiţi comanda PRTPUBAUT, puteţi specifica tipurile de obiect şi bibliotecile sau directoarele, pe care doriţi să le examinaţi. Opţiunile sunt disponibile la meniurile SECBATCH şi SECTOOLS pentru a tipări Raportul obiecte autorizate public pentru tipurile de obiecte care au în cele mai multe cazuri implicaţii de securitate. Puteţi tipări versiunea cu modificări a acestui raport în mod regulat pentru a vedea ce obiecte necesită atenţie.

Monitorizarea autorizării pentru noile obiecte

OS/400 furnizează funcţii pentru a vă ajuta să gestionaţi autorizarea şi proprietarul pentru noile obiecte de pe sistemul dumneavoastră. Când un utilizator creează un nou obiect, sistemul determină următoarele:

- Cine va fi proprietarul obiectului
- Care este autorizarea publică pentru obiect
- Dacă are vreo autorizare privată
- Unde să plaseze obiectul (ce bibliotecă sau director)
- Dacă accesul la obiect va fi verificat

Sistemul foloseşte variabile de sistem, parametri bibliotecă şi parametri profil utilizator pentru a lua aceste decizii. “Asocierea autorizării şi proprietarului pentru obiectele noi ” în capitolul 5 al cărţii *Referinţă securitate iSeries* furnizează câteva exemple ale opţiunilor care sunt disponibile.

Puteţi folosi comanda PRTUSRPRF pentru a tipări parametrii profil utilizator care influenţează proprietarul şi autorizarea pentru obiectele noi. Figura 5 la pagina 56 arată un exemplu al acestui raport.

Gestionarea listelor de autorizare

Puteţi grupa obiectele cu cereri similare de securitate utilizând o listă autorizări. Conceptual, o listă de autorizări conţine o listă de utilizatori şi autorizările pe care utilizatorii le au asupra obiectelor care sunt securizate de listă. Listele de autorizări furnizează o cale eficientă de a gestiona autorizarea obiectelor similare ale sistemului. Totuşi, în unele cazuri, fac dificilă urmărirea autorizărilor obiectelor.

Puteţi utiliza comanda Tipărire autorizări private (PRTPVTAUT) pentru a tipări informaţiile despre autorizările listei autorizări. Figura 3 arată un exemplu al raportului.

```
                        Autorizări private (Raport complet)
SYSTEM4
Listă                    Grup                              Listă  ----------Obiect----------  ------------Date------------
autorizare  Proprietar   principal   Utilizator  Autorizare Mgt   Opr  Mgt  Exist  Alter  Ref  Read  Add  Upd  Dlt  Execute
LIST1       QSECOFR      *NONE       *PUBLIC     *EXCLUDE
LIST2       BUDNIKR      *NONE       BUDNIKR     *ALL        X     X    X     X      X     X    X     X    X    X      X
                                     *PUBLIC     *CHANGE           X                              X     X    X    X      X
LIST3       QSECOFR      *NONE       *PUBLIC     *EXCLUDE
LIST4       CJWLDR       *NONE       CJWLDR      *ALL        X     X    X     X      X     X    X     X    X    X      X
                                     GROUP1      *ALL              X    X     X      X     X    X     X    X    X      X
                                     *PUBLIC     *EXCLUDE
```

Figura 3. Raport autorizări private pentru liste autorizări

Acest raport arată aceleaşi informaţii pe care le vedeţi la ecranul Editare listă autorizări (EDTAUTL). Avantajul raportului este că furnizează informaţii despre toate listele de autorizări într-un singur loc. Dacă setaţi securitatea pentru un nou grup de obiecte, de exemplu, puteţi consulta rapid raportul pentru a vedea dacă o listă de autorizări existentă vă satisface nevoile pentru aceste obiecte.

Puteţi tipări o versiune cu modificări a raportului pentru a vedea noile liste de autorizări cu modificările de autorizare de la ultimul raport tipărit. Aveţi, de asemenea, opţiunea de a tipări o listă a obiectelor securizate de fiecare listă de autorizări. Figura 4 la pagina 53 arată un exemplu de raport pentru o listă de autorizări:

```
                    Afişare obiecte listă autorizări
Listă autorizare . . . . . :   CUSTAUTL
Bibliotecă . . . . . :     QSYS
Proprietar . . . . . :   AROWNER
Grup principal  . . . . . :   *NONE

                                                        Grup
Obiect       Bibliotecă       Tip        Proprietar     principal      Text
CUSTMAS        CUSTLIB       *FILE        AROWNER       *NONE
CUSTORD        CUSTORD       *FILE        OEOWNER       *NONE
```

Figura 4. Raportul afişare obiecte listă de autorizări

Puteţi utiliza acest raport, de exemplu, pentru a înţelege efectele adăugării unui nou utilizator la o listă de autorizări (ce autorizări va primi utilizatorul).

Folosirea listelor de autorizare

Navigator iSeries furnizează caracteristici de securitate proiectate să vă ajute în dezvoltarea unui plan de securitate şi a unei politici şi să configuraţi sistemul dumneavoastră pentru a îndeplini nevoile companiei dumneavoastră. Una dintre funcţiile disponibile este folosirea listelor de autorizare.

Listele de autorizare au următoarele facilităţi.

- O listă de autorizare grupează obiecte care au cerinţe similare în ceea ce priveşte securitatea.
- O listă de autorizare conţine în mod conceptual o listă a utilizatorilor şi grupurilor ca şi a autorizărilor pe care le are fiecare dintre obiectele asigurate de listă.
- Fiecare utilizator şi grup pot avea o altă autorizare pentru setul de obiecte pe care le asigură lista.
- Autorizarea poate fi dată după tipul listei, mai degrabă decât pentru utilizatori şi grupuri individuale.

Task-urile ce pot fi efectuate folosindu-se listele de autorizări includ:

- Crearea unei liste de autorizare.
- Modificarea unei liste de autorizare.
- Adăugarea utilizatorilor şi grupurilor.
- Modificarea permisiunilor pentru un utilizator.
- Afişarea obiectelor sigure.

Pentru a folosi această funcţie, realizaţi paşii care urmează:

1. Din Navigator iSeries, expandaţi serverul dumneavoastră—>Securitate. Veţi vedea **Liste de autorizare** şi **Politici**.
2. Faceţi clic dreapta pe **Liste de autorizare** şi selectaţi **Listă de autorizare nouă**. **Listă nouă de autorizare** vă permite să faceţi următoarele.
   - **Folosire:** Permite accesul la atributele obiectului ca şi folosirea acestuia. Publicul poate vedea, dar nu poate modifica obiectele.
   - **Modificare:** Permite modificarea conţinului obiectului (cu câteva excepţii).
   - **Toate:** Permite efectuarea tuturor operaţiilor asupra obiectului, cu excepţia acelora care sunt permise numai proprietarului. Utilizatorul sau grupul poate controla existenţa obiectului, specifica securitatea pentru acesta, îl poate modifica şi poate efectua funcţii de bază asupra lui. Utilizatorul sau grupul poate modifica şi proprietarul obiectului.
   - **Excludere:**Toate operaţiile ce se pot efectua asupra obiectului sunt interzise. Nu este permis accesul la obiect şi nici efectuarea de operaţii pentru utilizatorii şi grupurile care au această permisiune. Specifică faptul că publicul nu are voie să folosească acest obiect.

Când se lucrează cu liste de autorizare este nevoie să se acorde permisiuni şi pentru obiecte şi pentru date. Puteţi alege dintre permisiunile pentru obiect de mai jos.

- **Operaţional:** Furnizează permisiunea de a se vedea descrierea unui obiect şi folosirea acestuia aşa cum este determinat de permisiunile pentru date pe care utilizatorul sau grupul le are pentru acest obiect.
- **Management:** Furnizează permisiunea de a se specifica securitatea pentru obiect, mutarea sau redenumirea acestuia ca şi adăugarea de membrii la fişierele bază de date.
- **Existenţă:** Furnizează permisiunea de a se controla existenţa şi proprietarul pentru obiect. Utilizatorul sau grupul poate şterge obiectul, elibera memoria acestuia şi poate efectua operaţii de salvare sau restaurare ca şi de transferare a proprietăţii pentru obiect. Dacă utilizatorul sau grupul are permisiune specială de salvare, acesta nu are nevoie de permisiunea existenţă pentru obiect.
- **Alterare** (folosită numai pentru fişiere bază de date şi pachete SQL): Furnizează permisiunea necesară pentru modificarea atributelor unui obiect. Dacă utilizatorul sau grupul are această permisiune pentru un fişier bază de date, acesta poate adăuga şi înlătura declanşatori, adăuga şi elimina constrângeri de unicitate şi de referenţă ca şi modificarea atributelor fişierului bază de date. Dacă utilizatorul sau grupul are această permisiune pentru un pachet SQL, acesta poate modifica atributele pachetului SQL. Această permisiune este folosită în curent doar pentru fişierele bază de date şi pachetele SQL.
- **Referinţă** (folosită numai pentru fişiere bază de date şi pachete SQL): Furnizează permisiunea necesară pentru referenţierea unui obiect dintr-un alt obiect. Dacă utilizatorul sau grupul are această permisiune pentru un fişier fizic, acesta poate adăuga constrângeri de referenţă pentru care fişierul fizic este părinte. Această permisiune este folosită în curent doar pentru fişierele bază de date.

Puteţi alege dintre permisiunile pentru date de mai jos.

- **Citire:** Furnizează permisiunea necesară pentru obţinerea şi afişarea conţinutului unui obiect, cum ar fi vizualizarea înregistrărilor dintr-un fişier.
- **Adăugare:** Furnizează permisiunea de a se adăuga intrări într-un obiect, cum ar fi adăugarea de mesaje într-o coadă de mesaje sau adăugarea de înregistrări la un fişier.
- **Actualizare:** Furnizează permisiunea necesară pentru modificarea intrărilor într-un obiect, cum ar fi modificarea înregistrărilor dintr-un fişier.
- **Ştergere:** Furnizează permisiunea de a se elimina intrări dintr-un obiect, cum ar fi înlăturarea mesajelor dintr-o coadă de mesaje sau ştergerea înregistrărilor dintr-un fişier.
- **Execuţie:** Furnizează permisiunea necesară pentru rularea unui fişier, program serviciu sau pachet SQL. Utilizatorul poate localiza de asemenea obiectul într-o bibliotecă sau director.

Pentru informaţii suplimentare despre fiecare proces în timp ce creaţi sau editaţi listele dumneavoastră de editare, folosiţi ajutorul online disponibil în Navigator iSeries.

Accesarea politicilor în Navigator iSeries

Puteţi folosi Navigator iSeries pentru a vizualiza şi gestiona politicile pentru serverul dumneavoastră iSeries. Navigator iSeries are cinci zone de politici:

- **Politica de auditare**
  Aceasta vă permite să setaţi monitorizarea anumitor acţiuni şi accesul la anumite resurse din sistemul dumneavoastră.
- **Politica de securitate**
  Aceasta vă permite să specificaţi nivelul de securitate şi opţiunile suplimentare înrudite cu securitatea sistemului.
- **Politica de parole**
  Aceasta vă permite să specificaţi nivelul de parole pentru sistem.
- **Politică de restaurare**
  Această politică vă permite să specificaţi cum sunt restaurate anumite obiecte din sistem.

- **Politica de semnare**
  Această politică vă permite să specificaţi cum se poate înregistra utilizatorul la sistem.

Pentru a vizualiza sau modifica politicile cu Navigator iSeries, urmaţi aceşti paşi:

1. Din Navigator iSeries, expandaţi serverul dumneavoastră—>**Securitate**.
2. Faceţi clic dreapta pe **Politici** şi selectaţi **Explorare** pentru a afişa o listă de politici pe care le puteţi crea şi gestional. Consultaţi ajutorul din Navigator iSeries pentru specificaţii despre aceste politici.

Monitorizarea autorizării publice la obiecte

opţiuni meniu SECBATCH:
12 *pentru a trimite imediat* **41** *pentru a folosi planificatorul de joburi*

Puteţi folosi comanda Tipărire autorizări private (PRTPVTAUT) pentru a tipări o listă a autorizărilor private pentru obiectele de un tip specificat dintr-o bibliotecă specificată.

Puteţi folosi acest raport pentru a vă ajuta să detectaţi autorizări noi ale obiectelor. Vă poate ajuta, de asemenea, să menţineţi schema autorizărilor private clară şi gestionabilă.

Monitorizarea accesului la ieşire şi cozile de joburi

Uneori un administrator de securitate face un lucru foarte bun protejând accesul la fişiere şi apoi nu ştie ce se întâmplă când conţinutul unui fişier este tipărit. Serverele iSeries furnizează funcţii pentru a vă ajuta să protejaţi cozile de ieşire sensibile şi cozile de joburi. Protejaţi o coadă de ieşire pentru ca utilizatorii neautorizaţi să nu, de exemplu, vizualizeze sau copieze fişierele spool confidenţiale care aşteaptă să fie tipărite. Protejaţi cozile de joburi pentru ca utilizatorii neautorizaţi să nu poată nici redirecta un job confidenţial la o coadă de ieşire de neîncredere, nici opri jobul.

Opţiuni meniu SECBATCH:
24 pentru lansare imediată 63 *pentru a folosi planificatorul de joburi*

Cărţile *Securitate de bază şi planificare pentru sistem* din Centrul de informare şi *Referinţă securitate iSeries* descriu modul de protejare al cozilor dumneavoastră de ieşire şi de joburi.

Puteţi folosi comanda Tipărire autorizare coadă (PRTQAUT) pentru a tipări setăriile de securitate pentru cozile de ieşire şi de joburi de pe sistemul dumneavoastră. Puteţi apoi verifica joburile de tipărire ce tipăresc informaţii confidenţiale şi să vă asiguraţi că merg la cozile de ieşire şi de joburi protejate.

Pentru cozile de ieşire şi de joburi pe care le consideraţi a fi vulnerabile la securitate, puteţi compara setările dumneavoastră de securitate cu informaţiile din Anexa D a cărţii *Referinţă securitate iSeries*. Tabelele din Appendix D vă spun ce setări sunt cerute pentru a realiza diferite funcţii coadă de ieşire sau coadă de joburi .

Monitorizarea autorizărilor speciale

Când utilizatorii sistemului dumneavoastră au autorizări speciale nefolositoare, efortul dumneavoastră de a dezvolta o schemă bună autorizare obiect poate fi zadarnic. Autorizarea obiect este fără sens când un profil utilizator are autorizarea specială *ALLOBJ. Un utilizator cu autorizarea specială *SPLCTL poate vedea orice fişier spool de pe sistem, necontând efortul făcut de dumneavoastră pentru a securiza cozile de ieşire. Un utilizator cu autorizarea specială *JOBCTL poate influenţa operaţiile de sistem şi redirecta joburile. Un utilizator cu autorizarea specială *SERVICE poate utiliza instrumentele service pentru a accesa datele fără să treacă prin sistemul de operare.

opţiuni meniu SECBATCH:
29 pentru lansare imediată 68 *pentru a folosi planificatorul de joburi*

Puteţi utiliza comanda Tipărire profil utilizator (PRTUSRPRF) pentru a tipări informaţiile despre autorizările speciale şi clase utilizator pentru profilurile utilizator de pe sistemul dumneavoastră. Când rulaţi raportul, aveţi câteva opţiuni:
- Toate profilurile utilizator
- Profiluri utilizator cu autorizările speciale specificate
- Profiluri utilizator care au clase utilizator specifice
- Profiluri utilizator cu o neconcordanţă între clasa utilizator şi autorizările speciale.

Figura 5 arată un exemplu de raport care arată autorizările speciale pentru toate profilurile utilizator:

```
                                    Informaţii profil utilizator
  Tip raport . . . . . . . . . . :   *AUTINFO
  Selectat de  . . . . . . . . . :   *SPCAUT
  Autorizări speciale . . . . . . . . . :   *ALL
                    ------------Autorizări speciale-------------
                                *IO                                                                  Tip
Profil   Profiluri   *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  Clasă              Autorizare  autorizare  Capacitate
utilizator  grup     OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  utiliz.   Proprietar   grup        grup      limitată
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
```

Figura 5. Raportul informaţiilor utilizator: Exemplul 1

Pe lângă autorizările speciale, raportul arată următoarele:
- Dacă profilul utilizator are capabilităţi limitate.
- Dacă utilizatorul sau grupul utilizatorului deţine noi obiecte pe care utilizatorul le-a creat.
- Ce autorizare primeşte automat grupul utilizatorului pentru obiectele noi pe care le creează utilizatorul.

Figura 6 la pagina 57 arată un exemplu de raport pentru autorizările speciale nepotrivite şi clasele utilizator:

```
Informaţii profil utilizator
Tip raport . . . . . :   *AUTINFO
Selectat de  . . . . . :   *MISMATCH
--------------------------------Autorizări speciale-------------
                                *IO                                                                  Tip
Profil    Profiluri    *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  Clasă              Autorizare  autorizare  Capacitate
utilizator  grup      OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  utiliz.   Proprietar   grup        grup      limitată
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
```

Figura 6. Raportul informaţiilor utilizator: Exemplul 2

În Figura 6, observaţi următoarele:

- USERX are o clasă utilizator operator sistem (*SYSOPR), dar are autorizările speciale *ALLOBJ şi *SPLCTL.
- USERY are o clasă utilizator (*USER), dar are autorizare specială *SECADM.
- USERZ are, de asemenea, o clasă utilizator (*USER) şi autorizarea specială *SECADM. Puteţi, de asemenea, observa că USERZ este un membru al grupului QPGMR, care are autorizările speciale *JOBCTL şi *SAVSYS.

Puteţi rula aceste rapoarte regulat pentru a vă ajuta să monitorizaţi administrarea profilurilor utilizator.

Monitorizarea mediilor utilizator

Un rol al profilului utilizator este de a defini mediul pentru utilizator, inclusiv coada de ieşire, meniul iniţial şi descrierea de job. Mediul utilizatorului influenţează modul în care utilizatorul vede sistemul şi, deci, ceea ce se permite utilizatorului să facă. Utilizatorul trebuie să aibă autorizare pentru obiectele care sunt specificate în profilul utilizator. Totuşi, dacă schema dumneavoastră de autorizări nu este foarte restrictivă, mediul utilizator care este definit într-un profil utilizator poate provoca rezultate nedorite. Următoarele sunt câteva exemple:

opţiuni meniu SECBATCH:

29 *pentru a trimite imediat***68** *pentru a folosi planificatorul de joburi*

- Descrierea jobului utilizatorului poate specifica un profil utilizator care are mai multe autorizări decât utilizatorul.
- Utilizatorul poate avea un meniu iniţial care nu are linie de comandă. Totuşi, programul de tratare a tastei Attn a utilizatorului poate furniza o linie de comandă.
- Utilizatorul poate fi autorizat să ruleze rapoarte confidenţiale. Totuşi, ieşirea utilizatorului poate fi direcţionată la o coadă de mesaje care este disponibilă utilizatorilor care nu trebuie să vadă rapoartele.

Puteţi folosi opţiunea *ENVINFO a comenzii Tipărirea profilului utilizator (PRTUSRPRF) pentru a vă ajuta în monitorizarea mediilor care sunt definite pentru utilizatorii sistem. Figura 7 la pagina 58 arată un exemplu de raport:

```
                                    Informaţii profil utilizator
  Tip raport . . . . . :   *ENVINFO
  Selectare după . . . . . :   *USRCLS
                          Meniu          Program          Descriere       Coadă          Coadă           Program
Profil       Bibliotecă  iniţial/       iniţial/           job/          mesaje/        ieşire/       atenţionare/
utilizator    curentă    Bibliotecă     Bibliotecă       Bibliotecă     Bibliotecă     Bibliotecă     Bibliotecă
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
```

Figura 7. Imprimare profil utilizator-exemplu mediu utilizator

Gestionarea uneltelor de service

Uneltele service sunt folosite pentru configurarea, gestionarea şi service-ul serverului dumneavoastră. Uneltele service pot fi accesate din unelte de service dedicate (DST) sau unelte de service sistem (SST). ID-urile utilizator unelte de service sunt necesare pentru a accesa DST, SST şi pentru a folosi funcţiile Navigator iSeries pentru gestionarea partiţiei logice (LPAR) şi gestionarea unităţii de disc.

DST este disponibil când Codul intern licenţiat a fost pornit, chiar dacăOS/400 nu a fost încărcat. SST este disponibil de laOS/400. Următoarea tabelă evidenţiază diferenţele de bază între DST şi SST.

Caracteristică	DST	SST
Modul de acces	Accesul fizic prin consolă în timpul unui IPL manual sau selectând opţiunea 21 din panoul de control.	Accesul prin job interactiv cu posibilitatea de semnare cu QSRV sau cu următoarele autorizări: • Autorizare la comanda CL STRSST (Start SST - Pornire SST). • Autorizare specială service (*SERVICE) sau autorizare specială pentru toate obiectele (*ALLOBJ). • Posibilitate funcţională de folosire SST.
Când este disponibil	Disponibil chiar şi atunci când serverul a limitat capacităţile. OS/400 nu este necesar pentru a accesa DST.	Disponibil cândOS/400 a fost pornit. OS/400 este necesar pentru a accesa SST.
Cum se face autentificarea	Necesită ID utilizator unelte de service şi parolă.	Necesită ID utilizator unelte de service şi parolă.

ConsultaţiiSeries Centrul de informare—>Securitate—>Unelte de service pentru informaţii despre utilizarea uneltelor de service pentru a realiza următoarele operaţii:

- Accesarea uneltelor de service cu DST
- Accesarea uneltelor de service cu SST
- Accesarea uneltelor de service cu Navigator iSeries
- Crearea unui ID utilizator pentru unelte de service
- Modificarea avantajelor unui profil utilizator pentru unelte de service

- Modificarea descrierii unui ID utilizator pentru unelte de service
- Afişarea unui ID utilizator pentru unelte de service
- Activarea sau dezactivarea unui ID utilizator pentru unelte de service
- Ştergerea unui ID utilizator pentru unelte de service
- Modificrea ID-urilor utilizator şi a parolelor pentru unelte de service folosind SST sau DST
- Modificarea parolei ID-ului utilizator pentru unelte de service folosind STRSST
- Modificarea ID-urilor utilizator şi a parolelor pentru unelte de service folosind
- API-ul QSYCHGDS (Change Service Tools User ID - Modificare ID utilizator pentru unelte de service)
- Resetarea parolei profilului utilizator QSECOFR OS/400
- Resetarea uneltelor de service QSECOFR ID utilizator şi parolă
- Salvarea datelor de securitate pentru unelte de service. Restaurarea datelor de securitate pentru unelte de service
- Crearea propriei dumneavoastră versiuni de ID utilizator pentru unelte de service QSECOFR
- Configurarea serverului de unelte servie pentru DST
- Configurarea serverului de unelte de service pentruOS/400
- Funcţia de monitorizare service folosită prin DST
- Monitorizarea uneltelor de service prin istoricul de auditare securitate OS/400

Consultaţi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru informaţii despre accesarea Centrului de informare iSeries.

Capitolul 7. Folosirea securităţii partiţiilor logice (LPAR)

Având mai multe partiţii logice pe un singur server iSeries ar putea avea beneficii in următoarele scenarii:

- **Menţinerea sistemelor independente**: Dedicarea unei porţiuni din resurse (unitatea de stocare disc, procesoare, memorie şi dispozitive I/O) unei partiţii realizează o izolare logică a software-ului. De asemenea, dacă sunt configurate corect, partiţiile logice au câteva toleranţe la greşeli hardware. E posibil ca încărcăturile de lucru interactive şi batch care nu rulează bine împreună pe o singură maşină, să fie izolate şi să ruleze eficient pe partiţii separate.
- **Consolidare** : Un sitem partiţionat logic poate reduce numărul sistemelor server iSeries de care este nevoie într-o întreprindere. Puteţi consolida câteva sisteme într-un singur sistem partiţiont logic. Acest lucru elimină necesitatea cheltuielilor pentru echipament adiţional. Puteţi muta resurse de pe o partiţe logică pe alta, după cum se schimbă necesităţile.
- **Crearea unei producţii mixte şi testarea mediului:** Puteţi crea o combinaţie de producţie şi testa mediul. Puteţi crea o partiţie cu o singură producţie pe partiţia primară. Pentru partiţii cu producţii multiple, vezi *Crearea unui mediu cu partiţii cu producţii multiple* mai jos.

  O partiţie logică este fie o partiţie test fie de producţie. O partiţie de producţie rulează principalele dumneavoastră aplicaţii de afaceri. O cădere în partiţia de producţie poate dăuna semnificativ afacerii dumneavoastră şi să vă coste timp şi bani. O partiţie test testează software. Un eşec într-o partiţie de test, dacă nu este planificat, nu va încurca operaţiile de afaceri normale.
- **Crearea unui mediu de partiţionare a producţie multiplu:** Ar trebui să creaţi partiţii de producţie multiple doar în partiţiile dumneavoastră secundare. În această situaţie, trebuie să dedicaţi partiţia primară managementului de partiţii.
- **Copie de siguranţă imediată:** Când o partiţie secundară copie pe o altă partiţie logică în acelaşi sistem, comutarea pe copia de siguranţă în timpul erorii de partiţie poate cauya inconveniente minime. Această configuraţie minimizează de asemenea efectul ferestrelor lungi de salvare. Puteţi pune partiţia de backup off line, atâta vreme cât cealaltă partiţie logică continuă să efectueze lucru de producţie. Veţi avea nevoie de software special pentru a folosi această strategie de hot backup.
- **Cluster integrat:** Folosind OptiConnect/400 şi software de aplicaţii de disponibilitate ridicată, sistemul dumneavoastră partiţionat poate rula ca un cluster integrat. Puteţi folosi un cluster integrat pentru a vă proteja sistemul de căderile cele mai neplanificate cu o partiţie secundară.

Notă: Când setaţi o partiţie secundară, trebuie să faceţi consideraţii adiţionale pentru locaţiile plăcilor. Dacă procesorul Intrarae/Ieşire (IOP) pe care l-aţi selectat pentru consolă are de asemenea placă LAN şi placa LAN nu este intenţionată pentru folosire cu Consolă de operaţii, ca fi activat,pentru folosire de către consolă şi se poate să nu puteţi să-l folosiţi pentru scopurile intenţionate de dumneavoastră. Pentru mai multe informaţii depre lucrul cu Consolă de operaţii, vezi Capitolul 8, “Consolă de operaţii iSeries”, la pagina 63.

Vezi ″Partiţii Logice″ în Centru de informare iSeriespentru informaţii mai detaliate despre acest subiect.

Gestionarea securităţii pentru partiţiile logice

Sarcinile legate de securitate pe care le efectuaţi pe un sistem partiţionat, sunt aceleaţi ca şi pe sistemul fără partiţii logice. Oricum, când creaţi partiţii logice, lucraţi cu mai mult de un sistem independent. De aceea, va trebui să efectuaţi aceleaşi sarcini pe fiecare partiţie logică în loc de o singură dată pe un sistem fără partiţii logice.

Iată câteva reguli de bază pentru situaţiile în care avem de a face cu securitatea partiţiilor logice:

- Adăugaţi utilizatori la sistem pe fiecare partiţie logică pe rând. Trebuie să adăugaţi utilizatori la fiecare partiţie logică pe care doriţi să o poată accesa.
- Limitaţi numărul de persoane ce au dreptul de a folosi unelte de service dedicate (dedicated service tools (DST)) şi unelte de service sistem (system service tools (SST)) pe partiţia primară. Vedeţi subiectul ″Gestionarea partiţiilor logice folosind Navigator iSeries, DST şi SST″ din Centru de informare iSeries pentru mai multe informaţii despre DST şi SST. Vezi “Gestionarea uneltelor de service” la pagina 58 pentru informaţii despre folosirea profilurilor de utilizator unelte de service pentru a controla accesul la activităţile partiţiilor.

  Notă: Trebuie să iniţializaţi STS (Service Tools Server) înainte de a folosi Navigator iSeries pentru a accesa funcţiile LPAR. Consultaţi iSeries Centrul de informare —>Securitate—>Unelte de service pentru informaţii înrudite. Consultaţi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru informaţii despre accesarea Centrului de informareiSeries.
- Partiţiile secundare nu pot vedea sau folosi memoria principală şi unităţile de disc ale altor partiţii logice.
- Partiţiile secundare pot vedea doar propriile lor resurse hardware.
- Partiţia primară poate vedea toate resursele hardware în ecranele Lucrul cu partiţiile sistemului din DST şi SST.
- Sistemul de operare al partiţiei primare poate vedea doar resursele sale disponibile.
- Panoul de control al sistemului, controlează partiţia primară. Când setaţi modul panou pe Sigur, nu pot fi efectuate acţiuni în ecranul Lucru cu Starea Partiţiilor din SST. Pentru a forţa DST din panoul de control al sistemului, trebuie să schimbaţi modul în Manual.
- Când setaţi modul de operare al partiţiei secundare pe Sigur, restricţionaţi utilizarea Lucrului său cu Starea Partiţiei în următoarele moduri:
  - Puteţi folosi doar DST pe partiţia secundară pentru a schimba starea partiţiei; nu puteţi folosi SSt pentru a schimba starea partiţiei.
  - Puteţi doar forţa DST pe partiţia secundară, de pe ecranul Lucrul cu Starea Partiţiei al partiţiei primare, folosind fie DST, fie SST.
  - Puteţi folosi doar DST pe partiţia secundară pentru a schimba modul unei partiţii secundare din Sigur în orice altă valoare.

Odată ce modul unei partiţii secundare numai este sigur, puteţi folosi atât DST, cât şi SST pe partiţia secundară pentru a schimba starea partiţiei.

Pentru informaţii suplimentare despre securitatea pe serverul dumneavoastră iSeries, faceţi referire la cartea Referinţe de securitate şi la paginile de planificare şi securitate sistem de bază ale Centru de informare iSeries.

Capitolul 8. Consolă de operaţii iSeries

Consolă de operaţii vă permite să folosiţi PC-ul dumneavoastră pentru a accesa şi controla serverul dumneavoastră iSeries. Consola de operaţii include suport pentru dial-in PC la distanţă pe un server iSeries fără dispozitive consolă, permiţând PC-urilor de la distanţă să devină console. Când folosiţi Consolă de operaţii, notaţi următoarele:

- Puteţi rula orice task pe care îl puteaţi rula dintr-o consolă obinşnuită din Consolă de operaţii. De exemplu, profilurile utilizatorilor care au autorizările speciale *SERVICE sau *ALLOBJ sunt capabile să se conecteze la Consolă de operaţii sesiunea, chiar dacă ele sunt dezactivate.
- Consolă de operaţii foloseşte profiluri utilizator Unelte de service şi parole pentru a activa conexiunea la serverul iSeries. Acesta face să aibă o deosebită importanţă schimbarea profilului utilizator de Unelte de service şi a parolelor. Hacker-ii sunt familiarizaţi cu id-urile utilizator şi parolele implicite ale Uneltelor de service pentru profilurile utilizator şi le-ar putea folosi pentru a încerca o sesiune consolă la distanţă pe serverul dumneavoastră iSeries. Vezi “Modificarea parolelor cunoscute” la pagina 18 şi “Evitarea parolelor implicite” la pagina 23 pentru sugestii privind parolele.
- Pentru protejarea informaţiei când folosiţi Consolă de la distanţă, folosiţi opţiunea apel înapoi (call back) din Windows Dial-Up Networking .
- Când setaţi o partiţie secundară, trebuie să faceţi consideraţii adiţionale pentru locaţiile plăcilor. Dacă procesorul de I/E (IOP) pe care l-aţi selectat pentru consolă are de asemenea o placă LAN şi placa LAN nu este intenţionată pentru folosire cu Consolă de operaţii, ea fi activată pentru folosire de către consolă şi se poate să nu puteţi să o folosiţi pentru scopurile intenţionate de dumneavoastră.

În V5R1, Consolă de operaţii a fost îmbunătăţită pentru a permite ca activităţile din consolă să fie executate într-o reţea locală (LAN). Autentificarea sporită şi criptarea datelor furnizează securitatea reţelei pentru procedurile din consolă. La folosirea Consolă de operaţii cu conectivitate LAN , este recomandată instalarea următoarelor produse:

- Cryptographic Access Provider, 5722–AC2 sau 5722–AC3 pe serverul dumneavoastră iSeries
- Client Encryption, 5722–CE2 sau 5722–CE3 pe Consolă de operaţii PC

Pentru a cripta datele de la consolă, serverul iSeries trebuie să aibă unul din produsele Furnizor de acces criptografic instalat **şi** PC-ul trebuie să aibă instalat unul din produsele Criptare client.

Notă: Dacă nu este instalat nici un produs de criptare, nu va avea loc nici o criptare a datelor.

Tabelul următor rezumă rezultatele criptării pentru produsele disponibile:

Tabela 13. Rezultatele criptării

Furnizor de acces criptografic pentru serverul dumneavoastră iSeries	**Criptarea Client pe Consolă de operaţii PC**	**Date criptate rezultate**
Nimic	Nimic	Nimic
5722–AC2	5722–CE2	56 bit
5722–AC2	5722–CE3	56 bit
5722–AC3	5722–CE2	56 bit
5722–AC3	5722–CE3	128 bit

Pentru informaţii suplimentare despre setarea şi administrareaiSeries Consolă de operaţii, consultaţi Centrul de informareiSeries.

Privire generală asupra securităţii Consolă de operaţii

Consolă de operaţii securitatea constă în:

- autentificarea dispozitivului consolă
- autentificarea utilizatorului
- intimitatea datelor
- integritatea datelor

Consolă de operaţii cu conectare directă are implicite autentificarea dispozitivului, intimitatea datelor şi integritatea datelor datorită conexiunii sale punct-la-punct. Securitatea autentificării utilizatorului este necesară pentru conectarea la consolă.

Autentificare dispozitiv consolă

Autentificarea dispozitivului consolă asigură care dispozitiv fizic este consola. Consolă de operaţii cu conectare directă foloseşte o legăturră fizică similară cu cea a consolei twinax. Consolă de operaţii folosind o legătură directă poate fi securizată fizic similar cu cea a legăturii twinax pentru a controla accesul la dispozitivul consolă fizic.

Consolă de operaţii cu conectivitate LAN utilizează o versiune de SSL care suportă autentificarea utilizatorilor şi a dispozitivelor, dar nu foloseşte certificarea. Pentru această formă de conectare, autentificarea dispozitivului se bazează pe profilul unui dispozitiv de unelte de service. Recurgeţi la 65 pentru detalii.

Autentificare utilizator

Autentificarea utilizatorului furnizează garanţia despre cine foloseşte dispozitivul consolă. Problemele referitoare la autentificarea utilizatorului sunt aceleaşi indiferent de tipul consolei.

Confidenţialitatea datelor

Intimitatea datelor produce încrederea că datele consolei pot fi numai citite de recipientul intenţionat. Consolă de operaţii cu conectivitate directă foloseşte o conexiune fizică similară cu cea a consolei twinax sau o conexiune reţea sigură pentru conectivitate LAN pentru protecţia datelor consolei. Consolă de operaţii folosirea unei conexiuni directe furnizează o intimitate a datelor identică cu cea dintr-o conexiune twinax. Dacă legătura fizică este sigură, datele consolei rămân protejate.

Consolă de operaţii cu conectivitate LAN foloseşte o conexiune reţea sigură dacă produsele de criptare corespunzătoare sunt instalate (ACx şi CEx). Sesiunea consolă foloseşte cea mai puternică criptare posibilă în funcţie de produsele de criptare instalate pe serveruliSeries şi de PC-ul pe care rulează Consola de operaţii.

Notă: Dacă nu este instalat nici un produs de criptare, nu va avea loc nici o criptare a datelor.

Integritatea datelor

Integritatea datelor furnizează garanţia că datele consolei nu s-au schimbat în drum spre destinaţie. Consolă de operaţii cu conectivitate directă foloseşte o conexiune fizică similară cu cea a consolei twinax sau o conexiune reţea sigură pentru conectivitate LAN pentru protecţia

datelor consolei. Consolă de operaţii folosirea unei conexiuni directe furnizează o intimitate a datelor identică cu cea dintr-o conexiune twinax. Dacă legătura fizică este sigură, datele consolei rămân protejate.

Consolă de operaţii cu conectivitate LAN foloseşte o conexiune reţea sigură dacă produsele de criptare corespunzătoare sunt instalate (ACx şi CEx). Sesiunea consolă foloseşte cea mai puternică criptare posibilă în funcţie de produsele de criptare instalate pe serveruliSeries şi de PC-ul pe care rulează Consola de operaţii.

Notă: Dacă nu este instalat nici un produs de criptare, nu va avea loc nici o criptare a datelor.

Folosire Consolă de operaţii cu conectivitate LAN

Notă: Orice Consolă de operaţii poate fi o consolă, dar numai configuraţiile bazate pe LAN folosesc profilul utilizator unelte sevice.

Serverul iSeries este livrat împreună cu un profil dispozitiv de unelte de service implicit QCONSOLE cu parola implicită QCONSOLE. Consolă de operaţii cu conectivitate LAN va schimba parola în timpul fiecărei conexiuni reuşite. Vezi “Folosirea vrăjitorului de setare Consolă de operaţii” pentru mai multe informaţii.

Pentru informaţii suplimentare despre Consolă de operaţii cu conectivitate LAN iSeries, faceţi referire la subiectul Configurarea consolei de operaţii cu conectivitate LAN, în Centrul de informare.

Protecţie Consolă de operaţii cu conectivitate LAN

La folosirea Consolă de operaţii cu conectivitate LAN , sunt recomandate următoarele:

- Creaţi un alt profil dispozitiv unelte de service cu atributele consolei şi salvaţi informaţiile profilului într-un loc sigur.
- Instalaţi furnizorul de acces criptografic, 5722–AC2 sau 5722–AC3 pe serverul dumneavoastră iSeries şi Criptare client, 5722–CE2 sau 5722–CE3 pe PC-ul dumneavoastră Consolă de operaţii.
- Alegeţi o parolă pentru informaţia dispozitivului service.
- Protejaţi Consolă de operaţii PC în acelaşi fel în care aţi proteja consola twinax sau un Consolă de operaţii cu conectivitate directă.

Folosirea vrăjitorului de setare Consolă de operaţii

Vrăjitorul de setare va adăuga informaţiile necesare PC-ului la folosirea Consolă de operaţii cu conectivitate LAN . Vrăjitorul de setare cere profilul dispozitivului unelte de service, parola profilului dispozitivului unelte de service şi o parolă pentru protecţia informaţiei profilului dispozitivului unelte de service .

Notă: Parola informaţiei profilului dispozitivului de unelte de service este folosită pentru blocarea şi deblocarea informaţiei profilului dispozitivului unelte de service (profil dispozitiv unelte de service şi parole) pe PC.

La stabilirea unei conexiuni în reţea, vrăjitorul de setare din Consolă de operaţii vă va cere parola informaţiei dispozitivului service pentru pentru accesarea profilului dispozitiv unelte de service şi a parolei criptate. Vi se va cere de asemenea un identificator de utilizator unelte de service valid şi o parolă .

Capitolul 9. Detectarea programelor suspecte

Tendinţele recente în folosirea calculatoarelor au crescut instabilitatea deoarece sistemele au programe de la surse nesigure sau programe care realizează funcţii necunoscute. Următoarele sunt exemple:

- Un utilizator de calculator personal obţine uneori programe de la alţi utilizatori de PC. Dacă PC-ul este ataşat la sistemul dumneavoastră iSeries, acel program poate afecta serverul dumneavoastră iSeries.
- Utilizatorii care se conectează la reţele pot, de asemenea, să obţină programe, de la bulletin board-uri.
- Hacker-ii au devenit mai activi şi renumiţi. De multe ori îşi publică metodele şi rezultatele. Aceasta poate conduce la imitarea de către programatorii care respectau legile.

Aceste tendinţe au condus la o nouă problemă de securitate a calculatoarelor numită **viruşi de calculatoare**. Un virus este un program care modifică alte programe pentru a-şi include o copie proprie. Apoi celelalte programe se spune că sunt infectate de virus. În plus, virusul poate realiza alte operaţii care utilizează resursele sistemului sau distruge datele.

Arhitectura serverului iSeries furnizează unele protecţii la caracteristicile de infecţie ale unui virus de calculator. “Protecţie împotriva viruşilor de calculator” descrie aceasta. Un administrator de securitate al serverului iSeries trebuie să fie mult mai atent la programe care realizează funcţii neautorizate. Subiectele din acest capitol descriu modalităţi prin care cineva cu intenţii rele poate seta programe dăunătoare să ruleze pe sistemul dumneavoastră. Subiectele furnizează sfaturi pentru împiedicarea programelor de la executarea funcţiilor neautorizate.

Indiciu de securitate

Autorizarea obiectelor este întotdeauna prima linie de apărare. Dacă nu aveţi un plan bun de protejare a obiectelor dumneavoastră, sistemul dumneavoastră este fără apărare. Aceste informaţii descriu modalităţile pe care un utilizator autorizat ar trebui să le încerce pentru a beneficia de legăturile din schema dumneavoastră de autorizare obiecte.

Protecţie împotriva viruşilor de calculator

Un calculator care este infectat cu un virus are un program care poate modifica alte programe. Arhitectura de bază obiect pentru iSeries face mai dificilă producerea şi răspândirea de către răuvoitori a acestui tip de virus decât este pentru arhitecturile celorlalte calculatoare. Pe serverul iSeries, folosiţi anumite comenzi şi instrucţiuni pentru a lucra pe fiecare tip de obiecte. Nu puteţi folosi un fişier instrucţiuni pentru a modifica un obiect program operabil (care este ceea ce un creator de viruşi face de regulă). Nici nu puteţi crea cu uşurinţă un program care să modifice alt obiect program. Pentru a face aceasta se cere un timp considerabil, efort şi cunoştinţe tehnice şi cere accesul la instrumente şi documentaţii care nu sunt, în general, disponibile.

Totuşi, cum noile funcţii ale serverului iSeries devin disponibile pentru a participa în contextul sistemelor deschise, unele din funcţiile de protecţie bazate obiect ale serverelor iSeries nu se mai aplică în continuare. De exemplu, folosind Sistem de fişiere integrat (IFS), utilizatorii pot manipula direct unele obiecte în directoare, cum ar fi fişierele stream.

De asemenea, chiar dacă arhitectura serverului iSeries îngreunează desfăşurarea unui virus în cadrul programelor server iSeries, arhitectura lui nu împiedică serverul iSeries de la a fi purtător de virus. Ca server de fişiere, serverul iSeries poate stoca programe care sunt partajate de mai multe PC-uri. Oricare din aceste programe poate conţine un virus pe care serverul iSeries nu îl detectează. Pentru a împiedica infectarea cu acest tip de virus a PC-urilor care sunt ataşate la serverul dumneavoastră iSeries, trebuie să folosiţi software de scanare viruşi pentru PC.

Mai multe funcţii există pe serverul iSeries pentru a preveni pe cineva care foloseşte un limbaj de nivel scăzut cu posibilităţi de folosire a pointer-ilor să altereze un program obiect operabil:

- Dacă sistemul dumneavoastră rulează la nivelul de securitate 40 sau mai mult, protecţia integrităţii include protecţiile împotriva modificării obiectelor program. De exemplu, nu puteţi rula cu succes un program care conţine instrucţiuni maşină blocate (protejate).
- Valoarea de validare a programului este de asemenea protejată când restauraţi un program care a fost salvat (şi probabil modificat) pe alt sistem. Capitolul 2 din cartea *Referinţă securitate iSeries* descrie funcţiile de protecţie a integrităţii pentru nivelul de securitate 40 şi mai mare, inclusiv valorile de validare program.

  Notă: Valoarea de validare program nu este sigură şi nu este o înlocuire pentru vigilenţa în evaluarea programelor care sunt restaurate pe sistemul dumneavoastră.

Câteva instrumente sunt, de asemenea, disponibile pentru a vă ajuta să detectaţi începutul unui program modificat de pe sistemul dumneavoastră:

- Puteţi utiliza comanda Verificare integritate obiect (CHKOBJITG) pentru a scana obiectele (operabile) care corespund cu valorile căutate de dumneavoastră pentru a vă asigura că aceste obiecte nu au fost modificate. Aceasta este similară cu funcţia de scanare viruşi.
- Puteţi utiliza funcţia de verificare a securităţii pentru a monitoriza programele care au fost modificate sau restaurate. Valorile *PGMFAIL, *SAVRST şi *SECURITY pentru variabila de sistem a nivelului de autorizare furnizează înregistrări de verificare care vă pot ajuta să detectaţi încercările de introducere a programelor tip virus pe sistemul dumneavoastră. Capitolul 9 şi Anexa F din cartea *Referinţă securitate iSeries* furnizează mai multe informaţii despre valorile de auditare şi intrările în jurnalul de auditare.
- Puteţi utiliza parametrul de forţare creare (FRCCRT) al comenzii Modificare program (CHGPGM) pentru recrearea oricărui program care a fost restaurat pe sistemul dumneavoastră. Sistemul utilizează şablonul program pentru a recrea programul. Dacă obiectul program a fost modificat după ce a fost compilat, sistemul recrează obiectul modificat şi-l înlocuieşte. Dacă şablonul program conţine instrucţiuni blocate (protejate), sistemul nu va recrea programul cu succes.
- Puteţi folosi valoarea sistem QFRCCVNRST (forţare conversie la restaurare) pentru a recrea orice program imediat ce este restaurat pe sistemul dumneavoastră. Sistemul foloseşte şablonul program pentru a recrea programul. Această valoare sistem furnizează mai multe posibilităţi după care programele vor fi recreate.
- Puteţi utiliza valoarea sistem QVFYOBJRST (Verificare Obiecte în refacere) pentru a preveni refacerea programe care nu dispun de semnătură digitală sau care nu au semnătură digitală validă. Dacă o semnătură digitală nu este validă înseamnă că programul a fost modificat de când a fost semnat de producător . Ieşirea API-urilor vă permite semnarea programelor, salvarea fişierelor şi a fişierelor stream.

Pentru mai multe informaţii privind semnarea şi modul de protejarea sistemului împotriva riscurilor, vezi “Semnarea obiectelor” la pagina 78.

Utilizarea monitorului autorizării adoptate

Pe un server iSeries, puteţi crea un program care adoptă autorizarea proprietarului programului. Aceasta înseamnă că orice utilizator care rulează programul are aceleaşi autorizări (private şi speciale) ca şi profilul utilizator al proprietarului programului.

Autorizarea adoptată este un instrument de securitate valoros când este folosit corect. “Îmbunătăţirea meniului de control al accesului cu securitate obiect” la pagina 42, de exemplu, descrie cum să combinaţi autorizările adoptate şi meniurile pentru a vă ajuta să depăşiţi controlul acces meniu. Puteţi utiliza autorizările adoptate pentru a vă proteja fişierele importante împotriva modificărilor din afara programelor dumneavoastră aplicaţii aprobate atâta timp cât permiteţi încă cererile la fişiere.

Ca administrator de securitate, trebuie să vă asiguraţi că autorizările adoptate sunt folosite corect:

- Programele trebuie să adopte autorizările unui profil utilizator care are autorizări suficiente pentru a face funcţiile necesare, dar nu mai mult. Trebuie să fiţi precaut cu programele care adoptă autorizările unui profil utilizator care fie are autorizarea specială *ALLOBJ, fie deţine obiecte importante.
- Programele care adoptă autorizare trebuie să aibă o funcţie specifică, limitată şi nu trebuie să furnizeze facilităţi de intrare comandă.
- Programele care adoptă autorizare trebuie să fie securizate corespunzător.
- Utilizarea excesivă a autorizării adoptate poate avea un impact negativ asupra performanţei sistemului dumneavoastră. Pentru a vă ajuta să evitaţi problemele de securitate, revedeţi graficele de verificare a autorizării şi sugestiile pentru utilizarea autorizării adoptate din capitolul 5 al cărţii *Referinţă securitate iSeries*.

opţiuni meniu SECBATCH:
1 *pentru lansare imediată* , **40 pentru a folosi planificatorul de joburi**

Puteţi utiliza comanda Tipărire obiecte adoptate (PRTADPOBJ) (opţiunea 21 a meniului SECTOOLS) pentru a monitoriza folosirea autorizărilor adoptate pe sistemul dumneavoastră.

Raportul afişează autorizările speciale ale profilului utilizator specificat, programele care adoptă autorizarea profilului utilizator, ca şi dispozitivele ASP care folosesc autorizările profilului. După ce aţi stabilit o bază de informaţii, puteţi tipări regulat versiunea cu modificări a raportului obiecte adoptate. Listează noile programe care adoptă autorizare şi programele care au fost modificate să adopte autorizare de la ultima tipărire a raportului.

Dacă suspectaţi faptul că autorizarea adoptată este folosită incorect pe sistemul dumneavoastră, puteţi seta variabila de sistem QAUDLVL să includă *PGMADP. Când această valoare este activă, sistemul creează o intrare jurnal verificare oricând cineva porneşte sau opreşte un program care adoptă autorizare. Intrarea include numele utilizatorului care porneşte programul şi numele programului.

Limitarea folosirii autorizării adoptate

Când un program iSeries rulează, el poate utiliza autorizare adoptată pentru a câştiga accesul la obiecte prin două moduri diferite:

- Programul însuşi poate adopta autorizarea proprietarului său. Aceasta este specificată în parametrul profil utilizator (USRPRF) al programului sau programului serviciu.

- Programul poate utiliza (moşteni) autorizarea adoptată de la un program anterior care se mai află încă în stiva de apeluri joburi. Un program poate moşteni autorizarea adoptată de la programele anterioare chiar dacă programul însuşi nu adoptă autorizare. Utilizarea parametrului autorizare adoptată (USEADPAUT) a unui program sau program serviciu controlează dacă programul moşteneşte autorizare adoptată de la programele anterioare din stiva de programe.

Următorul este un exemplu de folosire autorizarea adoptată de la programele anterioare.

Presupuneţi că profilul utilizator ICOWNER are autorizare *CHANGE pentru fişierul ITEM şi că autorizarea publică a fişierului ITEM este *USE. Nici un alt profil utilizator nu are nici o autorizare definită explicit pentru fişierul ITEM. Tabela 14 arată atributele pentru trei programe care folosesc fişierul ITEM:

Tabela 14. Folosire autorizare adoptată (USEADPAUT) - Exemplu

Nume program	Proprietar program	Valoarea USRPRF	Valoarea USEADPAUT
PGMA	ICOWNER	*OWNER	*YES
PGMB	ICOWNER	*USER	*YES
PGMC	ICOWNER	*USER	*NO

Exemplul 1 – Autorizare adoptată:
1. USERA rulează programul PGMA.
2. Programul PGMA încearcă să deschidă fişierul ITEM cu facilităţi de actualizare.

Rezultat: Încercare cu succes. USERA are acces *CHANGE la fişierul ITEM deoarece PGMA adoptă autorizarea de la ICOWNER.

Exemplul 2 – Utilizarea autorizării adoptate:
1. USERA rulează programul PGMA.
2. Programul PGMA apelează programul PGMB.
3. Programul PGMB încearcă să deschidă fişierul ITEM cu facilităţi de actualizare.

Rezultat: Încercare cu succes. Deşi programul PGMB nu adoptă autorizare (*USRPRF este *USER), permite utilizarea autorizării adoptate anterior (*USEADPAUT este *YES). Programul PGMA se află încă în stiva de programe. În consecinţă, USERA are accesul *CHANGE la fişierul ITEM deoarece PGMA adoptă autorizarea de la ICOWNER.

Exemplul 3 – Neutilizarea autorizării adoptate
1. USERA rulează programul PGMA.
2. Programul PGMA apelează programul PGMC.
3. Programul PGMC încearcă să deschidă fişierul ITEM cu facilităţi de actualizare.

Rezultat: Eşec de autorizare. Programul PGMC nu adoptă autorizare. Programul PGMC nu permite, de asemenea, folosirea autorizării adoptate de la programele anterioare. În consecinţă, PGMA se găseşte încă în stiva de apeluri, autorizarea sa adoptată nu este folosită.

Împiedicarea noilor programe de la folosirea autorizării adoptate

Trecerea autorizării adoptate către programele mai noi din stivă furnizează o oportunitate pentru un programator cunoscător să creeze un program Cal troian. Programul Cal troian se poate baza pe programele anterioare din stivă pentru a prelua autorizarea necesară pentru a realiza stricăciuni. Pentru a împiedica aceasta, puteţi limita care utilizatori să creeze programe care folosesc autorizarea adoptată a programelor anterioare.

Când creaţi un nou program, sistemul setează automat parametrul USEADPAUT la *YES. Dacă nu doriţi ca programul să moştenească autorizare adoptată, trebuie să folosiţi comanda Modificare program (Change Program - CHGPGM) sau Modificare program serviciu (Change Service Program - CHGSRVPGM) pentru a seta parametrul USEADPAUT la *NO.

Puteţi folosi o listă de autorizare şi valoarea sistem (QUSEADPAUT) de autorizare adoptată pentru a controla cine creează programe care moştenesc autorizarea adoptată. Când specificaţi un nume de listă de autorizări în variabila de sistem QUSEADPAUT, sistemul foloseşte această listă de autorizări pentru a determina cine să creeze programe noi.

Când un utilizator creează un program sau program serviciu, sistemul verifică autorizarea utilizatorului din lista de autorizări. Dacă utilizatorul are autorizarea *USE, parametrul USEADPAUT pentru noul program este setat la *YES. Dacă utilizatorul nu are autorizarea *USE, parametrul USEADPAUT este setat la *NO. Autorizarea utilizatorului din lista de autorizări nu poate proveni de la autorizarea adoptată.

Lista de autorizări pe care o specificaţi în variabila de sistem QUSEADPAUT controlează, de asemenea, dacă un utilizator poate folosi comanda CHGxxx pentru a seta variabila USEADPAUT pentru un program sau program serviciu.

Note:

1. Nu trebuie să chemaţi lista dumneavoastră de autorizare QUESADPAUT. Puteţi crea o listă de autorizări cu un nume diferit. Apoi specificaţi această listă de autorizare pentru variabila de sistem QUSEADPAUT. În comanda din acest exemplu, substituiţi numele listei dumneavoastră de autorizare.
2. Variabila de sistem QUSEADPAUT nu afectează programele existente pe sistemul dumneavoastră. Folosiţi comanda CGHPGM sau comanda CHGSRVPGM pentru a seta parametrul USEADPAUT parameter pentru programe existente.

Mediu mai restrictiv: Dacă doriţi ca majoritatea utilizatorilor să creeze programe noi având parametrul USEADPAUT setat la valoarea *NO, efectuaţi următoarele:

1. Pentru a seta autorizarea publică pentru lista de autorizări la *EXCLUDE, introduceţi următoarele:

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

2. Pentru a seta utilizatori specifici să creeze programe care utilizează autorizarea adoptată a programelor anterioare, introduceţi următoarele:

   ```
   ADDAUTLE AUTL(QUSEADPAUT) USER(nume utilizator)
      AUT(*USE)
   ```

Mediu mai puţin restrictiv: Dacă doriţi ca majoritatea utilizatorilor să creeze programe noi cu parametrul USEADPAUT setat la *YES, faceţi următoarele:

1. Lăsaţi autorizarea publică a listei de autorizări setată la *USE.
2. Pentru a împiedica anumiţi utilizatori să creeze programe care să utilizeze autorizarea adoptată a programelor anterioare, introduceţi următoarele:

   ```
   ADDAUTLE AUTL(QUSEADPAUT)
      USER(nume utilizator) AUT(*EXCLUDE)
   ```

Utilizarea monitorului programelor de declanşare

DB2 UDB furnizează capacitatea de asociere a programelor sursă cu fişierele bazei de date. Caracteristicile programelor declanşatori sunt comune pentru industria gestiunii bazelor de date cu funcţii de nivel înalt.

Când asociaţi un program declanşator unei baze de date, specificaţi când declanşatorul va rula. De exemplu, puteţi seta fişierul comenzi clienţi să ruleze un program declanşator oricând o nouă înregistrare îi este adăugată. Când soldul scadent al clientului depăşeşte limita de credit, programul declanşator poate tipări o scrisoare de avertizare clientului şi trimite un mesaj gestionarului de credite.

Programele declanşatori sunt o cale productivă atât pentru a furniza funcţii aplicaţie, cât şi pentru a gestiona informaţiile. Programele declanşatori furnizează, de asemenea, posibilitatea cuiva cu intenţii răuvoitoare să creeze un "Cal troian" pe sistemul dumneavoastră. Un program distructiv poate sta şi aştepta să ruleze când un anumit eveniment are loc într-un fişier bază de date pe sistemul dumneavoastră.

Notă: În istorie, Calul troian a fost un cal de lemn gol pe dinăuntru care era plin cu soldaţi greci. După ce calul a fost introdus dincolo de zidurile Troiei, soldaţii au ieşit şi luptat cu troienii. În lumea calculatoarelor, un program care ascunde funcţii distructive este deseori numit un Cal troian.

opţiuni meniu SECBATCH:
27 *pentru lansare imediată* **66** *pentru a folosi planificatorul de joburi*

Când sistemul dumneavoastră este livrat, posibilitatea de a adăuga un program declanşator la un fişier bază de date este restrictivă. Dacă gestionaţi autorizările obiect cu grijă, utilizatorul tipic nu va avea autorizare suficientă să adauge un program declanşator la un fişier bază de date. (Anexa D a cărţii *Referinţă securitate iSeries* conţine autorizarea cerută sau toate comenzile, inclusiv comanda Adăugare declanşator fişier fizic (ADDPFTRG).

Puteţi utiliza comanda Tipărire programe declanşatori (PRTTRGPGM) pentru a tipări o listă a tuturor programelor declanşatori dintr-o bibliotecă specificată sau din toate bibliotecile.

Puteţi folosi raportul iniţial ca o bază de evaluare a programelor declanşatoare care există deja pe sistemul dumneavoastră. Apoi, puteţi tipări regulat raportul cu modificări pentru a vedea dacă noi programe declanşatoare au fost adăugate pe sistemul dumneavoastră.

Când evaluaţi programele declanşatoare, consideraţi următoarele:

- Cine a creat programele declanşatoare? Puteţi folosi comanda Afişare descriere obiect (DSPOBJD) pentru a determina aceasta.
- Ce face programul? Va trebui să vă uitaţi pe sursa programului sau să vorbiţi cu cel care a creat programul pentru a determina aceasta. De exemplu, programul declanşator verifică cine este utilizatorul? Poate programul declanşator aşteaptă un anumit utilizator (QSECOFR) pentru a obţine accesul la resursele sistemului.

După stabilirea unei baze de informaţii, puteţi tipări raportul modificat regulat pentru monitorizarea programelor sursă care au fost adăugate la sistem.

Verificarea programelor ascunse

Programele declanşatoare nu sunt singurul mod posibil de a introduce un cal troian în sistem. Programele declanşatoare sunt un exemplu de **programe de ieşire**. Când apare un anumit eveniment, cum ar fi actualizarea unui fişier, în cazul programului declanşator sistemul rulează programul de ieşire care este asociat evenimentului.

Tabela 15 descrie alte exemple de programe de ieşire care s-ar putea găsi pe sistemul dumneavoastră. Trebuie să utilizaţi aceeaşi metodă pentru a evalua utilizarea şi conţinutul acestor programe de ieşire pe care le utilizaţi pentru programele declanşatoare.

Notă: Tabela 15 nu este o listă completă cu programele de ieşire.

.

Tabela 15. Programe de ieşire furnizate de sistem

Nume program	**Când rulează programul**
Nume specificat de utilizator în atributul de reţea DDMACC.	Când un utilizator încearcă să deschidă un fişier DDM în sistemul dumneavoastră sau face o DRDA conexiune.
Nume specificat de utilizator în parametrul de reţea PCSACC.	Când un utilizator încearcă să utilizeze funcţiile Acces Client folosind Clienţi Originali pentru a accesa obiecte în sistem.
Nume specificate de utilizator în variabila de sistem QPWDVLDPGM	Când un utilizatior rulează funcţia Schimbare Parolă (Change Password).
Nume specificat de utilizator în variabila de sistem QRMTSIGN.	Când un utilizator încearcă să se conecteze interactiv de la un sistem la distanţă.
QSYS/QEZUSRCLNP	Când rulează funcţia de curăţire automată.
Nume specificat de utilizator în parametrul EXITPGM al comenzii CHGBCKUP.	Când utilizaţi funcţia de salvare Asistare Operaţie.
Nume specificate de utilizator în comanda CRTPRDLOD.	Înainte şi după ce salvaţi, restauraţi sau ştergeţi produsul care a fost creat cu comanda.
Nume specificate de utilizator în parametrul DFTPGM al comenzii CHGMSGD.	Dacă este specificat un program implicit pentru un mesaj, sistemul rulează programul atunci când mesajul este emis. Datorită numărului mare de descrieri de mesaje de pe un sistem tipic, utilizarea programelor implicite este dificil de monitorizat. Pentru a împiedica utilizatorii publici să adauge programe implicite pentru mesaje, luaţi în considerare configurarea autorizării publice pentru fişierele mesaje (obiectele *MSGF) pe *USE.
Nume specificat de utilizator în parametrul FKEYPGM din comanda STREML3270.	Când un utilizator apasă o tastă funcţională în timpul emulării dispozitivului 3270. Sistemul returnează controlul sesiunii de emulare a dispozitivului 3270 când se termină programul de ieşire.
Nume specificat de utilizator în parametrul EXITPGM al comenzilor monitorului de performanţe	Pentru a prelucra date care sunt colectate de următoarele comenzi: STRPFRMON, ENDPFRMON, ADDPFRCOL şi CHGPFRCOL. Programul rulează când se termină colecţia de date.
Nume specificate de utilizator în parametrul EXITPGM din comanda RCVJRNE.	Pentru fiecare intrare de jurnal sau grup de intrări jurnal citite din jurnalul specificat sau receptorii de jurnal.
Nume specificat de utilizator în API QTNADDCR.	În timpul unei operaţii COMMIT sau ROLLBACK.
Nume specificate de utilizator în API QHFRGFS.	Pentru a executa funcţiile sistemului de fişiere.
Nume specificat de utilizator în parametrul SEPPGM al unei descrieri de dispozitiv de tipărire	Pentru a determina ce trebuie tipărit în paginile separatoare înainte sau după un fişier spool sau un job de tipărire.
QGPL/QUSCLSXT	Când un fişier bază de date este închis pentru a permite preluarea informaţiilor de utilizare.
Nume specificat de utilizator în parametrul FMTSLR al unui fişier logic.	Când este scrisă o înregistrare într-un fişier bază de date şi un nume de format de înregistrare nu este inclus în programul scris în limbajul de nivel înalt. Programul selector primeşte înregistrarea ca o intrare, determină formatul înregistrării utilizat şi o returnează în baza de date.

Tabela 15. Programe de ieşire furnizate de sistem (continuare)

Nume program	Când rulează programul
Nume specificat de utilizator în variabila de sistem QATNPGM , în parametrul ATNPGM dintr-un profil de utilizator sau în parametrul PGM din comanda SETATNPGM.	Când un utilizator apasă tasta Attention.
Nume specificat de utilizator în parametrul EXITPGM al comenzii TRCJO.	Înainte de începerea procedurii Trace Job (Urmărire Job).

Pentru comenzi care vă permit să specificaţi un program de ieşire, trebuie să vă asiguraţi că respectiva comandă implicită nu a fost modificată pentru a specifica un program de ieşire. Trebuie să vă asiguraţi şi că autorizarea publică pentru aceste comenzi nu este suficientă pentru a modifica valorile implicite ale comenzii. Comanda CHGCMDDFT necesită autorizarea *OBJMGT pentru comandă. Nu aveţi nevoie de autorizarea *OBJMGT pentru a lansa comanda.

Evaluarea programelor de ieşire înregistrate

Puteţi utiliza funcţia sistemului de înregistrare pentru a înregistra programe de ieşire care trebuie să ruleze atunci când apar anumite evenimente. Pentru a afişa informaţiile de înregistrare pe sistemul dumneavoastră, tastaţi WRKREGINF OUTPUT(*PRINT). Figura 8 arată un exemplu de raport:

```
              Gestiunea informaţiilor de înregistrare
Punct de ieşire. . . . . . . . . . . . . :   QIBM_QGW_NJEOUTBOUND
Format punct de ieşire . . . . . . . . . :   NJEO0100
Punct de ieşire înregistrat. . . . . . . :   *YES
Permitere de-înregistrare . . . . . . . . :   *YES
Format . . . . . . . . . . . . . . . . . :
Numărul actual de programe de ieşire . . :   0
Preprocesare pentru adăugare . . . . . . :   *NONE
  Bibliotecă . . . . . . . . . . . . . . :
  Format . . . . . . . . . . . . . . . . :
Preprocesare pentru înlăturare . . . . . :   *NONE
  Bibliotecă . . . . . . . . . . . . . . :
  Format . . . . . . . . . . . . . . . . :
Preprocesare pentru recuperare . . . . . :   *NONE
  Bibliotecă . . . . . . . . . . . . . . :
```

Figura 8. Gestiunea informaţiilor de înregistrare - Exemplu

Pentru fiecare punct de ieşire de pe sistem, raportul arată dacă există vreun program de ieşire înregistrat. Când un punct de ieşire are programe care sunt înregistrate în prezent, puteţi selecta opţiunea 8 (Display programs - Afişare programe) din ecranul comenzii WRKREGINF pentru a afişa informaţii despre programe:

```
                    Gestiunea informaţiilor de înregistrare

Introduceţi opţiunea, apăsaţi Enter
5=Afişare punct de ieşire  8=Gestiune programe ieşire

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

Utilizaţi aceeaşi metodă pentru evaluarea acestor programe de ieşire ca cea pe care o folosiţi pentru alte programe de ieşire şi programe declanşatoare.

Verificarea programelor planificate

iSeries furnizează mai multe metode pentru rularea funcţiilor de programare la un timp viitor, incluzând programerul de funcţii. În mod normal, aceste metode nu reprezintă o problemă de securitate deoarece utilizatorul care planifică jobul trebuie să aibă aceeaşi autorizare ca cea care este cerută pentru a lansa un job în batch.

Totuşi, trebuie să verificaţi periodic joburile planificate în viitor. Un utilizator nemulţumit care nu mai este în organizaţie poate utiliza această metodă pentru a planifica un dezastru.

Restricţionarea salvării şi capacitatea de restaurare

Cei mai mulţi utilizatori nu trebuie să salveze sau să restaureze obiecte pe sistem. Comenzile de salvare oferă posibilitatea de copiere a informaţiilor importante ale organizaţiei pe medii de stocare sau pe un alt sistem. Cele mai multe comenzi suportă fişiere de salvare care pot fi transmise altui sistem (utilizând comanda SNDNETF) fără a avea acces la mediile de stocare sau la dispozitivul de salvare/restaurare.

Comenzile de restaurare oferă posibilitatea de a restaura pe sistem obiecte neautorizate, cum ar fi programe, comenzi şi fişiere. Puteţi restaura informaţii şi fără a avea acces la mediile de stocare sau la dispozitivele de salvare/restaurare, utilizând fişierele de salvare. Fişierele de salvare pot fi transmise de pe alt sistem utilizând comanda SNDNETF sau funcţia FTP.

În continuare sunt prezentate sugestii pentru restricţionarea operaţiilor de salvare şi restaurare pe sistemul dumneavoastră:

- Controlaţi care utilizatori au autorizarea specială *SAVSYS. Autorizarea specială *SAVSYS permite utilizatorului să salveze şi să restaureze obiecte chiar dacă utilizatorul nu are autorizarea necesară pentru acele obiecte.
- Verificare Fizică Acces pentru salvarea şi refacerea dispozitivelor.
- Restricţionaţi accesul la comenzile de salvare şi restaurare. Când instalaţi OS/400 programe licenţiate, autorizarea publică pentru comanda RSTxxx este *EXCLUDE. Autorizarea publică pentru comenzile SAVxxx este *USE. Luaţi în considerare modificarea autorizării publice pentru comenzile SAVxxx pe *EXCLUDE. Limitaţi numărul de utilizatori care au autorizare pentru comenzile RSTxxx.
- Utilizaţi variabila de sistem QALWOBJRST pentru a restricţiona restaurarea Programe statut-sistem, programe care adoptă authorităţi şi obiecte care au erori de validare.

- Utilizaţi valoarea sistem QVFYOBJRST pentru a controla refacerea obiectelor semnate din sistem.
- Folosiţi valoarea sistem QFRCCVNRST pentru a controla recrearea anumitor obiecte care au fost restaurate pe sistemul dumneavoastră.
- Utilizare auditare securitate pentru monitorizarea operaţiilor de restaurare. Includere *SAVRST în variabila de sistem QAUDLVL şi tipărirea periodică a înregistrărilor de verificare care sunt create de operaţiile de restaurare. (Capitolul 9 şi Anexa F din cartea *Referinţă securitate iSeries* furnizează mai multe informaţii despre operaţiile de auditare intrări.)

Verificarea obiectelor utilizator în bibliotecile protejate

Fiecare job server iSeries are o listă de biblioteci. Lista de biblioteci determină secvenţa în care sistemul caută un obiect dacă numele bibliotecii nu este specificat cu numele obiectului. De exemplu, când apelaţi un program fără să specificaţi unde este, sistemul caută lista dumneavoastră de biblioteci în ordine şi rulează prima copie a programului pe care o găseşte.

Cartea *Referinţă securitate iSeries* furnizează mai multe informaţii despre expunerile de securitate ale listelor de biblioteci şi apelarea programelor fără un nume de bibliotecă (numită **apel necalificat**). Furnizează, de asemenea, sugestii pentru controlul conţinutului listelor de biblioteci şi abilitatea de a modifica listele de biblioteci sistem.

Pentru ca sistemul dumneavoastră să ruleze corespunzător, anumite biblioteci sistem, cum ar fi QSYS şi QGPL, trebuie să fie în lista de biblioteci pentru fiecare job. Trebuie să utilizaţi autorizările obiect pentru a controla cine poate adăuga programe acestor biblioteci. Aceasta vă ajută să împiedicaţi plasarea unui program impostor într-una din aceste biblioteci cu acelaşi nume ca un program care apare într-o bibliotecă din lista de biblioteci mai târziu.

Trebuie, de asemenea, să determinaţi cine are autorizare pentru comanda CHGSYSLIBL şi monitorizează înregistrările SV din jurnalul verificare securitate. Un utilizator necinstit poate plasa o bibliotecă în faţa lui QSYS din lista de biblioteci şi determina ceilalţi utilizatori să ruleze comenzi neautorizate cu aceleaşi nume ca şi cele furnizate de IBM.

opţiuni meniu SECBATCH:
28 *pentru lansare automată* **67** *pentru a utiliza planificatorul de joburi*

Puteţi folosi comanda PRTUSROBJ (Print User Objects - Imprimare obiecte utilizator) pentru a imprima o listă de obiecte utilizator (obiecte care nu au fost create deIBM) care sunt în biblioteca specificată. Puteţi apoi aprecia programele din listă pentru a determina cine le-a creat şi ce funcţii îndeplinesc.

Obiectele utilizator altele decât programele pot, de asemenea, reprezenta o problemă de securitate când se găsesc în bibliotecile sistem. De exemplu, dacă un program scrie date confidenţiale într-un fişier al cărui nume nu este calificat, acest program poate fi păcălit să intre într-o versiune impostoare a acelui fişier dintr-o bibliotecă de sistem.

Capitolul 10. Prevenirea şi detectarea încercărilor de hacking (spargere)

Aceste informaţii sunt o colecţie de diverse indicii pentru a vă ajuta să detectaţi posibilele probleme de securitate.

Securitate fizică

Unitatea de sistem reprezintă un activ important al afacerii şi o poartă potenţială către sistemul dumneavoastră. Unele componente ale sistemului sunt mici şi valoroase. Trebuie să plasaţi unitatea de sistem într-o locaţie controlată pentru a împiedica mutarea componentelor sistemului.

Unitatea de sistem are un panou de control care oferă posibilitatea de rulare a funcţiilor de bază fără o staţie de lucru. De exemplu, puteţi utiliza panoul de control pentru a face următoarele:

- Oprirea sistemului.
- Pornirea sistemului.
- Încărcarea sistemului de operare.
- Pornirea funcţiilor de service.

Toate aceste activităţi îi pot întrerupe pe utilizatorii sistemului din activitatea normală. De asemenea, acestea reprezintă potenţiale probleme de securitate pentru sistem. Puteţi utiliza cheia de blocare care este livrată odată cu sistemul pentru a controla când sunt permise aceste activităţi. Pentru a preveni utilizarea panoului de control, setaţi cheia de de blocare la poziţia Sigur, apoi mutaţi şi stocaţi cheia într-un loc sigur.

Note:

1. Dacă trebuie să executaţi IPL-uri de la distanţă sau diagnostice sistem de la distanţă, ar trebui să alegeţi o altă poziţionare a cheii de blocare. Subiectul Pregătire Pornire Centru de informare iSeries furnizează mai multe informaţii privind setările cheii de blocare (vezi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru detalii).
2. Nu toate modelele sunt livrate cu o cheie de blocare ca o componentă standard.

Monitorizarea activităţii profilului utilizator

Profilurile utilizatorilor furnizează intrarea în sistem. Parametrii din profil utilizator determină un mediu utilizator şi caracteristici de securitate ale utilizatorului. Ca administrator de securitate, trebuie să controlaţi şi să verificaţi schimbările ce apar în profilurile utilizatorilor din sistem.

Puteţi seta auditarea securităţii astfel încât sistemul să scrie o înregistrare a modificărilor profilurilor utilizatorilor. Puteţi folosi comanda DSPAUDJRNE pentru a tipări un raport al acestor schimbări.

Puteţi crea programe de ieşire pentru a evalua acţiuni cerute la profiluri utilizator. Tabela 16 la pagina 78 arată punctele de ieşire disponibile pentru comenzile profil utilizator.

Tabela 16. Punte de ieşire pentru activitatea profilului utilizator

Comandă profil utilizator	Nume punct de ieşire
Creare profil utilizator (Create User Profile - CRTUSRPRF)	QIBM_QSY_CRT_PROFILE
Modificare profil utilizator (Change User Profile - CHGUSRPRF)	QIBM_QSY_CHG_PROFILE
Ştergere profil utilizator (Delete User Profile - DLTUSRPRF)	QIBM_QSY_DLT_PROFILE
Restaurare profil utilizator (Restore User Profile - RSTUSRPRF)	QIBM_QSY_RST_PROFILE

Programul de ieşire poate, de exemplu, să caute modificări care pot face ca utilizatorul să ruleze versiuni neautorizate ale unui program. Aceste modificări pot asocia o descriere de job diferită sau o nouă bibliotecă curentă. Programul de ieşire poate atenţiona o coadă de mesaje sau poate face câteva acţiuni (cum ar fi modificarea sau dezactivarea profilului utilizatorului) pe baza informaţiilor pe care programul de ieşire le primeşte.

Cartea *Referinţă securitate iSeries* furnizează mai multe informaţii despre programele de ieşire pentru acţiunile profilurilor utilizatorilor.

Semnarea obiectelor

Toate precauţiile de securitate pe care le-aţi luat sunt nesemnificative în cazul în care cineva poate să le depăşească prin introducerea de date amestecate în sistem. Serverul iSeries are multe opţiuni incluse pe care le puteţi folosi pentru a împiedica încarcarea de software pe sistemul dumneavoastră şi pentru a detecta orice astfel de software deja existent. Una din tehnicile adăugate în V5R1 este semnarea obiectelor.

Semnarea obiectelor este implementarea unui concept criptografic a serverului iSeries cunoscut ca ″semnături digitale″. Ideea este relativ simplă: odată ce un producător software este pregătit să vândă software la clienţi, the producătorul ″semnează″ software-ul. Această semnătură nu garantează faptul că software-ul efectuează orice funcţie specificată. Oricum, furnizează o modalitate de a demonstra că software-ul provine de la producătorul care l-a semnat şi că nu s-a modificat de când a fost produs şi semnat. Acest lucru este important în cazul în care software-ul a fost transmis prin Internet sau stocat în medii care au putut fi modificate.

Utilizarea semnăturilor digitale vă oferă un bun control asupra acelor software care pot fi încărcate în sistem şi vă permite să detectaţi modoficările după ce a fost încărcat. Noua valoare sistem pentru Refacere Obiect de Verificare (QVFYOBJRST) furnizează un mecanism pentru setarea politicii restrictive care solicită ca toate software-le încărcate în sistem să provină de la o sursă software cunoscută. Puteţi alege de asemenea o politică mai deschisă şi faceţi doar o simplă verificare a semnăturilor dacă acestea sunt prezente în sistem.

Toate produsele softwareOS/400, la fel ca şi software-ul pentru opţiuni şi programele licenţiate ale serveruluiiSeries, au fost semnate de o sursă de încredere. Aceste semnături ajută sistemul să-şi protejeze integritatea şi sunt verificate când sunt aplicate corecţii sistemului pentru a asigura faptul că sursa corecţiei este un sistem sigur şi că nu s-a modificat în tranzit. Aceste semnături pot fi verificate, de asemenea şi după ce software-ul este încărcat în sistem. Comanda CHKOBJITG (Verificare Integritate Obiect) a fost extinsă pentru a verifica semnăturile şi suplimentar pentru alte caracteristici de integritate ale obiectelor din sistem. Suplimentar, Digital Certificate Manager dispune de panouri pe care le puteţi utiliza la verificarea semnăturilor pe obiecte, inclusiv obiecte din sistemul de operare.

Imediat ce sistemul de operare a fost semnat, puteţi utiliza semnătura digitală pentru protecţia software esenţială pentru proces. Puteţi să cumpăraţi software care au fost semnate de un furnizor software, sau să semnaţi software pe care le-aţi cumpărat sau scris. În acest caz, o parte din politica de securitate constă în utilizarea periodică a CHKOBJITG, sau Digital Certificate Manager, pentru a verifica dacă semnăturile de pe software mai sunt valide — dacă obiectele nu s-au modificat de când au fost semnate. Mai departe, puteţi solicita ca tot software-ul care este restaurat în sistem să fie semnat de către dumneavoastră sau o sursă cunoscută. Totuşi, din moment ce toate produsele software ale serverului iSeries care nu sunt produse de către IBM nu sunt semnate, aceasta ar putea fi prea restrictivă pentru sistemul dumneavoastră. Noul suport de semnătură digitală vă oferă flexibilitate în luare deciziei privind cel mai bun mod de protejare a integrităţii software.

Semnăturile digitale care protejează software-ul sunt doar folosirea de certificate digitale. Informaţii suplimentare privind administrarea certificatelor digitale pot fi găsite în subiectul care tratează administrarea certificărilor digitale din Centru informaţii (vezi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru detalii).

Monitorizarea descrierilor de subsistem

Când porniţi un subsistem pe un server iSeries, sistemul creează un mediu pentru lucru pentru a intra în sistem şi a rula. O descriere de subsistem defineşte cu ce anume seamănă acest mediu. De aceea, descrierile de sistem oferă o posibilitate pentru utilizatorii rău intenţionaţi. Un astfel de utilizator poate folosi descrierea subsistemului pentru a lansa în mod automat un program sau pentru a face posibilă semnarea fără un profil de utilizator.

Când lansaţi comanda Revocarea autorizării publice (Revoke Public Authority - RVKPUBAUT), sistemul setează autorizarea publică a comenzilor pentru descrierile subsistemului pe *EXCLUDE. Acest lucru împiedică utilizatorii care nu sunt autorizaţi în mod specific (şi care nu au autorizarea specială *ALLOBJ) să modifice sau să creeze descrieri de subsistem.

Următoarele subiecte oferă sugestii pentru revizuirea descrierilor de subsistem care există în prezent pe sistemul dumneavoastră. Puteţi folosi comanda Gestiune descriere subsistem (Work with Subsystem Descriptions - WRKSBSD) pentru a crea o listă cu toate descrierile de subsistem. Când selectaţi 5 (Afişare) din listă, este afişat un meniu pentru descrierea de subsistem pe care aţi selectat-o. Afişează o listă cu componente ale unui mediu subsistem.

Selectaţi opţiuni pentru detalii. Folosiţi comanda Modificare descriere subsistem (Change Subsystem Description - CHGSBSD) pentru a modifica primele două elemente din meniu. Pentru a modifica alte elemente, utilizaţi comanda corespunzătoare de adăugare, înlăturare sau modificare pentru tipul de intrare. De exemplu, pentru a modifica intrarea unei staţii de lucru, folosiţi comanda Modificare intrare staţie de lucru (Change Workstation Entry - CHGWSE).

Cartea *Control funcţionare* furnizează mai multe informaţii despre administrarea descrierilor de subsistem. De asemenea, afişează valorile livrate pentru descrierile subsistemelor furnizate de IBM.

Intrări de joburi autostart

O intrare de job autostart conţine numele unei descrieri de job. Descrierea jobului poate conţine date cerere (RQSDTA) care fac ca un program sau o comandă să ruleze. De exemplu, RQSDTA poate fi CALL LIB1/PROGRAM1. Atunci când porneşte subsistemul, sistemul va rula programul PROGRAM1 din biblioteca LIB1.

Uitaţi-vă la intrările joburilor autostart şi la descrierile de job asociate. Asiguraţi-vă că înţelegeţi funcţia fiecărui program care rulează automat atunci când un subsistem porneşte.

Nume de staţii de lucru şi tipuri de staţii de lucru

Atunci când porneşte un subsistem, acesta alocă toate staţiile de lucru nealocate care sunt afişate (în mod specificat sau general) în intrările lui pentru nume de staţii de lucru şi tipuri de staţii de lucru. Atunci când un utilizator se semnează, utilizatorul se conectează la subsistemul care este alocat staţiei de lucru.

Intrarea staţiei de lucru specifică ce descriere de job va fi utilizată atunci când un job porneşte pe o staţie de lucru. Descrierea jobului poate conţine date cerere care fac să ruleze un program sau o comandă. De exemplu, parametrul RQSDTA poate fi CALL LIB1/PROGRAM1. Când un utilizator se semnează pe o staţie de lucru în acel subsistem, sistemul va rula PROGRAM1 din LIB1.

Uitaţi-vă la intrările staţiei de lucru şi la descrierile joburilor asociate. Asiguraţi-vă că nimeni nu a adăugat sau actualizat nici o intrare pentru a rula programe de care nu aveţi cunoştinţă.

O intrare a unei staţii de lucru poate specifica şi profilul de utilizator implicit. Pentru unele configuraţii de subsistem, aceasta permite unora să deschidă o sesiune prin simpla apăsare a tastei Enter. Dacă nivelul de securitate (variabila de sistem QSECURITY) de pe sistem este mai mic decât 40, trebuie să revizuiţi intrările staţiilor de lucru pentru utilizatorii impliciţi.

Intrări în coada de joburi

Atunci când un subsistem porneşte, acesta alocă toate cozile de joburi nealocate care sunt afişate în descrierea subsistemului. Intrările cozii de joburi nu determină în mod direct probleme de securitate. Totuşi, acestea oferă o posibilitate celor care vor să micşoreze performanţele sistemului prin lansarea de joburi în medii necorespunzătoare.

Trebuie să revizuiţi periodic intrările din coada de joburi din subsistemul dumneavoastră pentru a vă asigura că joburile batch rulează acolo unde vă aşteptaţi să ruleze.

Intrări de rutare

O intrare de rutare defineşte ce face un job odată ce intră în subsistem. Subsistemul utilizează intrările rutării pentru toate tipurile de joburi: batch, interactive şi joburi de comunicare. O intrare de rutare specifică următoarele:

- Clasa pentru job. Ca şi intrările cozi de joburi, clasa care este asociată unui job poate afecta performanţele acestuia, dar nu reprezintă o problemă de securitate.
- Programul care rulează atunci când porneşte jobul. Uitaţi-vă la intrările rutării şi asiguraţi-vă că nimeni nu a adăugat sau actualizat nici o intrare pentru a rula programe de care nu aveţi cunoştinţă.

Intrări de comunicaţii şi nume de locaţii la distanţă

Atunci când un job de comunicaţie intră în subsistemul dumneavoastră, sistemul utilizează intrările comunicaţiei şi numele locaţiilor la distanţă din subsistemul activ pentru a determina cum vor rula joburile de comunicaţie. Uitaţi-vă la următoarele pentru aceste intrări:

- Toate subsistemele capabile să ruleze joburi de comunicaţie. Dacă un subsistem pe care intenţionaţi să-l folosiţi pentru comunicaţii nu este activ, un job care încearcă să intre în sistem ar trebui să găsească o intrare în altă descriere de subsistem care îndeplineşte cerinţele sale. Trebuie să vă uitaţi la intrările din toate descrierile de subsisteme.
- O intrare de comunicaţie conţine o descriere de job. Descrierea jobului poate conţine date cerere care rulează o comandă sau program. Uitaţi-vă la intrările de comunicaţii şi la descrierile joburilor asociate pentru a vă asigura că înţelegeţi cum vor fi pornite joburile.

- O intrare de comunicaţie specifică şi un profil de utilizator implicit pe care sistemul îl utilizează în unele situaţii. Asiguraţi-vă că aţi înţeles rolul profilului implicit. Dacă sistemul conţine profiluri implicite, trebuie să vă asiguraţi că acestea sunt profiluri cu autorizări minime. Vezi Capitolul 12, “Securizarea comunicaţiilor APPC” pentru mai multe informaţii despre profilurile implicite.

  Puteţi utiliza comanda Tipărire descriere subsistem (Print Subsystem Description - PRTSBSDAUT) pentru a identifica intrările comunicaţiei care specifică un nume de profil de utilizator.

Intrări job prestart

Puteţi utiliza intrările joburilor prestart pentru a pregăti un subsistem pentru diferite tipuri de joburi astfel încât joburile să pornească mult mai repede. Joburile prestart pot porni atunci când un subsistem porneşte sau când este nevoie de ele. O intrare de job prestart specifică următoarele:

- Un program de rulat

  Un profil de utilizator implicit

  O descriere de job

Toate acestea pot genera probleme de securitate. Trebuie să vă asiguraţi că intrările joburilor prestart realizează numai funcţii autorizate.

Joburi şi descrieri de job

Descrierile joburilor conţin date cerere şi date rutare care pot face ca un anumit program să ruleze când este utilizată acea descriere de job. Atunci când descrierea unui job specifică un program în parametrul date cerere, sistemul rulează programul. Atunci când o descriere de job specifică o dată de rutare, sistemul rulează programul care este specificat în intrarea de rutare care corespunde datei de rutare.

Sistemul utilizează descrierea de job atât pentru joburile interactive, cât şi pentru joburile batch. Pentru joburile interactive, intrarea staţiei de lucru specifică descrierea de job. În mod tipic, valoarea intrării staţiei de lucru este *USRPRF şi sistemul utilizează descrierea de job care este specificat în profilul utilizatorului. Pentru joburile batch, specificaţi descrierea de job atunci când lansaţi jobul.

Trebuie să revizuiţi periodic descrierile joburilor pentru a vă asigura că acestea nu rulează alte programe. De asemenea, trebuie să folosiţi autorizarea obiectului pentru a împiedica modificarea descrierilor joburilor. Autorizarea *USE este suficientă pentru a rula un job cu o descriere de job. Un utilizator tipic nu are nevoie de autorizarea *CHANGE pentru descrierea de job.

opţiuni meniu SECBATCH:
15 *pentru lansare imediată* **54** *pentru utilizarea planificatorului de joburi*

Descrierea jobului poate specifica şi sub care profil de utilizator ar trebui să ruleze jobul. Pentru nivelul de securitate 40 şi mai mare, trebuie să aveţi autorizarea *USE pentru descrierea de job şi pentru profilul de utilizator care este specificat în descrierea de job. Pentru niveluri de securitate mai mici decât 40, aveţi nevoie de autorizarea *USE doar pentru descrierea de job.

Puteţi utiliza comanda Tipărire autorizare descriere job (Print Job Description Authority - PRTJOBDAUT) pentru a tipări o listă cu descrierile joburilor care specifică profilurile de utilizatori şi care au autorizarea publică *USE.

Raportul arată autorizările speciale ale profilului de utilizator care este specificat în descrierea de job. Raportul include autorizările speciale ale tuturor profilurilor de grup pe care le are profilul de utilizator. Puteţi utiliza următoarea comandă pentru a afişa autorizările private ale profilului de utilizator:

```
DSPUSRPRF
USRPRF(nume-profil) TYPE(*OBJAUT)
```

Descrierea jobului specifică lista cu bibliotecile pe care le utilizează jobul când rulează. Dacă cineva modifică lista cu biblioteci a unui utilizator, acel utilizator ar putea rula o altă versiune de program dintr-o altă bibliotecă. Trebuie să revizuiţi periodic listele de biblioteci care sunt specificate în descrieriole de job de pe sistemul dumneavoastră.

În final, trebuie să vă asiguraţi că valorile implicite pentru comenzile Lansare job (Submit Job - SBMJOB) şi pentru Creare profil utilizator (Create User Profile - CRTUSRPRF) nu au fost modificate pentru a indica o altă descriere de job.

Nume de program tranzacţie din arhitectură

Unele cereri de comunicaţie transmit un tip specific de semnal sistemului dumneavoastră. Această cerere este denumită **arhitectură TPN** deoarece numele programului de tranzacţie este parte a arhitecturii APPC pentru sistem. O solicitare de cerere pass-through terminal este un exemplu de arhitectură TPN. Arhitectura TPN este un mod normal de comunicare cu funcţiile şi nu reprezintă neapărat o problemă de securitate. Totuşi, arhitectura TPN poate furniza o intrare neaşteptată în sistemul dumneavoastră.

Unele TPN nu transferă un profil la cerere. Dacă cererea se asociază cu intrarea de comunicare al cărei utilizator implicit este *SYS, cererea poate fi iniţiată pe sistemul dumneavoastră. Totuşi, profilul *SYS poate rula numai funcţii de sistem, nu şi aplicaţii de utilizator.

Dacă nu vreţi ca arhitectura TPN să ruleze cu un profil implicit, puteţi modifica profilul implicit prin configurarea lui *SYS pe *NONE în intrarea comunicării. “Cereri TPN arhitecturale” la pagina 83 afişează arhitectura TPN şi profilurile de utilizatori asociate.

Dacă nu doriţi un anume TPN să ruleze pe sistem, faceţi următoarele:

1. Creaţi un program CL care acceptă mai mulţi parametri. Programul nu trebuie să realizeze nici o funcţie. Trebuie doar să aibă instrucţiunile (DCL) pentru parametri şi apoi să se termine.

2. Adăugaţi o intrare de rutare pentru TPN pe fiecare subsistem care are intrări de comunicaţii sau intrări nume locaţii la distanţă. Intrarea rutare trebuie să specifice următoarele:
   - O valoare *Compare value* (CMPVAL) egală cu numele programului pentru TPN (vezi Cereri TPN arhitecturale) cu poziţia de început 37.
   - O valoare *Program to call* (PGM) egală cu numele programului pe care l-aţi creat la pasul 1 la pagina 82. Aceasta împiedică TPN să localizeze altă intrare rutare, cum ar fi *ANY.

Unele TPN au deja propria intrare de rutare în subsistemul QCMN. Acestea au fost adăugate din motive de performanţă.

Cereri TPN arhitecturale

Tabela 17. Programe şi utilizatori pentru cereri TPN

Cerere TPN	Program	Profil utilizator	Descriere
X'30F0F8F1'	AMQCRC6A	*NONE	Punere în coadă mesaj
X'06F3F0F1'	QACSOTP	QUSER	Program tranzacţie conectare APPC
X'30F0F2D1'	QANRTP	QADSM	Configurare APPC ADSM/400
X'30F0F1F9'	QCNPCSUP	*NONE	Directoare partajate
X'07F0F0F1'	QCNTEDDM	QUSER	DDM
X'07F6C4C2'	QCNTEDDM	QUSER	SQL la distanţă –DRDA1
X'30F0F7F7'	QCQNRBAS	QSVCCS	SNA CC_Server
X'30F0F1F4'	QDXPRCV	QUSER	DSNX–Receptor PC
X'30F0F1F3'	QDXPSEND	QUSER	DSNX–Transmiţător PC
X'30F0F2C4'	QEVYMAIN	QUSER	Server ENVY**/400
X'30F0F6F0'	QHQTRGT	*NONE	Coadă de date PC
X'30F0F8F0'	QLZPSERV	*NONE	Gestionar licenţă Client Access
X'30F0F1F7'	QMFRCVR	*NONE	Receptor mesaj PC
X'30F0F1F8'	QMFSNDR	*NONE	Transmiţător mesaj PC
X'30F0F6F6'	QND5MAIN	QUSER	Controler staţii de lucru APPN 5394
DB2DRDA	QCNTEDDDM	QUSER	DB2DRDA
APINGD	QNMAPINGD	QUSER	APINGD
X'30F0F5F4'	QNMEVK	QUSER	Utilitare administrare sistem
X'30F0F2C1'	QNPSERVR	*NONE	Server tipărire reţea PWS-I
X'30F0F7F9'	QOCEVOKE	*NONE	Calendar al mai multor sisteme
X'30F0F6F1'	QOKCSUP	QDOC	Shadow director
X'20F0F0F7'	QOQSESRV	QUSER	DIA versiunea 2
X'20F0F0F8'	QOQSESRV	QUSER	DIA versiunea 2
X'30F0F5F1'	QOQSESRV	QUSER	DIA versiunea 2
X'20F0F0F0'	QOSAPPC	QUSER	DIA versiunea 1
X'30F0F0F5'	QPAPAST2	QUSER	Pass-through S/36—S/38
X'30F0F0F9'	QPAPAST2	QUSER	Pass-through imprimantă
X'30F0F4F6'	QPWFSTP0	*NONE	Directoare partajate tip 2
X'30F0F2C8'	QPWFSTP1	*NONE	Server de fişiere Client Access

Tabela 17. Programe şi utilizatori pentru cereri TPN (continuare)

Cerere TPN	Program	Profil utilizator	Descriere
X'30F0F2C9'	QPWFSTP2	*NONE	Server de fişiere Windows** Client Access
X'30F0F6F9'	QRQSRVX	*NONE	SQL la distanţă –server convergent
X'30F0F6F5'	QRQSRV0	*NONE	SQL la distanţă fără comitere
X'30F0F6F4'	QRQSRV1	*NONE	SQL la distanţă fără comitere
X'30F0F2D2'	QSVRCI	QUSER	SOC/CT
X'21F0F0F8'	QS2RCVR	QGATE	Receptor SNADS FS2
X'21F0F0F7'	QS2STSND	QGATE	Transmiţător SNADS FS2
X'30F0F1F6'	QTFDWNLD	*NONE	Funcţie transfer PC
X'30F0F2F4'	QTIHNPCS	QUSER	Funcţie TIE
X'30F0F1F5'	QVPPRINT	*NONE	Tipărire virtuală PC
X'30F0F2D3'	QWGMTP	QWGM	Server Ultimedia Mail/400
X'30F0F8F3'	QZDAINIT	QUSER	Server acces date PWS-I
X'21F0F0F2'	QZDRCVR	QSNADS	Receptor SNADS
X'21F0F0F1'	QZDSTSND	QSNADS	Transmiţător SNADS
X'30F0F2C5'	QZHQTRG	*NONE	Server coadă de date PWS-I
X'30F0F2C6'	QZRCSRVR	*NONE	Server comandă la distanţă PWS-I
X'30F0F2C7'	QZSCSRVR	*NONE	Server central PWS-I

Metode pentru Monitorizarea evenimentelor de securitate

Configurarea securităţii nu se realizează într-o singură etapă. Trebuie să evaluaţi în mod constant atât modificările de pe sistem, cât şi erorile de securitate. Apoi faceţi modificări în mediul de securitate pentru a răspunde la ceea ce aţi descoperit.

Rapoartele de securitate vă ajută să monitorizaţi modificările relevante de securitate care apar în sistem. Următoarele sunt alte funcţii de sistem pe care le puteţi utiliza pentru a vă ajuta să detectaţi erorile de securitate:

- Auditarea securităţii este un instrument puternic pe care îl puteţi utiliza pentru a observa diferite tipuri de evenimente relevante pentru securitate care apar în sistem. De exemplu, puteţi seta sistemul să scrie o înregistrare de auditare ori de câte ori un utilizator deschide un fişier bază de date particular pentru actualizare. Puteţi verifica toate modificările variabilelor de sistem. Puteţi verifica acţiuni care se petrec atunci când utilizatorii restaurează obiecte.

  Capitolul 9 din cartea *Referinţă securitate iSeries* furnizează informaţii complete despre funcţiile de auditare a securităţii. Puteţi folosi comanda Modificare auditare securitate (Change Security Auditing - CHGSECAUD) pentru a seta auditarea securităţii pe sistemul dumneavoastră. De asemenea, puteţi utiliza comanda Afişare intrări jurnal auditare (Display Audit Journal Entries - DSPAUDJRNE) pentru a tipări informaţiile selectate din jurnal auditare securitate.
- Puteţi crea coada de mesaje QSYSMSG pentru a captura mesaje critice operator-sistem. Coada de mesaje QSYSOPR primeşte multe mesaje cu o importanţă diferită într-o zi de lucru tipică. Mesajele critice, relevante pentru securitate pot fi scăpate din vedere datorită volumului de mesaje din coada de mesaje QSYSOPR.

  Dacă creaţi o coadă de mesaje QSYSMSG în biblioteca QSYS din sistemul dumneavoastră, sistemul indirectează în mod automat anumite mesaje critice spre coada de mesaje QSYSMSG în locul cozii de mesaje QSYSOPR.

Creaţi un program care să monitorizeze coada de mesaje QSYSMSG sau asociaţi-o pentru dumneavoastră în modul întrerupere sau pentru alt utilizator de încredere.

Partea 3. Aplicaţiile şi comunicaţiile de reţea

Capitolul 11. Folosirea Sistemului de fişiere integrat pentru securizarea fişierelor

Sistem de fişiere integrat vă furnizează mai multe modalităţi să stocaţi şi să vizualizaţi informaţii pe serverul iSeries. Sistem de fişiere integrat este o parte a sistemului de operare OS/400 care suportă operaţii de flux de intrare şi ieşire. Furnizează metode de administrare a stocării ce sunt similare cu (şi compatibile cu) sistemele de operare ale calculatoarelor personale şi UNIX sisteme de operare.

Cu Sistem de fişiere integrat, toate obiectele de pe sistem pot fi vizualizate din perspectiva structurii ierarhice de directoare . Totuşi, în cele mai multe cazuri, utilizatorii vizualizează obiectele în cel mai comun mod pentru un sistem de fişiere particular. De exemplu, obiectele ″tradiţionale″ iSeries sunt în sistemul de fişiere QSYS.LIB. În mod tipic, utilizatorii vizualizează aceste obiecte din perspectiva bibliotecilor. Utilizatorii vizualizează obiecte, în mod tipic, în sistemul de fişiere QDLS din perspectiva documentelor din directoare. Sistemele de fişiere root (/), QOpenSys şi cele definite de utilizator prezintă o structură ierarhică (imbricată) de directoare.

Ca administrator de securitate, trebuie să controlaţi şi să verificaţi schimbările ce apar în profilurile utilizatorilor din sistem.

- Care sisteme de fişiere sunt utilizate pe sistemul dumneavoastră
- Caracteristicile de securitate unice ale fiecărui sistem de fişiere

Subiectele care urmează furnizează câteva consideraţii generale pentru securitatea Sistem de fişiere integrat.

Caracteristici de securitate Sistem de fişiere integrat

Sistemul de fişiere rădăcină acţionează ca o umbrelă (sau ca o fundaţie) pentru toate celelalte sisteme de fişere de pe serverele iSeries. La un nivel înalt, furnizează o vedere integrată a tuturor obiectelor sistemului. Alte sisteme de fişiere care pot exista pe serverele iSeries furnizează diferite posibilităţi de integrare şi gestiune obiecte, în funcţie de scopul principal al fiecărui sistem de fişiere. Sistemul de fişiere (optic) QOPT, de exemplu, permite aplicaţiilor şi serverelor iSeries (care includ serverul de fişiere iSeries Access pentru Windows) să acceseze dispozitivul CD-ROM pe serverul iSeries. Similar, sistemul de fişiere QFileSvr.400 permite aplicaţiilor să acceseze date Sistem de fişiere integrat pe serverele iSeries la distanţă. Serverul de fişiere QLANSrv permite accesul la fişierele stocate în Server xSeries integrat pentru iSeries sau alte servere conectate în reţea.

Abordarea securităţii pentru fiecare sistem de fişiere depinde de datele pe care sistemul de fişiere le face disponibile. Sistemul de fişiere QOPT, de exemplu, nu furnizează securitate la nivel de obiect deoarece nu există tehnologie pentru a scrie informaţie de securitate pe un CD-ROM. Pentru sistemul de fişiere QFileSvr.400, controlul accesului are loc pe sistemul de la distanţă (unde fişierele sunt stocate fizic şi gestionate). Pentru sistemele de fişiere cum ar fi QLANS, Server xSeries integrat pentru iSeries furnizează controlul accesului. În ciuda diferitelor modele de securitate, multe sisteme de fişiere suportă gestionarea controlului accesului prin intermediul comenzilor sistemului de fişiere integrat, cum ar fi Modificare autorizare (Change Authority - CHGAUT) şi Modificare proprietar (Change Owner - CHGOWN).

Iată câteva sfaturi referitoare la fisurile din securitatea sistemului de fişiere integrat. Sistemul de fişiere integrat este proiectat să se conformeze cu standardele POSIX cât mai fidel. Aceasta conduce la un un comportament interesant acolo unde autorizarea serverului iSeries şi permisiunile POSIX sunt ″combinate″:

1. Nu înlăturaţi autorizarea privată pentru un utilizator către un director al cărui proprietar este acel utilizator, chiar dacă acel utilizator este autorizat prin autorizarea publică, de grup sau listă de autorizare. Când lucraţi cu biblioteci sau foldere în modelul standard de securitate al serverului iSeries, înlăturarea autorizării private a proprietarului ar reduce volumul informaţiilor de autorizare stocate pentru un profil utilizator şi nu ar afecta alte operaţii. Dar, datorită modului în care standradul POSIX defineşte moştenirea permisiunilor pentru directoare, proprietarul unui director nou creat va avea aceleaşi autorizări obiect către acel director ca şi cele pe care proprietarul părintelui le are asupra părintelui, chiar dacă proprietarul directorului nou creat are alte autorizări private pentru părinte. Aceasta poate fi dificil de înţeles, deci iată un exemplu: USERA este proprietarul directorului /DIRA, dar autorizările private ale lui USERA au fost înlăturate. USERB are autorizare privată către /DIRA.USERB creează directorul /DIRA/DIRB. Deoarece USERA nu are autorizări obiect spre /DIRA, USERB nu va avea autorizări obiect spre /DIRA/DIRB. USERB nu va putea renumi sau şterge /DIRA/DIRB fără acţiuni în plus pentru a modifica autorizările obiect ale lui USERB. Aceasta intervine de asemenea la crearea fişierelor cu API open() folosind flag-ul O_INHERITMODE. Dacă USERB a creat fişierul /DIRA/FILEB, USERB nu ar avea autorizări obiect şi nici autorizări de date asupra lui. USERB nu ar putea scrie în noul fişier.
2. Autorizarea adoptată nu este onorată de către majoritatea sistemelor de fişiere fizice. Aceasta include sistemele de fişiere rădăcină (root, /), QOpenSys, QDLS şi cele definite de utilizator.
3. Orice obiecte sunt în proprietatea profilului utilizator care a creat obiectele, chiar dacă câmpul OWNER al profilului utilizator este setat pe *GRPPRF.
4. Multe operaţii asupra sistemelor de fişiere necesită autorizarea de date *RX către fiecare componentă a căii, incluzând directorul rădăcină (root, /). Atunci când întâlniţi probleme de autorizare, asiguraţi-vă să verificaţi autorizarea utilizatorului pentru rădăcină.
5. Afişarea sau recuperarea directorului de lucru curent (DSPCURDIR, getcwd() etc.) necesită autorizare de date *RX spre fiecare componentă din cale. Totuşi, schimbarea directorului de lucru curent (CD, chdir() etc.) necesită numai autorizarea de date *X spre fiecare componentă. Prin urmare, un utilizator poate să schimbe directorul de lucru curent spre o anumită cale şi apoi să nu mai poată afişa acea cale.
6. Scopul comenzii COPY este de a duplica un obiect. Setările de autorizare asupra noului fişier vor fi aceleaşi ca şi originalele cu excepţia celor pentru proprietar. Scopul comenzii CPYTOSTMF, totuşi, este pur şi simplu de a duplica date. Setările de autorizare asupra noului fişier nu pot fi controlate de către utilizator. Creatorul/proprietarul va avea autorizări de date *RWX, dar autorizările de grup şi publice vor fi *EXCLUDE. Utilizatorul trebuie să utilizeze alte mijloace (CHGAUT, chmod() etc.) pentru a atribui autorizările dorite.
7. Un utilizator trebuie să fie proprietarul sau să aibe autorizarea obiect *OBJMGT către un obiect pentru a recupera informaţii de autorizare despre obiect. Aceasta se iveşte în unele situaţii neaşteptate, cum ar fi COPY, care trebuie să recupereze informaţii de autorizare asupra obiectului sursă pentru a seta autorizările echivalente asupra obiectului destinaţie.
8. Atunci când modifică proprietarul sau grupul unui obiect, utilizatorul trebuie să aibe nu numai autorizare corespunzătoare pentru obiect, dar de asemenea trebuie să aibe autorizare de date *ADD către noul profil de utilizator proprietar/grup şi autorizare de date *DELETE spre profilul proprietar/grup vechi. Aceste autorizări de date nu sunt înrudite cu autorizările de date ale sistemului de fişiere. Aceste autorizări de date pot fi afişate utilizând comanda DSPOBJAUT şi modificate utilizând comanda EDTOBJAUT. Aceasta se iveşte de asemenea neaşteptat la COPY atunci când se încearcă setarea ID de grup pentru un obiect nou.

9. Comanda MOV este cunoscută a genera erori de autorizare confuze, în special atunci când se mută de pe un sistem de fişiere fizic pe altul, sau atunci când se execută conversii de date. În aceste cazuri, mutarea devine de fapt o operaţie de copiere-şi-ştergere. Prin urmare, comanda MOV poate fi influenţată de către toate considerentele de autorizare aceleaşi cu cele ale comenzii COPY (vezi 7 şi 8 mai sus) şi ale comenzii RMVLNK, în plus faţă de alte considerente specifice MOV.

Următoarele secţiuni vă oferă consideraţii pentru câteva sisteme de fişiere reprezentative. Pentru informaţii suplimentare despre un anumit sistem de fişiere de pe serverul dumneavoastră iSeries, va trebui să consultaţi documentaţia pentru programul licenţiat care foloseşte sistemul de fişiere.

Sistemele de fişiere root (/), QOpenSys şi cele definite utilizator

Următoarele sunt consideraţii despre securitate pentru sistemele de fişiere root, QOpenSys şi definite de utilizator.

Cum funcţionează autorizarea

Sistemele de fişiere root, QOpenSys şi cele definite utilizator furnizează o combinaţie de capacităţi server iSeries, PC şi UNIX** ambele pentru gestiunea obiectelor şi pentru securitate. Când folosiţi comenzile Sistem de fişiere integrat de la o sesiune server iSeries (WRKAUT şi CHGAUT), puteţi seta toate autorizările obiect normale server iSeries. Aceasta include autorizările *R, *W şi *X care sunt compatibile cu Spec 1170 (sisteme de operare tip UNIX).

Notă: Sistemele de fişiere root, QOpenSys şi definite de utilizator sunt echivalente din punct de vedere funcţional. Sistemul de fişiere QOpenSys este sensibil la majuscule (case-sensitive). Sistemul de fişiere rădăcină nu este. Sistemele de fişiere definite de utilizator pot fi definite astfel încât să facă distincţie între literele mici şi majuscule. Deoarece aceste sisteme de fişiere au aceleaşi caracteristici de securitate, puteţi să consideraţi, în subiectele care urmează, că numele sistemelor de fişiere se pot schimba între ele.

Când accesaţi sistemul de fişiere ca un administrator de la o sesiune PC, puteţi seta atributele obiectelor pe care PC-ul le utilizează pentru a restricţiona anumite tipuri de acces:
- Sistem (System)
- Ascuns (Hidden)
- Arhivă (Archive)
- Doar pentru citire (Read-only)

Aceste atribute PC sunt în completare, nu înlocuiesc valorile de autorizare obiect ale serverului iSeries.

Când un utilizator încearcă să acceseze un obiect în sistemul de fişiere rădăcină, OS/400 impune toate valorile şi atributele de securitate ale obiectului, chiar dacă aceste autorizări sunt ″vizibile″ sau nu de la interfaţa utilizatorului. De exemplu, presupuneţi că atributul doar pentru citire (read-only) al unui obiect este setat. Un utilizator PC nu poate şterge obiectul prin intermediul unei interfeţe iSeries Access. Un utilizator server iSeries cu o funcţie staţie de lucru fixată nu poate şterge de asemenea obiectul, chiar dacă utilizatorul serverului iSeries are autorizarea specială *ALLOBJ. Înainte ca obiectul să poată fi şters, un utilizator autorizat trebuie să folosească o funcţie PC pentru a reseta valoarea doar pentru citire (read-only) pe off. Similar, un utilizator PC poate să nu aibă suficientă autorizare OS/400 pentru a schimba atributele de securitate relevante PC ale unui obiect.

Aplicaţiile tip UNIX care rulează pe servere iSeries folosesc interfeţe de programare aplicaţii (API-uri) gen UNIX pentru a accesa date din sistemul de fişiere root. Cu API-uri tip UNIX, aplicaţiile pot recunoaşte şi menţine următoarele informaţii de securitate:
- Proprietar de obiect
- Proprietar grup (autorizare grup principală pentru serverul iSeries)
- Citire (fişiere)
- Scriere (conţinut modificare)
- Executare (rulare programe sau căutare directoare)

Sistemul mapează aceste date de autorizare la obiecte server iSeries existente şi autorizări de date:

- Citire (*R) = *OBJOPR şi *READ
- Scriere (*W) = *OBJOPR, *ADD, *UPD, *DLT
- Executare (*X) = *OBJOPR şi *EXECUTE

Conceptele pentru alte autorizări de obiect (*OBJMGT, *OBJEXIST, *OBJALTER şi *OBJREF) nu există într-un mediu tip UNIX.

Totuşi, aceste autorizări pentru obiecte există pentru toate obiectele din sistemul de fişiere root. Când creaţi un obiect utilizând un API de tip UNIX, acel obiect moşteneşte aceste autorizări din directorul părinte, determinând următoarele:

- Proprietarul obiectului nou are aceeaşi autorizare pentru obiect ca şi proprietarul directorului părinte.
- Grupul primar al obiectului nou are aceeaşi autorizare pentru obiect ca şi grupul primar al directorului părinte.
- Publicul obiectului nou are aceeaşi autorizare pentru obiect ca şi publicul directorului părinte.

Autorizările datelor noului obiect pentru proprietar, grup primar şi public sunt specificate în API cu parametrul de mod. Când toate autorizările obiectului sunt setate ’on’, obţineţi o autorizare corespunzătoare unui mediu de tip UNIX. Este de preferat să le lăsaţi setate pe ’on’, în caz că nu doriţi să obţineţi o comportare de tip POSIX.

Când rulaţi aplicaţii ce folosesc API UNIX, sistemul impune toate autorizările obiect, chiar dacă sunt ″vizibile″ sau nu aplicaţiilor tip UNIX. De exemplu, sistemul va impune autorizarea din listele de autorizări chiar dacă conceptul de listă de autorizări nu există în sistemele de operare tip UNIX.

Dacă aveţi un mediu de aplicaţie compus, trebuie să vă asiguraţi că nu faceţi schimbări de autorizare într-un mediu care va bloca aplicaţiile din celălalt mediu.

Lucrul cu securitatea pentru sistemele de fişiere Root (/), QOpenSys şi definite de utilizator

Cu introducerea pentru Sistem de fişiere integrat, serverele iSeries furnizează de asemenea un nou set de comenzi pentru lucrul cu obiecte pe mai multe sisteme de fişiere. Acest set de comenzi include comenzile pentru gestiune securitate:
- Modificare auditare - Change Auditing (CHGAUD)
- Modificare autorizare - Change Authority (CHGAUT)
- Modificare proprietar - Change Owner (CHGOWN)
- Modificare grup primar - Change Primary Group (CHGPGP)
- Afişare autorizări - Display Authority (DSPAUT)
- Gestiune autorizări - Work with Authority (WRKAUT)

Aceste comenzi grupează datele importante şi autorizările obiect în subseturile autorizare tip UNIX:
***RWX** Citire/Scriere/Execuţie (Read/Write/Execute)

***RW** Citire/Scriere (Read/Write)
***R** Citire (Read)
***WX** Scriere/Execuţie (Write/Execute)
***W** Scriere (Write)
***X** Execuţie (Execute)

În plus, sunt disponibile API-uri de tip UNIX pentru gestiunea securităţii.

Autorizare publică la directorul root

La livrarea sistemului, autorizarea publică a directorului rădăcină este *ALL (toate autorizările obiect şi toate autorizările de date). Această setare furnizează flexibilitate şi compatibilitate atât cu ceea ce aşteaptă aplicaţiile gen UNIX cât şi cu ce aşteaptă utilizatorii normali ai serverului iSeries. Un utilizator server iSeries cu capacitatea de linie de comandă poate crea o nouă bibliotecă în sistemul de fişiere QSYS.LIB utilizând doar comanda CRTLIB. În mod normal, autorizarea pe un server iSeries normal permite aceasta. Similar, cu setările livrate pentru sistemul de fişiere rădăcină, un utilizator tipic poate crea un nou director în sistemul de fişiere rădăcină (aşa cum ar crea un nou director pe PC).

Ca administrator de securitate, trebuie să educaţi utilizatorii despre protejarea adecvată a obiectelor pe care le creează. Când un utilizator creează o bibliotecă, probabil autorizarea publică pentru bibliotecă nu trebuie să fie *CHANGE (implicită). Utilizatorul trebuie să seteze autorizarea publică fie la *USE, fie la *EXCLUDE, în funcţie de conţinutul bibliotecii.

Dacă utilizatorii dumneavoastră trebuie să creeze noi directoare în sistemul de fişiere root, QOpenSys sau definite de utilizator, aveţi câteva opţiuni de securitate:

- Puteţi învăţa utilizatorii dumneavoastră să suprascrie autorizarea implicită când creează directoare noi. Autorizarea implicită nu este cea moştenită de la directorul părinte. În cazul creării unui nou director în directorul rădăcină, autorizarea publică implicită va fi *ALL.
- Puteţi crea un subdirector ″master″ sub directorul rădăcină. Setaţi autorizarea publică pentru acest director master cu una potrivită pentru organizaţia dumneavoastră. Apoi instruiţi utilizatorii să creeze orice director personal în acest subdirector master. Noile lor directoare vor moşteni autorizarea sa.
- Puteţi schimba autorizarea publică pentru directorul rădăcină pentru a împiedica utilizatorii să creeze obiecte în acest director (Eliminaţi autorizările *W, *OBJEXIST, *OBJALTER, *OBJREF şi *OBJMGT). Totuşi, trebuie să evaluaţi dacă această modificare va cauza probleme oricărei aplicaţii a dumneavoastră. Puteţi, de exemplu, să aveţi aplicaţii tip UNIX care se aşteaptă să poată şterge obiectele din directorul rădăcină.

Comanda PRTPVTAUT (Print private authorities objects - Tipărire obiecte autorizări private)

Comanda Tipărire Autorizări Private (Print Private Authorities - PRTPVTAUT) vă permite să tipăriţi un raport al tuturor autorizărilor private pentru obiecte de un anumit tip dintr-o anumită bibliotecă sau director. Raportul conţine toate obiectele de tipul specificat şi utilizatorii care sunt autorizaţi pentru obiect. Acesta este un mod de a verifica diferitele surse de autorizare pentru obiecte.

Această comandă tipăreşte trei rapoarte pentru obiectele selectate. Primul raport (Full Report) conţine toate autorizările private pentru fiecare obiect selectat. Al doilea raport (Changed Report) conţine adăugările şi modificările autorizărilor private pentru obiectele selectate dacă a fost rulată anterior comanda PRTPVTAUT pentru obiectele specificate din biblioteca sau directorul specificat. Orice obiect nou de tipul selectat, noi autorizări pentru obiectele existente sau modificări ale autorizărilor pentru obiectele existente sunt listate în ’Changed Report’. Dacă comanda PRTPVTAUT nu a fost rulată anterior pentru obiectele specificate din biblioteca sau directorul specificat, atunci nu va fi ’Changed Report’. Dacă a fost rulată

anterior comanda, dar nu s-au făcut modificări pentru autorizările obiectelor, atunci 'Changed Report' este tipărit, dar nu va fi listat nici un obiect.

Al treilea raport (Deleted Report) conţine toate ştergerile de utilizatori autorizaţi în mod privat de la obiectele specificate de când comanda PRTPVTAUT a fost rulată ultima dată. Toate obiectele care au fost şterse sau utilizatorii care nu mai sunt ca utilizatori autorizaţi în mod privat sunt listaţi în 'Deleted Report'. Dacă comanda PRTPVTAUT nu a fost rulată anterior, atunci nu va fi 'Deleted Report'. Dacă comanda a fost rulată anterior, dar nu s-a executat nici o operaţie de ştergere pentru obiecte, atunci 'Deleted Report' este tipărit dar nici un obiect nu este listat.

Restricţii: Trebuie să aveţi autorizarea specială *ALLOBJ pentru a utiliza această comandă.

Exemple:

Această comandă creează raportul complet, cu modificări şi ştergeri pentru toate obiectele fişier din PAYROLLLIB:

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

Această comandă creează raportul complet, cu modificări şi ştergeri pentru toate obiectele fişier stream din director:

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

Această comandă creează raportul complet, cu modificări şi ştergeri pentru toate obiectele fişier stream din structura de subdirectoare ce porneşte din director:

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

Comanda PRTPUBAUT (Print private authorities objects - Tipărire obiecte autorizate public)

Comanda Tipărire Obiecte Autorizate Public (Print Publicly Authorized Objects - PRTPUBAUT) vă permite să tipăriţi un raport al obiectelor specificate care nu au autorizarea publică *EXCLUDE. Pentru obiectele *PGM, doar programele care nu au autorizarea publică *EXCLUDE pe care un utilizator le poate apela (fie programul este domeniu utilizator, fie nivelul de securitate sistem (variabila de sistem QSECURITY) este 30 sau mai mic) vor fi incluse în raport. Acesta este un mod de a verifica obiectele dacă orice utilizator al sistemului este autorizat să le acceseze.

Această comandă va tipări două rapoarte. Primul raport (Full Report) va conţine toate obiectele specificate care nu au autorizarea publică *EXCLUDE. Al doilea raport (Changed Report) va conţine obiectele care nu au acum autorizarea publică *EXCLUDE, care au autorizarea publică *EXCLUDE sau nu au existat când a fost rulată comanda PRTPUBAUT. Dacă comanda PRTPUBAUT nu a fost rulată pentru obiectele şi bibliotecile sau directoarele specificate, atunci nu va exista 'Changed Report'. Dacă comanda a fost rulată, dar nici un obiect adiţional nu are autorizarea publică *EXCLUDE, atunci 'Changed Report' va fi tipărit dar nu vor fi obiecte listate.

Restricţii: Trebuie să aveţi autorizarea specială *ALLOBJ pentru a folosi această comandă.

Exemple:

Această comandă creează raportul complet, cu modificări şi ştergeri pentru toate obiectele fişier din biblioteca GARRY ce nu au o autorizare publică *EXCLUDE:

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

Această comandă creează raportul complet, cu modificări şi ştergeri pentru toate obiectele fişier stream din structura de subdirectoare ce porneşte din directorul garry, ce nu au o autorizare publică *EXCLUDE:

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

Restricţionarea accesului la sistemul de fişiere QSYS.LIB

Deoarece sistemul de fişiere rădăcină este acoperirea sistemului de fişiere, sistemul de fişiere QSYS.LIB apare ca un subdirector al directorului rădăcină. Prin urmare, orice utilizator PC cu acces la serverul dumneavoastră iSeries poate manipula obiecte stocate în biblioteca serverului iSeries (sistemul de fişiere QSYS.LIB) cu acţiuni şi comenzi PC normale. Un utilizator PC poate, de exemplu, trage un obiect QSYS.LIB (cum ar fi biblioteca cu fişierele de date critice) la shredder.

Aşa cum aţi învăţat în “Sistemele de fişiere root (/), QOpenSys şi cele definite utilizator” la pagina 91, sistemul impune toate autorizările obiect chiar dacă este sau nu vizibil la interfaţă. În consecinţă, un utilizator nu poate şterge (shred) un obiect dacă nu are autorizarea *OBJEXIST pentru obiect. Totuşi, dacă iSeries depinde mai mult de securitatea accesului la meniu decât de securitatea obiectelor, utilizatorul de PC poate foarte bine să găsească obiectele din sistemul de fişiere QSYS.LIB care sunt disponibile pentru ştergere.

După îmbunătăţirea folosirii sistemului dumneavoastră şi furnizarea diferitelor metode de acces, veţi descoperi curând că securitatea accesului la meniu nu este suficientă. Capitolul 5, “Protejarea informaţiilor cu autorizare obiect”, la pagina 41 comentează strategiile dumneavoastră de suplimentare a controlului accesului la meniu cu securitatea obiectelor. Totuşi, serverele iSeries furnizează de asemenea o modalitate simplă pentru dumneavoastră de a preveni accesul la sistemul de fişiere QSYS.LIB prin structura de directoare a sistemului de fişiere root. Puteţi folosi lista de autorizări QPWFSERVER pentru a controla ce utilizatori pot accesa sistemul de fişiere QSYS.LIB prin directorul rădăcină.

Atunci când autorizarea unui utilizator în lista de autorizări QPWFSERVER este *EXCLUDE, utilizatorul nu poate intra în directorul QSYS.LIB din structura de director rădăcină. Când o autorizare utilizator este *USE, acesta poate intra în director. Odată ce utilizatorul are autorizare să intre în director, autorizarea obiect normală este aplicată oricărei acţiuni pe care utilizatorul încearcă să o facă asupra unui obiect din sistemul de fişiere QSYS.LIB. Cu alte cuvinte, autorizările din lista de autorizări QPWFSERVER acţionează ca o uşă pentru întregul sistem de fişiere QSYS.LIB. Pentru utilizatorul cu autorizarea *EXCLUDE, uşa este încuiată. Pentru utilizatorul cu autorizarea *USE (sau orice autorizare mai puternică), uşa este deschisă.

Pentru cele mai multe situaţii, utilizatorii nu trebuie să folosească o interfaţă cu directoarele pentru a accesa obiectele din sistemul de fişiere QSYS.LIB. Probabil că veţi dori să setaţi autorizarea publică a listei de autorizări QPWFSERVER pe *EXCLUDE. Reţineţi, această autorizare a listei de autorizări deschide sau închide uşa tuturor bibliotecilor din sistemul de fişiere QSYS.LIB, inclusiv bibliotecile utilizator. Dacă aveţi utilizatori care se opun acestei excluziuni, puteţi evalua cererile lor la nivel individual. Dacă corespunde, puteţi autoriza explicit un utilizator individual la lista autorizărilor. Totuşi, trebuie să vă asiguraţi că utilizatorul are autorizarea corespunzătoare pentru obiectele din sistemul de fişiere QSYS.LIB. Altfel, utilizatorul poate şterge neintenţionat obiectele sau întreaga bibliotecă.

Note:

1. Când vi se livrează sistemul, autorizarea publică a listei autorizărilor QPWFSERVER este *USE.

2. Dacă în mod explicit autorizaţi un utilizator, lista de autorizări controlează accesul numai cu servirea de fişiere iSeries Access, NetServer şi servirea de fişiere între serverele iSeries. Aceasta nu împiedică accesul la aceleaşi fişiere prin intermediul FTP, ODBC şi alte reţele.

Directoare de securitate

Pentru a accesa un obiect din sistemul de fişiere rădăcină, treceţi prin întreaga cale până la acel obiect. Pentru a căuta un director, trebuie să aveţi autorizarea *X (*OBJOPR şi *EXECUTE) pentru acel director. Să presupunem că, de exemplu, doriţi să accesaţi următorul obiect:

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

Trebuie să dispuneţi de autorizare *X pentru companii director şi clienţi director.

Cu sistemul de fişiere rădăcină, puteţi crea o legătură simbolică la un obiect. Conceptual, o legătură simbolică este un alias pentru un nume de cale. Uzual, este mai scurt şi mai uşor de amintit decât întregul nume al căii. O legătură simbolică nu creează fizic, totuşi, o cale diferită pentru obiect. Utilizatorul are încă nevoie de autorizarea *X pentru orice director şi subdirector din calea fizică a obiectului.

Pentru obiectele din sistemul de fişiere rădăcină, puteţi utiliza securizarea directoarelor aşa cum trebuie să folosiţi securizarea bibliotecilor din sistemul de fişiere QSYS.LIB. Puteţi, de exemplu, să setaţi securitatea publică a directorului la *EXCLUDE pentru a împiedica accesul utilizatorilor publici la toate obiectele din acel arbore.

Securitate pentru noile obiecte

Când creaţi un nou obiect în sistemul de fişiere root, interfaţa utilizată determină autorizările obiectului. De exemplu, dacă utilizaţi comanda CRTDIR şi parametrii impliciţi, noul director moşteneşte toate caracteristicile de autorizare ale directorului părinte, inclusiv autorizările private, autorizarea grup primar şi asocierea listei de autorizări. Următoarele secţiuni descriu modul în care sunt determinate autorizările pentru fiecare tip de interfaţă.

Autorizarea vine de la directorul părinte imediat, nu de la directoarele de mai sus, din arbore. În consecinţă, în calitate de administrator de securitate, trebuie să vizualizaţi autorizările pe care le asociaţi directoarelor dintr-o ierarhie din două perspective:

- Cum afectează autorizarea accesul la obiectele din arbore (ca şi autorizarea la bibliotecă).
- Cum afectează autorizarea noile obiecte create (ca şi valoarea CRTAUT pentru biblioteci).

Recomandare: Puteţi dori să daţi utilizatorilor care lucrează în sistemul de fişiere integrat un director home (de exemplu, /home/usrxxx), apoi setaţi corespunzător securitatea (cum ar fi PUBLIC *EXCLUDE). Orice director pe care utilizatorul îl creează în directorul lor home va moşteni autorizările sale.

Următoarele sunt descrierile moştenirii autorizărilor pentru diferite interfeţe:

Folosirea comenzii Creare director (Create Directory)

Când creaţi un nou subdirector folosind comanda CRTDIR, aveţi două opţiuni pentru a specifica autorizarea:

- Puteţi specifica autorizarea publică (autorizare date, obiecte sau ambele).
- Puteţi specifica *INDIR pentru autorizarea datelor, obiectelor sau a ambelor. Dacă specificaţi *INDIR pentru ambele autorizări, la date şi la obiecte, sistemul face o copie exactă a tuturor informaţiilor despre autorizare de la directorul părinte la noul obiect,

inclusiv lista autorizărilor, grup primar, autorizare publică şi autorizări private (Sistemul nu copiază autorizarea privată pe care profilul QSYS sau QSECOFR o are asupra obiectului).

Crearea unui director cu un API

Când creaţi un director utilizând API mkdir(), specificaţi autorizarea de date pentru proprietar, grupul primar şi public (folosind formatul de autorizare *R, *W şi *X). Sistemul foloseşte informaţiile din directorul părinte pentru a seta autorizările obiectului pentru proprietar, grup primar şi public.

Deoarece sistemele de operare tip UNIX nu au conceptul de autorizare obiect, mkdir() API nu poate specifica autorizările obiect. Dacă doriţi autorizări obiect diferite, puteţi folosi comanda (CHGAUT) a serverului iSeries. Totuşi, când ştergeţi anumite autorizări obiect, aplicaţiile tip UNIX pot să nu funcţioneze aşa cum vă aşteptaţi.

Crearea unui fişier flux cu API-ul open() sau creat()

Când utilizaţi API-ul creat() pentru a crea un fişier stream, puteţi specifica autorizările de date pentru proprietar, grup primar şi public (folosind autorizările tip UNIX *R, *W şi *X). Sistemul foloseşte informaţiile din directorul părinte pentru a seta autorizările obiectului pentru proprietar, grup primar şi public.

Puteţi specifica aceste autorizări şi atunci când folosiţi API-ul open() pentru a crea un fişier stream. În acelaşi timp, când folosiţi API-ul open() puteţi specifica dacă obiectul trebuie să moştenească toate autorizările de la directorul părinte. Acesta poartă denumirea de mod moştenit. Când specificaţi modul moştenire, sistemul creează o potrivire completă cu autorizările părintelui, inclusiv lista autorizărilor, grup primar, autorizare publică şi autorizările private. Această opţiune lucrează ca şi specificarea *INDIR la comanda CRTDIR.

Crearea unui obiect folosind o interfaţă PC

Când folosiţi o aplicaţie PC pentru a crea un obiect în sistemul de fişiere rădăcină, sistemul moşteneşte automat toate autorizările directorului părinte. Acestea includ lista autorizărilor, grup primar, autorizare publică şi autorizări private. Aplicaţiile PC nu au nici un echivalent pentru a specifica autorizarea când creaţi un obiect.

Sistemul de fişiere QFileSvr.400

Cu sistemul de fişiere QFileSvr.400, un utilizator (USERX) de pe sistemul iSeries (SYSTEMA) poate accesa datele sau alt sistem iSeries (SYSTEMB) conectat. USERX are o interfaţă care este asemănătoare cu interfaţa Client Access. Serverul iSeries la distanţă (SYSTEMB) apare ca un director cu toate sistemele lui de fişiere ca subdirectoare.

Când USERX încearcă să acceseze SYSTEMB cu această interfaţă, SYSTEMA trimite numele profilului utilizator şi parola criptată a lui USERX către SYSTEMB. Acelaşi profil utilizator şi parolă trebuie să existe pe SYSTEMB sau SYSTEMB refuză cererea.

Dacă SYSTEMB acceptă cererea, USERX apare pentru SYSTEMB ca orice alt utilizator Client Access. Aceleaşi reguli de verificare a autorizării se aplică pentru orice acţiune pe care USERX o încearcă.

Ca administrator de securitate, trebuie să ştiţi că sistemul de fişiere QFileSvr.400 reprezintă o altă posibilă uşă către sistemul dumneavoastră. Nu puteţi presupune că limitaţi conectarea interactivă a utilizatorilor dumneavoastră de la distanţă cu un passthrough terminal de afişare. Dacă subsistemul QSERVER rulează şi sistemul dumneavoastră este conectat la alt sistem iSeries, utilizatorii de la distanţă pot accesa sistemul dumneavoastră ca şi cum ar fi la un PC

local ce rulează Client Access. Este foarte probabil că sistemul dumneavoastră va avea o conectare care necesită subsistemul QSERVER în rulare. Acesta este încă un motiv pentru ca schema de autorizare a obiectului să fie bună.

Sistemul de fişiere reţea

Network File System (NFS) oferă acces la şi de la sistemele care au implementări NFS. NFS este o metodă standard industrială pentru partajarea informaţiilor între sistemele reţea şi utilizatori. Cele mai răspândite sisteme de operare (inclusiv sistemele de operare PC) furnizează NFS. Pentru UNIX sistemeel, NFS este metoda principală pentru accesarea datelor. Serverele iSeries pot acţiona atât ca client NFS cât şi ca server NFS.

Dacă sunteţi administratorul de securitate al unui sistem iSeries ce acţionează ca un server NFS, trebuie să înţelegeţi şi să gestionaţi aspectele de securitate ale NFS-ului. În continuare sunt prezentate sugestii şi consideraţii:

- Trebuie să porniţi explicit funcţia server NFS utilizând comanda STRNFSSVR. Controlaţi cine are autorizarea să utilizeze această comandă.
- Faceţi un director sau un obiect disponibil pentru clienţii NFS prin exportarea lui. În consecinţă, controlaţi foarte strict ce părţi din sistemul dumneavoastră vor fi disponibile clienţilor NFS din reţeaua dumneavoastră.
- Când exportaţi, puteţi specifica ce clienţi au acces la obiecte. Identificaţi un client după numele sistemului sau adresa IP. Un client poate fi un PC individual sau un server iSeries întreg sau sistem UNIX. În terminologia NFS, clientul (adresa IP) este considerat o maşină.
- Când exportaţi, puteţi specifica accesul doar pentru citire sau citire/scriere pentru fiecare maşină care are acces la un director sau obiect exportat. În cele mai multe cazuri, probabil că veţi dori să furnizaţi accesul doar pentru citire.
- NFS nu furnizează protecţie prin parolă. Este realizat pentru a partaja datele între sisteme de încredere. Când un utilizator cere accesul, Serverul primeşte uid-ul utilizatorului. Următoarele sunt câteva consideraţii despre uid:
  - Serverul iSeries încearcă să localizeze un profil utilizator cu acelaşi uid. Dacă găseşte un uid care corespunde, foloseşte drepturile profilului utilizator. Dreptul (privilegiul) este un termen NFS care descrie folosirea autorizărilor unui utilizator. Aceasta este similară cu swap-area profilului în alte aplicaţii server iSeries.
  - Când exportaţi un director sau un obiect, puteţi specifica dacă veţi permite accesul cu un profil cu autorizare root. Serverul NFS pe serverele iSeries modifică autorizarea root la autorizarea specială *ALLOBJ. Dacă specificaţi că nu permiteţi autorizarea root, un utilizator NFS cu un uid ce mapează un profil utilizator cu autorizare specială *ALLOBJ nu va putea accesa obiectul din acel profil. În schimb, dacă este permis accesul anonim, solicitantul va fi mapat la profilul anonymous.
  - Când exportaţi un director sau un obiect, puteţi specifica dacă veţi permite cereri anonymous. O cerere anonymous este o cerere cu un uid care nu corespunde nici unui uid de pe sistemul dumneavoastră. Dacă alegeţi să permiteţi cereri anonymous, sistemul mapează utilizatorul anonymous la profilul utilizator QNFSANON furnizat de IBM. Acest profil utilizator nu are nici o autorizare specială sau explicită (La exportare, puteţi specifica un alt profil utilizator pentru cererile anonymous, dacă doriţi).
- Când serverul dumneavoastră iSeries participă într-o reţea NFS (sau orice reţea cu sistemeUNIX care depind de uids), va fi nevoie probabil să gestionaţi propriile dumneavoastră uid-uri decât să lăsaţi sistemul să le aloce automat. Va trebui să coordonaţi uid-urile cu alte sisteme din reţeaua dumneavoastră.

  Puteţi descoperi că trebuie să schimbaţi uid-urile (chiar şi pentru profilurile utilizator furnizate de IBM) pentru a fi compatibile cu alte sisteme din reţeaua dumneavoastră. Este disponibil un program pentru a face mai simplă modificarea uid-ului pentru un profil

utilizator. (Când modificaţi uid-ul pentru un profil utilizator, va trebui de asemenea să modificaţi uid-ul pentru toate obiectele pe care le deţine profilul fie în directorul root fie în directorul QOpenSrv.) Programul QSYCHGID modifică automat uid atât în profilul utilizator cât şi în obiectele ce-i aparţin. Pentru informaţii despre cum să utilizaţi acest program, consultaţi cartea *System API Reference (Referinţă API sistem)*.

Capitolul 12. Securizarea comunicaţiilor APPC

Când sistemul dumneavoastră participă într-o reţea cu alte sisteme, un nou set de uşi şi ferestre devin disponibile pentru sistemul dumneavoastră. Ca administrator de securitate, trebuie să luaţi cunoştinţă de opţiunile pe care le puteţi utiliza pentru a controla intrările în sistemul dumneavoastră într-un mediu APPC.

APPC (Advanced program-to-program communications) reprezintă un mod prin care calculatoarele, inclusiv calculatoarele personale, comunică între ele. Passthrough staţie de afişare, gestiunea datelor distribuite şiiSeries Access pentru Windows pot folosi toate comunicaţiile APPC.

Subiectele care urmează oferă informaţii de bază despre cum funcţionează comunicaţiile APPC şi cum puteţi seta corect securitatea. Aceste subiecte se concentrează în primul rând asupra elementelor relevante pentru securitate ale configuraţiei APPC. Pentru a adapta acest exemplu la situaţia dumneavoastră, va trebui să aveţi grijă cu persoanele care administrează reţeaua dumneavoastră de comunicaţii şi probabil furnizorii dumneavoastră de aplicaţii. Folosiţi aceste informaţii ca un fundament pentru a vă ajuta să înţelegeţi problemele de securitate şi opţiunile care sunt disponibile pentru APPC.

Securitatea nu este niciodată "gratuită". Anumite sugestii pentru a face securitatea reţelei mai uşoară poate face administrarea reţelei mai dificilă. De exemplu, aceste informaţii nu pun accentul pe APPN (Advanced Peer-to-Peer Networking), deoarece securitate este mai uşor de înţeles şi de gestionat fără APPN. Oricum, fără APPN, administratorul de reţea trebuie să creeze manual informaţia de configurare APPN creează automat.

PC-urile utilizează comunicaţiile, de asemenea

Multe metode pentru conectarea de PC-uri la serverele dumneavoastră iSeries depind de comunicaţii, cum ar fi APPC sau TCP/IP. Când citiţi subiectele care urmează, asiguraţi-vă că luaţi în considerare problemele de securitate pentru conectatea atât la alte sisteme, cât şi la PC-uri. Când planificaţi protejarea reţelei, asiguraţi-vă că nu afectaţi în mod negativ PC-urile care sunt conectate la sistemul dumneavoastră.

Terminologia APPC

APPC oferă unui utilizator de pe un sistem posibilitatea de a realiza anumite acţiuni pe un alt sistem. Sistemul de pe care pornesc cererile este numit într-unul din următoarele feluri:

- **Sistem sursă**
- **Sistem local**
- **Client**

Sistemul care primeşte cererile este numit într-unul din următoarele feluri:

- **Sistem destinaţie**
- **Sistem la distanţă**
- **Server**

Elemente de bază ale comunicaţiilor APPC

Din perspectiva unui administrator de securitate, următoarele trebuie să se petreacă înainte ca un utilizator sau un sistem (SYSTEMA) să poată executa activităţi semnificative pe alt sistem (SYSTEMB):

- Sistemul sursă (SYSTEMA) trebuie să ofere o cale spre sistemul destinaţie (SYSTEMB). Această cale este denumită **sesiune APPC**.
- Sistemul destinaţie trebuie să identifice utilizatorul şi să asocieze utilizatorul cu un profil de utilizator. Sistemul destinaţie trebuie să suporte algoritmul de criptare a sistemului sursă (vezi “Nivele de parole” la pagina 14pentru mai multe informaţii).
- Sistemul destinaţie trebuie să pornească un job pentru utilizator cu un mediu corespunzător (valori administrare lucru).

Subiectele care urmează discută aceste elemente şi modul în care au legătură cu securitatea. Administratorul de securitate de pe sistemul destinaţie are ca principală responsabilitate asigurarea faptului că utilizatorii APPC nu încalcă securitatea. Totuşi, când administratorii de securitate de pe ambele sisteme lucrează împreună, administrarea securităţii APPC devine mult mai uşor de făcut.

Exemplu: O sesiune APPC de bază

Într-un mediu APPC, când un utilizator sau o aplicaţie de pe un sistem cere accesul la un alt sistem, cele două sistem stabilesc o sesiune. Pentru a stabili sesiunea, sistemele trebuie să lege două descrieri de dispozitive APPC care se potrivesc. Parametrul nume locaţie de la distanţă (RMTLOCNAME) din descrierea dispozitivului SYSTEMA trebuie să se potrivească cu parametrul nume locaţie locală (LCLLOCNAME) din descrierea dispozitivului sistemului SYSTEMB şi invers.

Pentru ca două sisteme să stabilească o sesiune APPC, parolele locaţiilor din descrierile dispozitivelor APPC de pe SYSTEMA şi SYSTEMB trebuie să fie identice. Ambele trebuie să specifice *NONE sau ambele trebuie să specifice aceeaşi valoare.

Dacă parolele au o altă valoare decât *NONE, ele sunt stocate şi transmise într-un format codificat. Dacă parolele se potrivesc, sistemele stabilesc o sesiune. Dacă parolele nu se potrivesc, cererea utilizatorului este respinsă. Când sistemele specifică parolele locaţiilor pentru a stabili o sesiune, acest lucru este numit **legătură sigură**.

Notă: Nu toate sistemele furnizează suport pentru funcţia legătură sigură.

Restricţionarea sesiunilor APPC

Ca administrator de securitate pe un sistem sursă, puteţi utiliza autorizarea obiectelor pentru a controla cine poate încerca să acceseze alte sisteme. Setaţi autorizarea publică pentru descrierile dispozitivelor APPC pe *EXCLUDE şi acordaţi autorizarea *CHANGE anumitor utilizatori. Utilizaţi variabila de sistem QLMTSECOFR pentru a împiedica utilizatorii cu autorizarea specială *ALLOBJ să utilizeze comunicaţiile APPC.

Ca administrator de securitate pe un sistem destinaţie, puteţi utiliza autorizarea pentru dispozitivele APPC pentru a împiedica utilizatorii să pornească o sesiune APPC pe sistemul dumneavoastră. Totuşi, trebuie să înţelegeţi ce ID utilizator va încerca să acceseze descrierea de dispozitiv APPC. “Accesul utilizatorului APPC la sistemul ţintă” la pagina 103 descrie cum asociază serverele iSeries un ID utilizator cu o cerere de la o sesiune APPC.

Notă: Puteţi utiliza comanda Tipărire Obiecte Autorizate Public (Print Publicly Authorized Objects - PRTPUBAUT *DEVD) şi comanda Tipărire Autorizări Private (Print Private Authorities) - PRTPVTAUT *DEVD) pentru a afla cine are autorizare pentru descrierile dispozitivelor de pe sistemul dumneavoastră.

Când sistemul utilizează APPN, creează automat un nou dispozitiv APPC când nici un dispozitiv existent nu este disponibil pentru ruta pe care a ales-o sistemul. O metodă de restricţionare a accesului la dispozitivele APPC dintr-un sistem utilizat APPN constă în

crearea unei liste de autorizare. Lista de autorizare conţine lista utilizatorilor care ar trebui autorizaţi pentru dispozitivele APPC. Folosiţi atunci comanda Modificare Valori Implicite Comandă (Change Command Default - CHGCMDDFT) pentru a modifica comanda CRTDEVAPPC. Pentru parametrul autorizare (AUT) din comanda CRTDEVAPPC, setaţi valoarea implicită pe lista de autorizare pe care aţi creat-o.

Notă: Dacă sistemul dumneavoastră utilizează altă limbă decât limba engleză, trebuie să modificaţi valoarea implicită a comenzii din biblioteca QSYSxxxx pentru fiecare limbă naţională care este pe sistemul dumneavoastră.

Utilizaţi parametrul parolă locaţie (LOCPWD) în descrierea dispozitivului APPC pentru a valida identitatea unui alt sistem care solicită o sesiune pe sistemul dumneavoastră (în numele unui utilizator sau al unei aplicaţii). Parola locaţiei vă poate ajuta să detectaţi un sistem impostor.

Când utilizaţi parolele locaţiilor, trebuie să vă coordonaţi cu administratorii de securitate de pe alte sisteme din reţea. De asemenea, trebuie să controlaţi cine poate crea sau modifica descrierile dispozitivelor APPC şi listele de configuraţie. Sistemul necesită autorizarea specială *IOSYSCFG pentru a utiliza comenzile care lucrează cu dispozitivele APPC şi cu listele de configuraţie.

Notă: Când utilizaţi APPN, parolele de locaţie sunt stocate în lista de configurare QAPPNRMT mai degrabă decât în descrierea dispozitivului.

Accesul utilizatorului APPC la sistemul ţintă

Când sistemele stabilesc sesiunile APPC, acestea creează o cale pentru utilizatorul solicitant pentru a ajunge la sistemul destinaţie. Multe alte elemente determină ce trebuie să facă utilizatorul pentru a intra pe alt sistem.

Subiectele care urmează descriu elementele care determină cum un utilizator APPC intră pe sistemul destinaţie.

Metode sistem pentru trimitere de informaţii despre un utilizator

Arhitectura APPC oferă trei metode pentru transmiterea informaţiilor de securitate despre utilizator de la sistemul sursă la sistemul destinaţie. Aceste metode sunt referite ca **valori de securitate proiectate**. Tabela 18 prezintă aceste metode:

Notă: Cartea *APPC Programming* oferă mai multe informaţii despre valorile de securitate proiectate.

Tabela 18. Valori de securitate în arhitectura APPC

Valoare de securitate arhitecturală	ID utilizator trimis sistemului destinaţie	Parolă trimisă serverului destinaţie
Nimic	Nu	Nu
Acelaşi	Da[1]	Vezi nota 2.
Program	Da	Da[3]

Tabela 18. Valori de securitate în arhitectura APPC (continuare)

Valoare de securitate arhitecturală	ID utilizator trimis sistemului destinaţie	Parolă trimisă serverului destinaţie

Note:

1. Sistemul sursă trimite identificatorul de utilizator dacă sistemul destinaţie specifică SECURELOC(*YES) sau SECURELOC(*VFYENCPWD).
2. Utilizatorul nu introduce o parolă la cerere deoarece parola este deja verificată de sistemul sursă. Pentru SECURELOC(*YES) şi SECURELOC(*NO), sistemul sursă nu transmite parola. Pentru SECURELOC(*VFYENCPWD), sistemul sursă extrage parola stocată, criptată şi o transmite (în forma criptată).
3. Sistemul trimite parola în formă criptată dacă ambele sisteme sursă şi destinaţie suportă criptarea parolei. În caz contrar, parola nu este criptată.

Aplicaţia pe care utilizatorul o solicită determină valorile de securitate proiectate. De exemplu, SNADS întotdeauna utilizează SECURITY(NONE). DDM utilizează SECURITY(SAME). Cu passthrough staţie de afişare, utilizatorul specifică valorile de securitate utilizând parametrii în comanda STRPASTHR.

În toate cazurile, sistemul destinaţie alege dacă să accepte o cerere cu valoarea de securitate care este specificată pe sistemul sursă. În unele situaţii, sistemul destinaţie poate respinge complet cererea. În alte situaţii, sistemul destinaţie poate impune o altă valoare de securitate. De exemplu, când un utilizator specifică identificatorul de utilizator şi parola în comanda STRPASTHR, cererea utilizează SECURITY(PGM). Totuşi, dacă valoarea de sistem QRMTSIGN este *FRCSIGNON pe sistemul destinaţie, utilizatorul încă vede ecranul Semnare. Cu *FRCSIGNON setat, sistemul întotdeauna utilizează SECURITY(NONE), care este echivalent cu neintroducerea de către utilizator a identificatorului de utilizator şi a parolei în comanda STRPASTHR.

Note:

1. Sistemele sursă şi destinaţie negociază valorile de securitate înainte ca datele să fie trimise. În situaţia în care sistemul destinaţie specifică SECURELOC(*NO) şi cererea este SECURITY(SAME), de exemplu, sistemul destinaţie spune sistemului sursă să utilizeze SECURITY(NONE). Sistemul sursă nu transmite identificatorul de utilizator.
2. Sistemul destinaţie refuză o cerere de sesiune când parola utilizatorului pe sistemul destinaţie a expirat. Aceasta se aplică numai cererilor de conexiune care transmit o parolă, inclusiv următoarele:
   - Cereri de sesiune de tipul SECURITY(PROGRAM).
   - Cereri de sesiune de tipul SECURITY(SAME) când valoarea lui SECURELOC este *VFYENCPWD.

Opţiuni pentru divizarea responsabilităţii de securitate reţea

Când sistemul dumneavoastră participă într-o reţea, trebuie să decideţi dacă să aveţi încredere în celelalte sisteme pentru a valida identitatea unui utilizator care încearcă să intre pe sistemul dumneavoastră. Veţi avea încredere că SYSTEMA se va asigura că USERA este chiar USERA (sau QSECOFR este chiar QSECOFR)? Sau veţi cere utilizatorului să introducă un identificator de utilizator şi o parolă din nou?

Parametrul locaţie sigură (SECURELOC) din descrierea dispozitivului APPC de pe sistemul destinaţie specifică dacă sistemul sursă este o locaţie sigură (de încredere).

Când ambele sisteme rulează o ediţie care suportă *VFYENCPWD, SECURELOC(*VFYENCPWD) furnizează protecţie suplimentară când aplicaţiile folosesc

SECURITY(SAME). Deşi solicitantul nu introduce o parolă la cerere, sistemul sursă extrage parola utilizatorului şi o trimite cu cererea. Pentru ca cererea să aibă succes, utilizatorul trebuie să aibă identificatorul de utilizator şi parola pe ambele sisteme.

Când sistemul destinaţie specifică SECURELOC(*VFYENCPWD) şi sistemul sursă nu suportă această valoare, sistemul destinaţie gestionează cererea ca SECURITY(NONE).

Tabela 19 arată cum lucrează împreună valorile de securitate proiectate şi valoarea SECURELOC:

Tabela 19. Cum lucrează împreună valoarea de securitate APPC şi valoarea SECURELOC

Sistem sursă	**Sistem destinaţie**	
Valoare de securitate arhitectură	**Valoare SECURELOC**	**Profil utilizator pentru job**
Nimic	Orice	Utilizator implicit[1]
Acelaşi	*NO	Utilizator implicit[1]
	*YES	Acelaşi profil de utilizator ca solicitantul de pe sistemul sursă
	*VFYENCPWD	Acelaşi profil de utilizator ca solicitantul de pe sistemul sursă Utilizatorul trebuie să aibă aceeaşi parolă pe ambele sisteme
Program	Orice	Profilul de utilizator care este specificat în cererea de pe sistemul sursă.

Note:

1. Utilizatorul implicit este determinat de intrarea de comunicaţii din descrierea subsistemului. "Asocierea de profiluri utilizator pe sistemul destinaţie pentru joburi" descrie acest lucru.

Asocierea de profiluri utilizator pe sistemul destinaţie pentru joburi

Când un utilizator solicită un job APPC pe alt sistem, cererea are asociat un nume mod. Nume mod poate veni de la cererea utilizatorului sau poate fi o valoare implicită din atributele reţelei sistemului sursă.

Sistemul destinaţie utilizează numele mod şi numele dispozitivului APPC pentru a determina cum va rula jobul. Sistemul destinaţie caută subsistemele active pentru o intrare de comunicaţii care se potriveşte cel mai bine cu numele dispozitivului APPC şi cu nume mod.

Intrarea de comunicaţii specifică ce profil de utilizator va utiliza sistemul pentru cererile SECURITY(NONE). În continuare este prezentat un exemplu de intrare de comunicaţii într-o descriere de subsistem:

```
                      Afişare intrări comunicaţii

Descriere subsistem:     QCMN           Stare:   ACTIVE

                          Descriere                    Utilizator    Maxim
Dispozitiv    Mod         job            Bibliotecă    implicit      Active
*ALL          *ANY        *USRPRF                      *SYS          *NOMAX
*ALL          QPCSUPP     *USRPRF                      *NONE         *NOMAX
```

Tabela 20 la pagina 106 prezintă valorile posibile pentru parametrul utilizator implicit dintr-o intrare de comunicaţii

Tabela 20. Valori posibile pentru parametrul utilizator implicit

Valoare	Rezultat
***NONE**	Nu este disponibil nici un utilizator implicit. Dacă sistemul sursă nu furnizează un identificator de utilizator la cerere, jobul nu va rula.
***SYS**	Numai programele furnizate de IBM (joburi de sistem) vor rula. Nici o aplicaţie utilizator nu va rula.
nume-utilizator	Dacă sistemul sursă nu transmite un identificator de utilizator, jobul rulează sub acest profil de utilizator.

Puteţi utiliza comanda Tipărire descriere subsistem (Print Subsystem Description - PRTSBSDAUT) pentru a tipări o listă cu toate subsistemele care au intrări de comunicaţii cu un profil de utilizator implicit.

Opţiuni passthrough staţie de afişare

Passthrough staţie de afişare este un exemplu de aplicaţie care utilizează comunicaţiile APPC. Puteţi utiliza passthrough staţie de afişare pentru a se semna pe un alt sistem care este conectat la sistemul dumneavoastră printr-o reţea.

Tabela 21 prezintă exemple de cereri passthrough (comanda STRPASTHR) şi cum le gestionează sistemul destinaţie. Pentru passthrough staţie de afişare, sistemul utilizează elementele de bază ale comunicaţiilor APPC şi variabila sistem semnare la distanţă (QRMTSIGN).

Notă: Cererile Passthrough staţie de afişare nu mai sunt rutate prin subsistemele QCMN sau QBASE. Începând cu V4R1, sunt rutate prin subsistemul QSYSWRK. Înainte de V4R1 aţi fi putut presupune că dacă nu sunt pornite subsistemele QCMD sau QBASE, Passthrough staţie de afişare nu va funcţiona. Acest lucru nu mai este adevărat. Puteţi forţa Passthrough staţie de afişare să treacă prin QCMN (sau QBASE dacă este activ) modificând variabila sistem QPASTHRSVR la 0.

Tabela 21. Exemplu de cereri de semnare pass-through

Valori la comanda STRPASTHR		**Sistem destinaţie**		
ID utilizator	**Parolă**	**Valoare SECURELOC**	**Valoare QRMTSIGN**	**Rezultat**
*NONE	*NONE	Orice	Orice	Utilizatorul trebuie să deschidă o sesiune pe sistemul destinaţie.
Un nume de profil utilizator	Neintrodus	Orice	Orice	Cererea eşuează.

Tabela 21. Exemplu de cereri de semnare pass-through (continuare)

Valori la comanda STRPASTHR		**Sistem destinaţie**		
ID utilizator	**Parolă**	**Valoare SECURELOC**	**Valoare QRMTSIGN**	**Rezultat**
*CURRENT	Neintrodus	*NO	Orice	Cererea eşuează.
		*YES	*SAMEPRF	Porneşte un job interactiv având numele de profil utilizator identic cu profilul utilizator din sistemul sursă.Nu se transmite parola la sistemul de la distanţă. Numele profilului de utilizator trebuie să existe pe sistemul destinaţie.
			*VERIFY	
			*FRCSIGNON	Utilizatorul trebuie să deschidă o sesiune pe sistemul destinaţie.
		*VFYENCPWD	*SAMEPRF	Porneşte un job interactiv având numele de profil utilizator identic cu profilul utilizator din sistemul sursă.Sistemul sursă extrage parola utilizatorului şi o transmite sistemului destinaţie. Numele profilului de utilizator trebuie să existe pe sistemul destinaţie.
			*VERIFY	
			*FRCSIGNON	Utilizatorul trebuie să deschidă o sesiune pe sistemul destinaţie.
*CURRENT (sau numele profilului de utilizator actual pentru job)	Introdus	Orice	*SAMEPRF	Porneşte un job interactiv având numele de profil utilizator identic cu profilul utilizator din sistemul sursă.Parola *este* trimisă sistemului de la distanţă. Numele profilului de utilizator trebuie să existe pe sistemul destinaţie.
			*VERIFY	
			*FRCSIGNON	Utilizatorul trebuie să deschidă o sesiune pe sistemul destinaţie.
Un nume profil utilizator (un nume diferit de profilul actual de utilizator pentru job)	Introdus	Orice	*SAMEPRF	Cererea eşuează.
			*VERIFY	Porneşte un job interactiv având numele de profil utilizator identic cu profilul utilizator din sistemul sursă.Parola *este* trimisă sistemului de la distanţă. Numele profilului de utilizator trebuie să existe pe sistemul destinaţie.
			*FRCSIGNON	Un job interactiv porneşte cu numele profilului de utilizator specificat. Parola este transmisă sistemului destinaţie. Numele profilului de utilizator trebuie să existe pe sistemul destinaţie.

Evitarea asocierilor de dispozitiv neaşteptate

Când apare o eroare pe un dispozitiv activ, sistemul încearcă să o rezolve. În anumite circumstanţe, când conexiunea este întreruptă, alt utilizator poate în mod neintenţionat să restabilească sesiunea care a avut eroarea. De exemplu, să presupunem că USERA închide o staţie de lucru fără să anuleze semnarea (sign off). USERB ar putea să pornească staţia de lucru şi să repornească sesiunea utilizatorului USERA fără a a se semna.

Pentru a împiedica această posibilitate, setaţi variabila de sistem Device I/O Error Action (QDEVRCYACN) pe *DSCMSG. Când un dispozitiv eşuează, sistemul va închide jobul utilizatorului.

Controlul comenzilor la distanţă şi joburi batch

Există mai multe opţiuni care vă pot ajuta să controlaţi ce comenzi şi joburi la distanţă puteţi rula pe sistemul dumneavoastră, inclusiv următoarele:

- Dacă sistemul utilizează DDM, puteţi restricţiona accesul la fişierele DDM pentru a împiedica utilizatorii să utilizeze comanda Lansare Comandă la Distanţă (Submit Remote Command - SBMRMTCMD) de pe un alt sistem. Pentru a utiliza SBMRMTCMD, utilizatorul trebuie să poată deschide un fişier DDM. De asemenea, trebuie să restricţionaţi posibilitatea de a crea fişiere DDM.
- Puteţi specifica un program de ieşire pentru variabila de sistem acces cerere DDM (DDMACC). În programul de ieşire, puteţi evalua toate cererile DDM înainte de a le accepta.
- Puteţi utiliza atributul de reţea acţiune job reţea (network job action - JOBACN) pentru a împiedica lansarea joburilor de reţea sau pentru a le împiedica să ruleze automat.
- Puteţi specifica explicit ce cerere de program poate rula într-un mediu de comunicaţii înlăturând intrarea de rutare PGMEVOKE din descrierile subsistemelor. Intrările de rutare PGMEVOKE permit solicitantului să specifice un program care rulează. Când înlăturaţi această intrare de rutare din descrierile subsistemelor, cum ar fi descrierea subsistemului QCMN, trebuie să adăugaţi intrări de rutare pentru cererile de comunicaţii care trebuie să ruleze cu succes.

  "Cereri TPN arhitecturale" la pagina 83 listează numele programelor pentru cererile de comunicaţii ale aplicaţiilor furnizate de IBM. Pentru fiecare cerere pe care doriţi să o acceptaţi, puteţi adăuga o intrare de rutare cu valoarea de comparare şi numele programului ambele egale cu numele programului.

  Când utilizaţi această metodă, trebuie să înţelegeţi mediul de administrare a lucrului de pe sistemul dumneavoastră şi tipurile de cereri de comunicaţii care pot să apară pe sistemul dumneavoastră. Dacă este posibil, trebuie să testaţi toate tipurile de cereri de comunicaţii pentru a vă asigura că funcţionează corect după ce aţi modificat intrările de rutare. Când o cerere de comunicaţie nu găseşte nici o intrare de rutare disponibilă, primiţi un mesaj CPF1269. O altă alternativă (mai puţin înclinată spre erori dar mai puţin eficientă) este de a seta autorizarea publică pe *EXCLUDE pentru programele de tranzacţii care nu doriţi să ruleze pe sistemul dumneavoastră.

  Notă: Cartea *Control funcţionare* oferă mai multe informaţii despre intrările de rutare şi despre cum gestionează sistemul cererile de pornire program.

Evaluarea configuraţiei dumneavoastră APPC

Puteţi utiliza comanda Tipărire Securitate Comunicaţii (Print Comunications Security - PRTCMNSEC) sau opţiunile din meniu pentru a tipări valorile relevante pentru securitate din configuraţia APPC. Subiectele care urmează descriu informaţiile din rapoarte.

Parametri semnificativi pentru dispozitive APPC

Figura 9 arată un exemplu de raport informaţii comunicaţii pentru descrierile dispozitivelor. Figura 10 prezintă un exemplu de raport pentru lista de configuraţie. Explicaţiile câmpurilor din rapoarte sunt prezentate după aceste rapoarte.

```
                          Informaţii comunicaţii (Raport complet)
                                                                                SYSTEM4
Tip obiect . . . . . :   *DEVD
                                                                                        Pre           SNUF
\Nume            Tip          Categorie       Locaţie     Locaţie    Permite      O singură   Sesiune      Start
obiect         obiect       dispozitiv      sigură      parolă      APPN         sesiune    stabilită    program
Nume           Tip         Categorie      Locaţie     Parolă     Posibilitate     Sesiune      Sesiune      Start

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

Figura 9. Descrieri dispozitive APPC - Exemplu de raport

```
                  Afişare listă configuraţie                        Pagina   1
                            SYSTEM4  12/17/95  07:24:36
Listă configuraţie . . . . . :   QAPPNRMT
Tip listă configuraţie . . . . . :   *APPNRMT
Text . . . . . :
-----------------Locaţii la distanţă APPN---------------
          Identif              Punct   Identif
Locaţia   reţea la  Locaţia   control   reţea     Locaţie
la dist.  distanţă  locală    la dist.  pct. ctrl. sigură
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
--------------------------Locaţii la distanţă APPN-----------------------
          Identif.                                  Punct
Locaţie   reţea la  Locaţie   O singură  Numărul de   control     Sesiune
la dist.  distanţă  locală    sesiune   conversaţii    local     prestabilită
SYSTEM36  APPN      SYSTEM4    *NO            10      *NO        *NO
SYSTEM32  APPN      SYSTEM4    *NO            10      *NO        *NO
```

Figura 10. Raport Listă Configuraţie - Exemplu

Câmp de locaţie sigură

Câmpul locaţie sigură (SECURELOC) specifică dacă sistemul local are încredere în sistemul de la distanţă să facă verificarea parolei în numele sistemului local. Câmpul SECURELOC se aplică numai aplicaţiilor care utilizează valoarea SECURITY(SAME), cum ar fi DDM sau aplicaţiile care utilizează API CPI-Communications.

SECURELOC(*YES) face ca sistemul local să fie vulnerabil la posibilele slăbiciuni de pe sistemul de la distanţă. Orice utilizator care există pe ambele sisteme poate apela programe de pe sistemul local. Aceasta este o trăsătură periculoasă deoarece profilul de utilizator QSECOFR (security officer - responsabilul cu securitatea) există pe toate sistemele iSeries şi are autorizarea specială *ALLOBJ. Dacă un sistem din reţea nu protejează bine parola QSECOFR, celelalte sisteme care tratează acel sistem ca pe o locaţie sigură sunt supuse riscului.

Când utilizaţi SECURELOC(*VFYENCPWD), sistemul dumneavoastră este mai puţin vulnerabil la alte sisteme care nu protejează în mod adecvat parolele. Un utilizator care solicită o aplicaţie care utilizează SECURITY(SAME) trebuie să aibă aceleaşi identificator de

utilizator şi parolă pe ambele sisteme. SECURELOC(*VFYENCPWD) cere politici de administrare a parolelor în toată reţeaua, astfel încât utilizatorii să aibă aceeaşi parolă pe toate sistemele.

Notă: SECURELOC(*VFYENCPWD) este suportat numai între sistemele care rulează V3R2, V3R7 sau V4R1. Dacă sistemul destinaţie specifică SECURELOC(*VFYENCPWD) şi sistemul sursă nu suportă această funcţie, cererea este tratată ca SECURITY(NONE).

Dacă un sistem specifică SECURELOC(*NO), aplicaţiile care utilizează SECURITY(SAME) vor avea nevoie de un utilizator implicit pentru a rula programe. Utilizatorul implicit depinde atât de descrierea dispozitivului cât şi de modul care este asociat cu cererea. (Vezi “Asocierea de profiluri utilizator pe sistemul destinaţie pentru joburi” la pagina 105.)

Câmp de parolă locaţie

Câmpul locaţie parolă determină dacă două sisteme vor schimba parole pentru a verifica dacă sistemul solicitant nu este un sistem impostor. “Exemplu: O sesiune APPC de bază” la pagina 102 furnizează mai multe informaţii despre locaţie parolă.

Câmp capabil APPN

Câmpul capabil- APPN (APPN) specifică dacă sistemul la distanţă poate suporta funcţii de reţea avansate sau este limitat la conexiuni de tipul singur-hop. APPN(*YES) înseamnă următoarele:

- Dacă un sistem de la distanţă este un nod de reţea, sistemul de la distanţă poate fi capabil să conecteze sistemul local la alte sisteme. Acest lucru este numit **rutare prin nod intermediar**. Înseamnă că utilizatorii de pe sistemul dumneavoastră pot utiliza sistemul de la distanţă ca o rută către o reţea mai mare.
- Dacă sistemul local este un nod de reţea, sistemul de la distanţă poate utiliza sistemul local pentru a se conecta la alte sisteme. Utilizatorii sistemului de la distanţă pot să utilizeze sistemul dumneavoastră ca o rută către o reţea mai mare.

  Notă: Puteţi utiliza comanda DSPNETA pentru a determina dacă un sistem este un nod de reţea sau un nod terminal.

Câmpul pentru o singură sesiune

Câmpul O singură sesiune (SNGSSN) specifică dacă sistemul de la distanţă poate rula mai mult de o sesiune la un moment dat utilizând aceeaşi descriere de dispozitiv APPC. SNGSSN(*NO) este folosită de obicei deoarece elimină nevoia de a crea multiple descrieri de dispozitive pentru un sistem la distanţă. De exemplu, un utilizator PC deseori doreşte mai mult de o sesiune de emulare 5250 şi sesiuni pentru funcţii server fişiere şi server tipărire. Cu SNGSSN(*NO), puteţi oferi aceste funcţii cu o descriere de dispozitiv pentru PC-ul de pe sistemul iSeries.

SNGSSN(*NO) înseamnă că vă bazaţi pe modul de operare conştient de securitate al utilizatorilor PC sau alţi utilizatori APPC. Sistemul dumneavoastră este vulnerabil la cineva de pe sistemul de la distanţă care porneşte o sesiune neautorizată care utilizează aceeaşi descriere de dispozitiv ca şi o sesiune existentă. (Această practică este uneori denumită **piggy-backing**.)

Câmpul prestabilire sesiune

Câmpul Prestabilire sesiune (PREESTSSN) pentru un dispozitiv cu o singură sesiune controlează dacă sistemul local porneşte o sesiune cu sistemul de la distanţă atunci când sistemul de la distanţă contactează primul sistemul local. PREESTSSN(*NO) înseamnă că sistemul local aşteaptă să pornească o sesiune până când o aplicaţie solicită o sesiune cu sistemul. PREESTSSN(*YES) este util pentru minimizarea timpului în care un program de aplicaţie stabileşte conexiunea.

PREESTSSN(*YES) împiedică sistemul să deconecteze o linie comutată (prin modem) care nu mai este utilizată. Aplicaţia sau utilizatorul trebuie să dezactiveze în mod explicit linia. PREESTSSN(*YES) poate prelungi timpul în care sistemul este vulnerabil la ″piggy-backing″ în acea sesiune.

Câmpul de pornire program SNUF

Câmpul Pornire program SNUF specifică dacă sistemului de la distanţă îi este permis să ruleze programe de pe sistemul local. *YES înseamnă că schema autorizărilor obiectelor trebuie să fie adecvată pentru a proteja obiectele atunci când utilizatorii de pe sistemul de la distanţă pornesc joburi şi rulează programe de pe sistemul local.

Parametri pentru controlerele APPC

Figura 11 prezintă un exemplu de Raport informaţii comunicaţii pentru descrierile controlerelor. După raport veţi găsi explicaţii despre câmpurile din acesta.

```
                    Informaţii comunicaţii (Raport complet)
                                                                    SYSTEM4
Tip obiect . . . . . . . . . . :   *CTLD

Nume      Tip       Categorie     Auto    Controler    Direcţie     Suportă  Sesiuni    Cronometru   Secunde   Nume
obiect    obiect    controler     creare    comutat       apel        APPN       CP      deconectare  ştergere  dispozitiv
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
```

Figura 11. Descrieri controlere APPC - Exemplu de raport

Câmpul creare automată

Într-o descriere de linie, câmpul Autocreare (AUTOCRTCTL) specifică dacă sistemul local va crea în mod automat o descriere de controler atunci când o cerere sosită nu poate găsi o descriere de controler corespunzătoare. Într-o descriere de controler, câmpul Autocreare (AUTOCRTDEV) specifică dacă sistemul local va crea în mod automat o descriere de dispozitiv atunci când o cerere sosită nu poate găsi o descriere de dispozitiv corespunzătoare.

Pentru controlerele care suportă APPN, câmpul Autocreare nu are efect. Sistemul creează în mod automat o descriere de dispozitiv atunci când este necesar, indiferent de cum este setat câmpul Autocreare.

Atunci când specificaţi *YES pentru o descriere de linie, orice persoană care are acces la linie se poate conecta la sistemul dumneavoastră Aceasta include site-uri care sunt conectate prin bridge-uri sau rutere.

Câmpul Sesiuni punct de control

Pentru controlerele care suportă APPN, câmpul Sesiuni punct control (CPSSN) controlează dacă sistemul stabileşte în mod automat o conexiune APPC cu sistemul de la distanţă. Sistemul utilizează sesiunile CP pentru a schimba informaţii despre reţea şi stări cu sistemul de la distanţă. Schimbul informaţiilor împrospătate între APPN noduri de reţea este important pentru funcţionarea reţelei .

Când specificaţi *YES, o linie comutată neactivă nu se deconectează automat. Acest lucru face ca sistemul dumneavoastră să fie şi mai vulnerabil la o sesiune piggy-back.

Câmpul cronometru deconectare

Pentru un controler APPC, câmpul Cronometru deconectare specifică cât timp trebuie să fie nefolosit un controler (fără sesiuni active) înainte ca sistemul să deconecteze linia cu sistemul de la distanţă. Acest câmp are două valori. Prima valoare specifică cât timp controlerul va sta

activ de la momentul în care a fost conectat iniţial. Cea de-a doua valoare specifică cât timp sistemul va aştepta după ce ultima sesiune a fost oprită de pe controler înainte ca sistemul să închidă linia.

Sistemul utilizează cronometrul deconectare doar când câmpul deconectare comutată (SWTDSC) este *YES.

Dacă acestea sunt valori mari, sistemul este mai vulnerabil la sesiuni ″piggy-back″.

Parametri pentru descrierile linie

Figura 12 prezintă un exemplu de Raport informaţii comunicaţii pentru descrierile de linii. După raport veţi găsi explicaţii despre câmpurile din acesta.

```
                    Informaţii comunicaţii (Raport complet)

Tip obiect . . . . . . . . . . . :   *LIND
Auto
Nume           Tip           Categorie       Auto      Secunde     Răspuns    Formare
obiect         obiect         linie         creare     ştergere    automat    automată
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
```

Figura 12. Descrieri linii APPC - Exemplu de raport

Câmpul Răspuns automat

Câmpul Răspuns automat (AUTOANS) specifică dacă linia comutată va accepta apelurile sosite fără intervenţia operatorului.

Dacă specificaţi *YES, sistemul este mai puţin sigur deoarece poate fi accesat mult mai uşor. Pentru a minimiza problemele de securitate atunci când specificaţi *YES, trebuie să închideţi linia când nu aveţi nevoie de aceasta.

Câmpul Apel automat

Câmpul Formare automată (AUTODIAL) specifică dacă linia comutată poate trimite apeluri fără intervenţia operatorului. Dacă specificaţi *YES, permiteţi utilizatorilor locali care nu au acces fizic la liniile de comunicaţie şi la modemuri să se conecteze la alte sisteme.

Capitolul 13. Securizarea comunicaţiilor TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) este o cale comună prin care calculatoarele de toate tipurile comunică între ele. Aplicaţiile TCP/IP sunt des folosite în "magistrala informaţiilor".

Acest capitol furnizează sfaturi pentru următoarele:

- Împiedicarea rulării aplicaţiilor TCP/IP pe sistemul dumneavoastră.
- Protejarea resurselor de sistem când rulaţi aplicaţii TCP/IP pe sistemul dumneavoastră.

Site-ul web iSeries Centru de informare—>Reţea—>TCP/IP este o sursă completă de informaţii pentru toate aplicaţiile TCP/IP. *SecureWay: iSeries şi Internet* (iSeries Centru de informare —>Securitate—>SecureWay descrie consideraţii de securitate când conectaţi serverul dumneavoastră iSeries fie la Internet (o reţea TCP/IP foarte mare) sau la o reţea internă. Consultaţi "Condiţii prealabile şi informaţii conexe" la pagina xii pentru informaţii despre accesarea Centrului de informare iSeries.

Reţineţi că serverele iSeries suportă multe aplicaţii TCP/IP posibile. Când vă decideţi să folosiţi o aplicaţie TCP/IP pe sistemul dumneavoastră, puteţi, de asemenea, să activaţi şi alte aplicaţii TCP/IP. Ca administrator de securitate, trebuie să cunoaşteţi limitele aplicaţiilor TCP/IP şi implicaţiile de securitate ale acestor aplicaţii.

Prevenirea procesării TCP/IP

Joburile server TCP/IP rulează pe subsistemul QSYSWRK. Folosiţi comanda Start TCP/IP (STRTCP) pentru a porni TCP/IP pe sistemul dumneavoastră. Dacă nu doriţi ca vreun proces sau aplicaţie TCP/IP să ruleze, nu folosiţi comanda STRTCP. Sistemul dumneavoastră este autorizat cu autorizarea publică pentru comanda STRTCP setată la *EXCLUDE.

Dacă suspectaţi pe cineva care are acces la comandă că a pornit TCP/IP (în timpul liber, de exemplu), puteţi seta o verificare de obiect pentru comanda STRTCP. Sistemul va crea şi introduce intrările jurnal de fiecare dată când un utilizator rulează comanda.

Componente de securitate TCP/IP

Puteţi folosi mai multe din componentele de securitate TCP/IP care îmbunătăţesc securitatea reţelei dumneavoastră şi adaugă flexibilitate. Deşi unele din aceste tehnologii se găsesc de asemenea în produsele firewall, aceste componente de securitate TCP/IP pentru OS/400 nu se intenţionează a fi folosite ca un firewall. Totuşi, puteţi folosi unele dintre aceste caracteristici, în anumite instanţe, pentru a elimina necesitatea folosirii unui produs firewall. Puteţi, de asemenea, folosi aceste caracteristici TCP/IP pentru a furniza securitate adiţională în mediile în care utilizaţi deja un firewall.

Următoarele componente pot fi utilizate pentru mărirea securităţii TCP/IP :

- Reguli pachet
- Server Proxy HTTP
- VPN (virtual private networking - reţea privată virtuală)
- SSL (secure sockets layer - nivelul socket-ilor de siguranţă)

Folosirea regulilor pachet pentru securizarea traficului TCP/IP

Regulile pachet, care este o combinaţie între filtrarea IP şi translatarea adreselor de reţea (NAT) acţionează ca un firewall pentru protecţia reţelei dumneavoastră interne de intruşi. Filtrarea IP vă permite să controlaţi ce trafic IP să permiteţi în şi afara reţelei dumneavoastră. La bază, vă protejează reţeaua prin filtrarea pachetelor în funcţie de regulile pe care le definiţi. NAT, pe cealaltă parte, vă permite să ascundeţi adresele dumneavoastră IP private neînregistrate în spatele unui set de adrese IP înregistrate. Aceasta ajută la protejarea reţelei dumneavoastră interne de reţelele exterioare. NAT vă ajută de asemenea să uşuraţi problema epuizării adreselor IP, deoarece multe adrese private pot fi reprezentate de un mic set de adrese înregistrate. Consultaţi Centrul de informare iSeries pentru mai multe detalii.

Server proxy HTTP

Serverul proxy HTTP vine împreună cu serverul IBM HTTP Server for iSeries. Serverul HTTP este o parte a OS/400. Serverul proxy primeşte cereri HTTP de la browser-ele Web şi le retrimite serverelor Web. Serverele Web care primesc cereri cunosc doar adresa IP a serverului proxy şi nu pot determina numele sau adresele PC-urilor care fac cererile. Serverul proxy poate realiza cereri URL pentru HTTP, FTP, Gopher şi WAIS.

Serverul proxy pune în cache paginile Web returnate de la cererile făcute de toţi utilizatorii serverului proxy. În consecinţă, când utilizatorii cer o pagină, serverul proxy verifică dacă pagina este în cache. Dacă da, serverul proxy întoarce pagina din cache. Folosind pagini în cache, Serverul proxy foloseşte paginile Web mai rapid, ceea ce elimină consumul de timp potenţial pentru cererile serverului Web.

Serverul proxy poate, de asemenea, înregistra toate cererile URL pentru scopuri de urmărire. Puteţi apoi revedea înregistrările pentru a monitoriza utilizarea şi eşecurile în folosirea resurselor de reţea.

Puteţi folosi suportul de server proxy HTTP în serverul HTTP IBM pentru a consolida accesul Web. Adresele clienţilor PC sunt ascunse pentru Serverul Web pe care-l accesează; doar adresa IP a serverului proxy este cunoscută. Ascunderea paginilor Web poate, de asemenea, reduce cererile lungimii de bandă pentru comunicare şi munca firewall-ului. Consultaţi pagina gazdă IBM HTTP Server for iSeries pentru informaţii suplimentare:http://www-1.ibm.com/servers/eserver/iseries/software/http/index.html

VPN (Virtual Private Networking - Reţea privată virtuală)

O reţea privată virtuală (VPN) permite companiei dumneavoastră să extindă în siguranţă reţeaua locală proprie peste un cadru de lucru existent al unei reţele publice, cum ar fi Internet-ul. Cu VPN, compania dumneavoastră poate controla traficul prin reţea în timp ce furnizează opţiuni de securitate importante cum ar fi autentificarea şi protecţia datelor.

OS/400 VPN este o componentă instalabilă opţional a Navigatorului iSeries, interfaţa grafică pentru OS/400. Aceasta vă permite să creaţi o cale capăt la capăt între orice combinaţie de gazdă şi gateway. OS/400 VPN foloseşte metode de autentificare, algoritmi de criptare şi alte precauţii pentru a asigura ca transmiterea datelor între două puncte finale ale conexiunii sale să rămână securizată.

VPN rulează pe nivelul reţea al modelului stivă de comunicaţii pe niveluri TCP/IP. Specifically, VPN uses the IP Security Architecture (IPSec) open framework. IPSec furnizează funcţii de bază de securitate pentru Internet, aşa cum furnizează blocuri flexibile din care puteţi crea reţele virtuale private robuste şi sigure.

VPN suportă de asemenea soluţii VPN pentru L2TP (Layer 2 Tunnel Protocol). Conexiunile L2TP care sunt numite de asemenea linii virtuale, furnizează acces pentru utilizatorii la

distanţă permiţând unui server de reţea să gestioneze adresele IP asociate utilizatorilor ei de la distanţă. Mai departe, conexiunile L2TP furnizează acces sigur la sistemul sau reţeaua dumneavoastră când le protejaţi folosind IPSec.

Este important să înţelegeţi impactul pe care îl va avea un VPN asupra întregii dumneavoastră reţele. Planificarea corespunzătoare şi implementarea sunt esenţiale pentru succesul dumneavoastră. Ar trebui să revedeţi subiectul VPN din Centrul de informare iSeriesiSeries pentru a vă asigura că ştiţi cum lucrează VPN-urileşi cum ar trebui să le folosiţi. Pentru informaţii suplimentare, consultaţiiSeries Centrul de informare—>Securitate—>Virtual Private Networking. Consultaţi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru informaţii despre accesarea Centrului de informare iSeries.

SSL (Secure Sockets Layer)

Nivelul socket-ilor de siguranţă (SSL) a devenit un standard industrial pentru a permite aplicaţiilor să folosească sesiuni de comunicaţii sigure într-o reţea neprotejată cum este Internet-ul. Protocolul SSL stabileşte o conexiune sigură între clienţi şi aplicaţiile server care furnizează autentificarea unuia sau ambelor puncte terminale ale sesiunii de comunicaţii. SSL furnizează de asemenea confidenţialitatea şi integritatea datelor care sunt schimbate între client şi aplicaţia server. Pentru informaţii suplimentare, consultaţi iSeries Centrul de informare–>Securitate—>Secure Sockets Layer (SSL). Consultaţi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru informaţii despre accesarea Centrului de informare iSeries.

Securizarea mediului dumneavoastră TCP/IP

Acest subiect vă oferă sugestii generale pentru paşii pe care trebuie să îi parcurgeţi pentru a reduce problemele de securitate din mediul TCP/IP de pe sistemul dumneavoastră. Aceste sfaturi se aplică mai degrabă întregului mediu TCP/IP decât unor anumite aplicaţii care sunt discutate în subiectele care urmează.

- Când scrieţi o aplicaţie pentru un port TCP/IP, asiguraţi-vă că aplicaţia este securizată corespunzător. Trebuie să presupuneţi că un utilizator din exterior ar putea încerca să acceseze acea aplicaţie prin acel port. Un utilizator cu cunoştinţe în domeniu ar putea încerca să facă TELNET la acea aplicaţie.
- Monitorizaţi utilizarea porturilor TCP/IP de pe sistemul dumneavoastră. O aplicaţie utilizator care este asociată cu un port TCP/IP poate oferi o intrare “pe uşa din spate” în sistemul dumneavoastră, fără un identificator de utilizator şi o parolă. O persoană cu suficientă autorizare pe sistemul dumneavoastră poate asocia o aplicaţie cu un port TCP sau UDP.
- În calitate de administrator de securitate, trebuie să aveţi cunoştinţă de tehnica numită *IP spoofing* pe care o utilizează hacker-ii. Orice sistem dintr-o reţea TCP/IP are o adresă de IP. O persoană care utilizează ″IP spoofing″ setează un sistem (de obicei, un PC) pentru a pretinde că este o adresă de IP existentă sau o adresă de IP de încredere. Astfel, impostorul poate stabili o conexiune cu sistemul dumneavoastră pretinzând că este un sistem cu care vă conectaţi de obicei.

  Dacă rulaţi TCP/IP pe sistemul dumneavoastră şi acesta este într-o reţea care nu este protejată fizic (toate liniile sunt necomutate şi legăturile predefinite), sunteţi vulnerabil la ″IP spoofing″. Pentru a vă proteja sistemul de deteriorările pe care le poate provoca un “″spoofer″”, începeţi cu sugestiile din acest capitol, cum ar fi protecţia la semnare şi securitatea obiectelor. De asemenea, trebuie să vă asiguraţi că sistemul dumneavoastră are setate limite de stocare auxiliară rezonabile. Acest lucru împiedică un ″spoofer″ să umple sistemul dumneavoastră cu scrisori sau cu fişiere spool până la punctul la care sistemul devine inoperabil.

În plus, trebuie să monitorizaţi regulat activitatea TCP/IP de pe sistemul dumneavoastră. Dacă detectaţi ″IP spoofing″, puteţi încerca să descoperiţi punctele slabe din configurarea TCP/IP şi să faceţi modificări.

- Pentru intranet (reţea de sisteme care nu au nevoie să se conecteze direct cu exteriorul), utilizaţi adresele de IP care sunt reutilizabile. Adresele reutilizabile sunt concepute pentru a fi utilizate într-o reţea privată. Internet nu rutează pachetele care au adrese de IP reutilizabile. De aceea, adresele reutilizabile oferă un nivel suplimentar de protecţie în interiorul firewall-ului.

  Site-ul webiSeries Centrul de informare—>Reţea—>TCP/IP furnizează informaţii suplimentare despre cum sunt asociate adresele IP şi despre limitele adreselor IP, ca şi informaţii despre TCP/IP.
- Dacă aveţi în vedere să conectaţi sistemul dumneavoastră la Internet sau într-o reţea internă, revedeţi informaţiile de securitateat*SecureWay: iSeries şi Internet* (iSeries Centrul de informare—>Securitate—>SecureWay). Consultaţi“Condiţii prealabile şi informaţii conexe” la pagina xii pentru informaţii despre accesarea Centrului de informare iSeries.

Controlul serverelor TCP/IP care să pornească automat

În calitate de administrator de securitate, trebuie să controlaţi care aplicaţii TCP/IP pornesc automat atunci când porniţi TCP/IP. Sunt disponibile două comenzi pentru pornirea TCP/IP. Pentru fiecare comandă, sistemul utilizează o metodă diferită pentru a determina care aplicaţii (servere) vor porni.

Tabela 22 prezintă cele două comenzi şi recomandările de securitate pentru ele. Tabela 23 la pagina 117 prezintă valorile de pornire automată implicite pentru servere. Pentru a modifica valoarea de autostart pentru un server, utilizaţi comanda CHGxxxA (Modificare atribute xxx - Change xxx Attributes) pentru server. De exemplu, comanda pentru TELNET este CHGTELNA.

Tabela 22. Cum determină comenzile TCP/IP care servere să pornească

Comandă	Ce servere pornesc	Recomandări de securitate
Pornire TCP/IP (Start TCP/IP - STRTCP)	Sistemul porneşte toate serverele care au specificat AUTOSTART(*YES). Tabela 23 la pagina 117prezintă valoarea transmisă pentru fiecare server TCP/IP.	• Asociaţi cu grijă autorizarea specială *IOSYSCFG pentru a controla cine poate modifica setările de autostart. • Controlaţi cu grijă cine are autorizarea de utilizare a comenzii STRTCP. Autorizarea publică implicită pentru comandă este *EXCLUDE. • Setaţi auditare obiect pentru comenzile Change *server-name* Attributes (cum ar fi CHGTELNA) pentru a monitoriza persoanele care încearcă să modifice valoarea AUTOSTART pentru server.
Pornire server TCP/IP (Start TCP/IP Server - STRTCPSVR)	Utilizaţi un parametru pentru a specifica ce servere să pornească. Când se livrează, implicit pentru această comandă este să pornească toate serverele.	• Utilizaţi comanda Modificare valori implicite comandă (Change Command Default - CHGCMDDFT) pentru a seta comanda STRTCPSVR să pornească numai un anumit server. Acest lucru nu împiedică alţi utilizatori să pornească alte servere. Totuşi, modificând valoarea implicită a comenzii, este mai puţin probabil ca utilizatorii să pornească toate serverele accidental. De exemplu, utilizaţi următoarea comandă pentru a seta valoarea implicită să pornească numai Serverul TELNET: CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*TELNET)') **Notă:** Când modificaţi valoarea implicită, puteţi specifica un singur server. Alegeţi ori un server pe care îl utilizaţi în mod regulat ori un server care este puţin probabil să provoace probleme de securitate (cum ar fi TFTP). • Controlaţi cu grijă cine are autorizarea să utilizeze comanda STRTCPSVR. Autorizarea publică implicită pentru comandă este *EXCLUDE.

Următorul tabel conţine valori de pornire automată pentru servereleTCP/IP. Pentru informaţii suplimentare despre fiecare din aceste servere, consultaţiiSeries Centrul de informare(**Reţea—>TCP/IP**). Consultaţi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru detalii despre accesarea Centrului de informareiSeries.

Tabela 23. Valori de pornire automată pentru serverele TCP/IP

Server	Valoare implicită	Valoarea dumneavoastră
TELNET	AUTOSTART(*YES)	
FTP (file transfer protocol)	AUTOSTART(*YES)	
BOOTP (Protocol Bootstrap)	AUTOSTART(*NO)	
TFTP (FTP (File Transfer Protocol) trivial)	AUTOSTART(*NO)	
REXEC (Server REmote EXECution)	AUTOSTART(*NO)	
RouteD (Demon Route)	AUTOSTART(*NO)	
SMTP (SMTP (Simple Mail Transfer Protocol))	AUTOSTART(*YES)	
POP (Post Office Protocol)	AUTOSTART(*NO)	
HTTP (Hypertext Transfer Protocol) [1]	AUTOSTART(*NO)	
ICS (Server conectare Internet)[1]	AUTOSTART(*NO)	
LPD (Demon imprimantă)	AUTOSTART(*YES)	
SNMP (SNMP (Simple Network Management Protocol))	AUTOSTART(*YES)	
DNS (sistem nume domeniu)	AUTOSTART(*NO)	
DDM	AUTOSTART(*NO)	
DHCP (dynamic host configuration protocol)	AUTOSTART(*NO)	
NSMI	AUTOSTART(*NO)	
INETD	AUTOSTART(*NO)	

Note:

1. Cu IBM HTTP Server pentru serverul iSeries, folosiţi comandaCHGHTTPA pentru a seta valoarea AUTOSTART.

Consideraţii de securitate pentru folosirea SLIP

Suportul TCP/IP al serverului iSeries include SLIP (Serial Interface Line Protocol) (SLIP). SLIP furnizează conectare ieftină punct la punct. Un utilizator SLIP se poate conecta la un LAN sau WAN stabilind o conectare punct la punct cu un sistem care face parte din LAN sau WAN.

SLIP rulează la o conectare asincronă. Puteţi folosi SLIP pentru conexiuni dial-up la şi de la serverele iSeries. De exemplu, puteţi utiliza SLIP pentru dial-in de la PC-ul dumneavoastră la un sistem iSeries. După stabilirea conexiunii, puteţi utiliza aplicaţia TELNET pe calculatorul dumnevoastră pentru a vă conecta la iSeries serverul TELNET. Sau, puteţi utiliza aplicaţia FTP pentru a transfera fişiere între cele două sisteme.

Nu există nici o configuraţie SLIP pe sistemul dumneavoastră când acesta este livrat. De aceea, dacă nu doriţi ca SLIP să ruleze pe sistemul dumneavoastră (şi dial-up TCP/IP), nu configuraţi nici un profil de configurare pentru SLIP. Folosiţi comanda Gestiune TCP/IP punct la punct (WRKTCPPTP) pentru a crea configuraţiile SLIP. Trebuie să aveţi autorizarea specială *IOSYSCFG pentru a utiliza comanda WRKTCPPTP.

Dacă doriţi ca SLIP să ruleze pe sistemul dumneavoastră, creaţi unul sau mai multe profiluri de configurare SLIP (punct la punct). Puteţi crea profiluri de configurare cu următoarele moduri de operare:
- Dial in (*ANS)
- Dial out (*DIAL)

Subiectul ce urmează tratează cum puteţi seta securitatea pentru profilurile de configurare SLIP.

Notă: Un**profil utilizator** este un obiect server iSeries care permite semnarea. Fiecare job server iSeries trebuie să aibă un profil utilizator pentru a rula. Un **profil de configurare** stochează informaţiile utilizate pentru stabilirea unei conexiuni SLIP cu un sistem iSeries. Când porniţi o conexiune SLIP la serverele iSeries, stabiliţi de fapt numai o legătură. Nu v-aţi înregistrat încă şi nu aţi pornit un job server iSeries. Prin urmare, nu aveţi nevoie neapărat de un profil utilizator pentru a porni o conexiune SLIP la serverele iSeries. Totuşi, aşa cum veţi vedea în ceea ce urmează, profilul de configurare SLIP ar putea necesita un profil utilizator pentru a determina dacă să permită conexiunea.

Controlul conexiunilor dial-in SLIP

Înainte ca cineva să poată stabili o conexiune dial-in la sistemul dumneavoastră cu SLIP, trebuie să porniţi un profil de configurare SLIP *ANS. Pentru a crea sau modifica un profil de configurare SLIP, folosiţi comanda Gestiune TCP/IP punct la punct (WRKTCPPTP). Pentru a porni un profil de configurare, folosiţi fie comanda Pornire TCP/IP punct la punct (STRTCPPTP), fie o opţiune a ecranului WRKTCPPTP. Când se livrează sistemul dumneavoastră, autorizarea publică pentru comenzile STRTCPPTP şi ENDTCPPTP este *EXCLUDE. Opţiunile de adăugare, modificare şi ştergere a profilurilor de configurare SLIP sunt disponibile doar dacă aveţi autorizarea specială *IOSYSCFG. Ca administrator de securitate, puteţi utiliza atât autorizarea comandă, cât şi autorizarea specială pentru a determina cine poate seta sistemul dumneavoastră să permită conexiuni dial-in.

Securizarea unei conexiuni dial-in SLIP

Dacă doriţi să validaţi sistemele care realizează dial-in la sistemul dumneavoastră, atunci doriţi ca sistemul solicitant să trimită un ID utilizator şi o parolă. Sistemul dumneavoastră poate apoi verifica ID-ul utilizator şi parola. Dacă ID-ul utilizator şi parola nu sunt valide, sistemul dumneavoastră poate respinge cererea sesiune.

Pentru a seta validarea pentru dial-in, faceţi următoarele:

__ Pasul 1. Creaţi un profil utilizator pe care-l poate folosi sistemul solicitant pentru a stabili conexiunea. ID-ul utilizator şi parola pe care le trimite solicitantul trebuie să se potrivească cu numele profil utilizator şi parola.

Notă: Pentru ca sistemul să realizeze validarea parolei, variabila de sistem QSECURITY trebuie să fie setată la 20 sau mai mult.

Ca protecţie suplimentară, probabil doriţi să creaţi profiluri utilizator speciale pentru stabilirea conexiunilor SLIP. Profilurile utilizator trebuie să aibă autorizare limitată la sistem. Dacă nu doriţi să folosiţi profilurile decât pentru stabilirea conexiunilor SLIP, puteţi seta următoarele variabile din profilurile utilizator:
- Un meniu iniţial (INLMNU) cu *SIGNOFF
- Un program iniţial (INLPGM) cu *NONE.
- Limitare capabilităţi (LMTCPB) cu *YES

Aceste variabile împiedică pe oricine să se conecteze interactiv cu un profil utilizator.

__ Pasul 2. Creaţi o listă de autorizări pentru ca sistemul să verifice când un solicitant încearcă să stabilească o conexiune SLIP.

Notă: Specificaţi această listă de autorizări în câmpul *Listă de autorizări acces sistem* când creaţi sau modificaţi profilul SLIP (Vedeţi pasul 4).

__ Pasul 3. Folosiţi comanda Adăugare intrare autorizare (ADDAUTLE) pentru a adăuga profilul utilizator pe care l-aţi creat la pasul 1 în lista de autorizări. Puteţi crea o listă unică de autorizări pentru fiecare profil de configurare punct la punct sau puteţi crea o listă de autorizări care partajează câteva profiluri de configurare.

__ Pasul 4. Folosiţi comanda WRKTCPPTP pentru a seta un profil *ANS TCP/IP punct la punct care are următoarele caracteristici:

- Profilul de configurare trebuie să folosească scriptul dialog conexiune ce include funcţiile de validare utilizator. Validările utilizator includ acceptarea unui ID utilizator şi parolă de la solicitant şi validarea lor. Sistemul furnizează mai multe exemple de script-uri dialog care pun la dispoziţie această funcţie.
- Profilul de configurare trebuie să specifice numele listei de autorizări pe care l-aţi creat la pasul 2. ID-ul utilizator pe care-l primeşte scriptul dialog conexiune trebuie să fie în lista de autorizări.

Ţineţi minte că variabila de configurare a securităţii dial-in este influenţată de practicile de securitate şi posibilităţile sistemelor care sunt în dial-in. Dacă cereţi un ID utilizator şi parolă, atunci scriptul dialog conexiune de pe sistemul solicitant trebuie să trimită un ID utilizator şi o parolă. Unele sisteme, cum ar fi serverele iSeries, furnizează o metodă sigură pentru stocarea ID-urilor utilizator şi a parolelor. (“Securitate şi sesiuni dial-out” la pagina 120 descrie metoda.) Alte sisteme stochează ID-ul utilizator şi parola în scriptul care poate fi accesibil oricui ştie unde să găsească scriptul de pe sistem.

Datorită diferitelor practici de securitate şi posibilităţi ale partenerilor dumneavoastră de comunicaţie, puteţi dori să creaţi profiluri de configurare diferite pentru diferite medii solicitante. Folosiţi comanda STRTCPPTP pentru a seta sistemul dumneavoastră să accepte o sesiune pentru un profil de configurare specific. Puteţi porni sesiunile pentru anumite profiluri de configurare doar la anumite momente ale zilei, de exemplu. Puteţi folosi auditarea securităţii pentru a înregistra activitatea profilurilor utilizator asociate.

Împiedicarea utilizatorilor dial-in de la accesarea altor sisteme

În funcţie de sistemul dumneavoastră şi configurarea reţelei, un utilizator care porneşte o conexiune SLIP poate accesa alt sistem din reţeaua dumneavoastră fără a se conecta la sistemul dumneavoastră. De exemplu, un utilizator poate stabili o conexiune SLIP la sistemul dumneavoastră. Apoi utilizatorul poate stabili o conexiune FTP la alt sistem din reţeaua dumneavoastră care nu permite dial-in.

Puteţi împiedica un utilizator SLIP de a accesa alte sisteme din reţeaua dumneavoastră specificând N (Nu) pentru câmpul *Permite rutarea datagramelor IP* din profilul de configurare. Aceasta împiedică un utilizator de a accesa reţeaua dumneavoastră înainte ca utilizatorul să se lege la sistemul dumneazoastră. Totuşi, după ce utilizatorul s-a legat cu succes la sistemul dumneavoastră, variabila de rutare a datagramei nu are efect. Nu restricţionează capacitatea utilizatorilor de a utiliza aplicaţia TCP/IP în sistemul iSeries (cum sunt FTP sau TELNET), de stabilire a unei conexiuni cu alt sistem din reţea.

Controlul sesiunilor dial-out

Înainte ca cineva să poată folosi SLIP pentru a stabili o conexiune dial-out de la sistemul dumneavoastră, trebuie să porniţi un profil de configurare SLIP *DIAL. Pentru a crea sau modifica un profil de configurare SLIP, folosiţi comanda WRKTCPPTP. Pentru a porni un profil de configurare, folosiţi fie comanda Pornire TCP/IP punct la punct (STRTCPPTP), fie o

opţiune a ecranului WRKTCPPTP. Când se livrează sistemul dumneavoastră, autorizarea publică pentru comenzile STRTCPPTP şi ENDTCPPTP este *EXCLUDE. Opţiunile de adăugare, modificare şi ştergere a profilurilor de configurare SLIP sunt disponibile doar dacă aveţi autorizarea specială *IOSYSCFG. Ca administrator de securitate, puteţi utiliza atât autorizarea comandă, cât şi autorizarea specială pentru a determina cine poate seta sistemul dumneavoastră să permită conexiuni dial-out.

Securitate şi sesiuni dial-out

Utilizatorii sistemului dumneavoastră iSeries pot dori să stabilească conexiuni dial-out la sisteme care cer validare utilizator. Scriptul de dialog al conexiunii de pe serverul dumneavoastră iSeries trebuie să trimită un ID utilizator şi o parolă sistemului la distanţă. Serverele iSeries furnizează o metodă sigură pentru stocarea acelei parole. Parola nu trebuie să fie stocată în scriptul dialog conexiune.

Note:

1. Chiar dacă sistemul dumneavoastră stochează parola de conexiune în formă criptată, sistemul decriptează parola înainte de a o transmite. Parolele SLIP, ca şi parolele FTP şi TELNET, sunt transmise necriptate (“în clar”). Totuşi, spre deosebire de FTP şi TELNET, parola SLIP este transmisă înainte ca sistemul să stabilească modul TCP/IP.

   Deoarece SLIP foloseşte o conexiune punct la punct în mod asincron, expunerea de securitate când se transmit parole necriptate este diferită de cea cu parolele FTP şi TELNET. Parolele necriptate FTP şi TELNET pot fi transmise ca trafic IP pe o reţea şi sunt, de aceea, vulnerabile la interceptarea electronică. Transmiterea parolei dumneavoastră SLIP este la fel de sigură ca şi legătura telefonică între cele două sisteme.
2. Fişierul implicit pentru stocarea scripturilor dialog conexiune SLIP este QUSRSYS/QATOCPPSCR. Autorizarea publică a acestui fişier este *USE, care împiedică utilizatorii publici de la modificarea scripturilor dialog conexiune implicite.

Când creaţi un profil de conexiune pentru o sesiune la distanţă care cere validare, faceţi următoarele:

__ Pasul 1. Asiguraţi-vă că variabila sistem Păstrare date securitate server (Retain Server Security Data - QRETSVRSEC) este 1 (Da). Această variabilă de sistem determină dacă permiteţi ca parolele care pot fi decriptate să fie stocate într-o zonă protejată pe sistemul dumneavoastră.

__ Pasul 2. Folosiţi comanda WRKTCPPTP pentru a crea un profil de configurare care are următoarele caracteristici:

- Pentru modul profilului de configurare specificaţi *DIAL.
- Pentru *Nume serviciu acces la distanţă* specificaţi ID-ul utilizator pe care sistemul de la distanţă îl aşteaptă. De exemplu, dacă vă conectaţi la un alt server iSeries, specificaţi numele profilului utilizator al acelui server iSeries.
- Pentru *Parolă serviciu acces la distanţă*, specificaţi parola pe care sistemul de la distanţă o aşteaptă pentru acest ID utilizator. Pe serverul dumneavoastră iSeries, această parolă este stocată într-o zonă protejată într-o formă care poate fi decriptată. Numele şi parolele pe care le asignaţi profilurilor de configurare sunt asociate cu profilul utilizator QTCP. Numele şi parolele nu sunt accesibile cu nici o comandă sau interfaţă utilizator. Doar programele sistem înregistrate pot accesa aceste informaţii parolă.

  Notă: Reţineţi că parolele pentru profilurile de configurare nu sunt salvate când salvaţi fişierele de configurare TCP/IP. Pentru a salva parolele SLIP, trebuie să folosiţi comanda Salvare date de securitate (SAVSECDTA) pentru a salva profilul utilizator QTCP.
- Pentru scriptul dialog conexiune, specificaţi un script care transmite ID-ul utilizator şi parola. Sistemul furnizează mai multe exemple de script-uri

dialog care pun la dispoziţie această funcţie. Când sistemul rulează scriptul, sistemul recuperează parola, o decriptează şi o transmite sistemului de la distanţă.

Consideraţii de securitate pentru protocolul punct-la-punct

Protocolul punct-la-punct (PPP) este disponibil ca parte a lui TCP/IP. PPP este un standard industrial pentru conexiunile punct la punct ce furnizează funcţii adiţionale faţă de ceea ce este disponibil cu SLIP.

Cu PPP, serverul dumneavoastră iSeries poate avea conexiuni de viteză ridicată direct la un Furnizor de servicii Internet sau la alte sisteme într-o reţea locală sau externă. LAN-urile la distanţă pot face conexiuni la serverul dumneavoastră iSeries.

Ţineţi minte că PPP, ca şi SLIP, furnizează o conexiune reţea la serverul dumneavoastră iSeries. O conexiune PPP, în principal, aduce solicitantul la uşa sistemului dumneavoastră. Solicitantul necesită, încă, un ID utilizator şi parolă pentru a intra în sistemul dumneavoastră şi a se conecta la un server TCP/IP cum ar fi TELNET sau FTP. Următoarele sunt consideraţii de securitate despre această nouă posibilitate de conectare:

Notă: Configuraţi PPP folosind Navigator iSeries pe o staţie de lucru IBM iSeries Access pentru Windows.

- PPP oferă posibilitatea de a avea conexiuni dedicate (când acelaşi utilizator are întotdeauna aceeaşi adresă IP). Cu o adresă dedicată, aveţi posibilitate pentru spoofing IP (un sistem impostor care pretinde că este un sistem de încredere cu o adresă IP cunoscută). Totuşi, îmbunătăţirile posibilităţilor de autentificare pe care PPP le furnizează ajută protecţia împotriva spoofing-ului IP.
- Cu PPP, ca şi cu SLIP, creaţi profiluri de conexiune care au un nume de utilizator şi o parolă asociată. Totuşi, spre deosebire de SLIP, utilizatorul nu trebuie să aibă un profil utilizator şi o parolă valide. Numele utilizator şi parola nu sunt asociate cu un profil utilizator. În schimb, sunt utilizate listele de validări pentru autentificare PPP. În plus, PPP nu are nevoie de un script de conectare. Autentificarea (schimbul numelui utilizator şi parolei) este parte a arhitecturii PPP şi se petrece la un nivel mai jos decât cu SLIP.
- Cu PPP, aveţi opţiunea să folosiţi CHAP (challenge handshake authentication protocol). Nu va mai trebui să vă îngrijoraţi din cauza impostorilor care interceptează parole deoarece CHAP criptează numele utilizator şi parolele.

  Conexiunea dumnevoastră PPP foloseşte CHAP doar dacă ambele părţi au suport CHAP. În timpul schimbului de semnale pentru configurarea comunicaţiilor dintre două modem-uri, cele două sisteme negociază. De exemplu, dacă SYSTEMA suportă CHAP iar SYSTEMB nu, SYSTEMA poate fie să interzică sesiunea, fie să accepte să folosească un nume utilizator şi parolă necriptate. Acceptarea folosirii numelui utilizator şi parolei necriptate este considerată o negociere slabă. Decizia negocierii slabe este o opţiune de configurare. La intranet-ul dumneavoastră, de exemplu, când ştiţi că toate sistemele dumneavoastră au posibilităţi CHAP, trebuie să configuraţi profilul dumneavoastră conexiune să nu permită o negociere slabă. La o conexiune publică unde sistemul dumneavoastră face dial-out, puteţi dori să negociaţi slab.

  Profilul conexiune pentru PPP furnizează abilitatea de a specifica adrese IP valide. Puteţi, de exemplu, să indicaţi că solicitaţi o anumită adresă sau nivel de adrese pentru un anumit utilizator. Această posibilitate, împreună cu criptarea parolelor, furnizează protecţie suplimentară împotriva spoofing-ului.

  Ca protecţie adiţională împotriva spoofing-ului sau piggy-backing-ului la o sesiune activă, puteţi configura PPP-ul să se modifice la anumite intervale de timp. De exemplu, în timp ce o sesiune PPP este activă, serverul dumneavoastrăiSeries va trebui să ceară celuilalt sistem un utilizator şi o parolă. O face la fiecare 15 minute pentru a se asigura că este acelaşi profil

utilizator (Utilizatorul final nu va şti despre această activitate. Sistemele schimbă nume şi parole în spatele nivelului pe care utilizatorul final îl vede.)

Cu PPP, vă puteţi aştepta că LAN-urile la distanţă să poată stabili o conexiune la serverul dumneavoastră iSeries şi la reţeaua dumneavoastră extinsă. În acest mediu, a avea expediere IP activă este probabil o cerinţă. Expedierea IP poate permite unui intrus să hoinărească prin reţeaua dumneavoastră. Totuşi, PPP are protecţii mai puternice (cum ar fi criptarea parolei şi validarea adreselor IP). Aceasta face, în primul rând, mai puţin probabil ca un intrus să poată stabili o conexiune reţea.

Pentru informaţii suplimentare despre PPP, consultaţiiSeries Centrul de informare..

Consideraţii de securitate pentru folosirea serverului Protocol Bootstrap

Protocol Bootstrap (BOOTP) oferă o metodă dinamică pentru asocierea staţiilor de lucru cu servere şi pentru asocierea adreselor de IP ale staţiilor de lucru şi surselor IPL (Initial Program Load).

BOOTP este un protocol TCP/IP utilizat pentru a permite unei staţii de lucru fără suport de stocare (client) să solicite un fişier ce conţine codul iniţial de pe un server din reţea. Serverul BOOTP ascultă binecunoscutul port 67 al serverului BOOTP. Când este primită o cerere client, Serverul caută adresa de IP definită pentru client şi returnează clietului un răspuns cu adresa de IP a clientului şi numele fişierului de încărcat. Atunci clientul iniţiază o cerere TFTP către server pentru fişierul de încărcat. Maparea între adresa hardware a clientului şi adresa IP este ţinută în tabela BOOTP de pe serverul iSeries.

Împiedicarea accesului BOOTP

Dacă nu aveţi clienţi rari ataşaţi la reţeaua dumneavoastră, nu aveţi nevoie să rulaţi serverul BOOTP pe sistemul dumneavoastră. Poate fi folosit pentru alte dispozitive, dar soluţia preferată pentru aceste dispozitive este de a utiliza DHCP. Realizaţi următoarele pentru a împiedica Serverul BOOTP să ruleze:

__ Pasul 1. Pentru a împiedica joburile de server BOOTP să pornească automat când porniţi TCP/IP, introduceţi următoarele:

```
CHGBPA AUTOSTART(*NO)
```

Note:

a. AUTOSTART(*NO) este valoarea implicită.

b. “Controlul serverelor TCP/IP care să pornească automat” la pagina 116 furnizează mai multe informaţii despre controlarea serverelor TCP/IP care sunt lansate automat.

__ Pasul 2. Pentru a interzice ca cineva să asocieze o aplicaţie utilizator, cum ar fi o aplicaţie socket, cu portul pe care sistemul în mod normal îl utilizează pentru BOOTP, faceţi următoarele:

Notă: Deoarece DHCP şi BOOTP folosesc acelaşi număr de port, acest lucru inhibă, de asemenea, portul utilizat de către DHCP. Nu interziceţi portul dacă doriţi să utilizaţi DHCP.

__ Pasul a. Introduceţi GO CFGTCP pentru a afişa meniul de configurare TCP/IP.

__ Pasul b. Selectaţi opţiunea 4 (Work with TCP/IP port restrictions - Gestiune restricţii port TCP/IP).

__ Pasul c. În ecranul Gestiune restricţii port TCP/IP (Work with TCP/IP Port Restrictions), specificaţi opţiunea 1 (Adăugare).

__ Pasul d. Pentru limita inferioară a intervalului portului, specificaţi 67.

__ Pasul e. Pentru limita superioară a intervalului portului, specificaţi *ONLY.

Note:

1) Restricţiile de port au efect la următoarea pornire TCP/IP. Dacă TCP/IP este activ atunci când setaţi restricţiile de port, trebuie să opriţi TCP/IP şi să îl porniţi din nou.
2) RFC1700 furnizează informaţii despre atribuirile obişnuite ale numerelor de porturi.

__ Pasul f. Pentru protocol, specificaţi *UDP.

__ Pasul g. Pentru câmpul profil utilizator, specificaţi un nume de profil utilizator care este protejat de sistem (Un profil de utilizator protejat de sistem este un profil care nu deţine programe care adoptă autorizare şi care nu are o parolă care este cunoscută de alţi utilizatori). Restricţionând portul pentru un anumit utilizator, automat îi excludeţi pe toţi ceilalţi utilizatori.

Securizarea serverului BOOTP

Serverul BOOTP nu oferă acces direct la sistemul dumneavoastră iSeries şi, de aceea, reprezintă o problemă de securitate limitată. Prima dumneavoastră sarcină ca administrator de securitate este să asiguraţi că sunt asociate informaţiile corecte cu clientul corect. Cu alte cuvinte, un răuvoitor ar putea altera tabela BOOTP şi ar putea cauza clienţilor dumneavoastră să lucreze incorect sau deloc.

Pentru a administra Serverul BOOTP şi tabela BOOTP, trebuie să aveţi autorizarea specială *IOSYSCFG. Trebuie să controlaţi cu grijă profilurile utilizatorilor care au autorizarea specială *IOSYSCFG pe sistemul dumneavoastră.

Consideraţii de securitate pentru folosirea serverului DHCP

Dynamic host configuration protocol (DHCP) oferă cadrul de lucru pentru transmiterea informaţiilor de configurare către gazdă într-o reţea TCP/IP. Pentru staţiile de lucru client, DHCP poate oferi o funcţie similară cu autoconfigurarea. Un program care permite DHCP de pe staţia de lucru client, emite o cerere pentru informaţii de configurare. Un program cuDHCP activat pe staţia de lucru client difuzează o cerere pentru informaţii de configurare. Dacă serverul DHCP rulează pe serverul dumneavoastră iSeries, serverul răspunde la cerere trimiţând informaţiile de care are nevoie staţia de lucru client pentru a-şi configura corect TCP/IP-ul.

Puteţi folosi DHCP pentru a face mai simplă conectarea utilizatorilor la serverul dumneavoastră iSeries pentru prima dată. Aceasta deoarece utilizatorul nu trebuie să introducă informaţii de configurare TCP/IP. Puteţi utiliza DHCP şi pentru a reduce numărul de adrese TCP/IP interne de care aveţi nevoie într-o subreţea. Serverul DHCP poate aloca temporar adrese IP utilizatorilor activi (din intervalul său de adrese IP).

Pentru mai puţini clienţi, puteţi folosi DHCP în locul lui BOOTP. DHCP furnizează mai multe funcţii decât BOOTP şi poate suporta configurare dinamică atât a clienţilor cât şi a PC-urilor.

Împiedicarea accesului DHCP

Dacă *nu* doriţi ca cineva să utilizeze Serverul DHCP de pe sistemul dumneavoastră, faceţi următoarele:

1. Pentru a împiedica joburile de server DHCP să pornească automat când porniţi TCP/IP, introduceţi următoarele:

   ```
   CHGDHCPA AUTOSTART(*NO)
   ```

   Note:

   a. AUTOSTART(*NO) este valoarea implicită.

   b. “Controlul serverelor TCP/IP care să pornească automat” la pagina 116 furnizează mai multe informaţii despre controlarea serverelor TCP/IP care sunt lansate automat.

2. Pentru a interzice ca cineva să asocieze o aplicaţie utilizator, cum ar fi o aplicaţie socket, cu portul pe care sistemul în mod normal îl utilizează pentru DHCP, faceţi următoarele:

   a. Introduceţi GO CFGTCP pentru a afişa meniul de configurare TCP/IP.

   b. Selectaţi opţiunea 4 (Work with TCP/IP port restrictions - Gestiune restricţii port TCP/IP).

   c. În ecranul Gestiune restricţii port TCP/IP (Work with TCP/IP Port Restrictions), specificaţi opţiunea 1 (Adăugare).

   d. Pentru limita inferioară a intervalului portului, specificaţi 67.

   e. Pentru limita superioară a intervalului portului, specificaţi 68.

      Note:

      1) Restricţiile de port au efect la următoarea pornire TCP/IP. Dacă TCP/IP este activ atunci când setaţi restricţiile de port, trebuie să opriţi TCP/IP şi să îl porniţi din nou.

      2) RFC1700 furnizează informaţii despre atribuirile obişnuite ale numerelor de porturi.

   f. Pentru protocol, specificaţi *UDP.

   g. Pentru câmpul profil utilizator, specificaţi un nume de profil utilizator care este protejat de sistem (Un profil de utilizator protejat de sistem este un profil care nu deţine programe care adoptă autorizare şi care nu are o parolă care este cunoscută de alţi utilizatori). Restricţionând portul pentru un anumit utilizator, automat îi excludeţi pe toţi ceilalţi utilizatori.

Securizarea serverului DHCP

În continuare sunt prezentate câteva consideraţii despre securitate când alegeţi să rulaţi DHCP pe sistemul iSeries:

- Limitaţi numărul utilizatorilor care au autorizarea de a administra DHCP. Administrarea DHCP necesită următoarele autorizări:
  - autorizarea specială *IOSYSCFG
  - autorizarea *RW pentru următoarele fişiere:

    ```
    /QIBM/UserData/OS400/DHCP/dhcpsd.cfg
    /QIBM/UserData/OS400/DHCP/dhcprd.cfg
    ```

- Evaluaţi cum este accesibil din punct de vedere fizic LAN-ul dumneavoastră. Poate un utilizator din exterior intra în locaţia dumneavoastră cu un laptop şi să se conecteze fizic la LAN-ul dumneavoastră? Dacă aceasta este o problemă, DHCP oferă facilitatea de a crea o listă a clienţilor (adresele hardware) pe care Serverul DHCP le va configura. Când utilizaţi această facilitate, înlăturaţi unele din beneficiile productivităţii pe care DHCP le oferă administratorilor de reţea. Totuşi, împiedicaţi sistemul să configureze staţii de lucru necunoscute.
- Dacă este posibil, utilizaţi un interval de adrese IP care este reutilizabil (nu este proiectat pentru Internet). Acest lucru vă ajută să împiedicaţi o staţie de lucru din afara reţelei să obţină informaţii de configurare utilizabile de pe server.

- Utilizaţi punctele de ieşire DHCP dacă aveţi nevoie de protecţie suplimentară. În continuare este prezentată o privire de ansamblu asupra punctelor de ieşire şi a facilităţilor acestora. *iSeries Referinţa API Sistem* descrie cum trebuie folosite punctele de ieşire.

  Intrare port
  Sistemul apelează programul dumneavoastră de ieşire ori de câte ori citeşte un pachet de date de la portul 67 (portul DHCP). Programul dumneavoastră de ieşire primeşte pachetul de date complet. Poate decide dacă sistemul ar trebui să prelucreze sau să-l ignore. Puteţi utiliza acest punct de ieşire când facilităţile DHCP de afişare existente nu sunt suficiente pentru nevoile dumneavoastră.

  Asociere adrese
  Sistemul apelează programul dumneavoastră de ieşire ori de câte ori DHCP asociază în mod formal o adresă unui client.

  Eliberare adrese
  Sistemul apelează programul dumneavoastră de ieşire ori de câte ori DHCP eliberează în mod formal o adresă şi o plasează înapoi în intervalul de adrese.

Consideraţii de securitate pentru folosirea serverului TFTP

FTP (File Transfer Protocol) trivial (TFTP) oferă un transfer de bază al fişierelor fără autentificarea utilizatorului. TFTP lucrează fie cu Protocol Bootstrap (BOOTP), fie cu Dynamic Host Configuration Protocol (DHCP).

Clientul se conectează iniţial fie la serverul BOOTP, fie la serverul DHCP. Serverul BOOTP sau Serverul DHCP răspunde cu adresa de IP a clientului şi cu numele fişierului de încărcat. Atunci clientul iniţiază o cerere TFTP către server pentru fişierul de încărcat. Când clientul termină de preluat fişierul respectiv, sesiunea TFTP se încheie.

Împiedicarea accesului TFTP

Dacă nu aveţi nici un client rar ataşat la reţeaua dumneavoastră, probabil nu veţi avea nevoie să rulaţi serverul TFTP pe sistemul dumneavoastră. Realizaţi următoarele pentru a împiedica Serverul TFTP să ruleze:

__ Pasul 1. Pentru a împiedica joburile de server TFTP să pornească automat când porniţi TCP/IP, introduceţi următoarele:

```
CHGTFTPA AUTOSTART(*NO)
```

Note:

a. AUTOSTART(*NO) este valoarea implicită.

b. “Controlul serverelor TCP/IP care să pornească automat” la pagina 116 furnizează mai multe informaţii despre controlarea serverelor TCP/IP care sunt lansate automat.

__ Pasul 2. Pentru a interzice ca cineva să asocieze o aplicaţie utilizator, cum ar fi o aplicaţie socket, cu portul pe care sistemul în mod normal îl utilizează pentru TFTP, faceţi următoarele:

__ Pasul a. Introduceţi GO CFGTCP pentru a afişa meniul de configurare TCP/IP.

__ Pasul b. Selectaţi opţiunea 4 (Work with TCP/IP port restrictions - Gestiune restricţii port TCP/IP).

__ Pasul c. În ecranul Gestiune restricţii port TCP/IP (Work with TCP/IP Port Restrictions), specificaţi opţiunea 1 (Adăugare).

__ Pasul d. Pentru limita inferioară a intervalului portului, specificaţi 69.

__ Pasul e. Pentru limita superioară a intervalului portului, specificaţi *ONLY.

Note:

1) Restricţiile de port au efect la următoarea pornire TCP/IP. Dacă TCP/IP este activ atunci când setaţi restricţiile de port, trebuie să opriţi TCP/IP şi să îl porniţi din nou.
2) RFC1700 furnizează informaţii despre atribuirile obişnuite ale numerelor de porturi.

__ Pasul f. Pentru protocol, specificaţi *UDP.

__ Pasul g. Pentru câmpul profil utilizator, specificaţi un nume de profil utilizator care este protejat de sistem (Un profil de utilizator protejat de sistem este un profil care nu deţine programe care adoptă autorizare şi care nu are o parolă care este cunoscută de alţi utilizatori). Restricţionând portul pentru un anumit utilizator, automat îi excludeţi pe toţi ceilalţi utilizatori.

Securizarea serverului TFTP

Implicit, serverul TFTP furnizează acces foarte limitat la iSeries sistem. Este configurat special pentru a furniza codul iniţial pentru clienţi rari. În calitate de administrator de securitate, trebuie să fiţi conştienţi de următoarele caracteristici ale serverului TFTP:

- Serverul TFTP nu necesită autentificare (un identificator de utilizator şi o parolă). Toate joburile TFTP rulează sub profilul de utilizator QTFTP. Profilul de utilizator QTFTP nu are parolă. De aceea, nu este disponibil pentru semnările interactive. Profilul de utilizator QTFTP nu are autorizări speciale şi nici nu este autorizat explicit pentru resursele sistemului. Foloseşte autorizarea publică pentru a accesa resurserle de care are nevoie pentru clienţii rari.
- Când soseşte, serverul TFTP este configurat pentru a accesa directorul care conţine informaţii despre clienţii rari. Trebuie să aveţi *PUBLIC sau QTFTP autorizat pentru a citi sau scrie în acel director. Pentru a scrie în director trebuie să aveţi specificat *CREATE în parametrul ″Permitere scrieri fişier″ al comenzii CHGTFTPA. Pentru a scrie într-un fişier existent trebuie să aveţi specificat *REPLACE în parametrul ″Permitere scrieri fişier″ al comenzii CHGTFTPA. *CREATE vă permite să înlocuiţi fişiere existente sau să creaţi fişiere noi. *REPLACE vă permite numai să înlocuiţi fişiere existente.

  Un client TFTP nu poate accesa nici un alt director decât dacă definiţi în mod explicit directorul cu comanda Modificare Atribute TFTP (Change TFTP Attributes - CHGTFTPA). De aceea, dacă un utilizator local sau de la distanţă încearcă să pornească o sesiune TFTP pe sistemul dumneavoastră, posibilităţile utilizatorului de a accesa informaţii sau de a cauza deteriorări sunt extrem de limitate.
- Dacă alegeţi să configuraţi serverul dumneavoastră TFTP pentru a furniza alte servicii suplimentare pentru manipularea clienţilor rari, puteţi defini un program de ieşire care să evalueze şi să autorizeze orice cerere TFTP. Serverul TFTP oferă o ieşire de validare a cererilor similară cu cea care este disponibilă pe Serverul FTP. Pentru informaţii suplimentare, consultaţi iSeries Centru de informare—>Reţea—>TCP/IP—>TFTP. Consultaţi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru informaţii despre accesarea Centrului de informare iSeries.

Consideraţii de securitate pentru folosirea serverului REXEC

Server REmote EXECution (REXEC) primeşte şi rulează comenzi de la un client REXEC. Un client REXEC este un calculator sau UNIX aplicaţie ce suportă trimiterea comenzii REXEC. Suportul pe care îl oferă acest server este similar cu facilitatea care este disponibilă atunci când utilizaţi subcomanda RCMD (Remote Command - Comandă de la distanţă) pentru Serverul FTP.

Împiedicarea accesului REXEC

Dacă doriţi ca serverul dumneavoastră iSeries să nu accepte comenzi de la un client REXEC, faceţi următoarele pentru a împiedica serverul REXEC să ruleze:

__ Pasul 1. Pentru a împiedica joburile de server REXEC să pornească automat când porniţi TCP/IP, introduceţi următoarele:

```
CHGRXCA AUTOSTART(*NO)
```

Note:

a. AUTOSTART(*NO) este valoarea implicită.

b. “Controlul serverelor TCP/IP care să pornească automat” la pagina 116 furnizează mai multe informaţii despre controlarea serverelor TCP/IP care sunt lansate automat.

__ Pasul 2. Pentru a interzice ca cineva să asocieze o aplicaţie utilizator, cum ar fi o aplicaţie socket, cu portul pe care sistemul în mod normal îl utilizează pentru REXEC, faceţi următoarele:

__ Pasul a. Introduceţi GO CFGTCP pentru a afişa meniul de configurare TCP/IP.

__ Pasul b. Selectaţi opţiunea 4 (Work with TCP/IP port restrictions - Gestiune restricţii port TCP/IP).

__ Pasul c. În ecranul Gestiune restricţii port TCP/IP (Work with TCP/IP Port Restrictions), specificaţi opţiunea 1 (Adăugare).

__ Pasul d. Pentru limita inferioară a intervalului portului, specificaţi 512.

__ Pasul e. Pentru limita superioară a intervalului portului, specificaţi *ONLY.

__ Pasul f. Pentru protocol, specificaţi *TCP.

__ Pasul g. Pentru câmpul profil utilizator, specificaţi un nume de profil utilizator care este protejat de sistem (Un profil de utilizator protejat de sistem este un profil care nu deţine programe care adoptă autorizare şi care nu are o parolă care este cunoscută de alţi utilizatori). Restricţionând portul pentru un anumit utilizator, automat îi excludeţi pe toţi ceilalţi utilizatori.

Note:

a. Restricţiile de port au efect la următoarea pornire TCP/IP. Dacă TCP/IP este activ atunci când setaţi restricţiile de port, trebuie să opriţi TCP/IP şi să îl porniţi din nou.

b. RFC1700 furnizează informaţii despre atribuirile obişnuite ale numerelor de porturi.

Securizarea serverului REXEC

În continuare sunt prezentate câteva consideraţii pentru când veţi alege să rulaţi Server REmote EXECution pe sistemul dumneavoastră:

- O cerere REXCD include un identificator de utilizator, o parolă şi comanda de executat. Autentificarea normală a serverului iSeries şi verificarea autorizării se aplică:
  - Profilul de utilizator şi parola trebuie să fie valide.
  - Sistemul impune *Limite de capacitate*valoarea (LMTCPB) pentru profilul de utilizator.
  - Utilizatorul trebuie să fie autorizat pentru comandă şi pentru toate resursele pe care comanda le utilizează.
- Serverul REXEC furnizează puncte de ieşire similare punctelor de ieşire disponibile pentru Serverul FTP. Puteţi folosi Punct ieşire validare (Validation exit point) pentru a evalua comanda şi pentru a decide dacă o veţi accepta. Pentru informaţii suplimentare, consultaţi

iSeries Centrul de informare—>Reţea—>TCP/IP—>REXEC. Consultaţi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru informaţii despre accesarea Centrului de informare iSeries.

- Când alegeţi să rulaţi Serverul REXEC, rulaţi în afara oricărui control de acces la meniu pe care îl aveţi pe sistemul dumneavoastră. Trebuie să vă asiguraţi că schema de autorizări pentru obiectele dumneavoastră este potrivită pentru a vă proteja resursele.

Consideraţii de securitate pentru folosirea RouteD

Serverul (RouteD) Demon Route furnizează suport pentru Protocolul de informaţii de rutare (RIP) pe serverele iSeries. RIP este cel mai utilizat dintre protocoalele de rutare. Este un protocol gateway intern (Interior Gateway Protocol) care asistă TCP/IP în rutarea pachetelor IP într-un sistem autonom.

RouteD este conceput pentru a creşte eficienţa traficului din reţea, permiţând sistemelor dintr-o reţea de încredere să se actualizeze reciproc cu informaţii despre rutele curente. Când rulaţi RouteD, sistemul dumneavoastră poate primi actualizări de la alte sisteme participante despre cum ar trebui rutate transmisiile (pachetele). De aceea, dacă serverul dumneavoastră RouteD este accesibil unui hacker, hacker-ul l-ar putea utiliza pentru a reruta pachetele dumneavoastră către un sistem care poate intercepta sau modifica aceste pachete. În continuare sunt prezentate câteva sugestii pentru securitatea RouteD:

- ServereleiSeries folosesc RIPv1, care nu furnizează nici o metodă pentru autentificarea ruterelor. Este conceput pentru utilizarea într-o reţea de încredere. Dacă sistemul este într-o reţea cu alte sisteme în care nu aveţi încredere, nu ar trebui să rulaţi Serverul RouteD. Pentru a vă asigura că Serverul RouteD nu porneşte automat, introduceţi următoarele:

  ```
  CHGRTDA AUTOSTART(*NO)
  ```

  Note:

  1. AUTOSTART(*NO) este valoarea implicită.
  2. “Controlul serverelor TCP/IP care să pornească automat” la pagina 116 furnizează mai multe informaţii despre controlarea serverelor TCP/IP care sunt lansate automat.
- Asiguraţi-vă că dumneavoastră controlaţi cine poate modifica configuraţia RouteD, care necesită autorizarea specială *IOSYSCFG.
- Dacă sistemul dumneavoastră participă în mai mult de o reţea (de exemplu, intranet şi Internet), puteţi configura Serverul RouteD pentru a transmite şi a accepta actualizări numai cu reţele sigure.

Consideraţii de securitate pentru folosirea serverului DNS

Serverul Domain Name System (DNS) realizează translatarea numelui de gazdă în adresă IP şi invers. Pe serverele iSeries, serverul DNS este folosit pentru a furniza translatarea adreselor pentru reţeaua securizată, internă (intranet).

Prevenirea accesului DNS

Dacă *nu* doriţi ca cineva să utilizeze Serverul DNS de pe sistemul dumneavoastră, faceţi următoarele:

1. Pentru a împiedica joburile de server DNS să pornească automat când porniţi TCP/IP, introduceţi următoarele:

   ```
   CHGDNSA AUTOSTART(*NO)
   ```

   Note:

   a. AUTOSTART(*NO) este valoarea implicită.
   b. “Controlul serverelor TCP/IP care să pornească automat” la pagina 116 furnizează mai multe informaţii despre controlarea serverelor TCP/IP care sunt lansate automat.

2. Pentru a interzice ca cineva să asocieze o aplicaţie utilizator, cum ar fi o aplicaţie socket, cu portul pe care sistemul în mod normal îl utilizează pentru DNS, faceţi următoarele:
   a. Introduceţi GO CFGTCP pentru a afişa meniul de configurare TCP/IP.
   b. Selectaţi opţiunea 4 (Work with TCP/IP port restrictions - Gestiune restricţii port TCP/IP).
   c. În ecranul Gestiune restricţii port TCP/IP (Work with TCP/IP Port Restrictions), specificaţi opţiunea 1 (Adăugare).
   d. Pentru limita inferioară a intervalului portului, specificaţi 53.
   e. Pentru limita superioară a intervalului portului, specificaţi *ONLY.

      Note:

      1) Restricţiile de port au efect la următoarea pornire TCP/IP. Dacă TCP/IP este activ atunci când setaţi restricţiile de port, trebuie să opriţi TCP/IP şi să îl porniţi din nou.
      2) RFC1700 furnizează informaţii despre atribuirile obişnuite ale numerelor de porturi.

   f. Pentru protocol, specificaţi *TCP.
   g. Pentru câmpul profil utilizator, specificaţi un nume de profil utilizator care este protejat de sistem (Un profil de utilizator protejat de sistem este un profil care nu deţine programe care adoptă autorizare şi care nu are o parolă care este cunoscută de alţi utilizatori). Restricţionând portul pentru un anumit utilizator, automat îi excludeţi pe toţi ceilalţi utilizatori.
   h. Repetaţi paşii 2c până la 2g pentru protocolul *UDP (Datagramă utilizator).

Securizarea serverului DNS

În continuare sunt prezentate câteva consideraţii despre securitate când alegeţi să rulaţi DNS pe sistemul iSeries:

- Funcţia pe care Serverul DNS o furnizează este translatarea adreselor IP şi translatarea numelor. Nu furnizează acces la obiectele de pe iSeries. Riscul la care sunteţi supus când un utilizator din exterior accesează Serverul DNS este acela că Serverul oferă un mod uşor de vizualizare a topologiei reţelei dumneavoastră. DNS poate scuti un hacker de efortul de a determina adresele ţintelor potenţiale. Totuşi, DNS nu furnizează informaţii care îl vor ajuta să intre în acele sisteme ţintă.
- În mod tipic, utilizaţi Serverul DNS iSeries pentru intranet. De aceea, probabil că nu este nevoie să restricţionaţi facilitatea de a interoga DNS. Totuşi, s-ar putea să aveţi, de exemplu, câteva subreţele în intranet. Nu veţi dori probabil ca utilizatori de pe o altă subreţea să poată interoga DNS-ul de pe serverul dumneavoastră iSeries. O opţiune de securitate a DNS vă permite să limitaţi accesul la domeniul principal. Folosiţi Navigator iSeries pentru a specifica adresele IP la care serverul DNS să trebuiască să răspundă.

  Altă opţiune de securitate vă permite să specificaţi care servere secundare pot copia informaţii de pe Serverul DNS principal. Când utilizaţi această opţiune, Serverul va accepta cereri de transfer zonă (o cerere de copiere de informaţii) numai de la serverele secundare pe care le-aţi introdus în mod explicit.
- Asiguraţi-vă că restricţionaţi cu grijă facilitatea de schimbare a fişierului de configurare pentru Serverul DNS. O persoană cu intenţii răutăcioase, de exemplu, modifică fişierul serverului DNS să puncteze către o adresă IP din afara reţelei dumneavoastră. Persoana ar putea simula un server în reţeaua dumneavoastră şi probabil că ar căpăta acces la informaţii confidenţiale de la utilizatorii care vizitează Serverul.

Consideraţii de securitate pentru folosirea serverului HTTP pentru iSeries

Serverul HTTP furnizează clienţi browser World Wide Web cu acces la obiectele multimedia ale serverului iSeries, cum ar fi documente HTML (Hypertext Markup Language - Limbajul de marcare al hipertextului). De asemenea, suportă specificaţia *Common Gateway Interface (CGI)*. Programatorii de aplicaţii pot scrie programe CGI pentru a extinde funcţionalitatea serverului.

Administratorul poate folosi Server conectare Internet sau server IBM HTTP pentru iSeries pentru a rula concurent mai multe servere pe acelaşi server iSeries. Fiecare server care rulează este numit **instanţă server**. Fiecare instanţă server are un nume unic. Administratorul controlează care instanţe sunt pornite şi ce poate face fiecare instanţă.

Notă: Trebuie să aveţi instanţa *ADMIN a serverului HTTP ce rulează atunci când utilizaţi un browser de web pentru a configura sau administra una din următoarele:

- Firewall pentru iSeries
- Server conectare Internet
- Server sigur conectare Internet
- IBM HTTP Server pentru iSeries

Un utilizator (vizitator de site Web) nu vede niciodată un ecran de semnare al serverului iSeries. Totuşi, administratorul serverului iSeries trebuie să autorizeze explicit toate documentele HTML şi programele CGI prin definirea lor în directive HTTP. În plus, administratorul poate seta atât securitatea resurselor, cât şi autentificarea utilizatorului (identificator utilizator şi parolă) pentru unele cereri sau pentru toate.

Un atac al unui hacker poate determina interzicerea serviciului pentru Serverul dumneavoastră Web. Serverul dumneavoastră poate detecta un atac interzicere-serviciu cronometrând cererile anumitor clienţi. Dacă Serverul nu primeşte o cerere de la client, atunci Serverul dumneavoastră determină faptul că este în desfăşurare atacul de interzicere-serviciu. Acest lucru apare după realizarea conexiunii client iniţiale le Serverul dumneavoastră Configurarea implicită a serverului este de a realiza detectarea şi penalizarea atacurilor.

Împiedicarea accesului HTTP

Dacă *nu* doriţi ca cineva să utilizeze programul pentru a accesa sistemul dumneavoastră, trebuie să împiedicaţi Serverul HTTP să ruleze. Faceţi următoarele:

__ Pasul 1. Pentru a împiedica joburile de server HTTP să pornească automat când porniţi TCP/IP, introduceţi următoarele:

```
CHGHTTPA AUTOSTART(*NO)
```

Note:

a. AUTOSTART(*NO) este valoarea implicită.

b. “Controlul serverelor TCP/IP care să pornească automat” la pagina 116 furnizează mai multe informaţii despre controlarea serverelor TCP/IP care sunt lansate automat.

__ Pasul 2. Implicit, jobul de server HTTP utilizează profilul de utilizator QTMHHTTP. Pentru a împiedica Serverul HTTP să pornească, setaţi starea profilului de utilizator QTMHHTTP pe *DISABLED.

Controlul accesului la serverul HTTP

Principalul scop al rulării serverului HTTP este de a furniza accesul pentru vizitatori la un site Web în iSeries sistem. Vă puteţi gândi la o persoană care vizitează site-ul dumneavoastră de

Web ca la cineva care vede o reclamă într-un ziar economic. Vizitatorul nu cunoaşte hardware-ul şi software-ul de pe site-ului dumneavoastră de Web, cum ar fi tipul de server utilizat şi unde este acesta localizat fizic. De obicei, nu doriţi să puneţi nici o barieră (cum ar fi un ecran de semnare) între un potenţial vizitator şi site-ul de Web. Totuşi, poate doriţi să restricţionaţi accesul la unele documente sau programe CGI pe care site-ul de Web le oferă.

De asemenea, poate doriţi ca un singur sistem iSeries să ofere mai multe site-uri de Web logice. De exemplu, sistemul dumneavoastră iSeries ar putea suporta diferite ramuri ale afacerii dumneavoastră care au setaţi diferiţi clienţi. Pentru fiecare din aceste ramuri ale afacerii, doriţi un site de Web unic care apare total independent de vizitator. În plus, poate doriţi să oferiţi site-uri de Web interne (intranet) cu informaţii confidenţiale despre afacerea dumneavoastră.

În calitate de administrator de securitate, va trebui să protejaţi conţinutul site-ului de Web şi, în acelaşi timp, să vă asiguraţi că practicile de securitate nu afectează negativ valoarea site-ului de Web. În plus, trebuie să vă asiguraţi că activitatea HTTP nu pune în pericol integritatea sistemului dumneavoastră sau a reţelei. Subiectele care urmează vă oferă sugestii legate de securitate când utilizaţi programul.

Consideraţii de administrare

În continuare sunt prezentate câteva consideraţii despre administrarea serverului dumneavoastră de Internet.

- Puteţi executa funcţii de setare şi configurare utilizând un browser de Web şi instanţa *ADMIN. Pentru unele funcţii, cum ar fi crearea unor instanţe adiţionale pe server, *trebuie* să utilizaţi Serverul *ADMIN.
- URL implicit pentru pagina home de administrare (pagina home pentru Serverul *ADMIN) este publicat în documentaţia produselor care oferă funcţii de administrare de browser. De aceea, URL-ul implicit va fi cunoscut de către hacker-i şi publicat în forumurile lor, aşa cum şi parolele implicite pentru profilurile de utilizatori furnizate de IBM sunt cunoscute şi publicate. Vă puteţi proteja aceste puncte slabe în mai multe feluri:
  - Rulaţi instanţa *ADMIN a serverului HTTP doar atunci când trebuie să executaţi funcţii administrative. Nu rulaţi tot timpul instanţa *ADMIN.
  - Activaţi suportul SSL pentru instanţa *ADMIN (utilizând Digital Certificate Manager). Instanţa *ADMIN utilizează directivele de protecţie HTTP pentru a cere un identificator de utilizator şi o parolă. Când utilizaţi SSL, ID-ul dumneavoastră de utilizator şi parola sunt codificate (împreună cu toate celelalte informaţii despre configuraţia dumneavoastră, care apar în formularele de administrare).
  - Utilizaţi un firewall atât pentru a împiedica accesul din Internet la Serverul *ADMIN cât şi pentru a ascunde numele de sistem şi de domeniu, care sunt părţi ale URL.
- Când executaţi funcţii de administrare, trebuie să deschideţi o sesiune cu un profil de utilizator care are autorizarea specială *IOSYSCFG. De asemenea, va trebui să aveţi autorizare pentru anumite obiecte de pe sistem, cum ar fi următoarele:
  - Bibliotecile sau directoarele care conţin documentele HTML şi programele CGI.
  - Orice profil de utilizator pe care planificaţi să comutaţi din directivele pentru server.
  - Listele de control a accesului (Access Control Lists - ACLs) pentru orice director pe care directivele dumneavoastră le utilizează.
  - Un obiect listă de validare pentru crearea şi întreţinerea identificatorilor de utilizatori şi a parolelor.

  Cu Serverul *ADMIN şi cu TELNET puteţi executa funcţii de administrare de la distanţă, probabil printr-o conexiune Internet. Fiţi conştient de faptul că, dacă executaţi funcţii de administrare peste o legătură publică (Internet), există riscul de a fi interceptate identificatorul şi parola unui utilizator foarte puternic. Persoana care ″interceptează″ poate

utiliza acest identificator de utilizator şi parola pentru a încerca să acceseze sistemul dumneavoastră utilizând, de exemplu, TELNET sau FTP.

Note:

1. Cu TELNET, ecranul de conectare este tratat ca oricare alt ecran. Deşi parola nu este afişată când o introduceţi, sistemul o transmite fără a fi codificată sau criptată.
2. Cu Serverul *ADMIN, parola este codificată şi nu criptată. Schema de codificare este un standard industrial şi, de aceea, este cunoscută în comunitatea hacker-ilor. Deşi codificarea nu este uşor de înţeles de un interceptor obişnuit, un interceptor sofisticat probabil că deţine instrumentele cu care să încerce să decodifice parola.

Indiciu pentru securitate

Dacă planificaţi să administraţi de la distanţă prin Internet, trebuie să utilizaţi instanţa *ADMIN cu SSL, astfel încât transmisiile să fie criptate. Nu utilizaţi o aplicaţie nesigură, cum ar fi o versiune mai veche decât V4R4 a TELNET (TELNET asigură suport pentru SSL începând cu V4R4). Dacă utilizaţi Serverul *ADMIN într-o reţea cu utilizatori *de încredere*, probabil că îl puteţi utiliza cu grijă pentru administrare.

- Directivele HTTP oferă baza pentru toate activităţile de pe Serverul dumneavoastră Configuraţia furnizată oferă facilitatea de a servi o pagină Welcome implicită . Un client nu poate vedea nici un document cu excepţia paginii Welcome până când administratorul nu va defini directivele pentru server. Pentru a defini directivele, utilizaţi un browser Web şi Serverul *ADMIN sau comanda Gestiune configuraţii HTTP (Work with HTTP Configuration - WRKHTTPCFG). Ambele metode necesită autorizarea specială *IOSYSCFG. Când conectaţi serverul dumneavoastră iSeries la Internet, devine şi mai greu să controlaţi şi să evaluaţi numărul utilizatorilor din organizaţia dumneavoastră care au autorizarea specială *IOSYSCFG.

Protecţia resurselor

IBM HTTP server for iSeries include directive HTTP care pot furniza controlul detaliat al informaţiilor pe care le foloseşte serverul. Puteţi folosi directive pentru a controla din ce directoare serverul Web serveşte URL-urile atât pentru fişierele HTML cât şi pentru programele CGI, pentru a cumuta pe alte profiluri utilizator şi pentru a cere autentificarea pentru anumite resurse.

Notă: Documentaţia pentru ″Web serving″ (Servire Web) din Centru informaţii furnizează descrieri complete ale directivelor HTTP disponibile şi cum să le folosiţi. În continuare sunt prezentate câteva sugestii şi consideraţii privind utilizarea acestui suport:

- Serverul HTTP porneşte de la baza ″autorizării explicite″. Serverul nu acceptă o cerere decât dacă cererea este definită în mod explicit în directive. Altfel spus, Serverul respinge imediat cererile pentru un URL dacă acel URL nu este definit în directive (ori cu numele ori generic).
- Puteţi utiliza directivele de protecţie pentru a cere un identificator de utilizator şi o parolă înainte de a accepta o cerere pentru anumite resurse sau pentru toate.
  - Când un utilizator (client) solicită o resursă protejată, Serverul cere browser-ului un identificator de utilizator şi o parolă. Browser-ul cere utilizatorului să introducă identificatorul de utilizator şi parola şi trimite informaţiile către server. Unele browser-e stochează identificatorul de utilizator şi parola şi le trimit automat cu cererile ulterioare. Acest lucru scuteşte utilizatorul de introducerea repetată a aceluiaşi identificator de utilizator şi a aceleiaşi parole.

    Deoarece unele browser-e păstrează ID-ul utilizator şi parola, aveţi aceleaşi operaţii ca şi atunci când utilizatorii intră pe sistemul dumneavoastră prin ecranul de semnare al serverului iSeries sau printr-un ruter. O sesiune de browser nesupravegheată reprezintă o problemă de securitate potenţială.

– Sistemul poate administra identificatorii de utilizator şi parolele în trei moduri (specificate prin directive de protecţie):

1. Puteţi folosi profilul utilizator normal al serverului iSeries şi validarea parolei. Această metodă este cea mai utilizată pentru protejarea resurselor în intranet (reţea sigură).
2. Puteţi crea ″Internet users″(Utilizatori Internet): utilizatori care pot fi validaţi dar care nu pot avea un profil utilizator pe serverul iSeries. Utilizatorii Internet suntimplementaţi printr-un obiect server iSeries numit ″listă de validare″. Obiectele listă de validare conţin liste de utilizatori şi de parole ce sunt definite în mod special pentru utilizarea împreună cu o anumită aplicaţie.

   dumneavoastră decideţi cum sunt creaţi identificatorii şi parolele de utilizatori Internet (de către o aplicaţie sau de către un administrator ca răspuns la o cerere prin poştă electronică), cât şi modul de gestionare al utilizatorilor de Internet. Utilizaţi interfaţa browser a serverului HTTP pentru a seta aceasta.

   Pentru reţelele nesigure (the Internet), folosirea utilizatorilor Internet furnizează o protecţie mai bună decât în cazul folosirii profilurilor utilizator şi ale parolelor normale. Setul unic de ID-uri utilizator şi parole creează o limitare implicită asupra acţiunilor permise acelor utilizatori. Identificatorii de utilizatori şi parolele nu sunt disponibile pentru o semnare normală (cum ar fi cu TELNET sau FTP). În plus, nu expuneţi ID-urile utilizator şi parolele pentru a putea fi interceptate.
3. Protocolul de acces director marcat (LDAP) este un protocol de servicii de directoare ce furnizează accesul la directoare în Protocolul de Control Trasmisie (TCP). Vă permite stocarea informaţiilor în acel serviciu de directoare şi-l interoghează. LDAP este de acum suportat ca opţiune pentru autorizarea utilizatorilor.

   Note:

   1. Când browser-ul trimite ID-ul utilizator şi parola (fie pentru un profil utilizator sau pentru un utilizator Internet), acestea sunt codate, nu criptate. Schema de codificare este un standard industrial şi, de aceea, este cunoscută în comunitatea hacker-ilor. Deşi codificarea nu este uşor de înţeles de un interceptor obişnuit, un interceptor sofisticat probabil că deţine instrumentele cu care să încerce să le decodifice.
   2. Serverul iSeries memorează obiectul de validare într-o zonă protejată a sistemului. Îl puteţi accesa doar cu interfeţele de sistem definite (API) şi cu autorizarea corespunzătoare.

– Puteţi utiliza Administrare certificat digital (Digital Certificate Manager, DCM) pentru a crea propriul dumneavoastră Certificat de autorizare intranet. Certificarea digitală asociază automat un certificat cu profilul utilizator al proprietarului. Certificatul are aceleaşi autorizări şi drepturi ca şi profilul asociat.

- Când serverul acceptă o cerere, securitatea normală pentru resurse aserverului iSeries se termină. Profilul utilizator care cere resursa trebuie să aibă autorizare la resursă (cum ar fi directorul sau fişierul fizic sursă care conţine documentul HTML). Implicit, joburile rulează sub profilul de utilizator QTMHHTTP. Puteţi folosi o directivă pentru a comuta pe un profil utilizator diferit. Atunci, sistemul utilizează autorizarea acelui profil de utilizator pentru a accesa obiecte. În continuare sunt prezentate câteva consideraţii despre utilizarea acestui suport:

  – Comutarea între profilurile de utilizator poate fi utilă mai ales atunci când Serverul dumneavoastră furnizează mai mult de un site de Web logic. Puteţi asocia un profil utilizator diferit cu directivele pentru fiecare site Web şi acestea folosesc securitatea normală pentru resurse a serverului iSeries pentru a proteja documentele pentru fiecare site.

  – Puteţi utiliza facilitatea de a comuta între profilurile de utilizator în combinaţie cu obiectul de validare. Serverul foloseşte o parolă şi un ID utilizator unice (diferite de ID-ul utilizator şi parola dumneavoastră normale) pentru a evalua cererea iniţială. După

ce serverul a autentificat utilizatorul, sistemul comută apoi pe un alt profil utilizator şi aceasta constituie un avantaj în asigurarea securităţii resurselor. Astfel, utilizatorul nu cunoaşte numele adevăratului profil de utilizator şi nu poate încerca să îl utilizeze în alte feluri (cum ar fi FTP).

- Unele cereri de server HTTP necesită rularea unui program pe Serverul HTTP. De exemplu, un program ar putea să acceseze date de pe sistemul dumneavoastră Înainte ca programul să poată rula, administratorul serverului trebuie să mapeze cererea (URL) pe un program definit de utilizator care este în conformitate cu standardele interfeţei utilizator CGI. În continuare sunt prezentate câteva consideraţii despre programele CGI:
  - Puteţi utiliza directivele de protecţie pentru programele CGI aşa cum faceţi pentru documentele HTML. De aceea, puteţi solicita un profil de utilizator şi o parolă înainte de a rula programul.
  - Implicit, programele CGI rulează sub profilul de utilizator QTMHHTP1. Puteţi comuta pe un profil utilizator diferit înainte de a rula programul. Prin urmare, puteţi seta securitatea normală a resurselor pentru serverul iSeries pentru resursele care sunt accesate de programele CGI.
  - În calitate de administrator de securitate, ar trebui să executaţi o revizuire a securităţii înainte de a autoriza utilizarea unui program CGI pe sistemul dumneavoastră. Trebuie să ştiţi de unde vine programul şi ce funcţii execută programul CGI. De asemenea, trebuie să monitorizaţi capacităţile profilurilor de utilizator sub care rulaţi programele CGI. Trebuie să efectuaţi teste cu programele CGI pentru a determina, de exemplu, dacă puteţi obţine accesul la o linie de comandă. Trataţi programele CGI cu aceeaşi vigilenţă cu care trataţi şi programele care adoptă autorizare.
  - În plus, asiguraţi-vă că aţi evaluat ce obiecte sensibile ar putea avea o autorizare publică nepotrivită. Un program CGI slab proiectat ar putea permite, în unele cazuri, unui utilizator răuvoitor care are cunoştinţe în domeniu să încerce să navigheze prin sistemul dumneavoastră.
  - Utilizaţi o anumită bibliotecă utilizator, cum ar fi CGILIB, pentru a păstra toate programele dumneavoastră CGI. Utilizaţi autorizarea obiectelor pentru a controla şi cine poate introduce noi obiecte în bibliotecă şi cine poate rula programe din această bibliotecă. Utilizaţi directivele pentru a limita Serverul HTTP să ruleze programe CGI care sunt în această bibliotecă.

    Notă: Dacă Serverul dumneavoastră furnizează mai multe site-uri de Web logice, s-ar putea să doriţi să setaţi o bibliotecă separată pentru programele CGI ale fiecărui site.

Alte consideraţii de securitate

În continuare sunt prezentate şi alte consideraţii despre securitate:

- HTTP furnizează doar accesul citire-scriere îniSeries sistem. Cererile serverului HTTP nu pot actualiza sau şterge date de pe sistemul dumneavoastră în mod direct. Totuşi, aţi putea avea programe CGI care actualizează date. Suplimentar, puteţi activa programul CGI Net.Data pentru accesarea bazei de date de pe serverul dumneavoastră iSeries. Sistemul utilizează un documenta (similar cu un program de ieşire) pentru evaluarea cererilor Net.Data programului. De aceea, administratorul de sistem poate controla ce acţiuni pot fi efectuate de Net.Data program.
- Serverul HTTP furnizează un istoric acces pe care îl puteţi utiliza pentru a monitoriza şi accesurile şi încercările de acces la server.

Consideraţii de securitate pentru folosirea SSL împreună cu IBM HTTP Server for iSeries

IBM HTTP Server for iSeries poate furniza conexiuni Web sigure la serverul dumneavoastră iSeries. Un **site web sigur** înseamnă că transmisiile între client şi server (în ambele direcţii)

sunt criptate. Aceste transmisii codificate sunt protejate atât de cei ce vor să le intercepteze, cât şi de cei ce încearcă fie să le captureze, fie să le modifice.

Notă: Reţineţi că un site de Web sigur se referă strict la informaţiile schimbate între client şi server. Intenţia acestuia nu este de a reduce vulnerabilitatea serverului la atacurile hackerilor. Totuşi, limitează cu siguranţă informaţiile pe care un aşa zis hacker le poate obţine cu uşurinţă prin interceptare.

Subiectele despre SSL şi Webserving (HTTP) din Centrul de informare oferă informaţii complete despre instalarea, configurarea şi administrarea procesului de criptare. Aceste subiecte oferă atât o trecere în revistă a caracteristicilor serverului cât şi câteva consideraţii referitoare la utilizarea serverului.

Server conectare Internet furnizează suport HTTP şi HTTPS când este instalat unul din următoarele programe licenţiate:

- 5722–NC1
- 5722–NCE

Când sunt instalate aceste opţiuni, la produs se face referire ca fiind un ICSS.

IBM HTTP Server for iSeries (5722–DG1) furnizează atât suport pentru http cât şi pentru https. Trebuie să instalaţi unul din următoarele programe de criptografiere pentru a activa SSL:

- 5722–AC2
- 5722–AC3

Securitatea care depinde de codificare are mai multe cerinţe:

- Atât expeditorul, cât şi destinatarul (Serverul şi clientul), trebuie să ″înţeleagă″ mecanismul de codificare şi trebuie să fie capabili să codifice şi să decodifice. Serverul HTTP necesită un client SSL. (Cele mai folosite browser-e Web sunt activate-SSL.) Programele licenţiate de codificare iSeries suportă multe metode de codificare standard. Când un client încearcă să stabilească o sesiune, Serverul şi clientul negociază pentru a găsi cea mai sigură metodă de codificare pe care o suportă amândoi.
- Transmisia nu trebuie să poată fi decodificată de către o persoană care ″trage cu urechea″. De aceea, metodele de codificare necesită ca ambele părţi să aibă o **cheie privată** de codificare/decodificare pe care numai ele o cunosc. Dacă vreţi să aveţi un site web securizat *extern*, trebuie să folosiţi un CA (Certificate Authority) pentru a crea şi a emite certificate utilizatorilor şi serverelor. Autoritatea de certificare este cunoscută ca parte de încredere (trusted party).

Codificarea protejează confidenţialitatea informaţiilor transmise. Totuşi, pentru informaţii sensibile, cum ar fi informaţii financiare, doriţi şi integritate şi autenticitate, pe lângă confidenţialitate. Altfel spus, clientul şi (opţional) Serverul trebuie să aibă încredere în cel de la capătul celălalt (printr-o referinţă independentă) şi trebuie să fie siguri că transmisia nu a fost modificată. Semnătura digitală care este furnizată de autoritatea de certificare (CA) garantează autenticitatea şi integritatea. Protocolul SSL oferă autentificare prin verificarea semnăturii digitale a certificatului serverului (şi opţional a certificatului clientului).

Codificarea şi decodificarea necesită timp de prelucrare şi vor afecta performanţele transmisiei. Prin urmare, servereleiSeries furnizează capacitatea de a rula ambele programe pentru funţionare sigură şi nesigură în acelaşi timp. Puteţi utiliza Serverul HTTP nesigur pentru documentele care nu necesită securitate, cum ar fi cataloagele de produse. Aceste documente vor avea un URL care începe cu http://. Puteţi utiliza un server HTTP sigur pentru

informaţii importante, cum ar fi formularele în care clientul introduce informaţii despre cartea de credit. Programul poate trata documente ale căror URL porneşte fie cu http:// fie cuhttps://.

Notă

Este un gest frumos să vă informaţi clienţii când transmisiile sunt sigure sau nesigure, mai ales când site-ul dumneavoastră de Web utilizează un server sigur numai pentru anumite documente.

Reţineţi că procesul de codificare necesită şi un server sigur şi un client sigur. Browser-ele sigure (clienţi HTTP) au devenit un lucru relativ obişnuit.

Consideraţii de securitate pentru LDAP

Elemente de securitate LDAP include Nivelul Sigur de Sockets (Secure Sockets Layer (SSL)), Liste de Control Acces şi criptare de parole CRAM-MD5. În V5R1, conexiunile Kerberos şi suportul de auditare securitate au fost adăugate pentru a îmbunătăţi securitatea LDAP.

Pentru informaţii suplimentare despre aceste subiecte, consultaţi iSeries Centrul de informare —>Reţea–>TCP/IP–>Servicii director (LDAP). Consultaţi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru informaţii despre accesarea Centrului de informareiSeries.

Consideraţii de securitate pentru LPD

LPD (line printer daemon - demon imprimantă) oferă facilităţi de distribuire a ieşirilor de imprimantă pe sistemul dumneavoastră. Sistemul nu execută nici o procesare semnare pentru LPD.

Împiedicarea accesului LPD

Dacă *nu* doriţi ca cineva să folosească LPD pentru a accesa sistemul dumneavoastră, trebuie să împiedicaţi Serverul LPD să ruleze. Faceţi următoarele:

__ Pasul 1. Pentru a împiedica joburile de server LPD să pornească automat când porniţi TCP/IP, introduceţi următoarele:

```
CHGLPDA AUTOSTART(*NO)
```

Note:

a. AUTOSTART(*YES) este valoarea implicită.

b. “Controlul serverelor TCP/IP care să pornească automat” la pagina 116 furnizează mai multe informaţii despre controlarea serverelor TCP/IP care sunt lansate automat.

__ Pasul 2. Pentru a interzice ca cineva să asocieze o aplicaţie utilizator, cum ar fi o aplicaţie socket, cu portul pe care sistemul în mod normal îl utilizează pentru LPD, faceţi următoarele:

__ Pasul a. Introduceţi GO CFGTCP pentru a afişa meniul de configurare TCP/IP.

__ Pasul b. Selectaţi opţiunea 4 (Work with TCP/IP port restrictions - Gestiune restricţii port TCP/IP).

__ Pasul c. În ecranul Gestiune restricţii port TCP/IP (Work with TCP/IP Port Restrictions), specificaţi opţiunea 1 (Adăugare).

__ Pasul d. Pentru limita inferioară a intervalului portului, specificaţi 515.

__ Pasul e. Pentru limita superioară a intervalului portului, specificaţi *ONLY.

Note:

1) Restricţiile de port au efect la următoarea pornire TCP/IP. Dacă TCP/IP este activ atunci când setaţi restricţiile de port, trebuie să opriţi TCP/IP şi să îl porniţi din nou.
2) RFC1700 furnizează informaţii despre atribuirile obişnuite ale numerelor de porturi.

__ Pasul f. Pentru protocol, specificaţi *TCP.

__ Pasul g. Pentru câmpul profil utilizator, specificaţi un nume de profil utilizator care este protejat de sistem (Un profil de utilizator protejat de sistem este un profil care nu deţine programe care adoptă autorizare şi care nu are o parolă care este cunoscută de alţi utilizatori). Restricţionând portul pentru un anumit utilizator, automat îi excludeţi pe toţi ceilalţi utilizatori.

__ Pasul h. Repetaţi paşii 2c - 2g pentru protocolul *UDP.

Controlul accesului LPD

Dacă doriţi să permiteţi clienţilor LPD să acceseze sistemul dumneavoastră, luaţi cunoştinţă de următoarele subiecte:

- Pentru a împiedica un utilizator să vă umple sistemul cu obiecte nedorite, asiguraţi-vă că aţi setat limite prag adecvate pentru ppol-urile de memorie auxiliară (ASPs -Auxiliary Storage Pools). Puteţi afişa şi seta aceste limite prag pentru ASPs utilizând fie SST (System Service Tools), fie DST (Dedicated Service Tools - DST). Cartea *Backup and Recovery* vă oferă mai multe informaţii despre limitele prag ale ASP.
- Puteţi utiliza autorizarea pentru cozile de ieşire pentru a restricţiona posibilitatea de expediere a fişierelor spool către sistemul dumneavoastră. Utilizatorii LPD fără un ID utilizator folosesc profilul utilizator QTMPLPD. Puteţi da acestui profil de utilizator acces doar la câteva cozi de ieşire.

Consideraţii de securitate pentru SNMP

ServeruliSeries poate acţiona ca un agent protocol de gestiune a reţelei simplu (SNMP) într-o reţea. SNMP oferă un mijloc pentru administrarea gateway-urilor, router-elor şi gazdelor într-un mediu de reţea. Un agent SNMP adună informaţii despre sistem şi execută funcţii pe care le cer administratorii de reţea SNMP la distanţă.

Împiedicarea accesului SNMP

Dacă *nu* doriţi ca cineva să folosească SNMP pentru a accesa sistemul dumneavoastră, trebuie să împiedicaţi Serverul SNMP să ruleze. Faceţi următoarele:

__ Pasul 1. Pentru a împiedica joburile de server SNMP să pornească automat când porniţi TCP/IP, introduceţi următoarele:

```
CHGSNMPA AUTOSTART(*NO)
```

Note:

a. AUTOSTART(*YES) este valoarea implicită.
b. “Controlul serverelor TCP/IP care să pornească automat” la pagina 116 furnizează mai multe informaţii despre controlarea serverelor TCP/IP care sunt lansate automat.

__ Pasul 2. Pentru a interzice ca cineva să asocieze o aplicaţie utilizator, cum ar fi o aplicaţie socket, cu portul pe care sistemul în mod normal îl utilizează pentru SNMP, faceţi următoarele:

__ Pasul a. Introduceţi GO CFGTCP pentru a afişa meniul de configurare TCP/IP.

__ Pasul b. Selectaţi opţiunea 4 (Work with TCP/IP port restrictions - Gestiune restricţii port TCP/IP).

__ Pasul c. În ecranul Gestiune restricţii port TCP/IP (Work with TCP/IP Port Restrictions), specificaţi opţiunea 1 (Adăugare).

__ Pasul d. Pentru limita inferioară a intervalului portului, specificaţi 161.

__ Pasul e. Pentru limita superioară a intervalului portului, specificaţi *ONLY.

Note:

1) Restricţiile de port au efect la următoarea pornire TCP/IP. Dacă TCP/IP este activ atunci când setaţi restricţiile de port, trebuie să opriţi TCP/IP şi să îl porniţi din nou.
2) RFC1700 furnizează informaţii despre atribuirile obişnuite ale numerelor de porturi.

__ Pasul f. Pentru protocol, specificaţi *TCP.

__ Pasul g. Pentru câmpul profil utilizator, specificaţi un nume de profil utilizator care este protejat de sistem (Un profil de utilizator protejat de sistem este un profil care nu deţine programe care adoptă autorizare şi care nu are o parolă care este cunoscută de alţi utilizatori). Restricţionând portul pentru un anumit utilizator, automat îi excludeţi pe toţi ceilalţi utilizatori.

__ Pasul h. Repetaţi paşii 2c - 2g pentru protocolul *UDP.

Controlul accesului SNMP

Dacă doriţi să permiteţi administratorilor de SNMP să acceseze sistemul dumneavoastră, fiţi conştienţi de următoarele aspecte referitoare la securitate:

- O persoană care poate accesa reţeaua dumneavoastră cu SNMP poate aduna informaţii despre reţeaua dumneavoastră. Informaţiile pe care le-aţi ascuns utilizând alias-uri şi server nume domeniu (DNS) devin disponibile aşa-zisului intrus prin SNMP. În plus, un intrus ar putea folosi SNMP pentru a modifica configuraţia reţelei şi pentru a întrerupe comunicaţiile.
- SNMP se bazează pe un nume de comunitate pentru acces. Conceptual, numele de comunitate este similar cu o parolă. Numele de comunitate nu este criptat. De aceea este vulnerabil la interceptare. Folosiţi comanda Adăugare comunitate pentru SNMP (Add Community for SNMP, ADDCOMSNMP) pentru a seta parametrul adresă internet administrator (INTNETADR) la una sau mai multe adrese IP particulare în loc de *ANY. Puteţi seta şi parametrul OBJACC al comenzilor ADDCOMSNMP sau CHGCOMSNMP la *NONE pentru a împiedica accesul administratorilor dintr-o comunitate la obiectele MIB. Acest lucru se intenţionează să fie făcut temporar pentru a interzice accesul administratorilor dintr-o comunitate fără a înlătura comunitatea.

Consideraţii de securitate pentru serverul INETD

Spre deosebire de majoritatea serverelor TCP/IP, Serverul INETD nu furnizează un singur serviciu clienţilor. În schimb, el furnizează o varietate de servicii pe care administratorii le pot personaliza. Din acest motiv, Serverul INETD este denumit uneori ″super server″. Serverul INETD are următoarele servicii incorporate:

- time
- daytime
- echo

- discard
- changed

Aceste servicii sunt suportate atât pentru TCP, cât şi pentru UDP. Pentru UDP, serviciile echo, time, daytime şi changed primesc pachete UDP şi apoi trimit pachetele înapoi la expeditor. Serverul echo trimite înapoi pachetele primite, serverele time şi daytime generează ora într-un format specific şi o trimite înapoi, iar serverul changed generează un pachet de caractere ASCII care pot fi tipărite şi îl trimite înapoi.

Natura acestor servicii UDP face sistemul vulnerabil la un atac de interzicere serviciu. De exemplu, consideraţi că aveţi două serviceiSeries: SYSTEMA şi SYSTEMB. Un programator rău intenţionat ar putea prelua antetul IP şi UDP cu adresa sursă SYSTEMA şi un număr de port UDP al serverului time. El poate apoi să trimită pachetul la Serverul de oră de pe SYSTEMB, care va trimite ora la SYSTEMA, care, la rândul său, îi va răspunde lui SYSTEMB şi aşa mai departe, generând o buclă continuă şi consumând resursele CPU de pe ambele sisteme, cât şi lăţimea de bandă a reţelei.

De aceea, trebuie să luaţi în considerare riscul unui astfel de atac la iSeriessistem şi rulaţi aceste servicii doar într-o reţea sigură. Serverul INETD este configurat astfel încât să nu pornească singur când porniţi TCP/IP. Puteţi configura dacă să porniţi sau nu serviciile când porniţi INETD. Implicit, serverele time şi daytime TCP şi UDP sunt amândouă pornite când porniţi Serverul INETD.

Există două fişiere de configurare pentru Serverul INETD:

```
/QIBM/UserData/OS400/inetd/inetd.conf
/QIBM/ProdData/OS400/inetd/inetd.conf
```

Aceste fişiere determină ce programe să pornească odată cu INETD. Ele decid de asemenea profilul de utilizator sub care aceste programe rulează atunci când INETD le porneşte.

Notă: Fişierul de configuraţie din proddata ar trebui să nu fie niciodată modificat. El este înlocuit de fiecare dată când sistemul este reîncărcat. Modificările de configurare personalizate ar trebui plasate numai în fişierul din structura de directoare userdata, întrucât acel fişier **nu** este actualizat în timpul actualizărilor de ediţie.

Dacă un programator rău intenţionat obţine accesul la aceste fişiere, le-ar putea configura să pornească orice program la pornirea INETD. De aceea este foarte important să protejaţi aceste fişiere. Implicit ele au nevoie de autorizare QSECOFR pentru a face modificări. Ar trebui să nu limitaţi autorizarea necesară pentru a le accesa.

Notă: Nu modificaţi fişierul de configurare din directorul ProdData. Acel fişier este înlocuit la fiecare reînărcare a sistemului. Modificările de configurare personalizate ar trebui plasate numai în fişierul din structura de directoare UserData, deoarece acel fişier nu este actualizat în timpul actualizărilor de ediţie.

Consideraţii de securitate pentru limitarea roaming-ului TCP/IP

Dacă sistemul este conectat la o reţea, poate doriţi să limitaţi capacităţile utilizatorilor de a naviga prin reţea cu ajutorul aplicaţiilor TCP/IP. Un mod de a face acest lucru este restricţionarea accesului la următoarele comenzi client TCP/IP:

Notă: Aceste comenzi ar putea exista în mai multe biblioteci de pe sistemul dumneavoastră. Ele se găsesc cel puţin în bibliotecile QSYS şi QTCP. Asiguraţi-vă că aţi localizat şi securizat toate apariţiile acestora.
- STRTCPFTP
- FTP

- STRTCPTELN
- TELNET
- LPR
- SNDTCPSPLF
- RUNRMTCMD (REXEC client)

Destinaţiile posibile ale utilizatorilor sunt determinate de următoarele:

- Intrări în tabela dumneavoastră de gazde TCP/IP.
- Intrarea *DFTROUTE din tabela de rute TCP/IP. Acest lucru permite utilizatorilor să introducă adresa de IP a sistemului din nodul următor când destinaţia lor este o reţea necunoscută. Un utilizator poate atinge sau contacta o reţea de la distanţă utilizând ruta implicită.
- Configurare nume server la distanţă. Acest suport permite altui server din reţea să localizeze numele gazdelor pentru utilizatorii dumneavoastră.
- Tabelă sistem de la distanţă.

Trebuie să controlaţi cine poate adăuga intrări în aceste tabele şi cine poate modifica configuraţia dumneavoastră. De asemenea, trebuie să înţelegeţi implicaţiile intrărilor din tabela dumneavoastră şi ale configuraţiei dumneavoastră.

Fiţi conştient că un utilizator cu cunoştinţe în domeniu, cu acces la un compilator ILE C, poate crea un program socket care se poate ataşa la un port TCP sau UDP. Puteţi face acest lucru mai complicat restricţionând accesul la următoarele fişiere de interfaţă socket din biblioteca QSYSINC:

- SYS
- NETINET
- H
- ARPA
- socket-uri şi SSL

Pentru programele service, puteţi împiedica utilizarea aplicaţiilor SSL şi socket care sunt deja compilate prin restricţionarea folosirii acestor programe service:

- QSOSRV1
- QSOSRV2
- QSOSKIT(SSL)
- QSOSSLSR(SSL)

Programele de service sunt furnizate cu autorizarea publică *USE, dar autorizarea poate fi schimbată pe *EXCLUDE (sau altă valoare, după cum este novoie).

Capitolul 14. Securizarea accesului la staţia de lucru

Mulţi din utilizatorii sistemului dumneavoastră au calculatoare personale (PC-uri) pe birourile lor ca staţii de lucru. Ei folosesc unelte care rulează pe PC şi folosesc PC-ul pentru a se conecta la serverul iSeries.

Cele mai multe metode de conectarea a unui PC la serverele iSeries furnizează mai multe funcţii decât emularea staţiei de lucru. PC-ul poate arăta ca un monitor pentru iSeries şi furnizează utilizatorului sesiuni interactive pentru semnare. În plus, PC-ul ar putea arăta serverelor iSeries ca un alt calculator şi furniza funcţii cum ar fi transferul de fişiere şi apelul de proceduri la distanţă.

Ca administrator de securitate pe serverul iSeries, trebuie să fiţi atenţi la următoarele:

- Funcţiile care sunt disponibile utilizatorilor de PC care sunt conectaţi la sistemul dumneavoastră
- Resursele server iSeries pe care utilizatorii de PC le pot accesa.

Veţi putea dori să împiedicaţi funcţii PC avansate (cum ar fi transferul de fişiere şi apelul procedurilor la distanţă) dacă schema de securitate a serverului dumneavoastră iSeries nu este încă pregătită pentru aceste funcţii. Probabil, scopul dumneavoastră principal este să permiteţi funcţii avansate pentru PC atâta timp cât protejaţi încă informaţiile pe sistemul dumneavoastră. Subiectele următoare se referă la anumite probleme de securitate ce sunt asociate cu accesul PC-urilor.

Împiedicarea viruşilor staţiilor de lucru

Aceste informaţii sugerează modalităţi prin care administratorii de securitate se pot apăra împotriva viruşilor PC.

Securizarea accesului la date al staţiei de lucru

Unii clienţi PC folosesc directoare partajate pentru stocarea informaţiilor pe server. Pentru a accesa fişierele baze de date de pe iSeries, utilizatorul de PC are un limitat, bine definit set de interfeţe. Cu posibilitatea de transfer de fişiere care face parte din cele mai multe produse software client/server, utilizatorul PC poate copia fişiere între server şi PC. Cu capacitatea de acces la baza de date, cum ar fi un fişier DDM, SQL la distanţă, sau un driver ODBC, utilizatorul PC poate accesa datele de pe server.

În acest mediu, puteţi crea programe care să intercepteze şi să evalueze cererile utilizatorilor PC penru accesarea resurselor server. Când cererile folosesc un fişier DDM, specificaţi programul de ieşire în atributul de reţea DDMACC (DDMACC - Distributed Data Management Access). Pentru anumite metode de transfer de fişiere ale PC-ului, specificaţi programul de ieşire în atributul de reţea Acces cerere client (PCSACC). Sau puteţi specifica PCSACC(*REGFAC) pentru a folosi funcţia de înregistrare. Când cererile folosesc alte funcţii de server pentru a accesa datele, puteţi utiliza comanda WRKREGINF pentru a înregistra programele de ieşire pentru aceste funcţii server.

Programele de ieşire, totuşi, pot fi dificil de descris şi adesea eşuează. Programele de ieşire nu sunt un înlocuitor pentru autorizările obiectelor, care sunt create pentru a proteja obiectele dumneavoastră de la accesul neautorizat de la orice sursă.

Unele produse software client, cum ar fiIBM iSeries Access pentru Windows, folosesc Sistem de fişiere integrat pentru stocarea şi accesarea datelor de pe serverele iSeries. Folosind Sistem de fişiere integrat, întreg serverul devine mult mai uşor disponibil utilizatorilor de PC-uri. Autorizarea obiectelor devine mult mai importantă. Prin Sistem de fişiere integrat, un utilizator cu autorizare suficientă poate vizualiza o bibliotecă server ca şi cum aceasta este un director PC. Comenzile simple de mutare şi copiere pot muta instantaneu datele de pe o bibliotecă server iSeries pe un director PC şi invers. Sistemul face automat modificările corespunzătoare ale formatului de date.

Note:

1. Puteţi folosi o listă de autorizări pentru a controla utilizarea obiectelor în sistemul de fişiere QSYS.LIB. Consultaţi “Restricţionarea accesului la sistemul de fişiere QSYS.LIB” la pagina 95 pentru mai multe informaţii.
2. Capitolul 11, “Folosirea Sistemului de fişiere integrat pentru securizarea fişierelor”, la pagina 89 furnizează mai multe informaţii despre probleme de securitate cu Sistem de fişiere integrat.

Puterea Sistem de fişiere integrat este simplitatea sa pentru utilizatori şi dezvoltatori. Cu o interfaţă unică, utilizatorul poate lucra cu obiecte în mai multe medii. Utilizatorul de PC nu are nevoie de software special sau API pentru a accesa obiectele. În schimb, utilizatorul de PC poate folosi comenzi comune PC-ului sau poate “puncta” şi lucra cu obiectele direct.

Pentru toate sistemele care au ataşate PC-uri, dar în mod special sistemele care au software client ce utilizează Sistem de fişiere integrat, o schemă bună de autorizare a obiectelor este critică. Deoarece securitatea este integrată în produsul OS/400, orice cerere de accesare a datelor trebuie să treacă prin procesul de verificare a autorizării. Verificarea autorizării se aplică cererilor de la orice sursă şi accesului datelor prin orice metodă.

Autorizare obiect la accesul staţiei de lucru

Când setaţi autorizarea obiectelor, trebuie să evaluaţi ce furnizează acea autorizare utilizatorilor de PC. De exemplu, când un utilizator are autorizare *USE pentru un fişier, el poate vizualiza sau tipări datele din acest fişier. Utilizatorul nu poate modifica informaţiile din fişier sau să-l şteargă. Pentru utilizatorul de PC, vizualizarea este echivalentă cu “citirea”, ceea ce furnizează suficientă autorizare pentru utilizator pentru a face o copie a fişierului pe PC. Aceasta poate să nu fie ceea ce intenţionaţi.

Pentru anumite fişiere critice, puteţi dori să setaţi autorizarea publică cu *EXCLUDE pentru a împiedica transferul (downloading). Puteţi apoi furniza o altă metodă pentru a “vizualiza” fişierul pe server, cum ar fi folosirea unui meniu şi a unor programe care folosesc autorizare.

O altă opţiune pentru împiedicarea descărcării de fişiere este să se folosească un program de ieşire care rulează ori de câte ori un utilizator PC porneşte o funcţie server (alta decât semnarea interactivă). Puteţi specifica un program de ieşire în atributul de reţea PCSACC utilizând comanda Modificare atribut reţea (Change Network Attribute - CHGNETA). Sau puteţi înregistra programele de ieşire folosind comanda Gestiune informaţii înregistrare (Work with Registration Information - WRKREGINF). Comanda pe care o utilizaţi depinde de cum PC-urile accesează datele de pe sistem şi de ce program client este folosit de PC-uri. Programul de ieşire (QIBM_QPWFS_FILE_SERV) se aplică la accesul iSeries Access şi NetServer la IFS (sistemul de fişiere integrat). Nu este împiedicat accesul de la un PC cu alte mecanisme, cum ar fi FTP sau ODBC.

Software-ul PC furnizează de asemenea capacitate de încărcare, astfel încât un utilizator poate copia date de pe PC într-un fişier bază de date de pe server. Dacă nu aţi setat schema dumneavoastră de autorizare corect, un utilizator de PC poate suprascrie toate datele dintr-un

fişier cu datele de pe PC. Trebuie să atribuiţi autorizarea *CHANGE cu atenţie. Revedeţi Anexa D a cărţii *Referinţă securitate iSeries* pentru a înţelege ce autorizare este cerută pentru operaţii cu fişiere.

Centru de informare iSeries furniează mai multe informaţii privind autorizarea pentru funcţiile calculatoarelor şi despre folosirea programelor de ieşire. Vezi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru detalii.

Administrarea aplicaţiei

Administrarea aplicaţiei este o componentă care poate fi instalată opţional a interfeţei grafice cu utilizatorul (GUI) Navigator iSeries, pentru serverul iSeries. Administrarea aplicaţiei permite administratorilor de sistem să controleze funcţiile sau aplicaţiile disponibile utilizatorilor şi grupurilor pe un anumit server. Aceasta include controlul funcţiilor disponibile utilizatorilor care accesează serverul lor prin clienţi. Este important de notat aici, că dacă accesaţi serverul de pe un client Windows, utilizatorul serverului iSeries şi nu utilizatorul Windows determină care funcţii sunt disponibile pentru administrare.

Pentro o documentaţie completă în legătură cu Administrarea aplicaţiilor din Navigator iSeries, vedeţi Centru informaţii iSeries –>Conectarea la iSeries—>Ce se conectează cu —>Navigator iSeries (../html/as400/v5r2/ic2924/info/rzaj3/rzaj3overview.htm).

Administrarea politicilor

Politicile sunt un instrument folosit de administratori în configurarea programelor aflate pe PC-urile lor client. Politicile pot restricţiona funcţiile şi aplicaţiile la care are acces un utilizator de pe PC. Politicile pot de asemenea sugera sau impune configuraţiile spre a fi folosite de către anumiţi utilizatori sau anumite PC-uri.

Notă: Politicile nu oferă control peste resursele server. Politicile nu sunt un substituient pentru securitatea serverului. Politicile pot fi folosite pentru a afecta modul în care iSeries Access este capabil să acceseze serverul de pe un anumit PC, de către un anumit utilizator. Totuşi, nu modifică modul în care resursele server pot fi accesate folosind alte mecanisme.

Politicile sunt stocate pe un server de fişiere. De fiecare dată când utilizatorul se loghează la staţia de lucru Windows, politicile care se aplică la acel utilizator Windows sunt descărcate de serverul de fişiere. Politicile sunt aplicate regiştrilor înainte ca utilizatorul să realizeze ceva pe staţia de lucru.

Politicile **Microsoft şi administrarea aplicaţiei**

iSeries Access Express suportă două strategii diferite pentru implementarea controlului administrativ într-o reţea: politicile de sistem Microsoft şi Administrarea aplicaţiilor din Navigator iSeries. Luaţi următoarele în considerare atunci când decideţi ce strategie se potriveşte cel mai bine pentru nevoile dumneavoastră.

Microsoft politicile sistemului

Politicile sunt conducătoarele calculatoarelor, nedepinzând de specificeOS/400 eliberări. Politicile se pot aplica la fel de bine atât calculatoarelor Windows cât şi utilizatorilor. Aceasta înseamnă că utilizatorii fac referire la profilul utilizator Windows, nu la profilul utilizator al serverului. Politicile pot fi folosite pentru a ″configura″, cât şi pentru a limita. Politicile oferă de obicei granularitate mai mare faţă de Administraţie aplicaţii şi pot oferi o gamă mai largă de funcţii. Aceasta deoarece o conexiune la server nu este necesară pentru a determina dacă utilizatorul poate folosi funcţia sau nu. Implementarea politicilor este mai complicată decât

implementarea Administrării aplicaţiilor datorită necităţii folosirii editorului de politici sistem Microsoft, iar calculatoarele trebuie configurate individual pentru descărcarea politicilor de la server.

Administrarea aplicaţiei din Navigator **iSeries**

Administrarea aplicaţiei asociază date cu profilul utilizator, în locul profiluluiWindows cu care face asociereea sistemul de politici Microsoft. În timp ce servereleiSeries pe care rulează V4E3 sau mai nouă a produsuluiOS/400 sunt necesare pentru a folosi Administrarea aplicaţiei, unele funcţii sunt disponibile doar începând cu V4E4. Administrarea aplicaţiei foloseşte interfaţa grafică cu utilizatorul din Navigator iSeries pentru administrare, care este mult mai uşor de folosit decât editorul de politici. Informaţiile referitoare la Administraţie aplicaţii se aplică utilizatorului indiferent de PC-ul de pe care se conectează. Anumite funcţii din Navigator iSeries pot fi restricţionate. Administrarea aplicaţiilor este preferabilă dacă toate funcţiile pe care doriţi să le restricţionaţi sunt disponibile Administrării aplicaţiilor şi dacă versiunea OS/400 folosită suportă Administrarea aplicaţiilor.

Folosirea SSL cu iSeries Access pentru Windows

Pentru informaţii despre folosirea iSeries Access Express cu SSL, treceţi în revistă subiectele din Centru de informare iSeries *Administrare SSL (Secure Sockets Layer), Securizarea iSeries Access Express şi Navigator iSeries, iSeries Developer Kit pentru Java şi Trusa de unelte iSeries pentru Java* sub subiectul principal Java. Puteţi de asemenea revedea aceste informaţii pe CD-ul furnizat odată cu sistemul dumneavoastră.

Securitate Navigator iSeries

Navigator iSeries oferă o interfaţă uşor de folositla server pentru utilizatori care au iSeries Access. Cu fiecare nouă ediţia a produsului OS/400, mai multe funcţii server devin disponibile prin Navigator iSeries. O interfaţă uşor de folosit furnizează mai multe beneficii, incluzând costuri reduse pentru suport tehnic şi o imagine mai bună pentru sistemul dumneavastră . Prezintă, de asemenea, provocări de securitate.

Ca administrator de securitate, puteţi să nu vă mai bazaţi pe ignoranţa utilizatorilor dumneavoastră pentru a proteja resursele. Navigator iSeries face multe funcţii disponibile şi vizibile pentru utilizatorii dumneavoastră. Trebuie să vă asiguraţi că aţi desemnat şi implementat politica de securitate pentru profilurile utilizator şi securitatea obiectelor pentru a avea necesarul dumneavoastră de securitate.

V4E4 sau versiunile mai noi de IBM e(logo)server iSeries Access pentru Windows furnizează următoarele metode pentru controlul funcţiilor pe care utilizatorii le pot realiza prin Navigator iSeries:

- Instalare selectivă
- Administrarea aplicaţiei
- Suportul de politici pentru sistemulWindows NT

Navigator iSeries împachetat în mai multe componente pe care le puteţi instala separat. Aceasta vă permite să instalaţi doar funcţiile de care aveţi nevoie. Administrarea aplicaţiilor permite unui administrator să controleze funcţiile pe care un utilizator sau un grup le poate accesa prin Navigator iSeries. Administrare aplicaţii organizează aplicaţiile în următoarele categorii:

Navigator iSeries
: Include Navigator iSeries şi orice plug-in-uri.

Aplicaţii client
: Include toate celelalte aplicaţii client, inclusiv iSeries Access, care oferă funcţii pe client care sunt administrate de Administrare aplicaţii.

Aplicaţii gazdă

Include toate aplicaţiile care se află în întregime pe serverul dumneavoastră şi furnizează funcţii care sunt administrate prin Administrarea aplicaţiei.

Puteţi folosi instalarea selectivă, administrarea aplicaţiei şi politici pentru a limita funcţiile Navigator iSeries pe care le poate accesa un utilizator. Totuşi, nici una dintre acestea nu trebuie folosită pentru securitatea resurselor.

Începând cu V4R4, IBM e(logo)server iSeries Access pentru Windows suportă de asemenea Windows NT Editorul Politicilor Sistem pentru a controla care funcţii pot fi rulate de un calculator client particular, neţinând cont de utilizatorul acelui calculator.

Vezi Centru de informare iSeries pentru informaţii suplimentare privind instalarea selectivă, Administrarea Aplicaţiilor şi Administrarea Politicilor. “Funcţia de limitare a acesului la program” la pagina 5 secţiunea acestei cărţi conţine de asemenea unele discuţii despre administrarea aplicaţiilor.

Împiedicarea accesului ODBC

Open database connectivity (ODBC) este un instrument pe care aplicaţiile PC îl pot utiliza ca să acceseze datele iSeries ca şi cum ar fi date PC. Programatorul ODBC poate face transparente locaţiile fizice de date pentru utilizatorul aplicaţiilor de PC. Pentru informaţii suplimentare cu privire la consideraţii de securitate ODBC, mergeţi la informaţiile ″Securitate ODBCiSeries Access pentru Windows″ (/rzaii/rzaiiodbc09.HTM), localizate în Centrul de informare iSeries.

Consideraţii de securitate pentru parolele sesiunilor staţie de lucru

În mod normal, când un utilizator PC porneşte software-ul de conectare, cum ar fi iSeries Access, utilizatorul introduce ID-ul utilizator şi parola pentru server o singură dată. Parola este criptată şi stocată în memoria PC. Ori de câte ori utilizatorul deschide o nouă sesiune pe acelaşi server, PC-ul trimite automat ID-ul utilizator şi parola.

Unele produse software client/server furnizează, de asemenea, opţiunea de a trece de ecranul de semnare pentru sesiunile interactive. Software-ul va trimite ID-ul utilizator şi parola criptată când utilizatorul porneşte o sesiune interactivă (emulare 5250). Pentru a suporta această opţiune, valoarea sistem QRMTSIGN de pe server trebuie setată la *VERIFY.

Când alegeţi să se ocolească ecranul de semnare, aveţi în vedere compromisurile de securitate.

Probleme de securitate: Pentru emularea 5250 sau orice alt tip de sesiune interactivă, ecranul Semnare este la fel ca oricare alt ecran. Deoarece parola nu este afişată pe ecran când este introdusă, parola este trimisă de-a lungul legăturii în forma necriptată, ca orice alt câmp de dată. Pentru anumite tipuri de legături, aceasta poate furniza oportunitatea pentru un posibil intrus să monitorizeze legătura şi să detecteze un ID utilizator şi o parolă. Monitorizarea unei legături folosind echipament electronic este deseori referită ca **interceptare**. Începând cu V4R4, puteţi folosi SSL pentru a cripta comunicaţia între iSeries Access şi serverul iSeries. Aceasta vă protejează datele, ca şi parolele incluse, de a fi interceptate (sniffing).

Când alegeţi să ocoliţi ecranul de semnare, PC-ul criptează parola înainte de a fi trimisă. Criptarea nu dă posibilitatea ca parola să fie detectată prin interceptare. Totuşi, trebuie să vă asiguraţi că utilizatorii dumneavoastră de PC practică securitatea operaţională. Un PC neasigurat, cu o sesiune activă la sistemul iSeries, oferă oportunitatea cuiva să pornească altă sesiune fără să ştie ID-ul utilizator şi parola. PC-urile trebuie să fie setate să se blocheze când sistemul este inactiv pentru o perioadă lungă de timp şi trebuie să ceară o parolă pentru a continua sesiunea.

Chiar dacă nu alegeţi să ocoliţi ecranul de semnare, un PC neasigurat, cu o sesiune activă, reprezintă o problemă de securitate. Folosind software de PC, cineva poate porni o sesiune server şi accesa datele, din nou fără să cunoască un ID utilizator şi o parolă. Problema de securitate datorată emulării 5250 este într-un fel mai gravă, deoarece necesită mai puţine cunoştinţe pentru a porni o sesiune şi a accesa datele.

Trebuie să-i învăţaţi pe utilizatori despre efectele deconectării din sesiunile lor iSeries Access. Mulţi utilizatori consideră (logic dar incorect) că opţiunea de deconectare opreşte complet conexiunea lor cu serverul. De fapt, când un utilizator selectează opţiunea de deconectare, serverul face sesiunea (licenţa) utilizatorului disponibilă pentru alt utilizator. Totuşi, conexiunea clientului cu serverul este încă deschisă. Alt utilizator ar putea trece la PC-ul neprotejat şi ar obţine accesul la resursele serverului fără să introducă un ID utilizator şi o parolă.

Puteţi sugera două opţiuni utilizatorilor dumneavoastră pentru a deconecta sesiunile lor:

- Asiguraţi-vă că PC-urile lor au o funcţie de verificare care cere o parolă. Aceasta face un PC neasigurat indisponibil pentru oricine nu cunoaşte parola.
- Pentru a deconecta complet o sesiune, trebuie ori să vă relogaţi Windows ori să restartaţi calculatorul. Aceasta termină sesiunea la iSeries.

Va trebui să relataţi de asemenea utilizatorilor dumneavoastră despre posibilele probleme de securitate când folosesciSeries Access pentru Windows. Când un utilizator specifică UNC (convenţia de numire universală) pentru a identifica o resursă iSeries, clientul Win95 sau NT construieşte o conexiune reţea pentru a se lega la server. Deoarece utilizatorul specifică un UNC, nu-l vede ca un drive de reţea mapat. De multe ori, utilizatorul nici măcar nu ştie de existenţa conexiunii de reţea. Totuşi, această conexiune la reţea reprezintă o expunere de securitate la un calculator care nu este prezent deoarece serverul apare în arborele de directoare al PC-ului. Dacă sesiunea utilizatorului are un profil utilizator puternic, resursele server pot fi expuse pe un PC care nu este prezent. Ca şi în exemplul anterior, remediul este să vă asiguraţi că utilizatorii înţeleg problema şi că folosesc funcţia de verificare pe PC-ul lor.

Protejarea serverului de proceduri şi comenzi la distanţă

Un utilizator cu cunoştinţe PC şi cu un software cum esteiSeries Access poate rula comenzi pe server fără a trece prin ecranul de semnare. În continuare sunt mai multe metode care sunt disponibile pentru utilizatorii PC pentru a rula comenzi server. Software-ul client/server determină metodele pe care utilizatorii dumneavoastră de PC le au disponibile.

- Un utilizator poate deschide un fişier DDM şi utiliza funcţia de comandă de la distanţă pentru a rula o comandă.
- Unele produse software, cum ar fi clienţii optimizaţiiSeries Access, furnizează funcţia de comandă la distanţă prin API-urile DPC (Distributed Program Call), fără a utiliza DDM.
- Anumite produse software, cum ar fi ODBC şi SQL de la distanţă, furnizează o funcţie de comandă de la distanţă fără DDM sau DPC.

Pentru software-ul client/server ce utilizează DDM pentru suport comenzi de la distanţă, puteţi folosi atributul de reţea DDMACC pentru a împiedica lansarea comenzilor de la distanţă complet. Pentru software-ul client/server ce utilizează alt suport server, puteţi înregistra programe de ieşire pentru server. Dacă doriţi să permiteţi comenzi la distanţă, trebuie să vă asiguraţi că schema de autorizare a obiectelor vă protejează datele adecvat. Posibilitatea comenzilor la distanţă este echivalentă cu a da utilizatorului o linie de comandă. În plus, când iSeries primeşte o comandă de la distanţă prin DDM, sistemul nu impune setarea Capabilităţi limitate (Limited capability - LMTCPB) din profilul utilizatorului.

Protejarea staţiilor de lucru de procedurile şi comenzile de la distanţă

IBM iSeries Access pentru Windows furnizează capacitatea de a primi comenzi la distanţă pe PC. Puteţi folosi comanda RUNRMTCMD (Run Remote Command - Rulare comandă la distanţă) pe server pentru a rula o procedură pe un PC ataşat. Posibilitatea RUNRMTCMD este un instrument valoros pentru administratorii de sistem şi personalul biroului de asistenţă (help-desk). Totuşi, oferă şi oportunitatea de a distruge datele de pe PC, fie deliberat, fie accidental.

PC-urile nu au aceleaşi funcţii de autorizare obiect ca serverele iSeries. Cea mai bună protecţie împotriva problemelor comenzii RUNRMTCMD este să restricţionaţi cu atenţie utilizatorii sistem care au acces la comandă. IBM iSeries Access pentru Windows furnizează posibilitatea de a înregistra utilizatorii care rulează comenzi la distanţă pe un anumit PC. Când conectarea se face prin TCP/IP, puteţi utiliza panoul de control proprietăţi de pe client pentru a controla accesul comenzilor la distanţă. Puteţi autoriza utilizatorii prin ID utilizator sau prin nume sistem la distanţă. Când conectarea este prin SNA, anumite produse software oferă posibilitatea de a seta securitatea conversaţiei. Cu alte produse software client, alegeţi dacă să setaţi sau nu capabilităţile comenzilor care sosesc.

Pentru fiecare combinaţie software client - tip de conectare (cum ar fi TCP/IP sau SNA), trebuie să revedeţi potenţialul comenzilor care sosesc pentru a ataşa PC-urile. Consultaţi documentaţia client căutând “comandă care soseşte” sau “RUNRMTCMD”. Pregătiţi-vă să vă sfătuiţi utilizatorii de PC şi administratorii de reţea despre modul corect (sigur) de a configura clienţii pentru a permite sau nu această posibilitate.

Servere gateway

Sistemul dumneavoastră poate fi într-o reţea cu un server intermediar sau gateway între sistemul iSeries şi PC-uri. De exemplu, sistemul dumneavoastră iSeries poate fi ataşat la un LAN cu un server PC care are PC-uri ce sunt ataşate la server. Problemele de securitate, în această situaţie, depind de software-ul care rulează pe Serverul gateway. Figura 13 prezintă un exemplu de configurare server gateway:

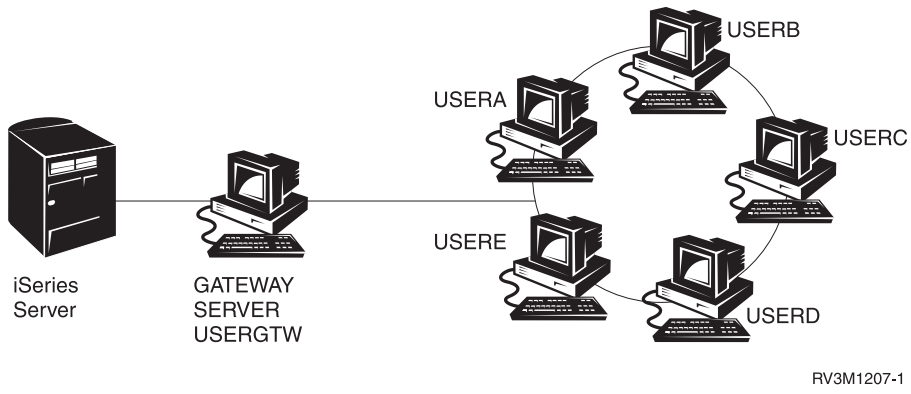

Figura 13. Sistem iSeries cu un server gateway

Cu anumite produse software, sistemul dumneavoastră iSeries nu va şti despre nici un utilizator (cum ar fi USERA sau USERC) care sunt după Serverul gateway. Serverul se va înregistra la sistem ca un singur utilizator (USERGTW). Va folosi ID utilizator USERGTW pentru a rezolva toate cererile utilizatorilor de pe flux. O cerere din partea USERA va apărea serverului ca o cerere din partea utilizatorului USERGTW.

Dacă acesta este cazul, trebuie să vă bazaţi pe Serverul gateway pentru impunerea securităţii. Trebuie să înţelegeţi şi să gestionaţi posibilităţile de securitate ale serverului gateway. Dintr-o

perspectivă a serverului iSeries, fiecare utilizator are aceeaşi autorizare ca şi ID-ul utilizator pe care serverul gateway îl foloseşte să pornească sesiunea. Vă puteţi gândi la aceasta ca la un echivalent pentru rularea unui program care adoptă autorizare şi furnizează o linie de comandă.

Cu alt software, serverul gateway face cereri din partea utilizatorilor individuali la serverele iSeries. Serverul iSeries ştie că USERA cere accesul la un anumit obiect. Gateway-ul este aproape transparent sistemului.

Dacă sistemul dumneavoastră este într-o reţea care are servere gateway, trebuie să evaluaţi câtă autorizare să furnizaţi ID-urilor utilizator care sunt folosite de Serverul gateway. Trebuie, de asemenea, să înţelegeţi următoarele:
- Mecanismele de securitate pe care le impune Serverul gateway.
- Cum apar utilizatorii în aval în iSeries sistemul dumneavoastră.

Comunicaţii LAN fără fir

Unii clienţi ar putea folosi iSeries Wireless LAN pentru a comunica cu sistemul dumneavoastră fără fire. iSeries Wireless LAN foloseşte tehnologia de comunicare prin frecvenţe radio. Ca administrator de securitate, trebuie să vă feriţi de următoarele caracteristici de securitate ale iSeries produselor LAN Wireless:

- Aceste produse LAN fără cablu folosesc tehnologie de spectru larg. Aceeaşi tehnologie a fost utilizată de guvern în trecut pentru a securiza transmisiile radio. Pentru cineva care încearcă să monitorizeze electronic transmisiile de date, transmisia pare să fie mai mult zgomot decât o transmisie actuală.
- Conexiunea fără cablu are trei parametri de configurare relevanţi pentru securitate:
  - Rata datelor (două rate de date posibile)
  - Frecvenţa (cinci frecvenţe posibile)
  - Identificatorul de sistem (8 milioane de identificatori posibili)

  Aceste elemente de configurare se combină pentru a furniza 80 milioane de configuraţii posibile, care face extrem de mică probabilitatea ca hacker-ul să ghicească configurarea corectă.
- Ca şi cu alte metode de comunicare, securitatea comunicaţiilor fără fir este influenţată de securitatea dispozitivului clientului. Informaţiile de identificare a sistemului şi alţi parametri de configurare sunt într-un fişier de la dispozitivul clientului şi trebuie să fie protejate.
- Dacă un dispozitiv wireless este pierdut sau furat, măsurile normale de securitate, cum ar fi parolele de semnare şi securitatea obiectelor, furnizează protecţie când un utilizator neautorizat încearcă să folosească unitatea pierdută sau furată pentru a accesa sistemul dumneavoastră.
- Dacă o unitate client fără cablu este pierdută sau furată, trebuie să schimbaţi informaţiile de identificare a sistemului pentru toţi utilizatorii, punctele de acces şi sisteme. Gândiţi-vă la aceasta ca la o schimbare a yalelor unei uşi ale cărui set de chei a fost furat.
- Poate doriţi să partajaţi Serverul în grupe de clienţi care au ID-uri de sistem unice. Aceasta limitează impactul dacă o unitate este pierdută sau furată. Această metodă funcţionează doar dacă puteţi limita un grup de utilizatori la o anumită parte a instalării dumneavoastră.
- Spre deosebire de tehnologia LAN cablat, tehnologia LAN necablat este brevetată. Prin urmare, nici un ascultător electronic nu este disponibil pentru aceste produse LAN wireless. Un ascultător este un dispozitiv electronic care realizează monitorizarea neautorizată a transmisiei.

Capitolul 15. Programe de ieşire de securitate

Unele funcţii server iSeries furnizează o ieşire astfel încât sistemul dumneavoastră să poată rula un program creat de utilizator pentru a realiza verificări suplimentare şi validări. De exemplu, puteţi seta sistemul dumneavoastră pentru a rula un program de ieşire de fiecare dată când cineva încearcă să deschidă un fişier DDM (distributed data management) pe sistemul dumneavoastră. Puteţi utiliza funcţiile de înregistrare pentru a specifica programele de ieşire care rulează în anumite condiţii.

Anumite publicaţii iSeries conţin exemple de programe de ieşire care realizează funcţii de securitate. Tabela 24 furnizează o listă a acestor programe de ieşire şi sursele programelor exemplificate.

Tabela 24. Surse pentru exemple de programe de ieşire

Tipul programului de ieşire	**Scop**	**Unde se găsesc exemple**
Validare parolă	Valoarea sistem QPWDVLDPGM poate specifica un nume program sau indica că programele de validare înregistrate pentru punctul de ieşire QIBM_QSY_VLD_PASSWRD să fie folosite pentru verificarea unei noi parole pentru cerinţe adiţionale care nu sunt folosite de valorile de sistem QPWDxxx. Utilizarea acestui program trebuie monitorizată cu atenţie deoarece primeşte parole necriptate. Acest program **nu trebuie** să stocheze parolele într-un fişier sau să le plaseze altui program.	• *Un Ghid de implementare pentru Securitate şi auditare iSeries, GG24–4200* • *Referinţă securitate iSeries*, SC41-5302-07
PC Support/400 sau Client Access acces[1]	Puteţi specifica acest nume de program în parametrul Acces cerere client - Client request access (PCSACC) al atributului de reţea pentru a controla următoarele funcţii: • Funcţii imprimantă virtuală • Funcţii transfer fişiere • Funcţii directoare partajate tip 2 • Funcţii mesaje acces clienţi • Cozi de date • Funcţii SQL la distanţă	*Un Ghid de implementare pentru Securitate şi auditareiSeries, GG24–4200*
Acces DDM (Distributed Data Management)	Puteţi specifica acest nume de program în parametrul acces cerere DDM (DDMACC) al atributului de reţea pentru a controla următoarele funcţii: • Funcţii directoare partajate tip 0 şi 1 • Funcţii lansare comenzi la distanţă	*Un Ghid de implementare pentru Securitate şi auditareiSeries, GG24–4200*
Conectare la distanţă	Puteţi specifica un program în variabila de sistem QRMTSIGN pentru a controla ce utilizatori se pot conecta automat şi de la ce locaţie (pass-through).	*Un Ghid de implementare pentru Securitate şi auditareiSeries, GG24–4200*

Tabela 24. Surse pentru exemple de programe de ieşire (continuare)

Tipul programului de ieşire	Scop	Unde se găsesc exemple
ODBC (Open Database Connectivity - Conectarea bazelor de date deschise) cu iSeries Access[1]	Controlaţi următoarele funcţii ale ODBC: • Dacă ODBC este permis. • Ce funcţii sunt permise pentru fişiere baze de date iSeries. • Ce instrucţiuni SQL sunt permise. • Ce informaţii se pot recupera despre obiectele server baze de date. • Ce funcţii de catalog SQL sunt permise.	Nu este nici una disponibilă.
Program tratare întrerupere QSYSMSG	Puteţi crea un program pentru a monitoriza coada de mesaje QSYSMSG şi a lua măsurile potrivite (cum ar fi anunţarea administratorului de securitate) în funcţie de tipul mesajului.	*Un Ghid de implementare pentru Securitate şi auditareiSeries, GG24–4200*
TCP/IP	Anumite servere TCP/IP (cum ar fi FTP, TFTP, TELNET şi REXEC) furnizează puncte de ieşire. Puteţi adăuga programe de ieşire pentru a manevra conectarea şi pentru a valida cererile utilizatori, cum ar fi cererile de a lua sau pune un anumit fişier. Puteţi, de asemenea, utiliza aceste ieşiri pentru a furniza FTP anonymous pe sistemul dumneavoastră.	"TCP/IP User Exits în carteai*Series System API Reference*"
Modificări profil utilizator	Puteţi crea programe de ieşire pentru următoarele comenzi profil utilizator: CHGUSRPRF CRTUSRPRF DLTUSRPRF RSTUSRPRF	• *Referinţă securitate iSeries*, SC41-5302-07 • "TCP/IP User Exits în carteai*Series System API Reference*"

Note:

1. Informaţii adiţionale despre acest subiect pot fi găsite în iSeries Centrul de Informare. Vezi "Condiţii prealabile şi informaţii conexe" la pagina xii pentru mai multe detalii.

Capitolul 16. Consideraţii de securitate pentru browser-ele de Internet

Mulţi utilizatori de PC din organizaţia dumneavoastră au browser-e pe staţiile de lucru. Ei s-ar putea conecta la Internet. Ele s-ar putea conecta de asemenea la sistemul dumneavoastră. În continuare sunt unele consideraţii de securitate atât pentru PC-uri cât şi pentru serverul dumneavoastră.

Risc: deteriorarea staţiei de lucru

O pagină Web pe care utilizatorul dumneavoastră o vizitează poate avea asociat un ″program,″ ca de exemplu Java aplet, un control Active-X, sau un alt tip de plug-in. Deşi este rar, acest tip de ″program″, când îl rulaţi pe un PC, are potenţialul de a deteriora informaţiile de pe PC. În calitate de administrator de securitate, pentru a proteja PC-urile din organizaţie luaţi în considerare următoarele:

- Încercaţi să înţelegeţi opţiunile de securitate ale diferitelor browser-e pe care le deţin utilizatorii. De exemplu, cu unele browser-e, puteţi controla accesul pe care Java aplett-urile le au în afara browser-ului (mediul de operare restricţionat al Java este numit *sandbox*). Acest lucru poate împiedica applet-urile să deterioreze datele de pe PC.

  Notă: Conceptul de ″sandbox″ şi restricţiile de securitate asociate nu există pentru Active-X şi alte plug-ins.
- Faceţi recomandări utilizatorilor despre setările browser-ului. Probabil că nu aveţi nici timp şi nici resurse pentru a vă asigura că utilizatorii v-au urmat recomandările. De aceea, trebuie să îi informaţi în legătură cu riscurile potenţiale ale unor setări nepotrivite.
- Luaţi în considerare standardizarea browser-elor, fapt ce oferă opţiunile de securitate de care aveţi nevoie.
- Instruiţi-vă utilizatorii să vă informeze despre orice comportament dubios sau simptome care ar putea fi asociate cu un anume site de web.

Risc: accesul la directoarele iSeries prin unităţi mapate

Consideraţi că un PC este conectat la serverul dumneavoastră cu o sesiune IBM iSeries Access pentru Windows. Sesiunea setează drive-urile mapate pentru legarea la iSeries Sistem de fişiere integrat. De exemplu, unitatea **G** a PC-urilor ar putea mapa laSistem de fişiere integrat ale serverului SYSTEM1 din reţea.

Acum să presupunem că acelaşi utilizator PC are un browser şi poate avea acces la Internet. Utilizatorul ce vizitează o pagină Web ce rulează un ″program″ rău ca de exemplu Java aplet sau control Active-X . Programul ar putea încerca să şteargă tot ce se găseşte pe drive-ul G al PC-ului.

Există câteva măsuri de protecţie împotriva deteriorării drive-urilor mapate:

- Cea mai importantă protecţie a dumneavoastră securitatea resurselor de pe serverul dumneavoastră. Applet-ul Java sau controlul Active-X apare serverului ca şi utilizatorul care a stabilit sesiunea PC. Trebuie să gestionaţi cu atenţie ce anume sunt autorizaţi să facă utilizatorii PC pe serverul dumneavoastră.
- Sfătuiţi utilizatorii dumneavoastră de PC-uri să-şi seteze browser-ele pentru a preveni încercările de accesare a unităţilor mapate. Acestea sunt valabile pentru Java aplet-uri dar nu şi pentru control Active-X, care nu are conceptul de sandbox.

- Explicaţi-le utilizatorilor dumneavoastră despre pericolele la care sunt expuşi când sunt conectaţi la serverul dumneavoastră şi la Internet în acelaşi timp. De asemenea, asiguraţi-vă că utilizatorii dumneavoastră de PC-uri (cu clienţi Windows 95, de exemplu) înţeleg că unităţile rămân mapate chiar şi atunci când sesiunea iSeries Access apare ca terminată.

Risc: încredere în applet-uri semnate

Utilizatorii s-ar putea să fi urmat sfaturile dumneavoastră şi să fi setat browser-ele pentru a împiedica applet-urile să scrie pe drive-urile de pe PC. Totuşi, utilizatorii PC trebuie să fie conştienţi că *applet-urile semnate* pot rescrie setările browser-ului.

Un applet semnat are asociată o semnătură digitală pentru a stabili autenticitatea lui. Când un utilizator accesează o pagină de web care are un applet semnat, utilizatorul vede un mesaj. Mesajul indică semnătura applet-ului (cine l-a semnat şi când a fost semnat). Când un utilizator acceptă applet-ul, utilizatorul permite applet-ului să rescrie setările de securitate pentru browser. Applet-ul semnat poate scrie pe drive-ul local al PC-ului, chiar dacă setările implicite ale browser-ului împiedică acest lucru. Applet-ul semnat poate de asemenea să scrie pe unităţile mapate pe serverul dumneavoastră deoarece ele apar PC-ului ca fiind unităţi locale.

Pentru propriile dumneavoastră applet-uriJava care vin de pe serverul dumneavoastră, se poate să aveţi nevoie să folosiţi applet-uri semnate. Totuşi, trebuie să îi instruiţi pe utilizatori ca, în general, să nu accepte applet-uri semnate din surse necunoscute.

Capitolul 17. Informaţii înrudite

Manuale

- *APPC Programming*, SC41-5443-00descrie suportul pentru comunicaţiile program-la-program avansate (APPC) pentru sistemul iSeries. Această carte vă ghidează în dezvoltarea programelor de aplicaţie ce folosesc APPC şi în definirea mediului de comunicaţie pentru comunicaţii APPC. El include consideraţii despre programe de aplicaţii, cerinţe şi comenzi de configurare, administrarea problemelor pentru APPC şi consideraţii generale despre reţele. Vedeţi CD-ul Centru de informare iSeries.
- *AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet* Redbook, SG24-4929 discută problemele de securitate şi riscurile asociate cu conectarea iSeries la Internet. Furnizează exemple, recomandări, sfaturi şi tehnici pentru aplicaţii TCP/IP.
- *Backup and Recovery*, SC41-5304-07 furnizează informaţii despre planificarea unei copii de siguranţă şi a unei strategii de recuperare, salvarea informaţiilor de pe sistemul dumneavoastră şi recuperarea sistemului. Vedeţi Centru de informare iSeries.Informaţii adiţionale despre aceste subiecte puteţi găsi în Centru de informare iSeries. Vezi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru mai multe detalii.
- *CL Programming*, SC41-5721-06 furnizează descrieri detaliate pentru codificarea specificaţiilor de descriere a datelor (data description specification, DDS) pentru fişiere care pot fi descrise extern. Aceste fişiere sunt fişiere fizice, logice, de ecran, de tipărire şi pentru funcţii de comunicaţie intersistem (intersystem communication function, ICF). Vedeţi Centru de informare iSeries.
- Subiectul CL din Centrul de informare (Consultaţi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru mai multe detalii.) furnizează o descriere completă a limbajului de control (CL)iSeries şi a comenzilor lui pentru OS/400. Comenzile OS/400 sunt folosite pentru a executa funcţii Operating System/400, programul licenţiat 5722-SS1. Toate comenzile CL non-OS/400 -- cele asociate cu alte programe licenţiate, incluzând toate limbajele şi utilitarele -- sunt descrise în cărţile care asigură suportul pentru respectivele programe licenţiate.
- *Implementing iSeriesSecurity, 3rd Edition* de Wayne Madden şi Carol Woodbury. Loveland, Colorado: 29th Street Press, o divizie a Duke Communications International, 1998. Oferă ghidare şi sugestii practice pentru planificarea, configurarea şi administrarea securităţii iSeries.

  Număr de ordine ISBN:

  1-882419-78-2
- Pentru informaţii suplimentare cu privire la serverul HTTP, consultaţi următorul URL:

  `http://www.ibm.com/eserver/iseries/software/http/docs/doc.htm`
- *Referinţă securitate iSeries*, SC41-5302-07, furnizează informaţii complete despre variabilele sistemului de securitate, profilurile utilizatorilor, securitatea resurselor şi auditarea securităţii. Acest manual nu descrie securitatea pentru programe licenţiate, limbaje şi utilitare specifice. Vedeţi Centru de informare iSeries.
- Subiectul ″Operaţii sistem de bază″ din Centrul de informare furnizează informaţii despre unele din conceptele cheie şi operaţiile necesare pentru operaţiile de bază iSeries. Vezi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru mai multe detalii.
- Centrul de informare descrie cum să folosiţi şi să configuraţi TCP/IP şi mai multe aplicaţii TCP/IP, cum ar fi FTP, SMTP şi TELNET. Vezi “Condiţii prealabile şi informaţii conexe” la pagina xii pentru mai multe detalii.
- *Suport sever fişiere TCP/IP pentru OS/400 Installation and User's Guide*, SC41-0125, furnizează informaţii introductive, instrucţiuni de instalare şi proceduri de configurare

pentru oferta de program licenţiat File Server Support. Explică funcţiile disponibile odată cu produsul şi include exemple şi sfaturi despre folosirea lor cu alte sisteme.

- *Trusted Computer Systems Evaluation Criteria* DoD 5200.28.STD, descrie criteriile pentru nivelurile de încredere pentru sistemele de calculatoare. TCSEC este o publicaţie a guvernului Statelor Unite. Pot fi obţinute copii de la:

  Office
  of Standards and Products
  National Computer Security Center
  Fort Meade, Maryland 20755-6000 USA
  În atenţia: Chief, Computer Security Standards
- Centrul de informare conţine mai multe subiecte cu privire la Administrare sistem şi Controlul funcţionării pe iSeries. Unele din aceste subiecte tratează colectarea datelor de performanţă, gestionarea valorilor sistem şi gestionarea spaţiului de stocare. Pentru detalii despre accesarea Centrului de informare, consultaţi “Condiţii prealabile şi informaţii conexe” la pagina xii. Controlul funcţionării, SC41-5306-03, furnizează informaţii despre cum să creaţi şi să modificaţi un mediu de control al funcţionării. Vedeţi Centru de informare iSeries.

În plus faţă de aceste subiecte ale Centrului de informare şi manuale suplimentare, puteţi folosi următoarele resurse pentru asistenţă:

- **IBM SecureWay**
  IBM SecureWay oferă un brand comun pentru portofoliul bogat de IBM de oferte legate de securitate, hardware, software, consultanţă şi servicii pentru a ajuta clienţii să-şi securizeze informaţiile electronice. Fie că se adresează unei nevoi individuale sau creează o soluţie pentru toată întreprinderea, ofertele IBM SecureWay asigură expertiza necesară pentru a planifica, a proiecta, a implementa şi a opera un mediu cu soluţii securizate pentru activitatea dumneavoastră. Pentru mai multe informaţii despre ofertele IBM SecureWay, vizitaţi pagina de bază IBM SecureWay:

  `http://www.ibm.com/secureway`
- **Servicii oferite**
  Instalarea de hardware sau software nou vă poate imbunătăţi eficienţa şi operaţiile comerciale. Dar de asemenea duce la apariţia pericolului de oprire a echipamentelor şi de întrerupere a activităţii şi poate suprasolicita resursele interne. IBM Global Services oferă servicii legate de securitatea iSeries. Următorul site Web vă permite să căutaţi liste complete de servicii pentru iSeries:

  `http://www.as.ibm.com/asus`

Observaţii

Aceste informaţii au fost dezvoltate pentru produse şi servicii oferite în S.U.A.

IBM ar putea să nu ofere produsele, serviciile, sau opţiunile discutate în acest document în alte ţări. Consultaţi reprezentantul dumneavoastră local IBM pentru informaţii despre produsele şi serviciile disponibile curent în zona dumneavoastră. Orice referinţă la un produs, program sau serviciu IBM nu implică faptul că numai acel produs, program sau serviciuIBM poate fi folosit. Orice produs, program sau serviciu echivalent din punct de vedere funcţional care nu încalcă nici un drept de proprietateIBM poate fi folosit în locul acestuia. Totuşi, este responsabilitatea utilizatorului să evalueze şi să verifice funcţionarea oricărui produs, program sau serviciu non-IBM.

IBM poate avea brevete sau aplicaţii în curs de brevetare care acoperă subiectul descris în acest document. Acest document nu vă acordă nici o licenţă pentru aceste patente. Puteţi trimite cererile de licenţiere, în scris, la:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
U.S.A.

Pentru cereri de licenţă cu privire la informaţii (DBCS) pe doi octeţi, contactaţi Departamentul de proprietate intelectuală alIBM din ţara dumneavoastră sau trimiteţi cereri, în scris, la:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

Următorul paragraf nu se aplică în cazul Marii Britanii sau al altor ţări unde asemenea prevederi nu sunt în concordanţă cu legile locale: INTERNATIONAL BUSINESS MACHINES CORPORATION OFERĂ ACEASTĂ PUBLICAŢIE “ CA ATARE”, FĂRĂ NICI UN FEL DE GARANŢIE, EXPRIMATĂ SAU PRESUPUSĂ, INCLUSIV, DAR NELIMITÂNDU-SE LA ELE, GARANŢIILE IMPLICITE DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME, DE VANDABILITATE SAU DE POTRIVIRE LA UN ANUMIT SCOP. Unele state nu permit declinarea responsabilităţii pentru garanţiile exprese sau implicite în anumite tranzacţii şi de aceea este posibil ca aceste clauze să nu fie valabile în cazul dumneavoastră.

Aceste informaţii pot include inexactităţi tehnice sau erori tipografice. Se efectuează modificări periodice la informaţiile incluse aici; aceste modificări vor fi încorporate în noi ediţii ale publicaţiei. IBM ar putea aduce îmbunătăţiri şi/sau modificări în produsul(le) şi/sau programul(ele) descrise în această publicaţie în orice moment fără înştiinţare.

Referirile din aceste informaţii la adrese de site-uri Web non-IBM sunt făcute numai pentru a vă ajuta, fără ca prezenţa lor să însemne un gir acordat acestor site-uri Web. Materialele de pe aceste site-uri Web nu fac parte din materialele pentru acest produs IBM şi folosirea acestor site-uri Web este pe propriul dumneavoastră risc.

IBM poate utiliza sau distribui oricare dintre informaţiile pe care le furnizaţi, în orice mod considerat adecvat, fără ca aceasta să implice vreo obligaţie faţă de dumneavoastră.

Posesorii de licenţe pentru acest program care doresc să aibă informaţii despre el în scopul de a permite: (I) schimbul de informaţii între programe create independent şi alte programe (inclusiv acesta) şi (II) utilizarea mutuală a informaţiilor care au fost schimbate, vor contacta:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52N
Rochester, MN 55901
U.S.A.

Aceste informaţii pot fi disponibile, să fie supuse unor termeni şi condiţii, inclusiv în unele cazuri, plata unor taxe.

Programul licenţiat descris în aceste informaţii şi toate materialele licenţiate disponibile pentru acesta sunt furnizate deIBM în termenii Acordului client IBM, IBM Acordului de licenţă program internaţional, sau orice alt acord echivalent între noi.

Orice informaţie referitoare la performanţă conţinută aici a fost determinată într-un mediu controlat. De aceea, rezultatele obţinute în alte medii de operare pot diferi semnificativ. Unele măsurători s-ar putea să fi fost făcute pe sisteme la nivel de dezvoltare şi nu există nici o garanţie că aceste măsurători vor fi identice pe sistemele disponibile pe piaţă. Mai mult de atât, unele măsurători s-ar putea să fi fost estimate prin extrapolare. Rezultatele reale pot varia. Utilizatorii acestui document trebuie să verifice datele aplicabile pentru mediul lor specific.

Informaţiile privind produsele non-IBM au fost obţinute de la furnizorii acestor produse, din anunţurile lor publicate sau din alte surse disponibile publicului. IBM Inu a testat aceste produse şi nu poate confirma acurateţea performanţelor, compatibilitatea sau oricare alte pretenţii legate de produsele non-IBM. Întrebări despre capacităţile produselor non-IBM ar trebui adresate furnizorilor acestor produse.

Toate declaraţiile privind direcţiile de viitor şi intenţiile IBM-ului pot fi schimbate sau se poate renunţa la ele, fără notificare prealabilă şi reprezintă doar scopuri şi obiective.

Aceste informaţii sunt numai pentru scopuri de planificare. Informaţiile conţinute aici se pot modifica înainte ca produsele descrise să devină disponibile.

Aceste informaţii conţin exemple de date şi rapoarte folosite în operaţiile comerciale de zi cu zi. Pentru a le arăta cât se poate de adevărate, exemplele includ nume de indivizi, companii, brand-uri şi produse. Toate aceste nume sunt fictive şi orice asemănare cu nume sau adrese folosite de o întreprindere reală este pură coincidenţă.

LICENŢĂ - COPYRIGHT:

Aceste informaţii conţin exemple de programe de aplicaţii în limbaje sursă, care ilustrează tehnici de programare pe diferite platforme de operare. Puteţi copia, modifica şi distribui aceste programe exemplu în orice formă fără să plătiţi la IBM, pentru intenţia de dezvoltare, folosire, marketing sau distribuţie a programelor aplicaţie în conformitate cu interfaţa de programare a aplicaţiei pentru platforma de operare pentru care programele exemplu au fost scrise. Aceste exemple nu au fost testate temeinic pentru toate condiţiile. IBM, prin urmare, nu poate garanta sau acorda încredere, service, sau funcţionareaacestor programe. Puteţi copia, modifica şi distribui aceste programe exemplu în orice formă fără să plătiţi la IBM pentru intenţia de dezvoltare, folosire, marketing sau distribuţie a programelor aplicaţie în conformitate cu interfeţele de programare a aplicaţiilor IBM.

Dacă vedeţi aceste informaţii folosind o copie electronică, fotografiile şi ilustraţiile color s-ar putea să nu apară.

Mărci comerciale

Următorii termeni sunt mărci comerciale ale International Business Machines Corporation în Statele Unite, în alte state sau în ambele:

Advanced Peer-to-Peer Networking
APPN
AS/400
DB2
DRDA
e (emblema)
IBM
iSeries
Net.Data
Operating System/400
OS/400
PowerPC
SecureWay
System/36
System/38
400

ActionMedia, LANDesk, MMX, Pentium şi ProShare sunt mărci comerciale sau înregistrate ale Intel Corporation în Statele Unite, în alte ţări sau ambele.

Microsoft, Windows, Windows NT şi emblema Windows sunt mărci comerciale ale Microsoft Corporation în Statele Unite, în alte ţări sau ambele.

Java şi toate mărcile comerciale bazate pe Java sunt mărci comerciale ale Sun Microsystems, Inc. în Statele Unite, în alte ţări sau ambele.

UNIX este o marcă înregistrată deţinută de The Open Group în Statele Unite în alte ţări sau ambele.

Alte nume de companii, produse şi servicii pot fi mărci comerciale sau mărci de serviciu ale altora.

Index

Caractere speciale

A

B

C

D

E

F

I

Î

J

L

M

N

O

P

Q

R

S

T

U

V

Comentarii cititori

iSeries
Sugestii pentru securizarea iSeries
Versiunea 5

Publicaţia nr. SA12-7296-07

Apreciem comentariile dumneavoastră despre această publicaţie. Nu ezitaţi să ne trimiteţi comentariile despre anumite erori sau lipsuri, despre claritatea, organizarea şi conţinutul subiectelor din această carte. Comentariile pe care le trimiteţi trebuie să se refere la informaţiile din acest manual şi la modul în care sunt prezentate.

Pentru întrebări cu caracter tehnic şi informaţii despre produse şi preţuri vă rugăm să luaţi legătura cu sucursala IBM din localitatea dumneavoastră, cu partenerul de afaceri IBM sau cu reprezentantul de vânzări autorizat.

Pentru întrebări generale, vă rugăm sunaţi la ″Hallo IBM″ (număr de telefon 01803/313233).

Când trimiteţi comentarii la IBM, acordaţi IBM-ului dreptul ne-exclusiv de a utiliza sau distribui aceste comentarii în orice mod pe care îl consideră corespunzător, fără ca din aceasta să rezulte vreo obligaţie faţă de dumneavoastră.

Comentarii:

Vă mulţumim pentru ajutorul acordat.

Pentru a trimite comentariile:

- Trimiteţi comentariile la adresa de pe spatele acestui formular.
- Trimiteţi un fax la următorul număr: Statele Unite şi Canada: 1-800-937-3430
- Trimiteţi comentariile prin e-mail la: RCHCLERK@us.ibm.com

Dacă doriţi un răspuns de la IBM, vă rugăm să completaţi următoarele informaţii:

Nume	Adresă
Companie sau organizaţie	
Număr de telefon	Adresă de e-mail

IBM

IBM CORPORATION
ATTN DEPT 542 IDCLERK
3605 Highway 52N
ROCHESTER MN

Tipărit în S.U.A.

SA12-7296-07