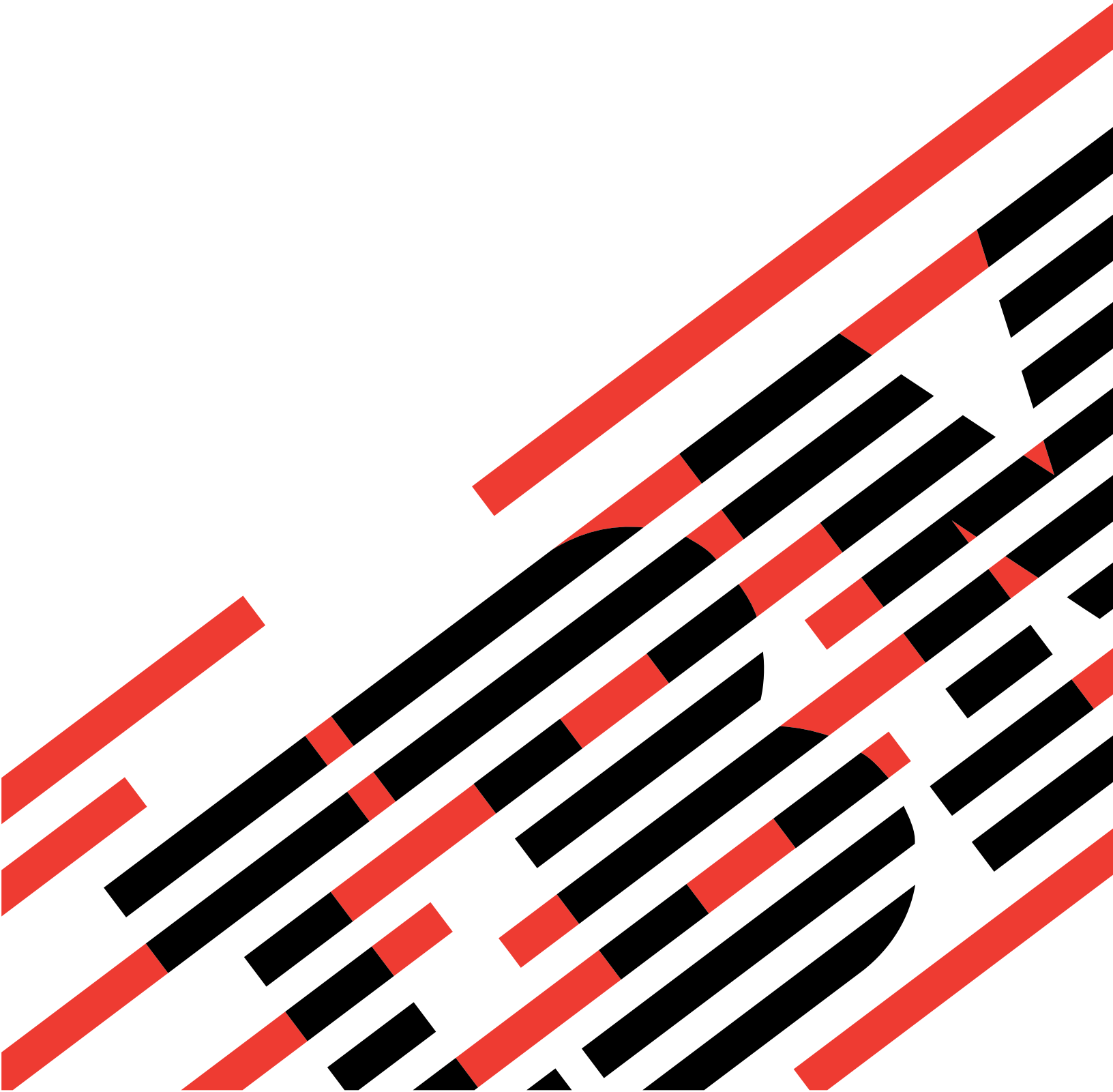
IBM

eserver

iSeries

Securitatea de bază a sistemului şi planificarea

Versiunea 5 Ediţia 3



IBM

@server

iSeries

Securitatea de bază a sistemului şi planificarea

Versiunea 5 Ediţia 3

Notă

Înainte de a folosi aceste informaţii şi produsul la care se referă, aveţi grijă să citiţi “Observaţii”, la pagina 129.

Ediţia a cincea (august 2005)

Această ediţie este valabilă pentru IBM Operating System/400 (număr de produs 5722-SS1) Versiunea 5, Ediţia 3, Modificarea 0 şi pentru toate ediţiile şi modificările următoare, până când se specifică altceva în noile ediţii. Această versiune nu rulează pe toate modelele RISC şi nici pe modelele CISC.

Cuprins

Securitate de bază a sistemului şi planificarea

Securitatea de bază a sistemului şi planificarea vă oferă informaţii detaliate privind planificarea şi setarea securităţii serverului iSeries. În acest subiect se pune accentul pe planificare, fiind incluse formulare pe care le puteţi folosi pentru planificare şi pentru înregistrarea deciziilor de securitate. Oferă de asemenea instrucţiuni pas cu pas pentru securitatea de bază a sistemului. Deoarece acest subiect poate fi folosit ca un manual este bine să-l tipăriţi, pentru a-l aprofunda.

Setarea celei mai bune soluţii de securitate pentru iSeries constă din două seturi principale de activităţi: task-urile de planificare şi task-urile de configurare. Pentru a fi sigur că setaţi securitatea care corespunde necesităţilor întreprinderii dumneavoastră, revedeţi aceste subiecte de planificare:

- Iniţiere în securitatea de bază a sistemului oferă o privire generală asupra conceptelor de securitate şi răspunde întrebărilor despre securitatea de bază a sistemului.
- Planificarea securităţii pentru utilizatori oferă informaţii depre cum să vă planificaţi securitatea care afectează utilizatorii din sistem. Aceasta include securitatea fizică, securitatea aplicaţiilor, strategia generală de securitate şi profilurile de utilizator de pe sistem.
- Planificarea securităţii pentru resurse oferă informaţii despre cum să planificaţi securitatea obiectelor din sistem, inclusiv bibliotecile şi obiectele din ele, imprimantele, ieşirea la imprimantă şi staţiile de lucru.

După ce terminaţi activităţile de planificare, puteţi revedea subiectele următoare care vă ajută să setaţi securitatea pentru sistem:

- Setare securitate utilizator oferă detalii despre setarea securităţii utilizatorilor şi grupurilor.
- Setare securitate resurse oferă informaţii despre cum să setaţi dreptul de proprietate pentru obiecte, autorizări publice sau specifice pentru obiecte şi securitatea pentru imprimante şi staţii de lucru.
- Testare securitate oferă informaţii despre testarea securităţii dumneavoastră.
- Modificare informaţii de securitate oferă informaţii despre actualizarea şi modificarea profilurilor de utilizator şi de grup şi a securităţii resurselor.
- Salvare informaţii securitate oferă informaţii despre salvarea informaţiilor de securitate.
- Monitorizare securitate oferă liste de verificare pentru a urmări securitatea şi informaţii despre auditarea securităţii.

În plus faţă de aceste subiecte, folosiţi formulare de planificare pentru a vă documenta strategiile de planificare şi deciziile de securitate.

Tipăriţi acest subiect

Puteţi vizualiza sau descărca o versiune PDF a acestui document pentru vizualizare sau tipărire. Pentru a vizualiza fişierele PDF, trebuie să aveţi instalat Adobe® Acrobat® Reader. Puteţi descărca o copie din pagina de bază Adobe 

Pentru a vizualiza sau descărca versiunea PDF, selectaţi Securitatea şi planificarea de bază a sistemului (950 KB sau 164 pagini).

Salvarea unui fişier PDF pe staţia de lucru pentru vizualizare sau tipărire:

1. Deschideţi PDF-ul în browser (faceţi clic pe legătura de mai sus).
2. În meniul browser-ului, faceţi clic pe **File**.
3. Faceţi clic pe **Save As...**
4. Navigaţi la directorul în care doriţi să salvaţi fişierul PDF.
5. Faceţi clic pe **Save**.

Iniţierea în securitatea de bază a sistemului

Toţi, de la administratorii de sistem la utilizatori, ar trebui să fie preocupaţi de securitatea sistemului. Securitatea sistemului protejează serverul iSeries şi informaţiile sensibile ale întreprinderii atât faţă de breşele de securitate intenţionate, cât şi faţă de cele neintenţionate.

Puteţi personaliza securitatea sistemului, în funcţie de mediul dumneavoastră de securitate şi de necesităţile specifice.

Gândiţi-vă la securitate ca şi la poarta de securitate a sistemului. Puteţi folosi caracteristici de securitate la **blocarea** sau protejarea informaţiilor de utilizatori neautorizaţi.

Puteţi, de asemenea folosi caracteristici de securitate la **deblocarea** flexibilităţii sistemului şi personalizarea lui pentru fiecare utilizator.

Un plan bun de securitate poate proteja sistemul, dar nu poate garanta siguranţa echipamentului sau a informaţiilor. Aţi putea împărţi responsabilităţile de sistem mai multor angajaţi pentru a vă asigura că nici o persoană nu are control exclusiv asupra sistemului.

Planificarea şi securitatea de bază a sistemului vă este furnizată cu abordarea pas cu pas a planificării şi setării de bază a sistemului. Acest subiect accentuează importanţa planificării securităţii sistemului şi furnizează plănuirea formularelor pe care să le folosiţi pentru a vă înregistra deciziile de securitate. Pentru a vă ajuta să luaţi decizii în legătură cu securitatea, în acest subiect veţi găsi un exemplu al unei afaceri care plănuieşte măsuri de securitate.

Pentru a vă asigura că realizaţi securitatea sistemului cu succes este esenţial să aveţi un plan bun. Revedeţi aceste subiecte pentru a învăţa despre necesitatea securităţii de bază şi importanţa plănuirii securităţii:

- Întrebări frecvente despre securitatea de bază a sistemului
- O privire generală asupra securităţii de bază a sistemului
- O metodă de planificare a securităţii de bază a sistemului

De asemenea, ar trebui să aveţi un plan bun de salvare de rezervă şi recuperare a tututor informaţiilor din sistem. În plus, ar trebui un plan pentru înlocuirea echipamentului în eventualitatea unui dezastru. Pentru mai multe informaţii despre proiectarea unui plan bun de salvare de rezervă, vedeţi subiectul Salvare de rezervă şi Recupereareîn Centrul de Informare.

Informaţii detaliate de planificare a securităţii utilizator

Următoarele subiecte furnizează tehnici pentru planificarea securităţii utilizator :

- Planificarea securităţii aplicaţiilor
- Planificarea strategiei de securitate
- Planificarea grupurilor utilizator
- Planificarea profilurilor de utilizator individuale

Informaţii detaliate de planificare a securităţii resurselor

Urmatoarele subiecte furnizează o abordare sistematică a planificării securităţii resurselor utilizatorilor.

- Înţelegerea tipurilor de autorizări
- Planificarea securităţii pentru bibliotecile aplicaţiilor
- Determinarea dreptului de proprietate asupra bibliotecilor şi obiectelor
- Gruparea obiectelor
- Protejarea ieşirilor imprimantă
- Protejarea staţiilor de lucru
- Planificarea instalării aplicaţiilor

Planificarea formularelor de tipărit

Securitatea de bază a sistemului şi planificarea furnizează planificarea formularelor de tipărit care vă permit să întregistraţi toate deciziile dumneavoastră de securitate. Puteţi tipări intregul subiect ca un PDF, sau formulare de planificare individuale folosind butonul de tipărire al browser-ului.

Instrucţiuni de setare pas cu pas pentru securitatea de bază a sistemului

După terminarea planificării securităţii, acest subiect vă furnizează paşii pentru a vă pune planul în aplicare. Subiectele următoare vă vor ajuta să setaţi securitatea sistemului.
- Setarea securităţii utilizator
- Setarea securităţii resurselor

Întrebări frecvente despre securitatea de bază a sistemului

Revederea răspunsului la aceste întrebări frecvente despre securitate vă ajută să înţelegeţi mai bine importanţa securităţii sistemului.

De ce este importantă securitatea?

Informaţiile stocate în sistem reprezintă bunul cel mai de preţ al afacerii. Păstraţi trei obiective importante în minte când vă gândiţi cum să protejaţi informaţiile preţioase:
- **Confidenţialitate:** Măsurile bune de securitate împiedică utilizatorii să vadă şi să divulge informaţiile confidenţiale.
- **Integritate:** La câteva extensii, o bună proiectare a securităţii sistemului poate asigura acurateţea informaţiilor din sistem. Cu o securitate corectă, puteţi împiedica modificările neautorizate sau ştergerea datelor.
- **Disponibilitate:** Dacă cineva în mod accidental sau intenţionat deteriorează datele din sistem, nu puteţi accesa aceste resurse până când nu le recuperaţi. O bună securitate a sistemului poate împiedica acest tip de deteriorări.

Când oamenii se gândesc la securitatea sistemului, de obicei se gândesc la modul de protejare a sistemului de utilizatori din exteriorul companiei, cum ar fi rivalii de afaceri. De fapt, protejarea împotriva curiozităţii sau a accidentelor de sistem este adesea cel mai mare beneficiu al proiectării securităţii sistemului. Într-un sistem fără opţiuni de securitate, un utilizator poate sterge neintenţionat fişiere importante. O proiectare bună a securităţii sistemului vă ajută să împiedicaţi acest tip de accidente.

Puneţi-vă aceste întrebări pentru a decide nivelul de securitate de care aveţi nevoie în sistem:
- Cât de important este calculatorul (şi datele pe care le stocaţi în el) în afacerea dumneavoastră?
- Aveţi o politică de companie care necesită anumite niveluri de securitate?
- Necesită auditorii un nivel de securitate pentru informaţiile stocate în calculator?
- Veţi avea nevoie de câteva grade de securitate în viitorul previzibil?

De ce să vă personalizaţi sistemul?

Serverul iSeries acoperă o gamă largă de utilizatori. Un sistem mic poate avea de la trei la cinci utilizatori care rulează câteva aplicaţii. Un sistem larg poate avea mii de utilizatori într-o reţea largă de comunicare rulând multe aplicaţii.

iSeries a fost proiectat astfel încât să asigure un grad înalt de flexibilitate, pentru a permite adaptarea la o gamă largă de utilizatori şi situaţii. Aveţi posibilitatea de a modifica multe lucruri cu privire la felul în care apare sistemul utilizatorilor şi cum operează.

Când primiţi sistemul de la furnizor, probabil nu va fi nevoie şi nu vreţi să faceţi foarte multe personalizări. Când IBM vă livrează sistemul, multe opţiuni au setările iniţiale, numite **implicite**. Aceste setări implicite sunt alegeri care în mod obişnuit determină sistemul să funcţioneze corespunzător în vedere noilor instalări.

Notă: Toate sistemele noi sunt puse la punct cu un nivel implicit de securitate de **40**. Acest nivel de securitate asigură că numai utilizatorii definiţi pot folosi sistemul. De asemenea, împiedică apariţia riscurilor de alterare a integrităţii securităţii datorită programelor cu o securitate circumspectă.

Oricum, dacă faceţi câteva personalizări, puteţi simplifica sistemul şi oferi mai multe unelte pentru utilizatori. De exemplu, puteţi să vă asiguraţi că un utilizator obţine meniul corect când semnează. Puteţi să vă asiguraţi că rapoartele fiecărui utililizator merg la imprimanta corespunzătoare. Utilizatorii se vor simţi mai încrezători în sistem dacă le oferiţi câteva personalizări iniţiale pentru a-l face să arate şi să reacţioneze precum propriul sistem.

Cine ar trebui să fie responsabil?

Companiile abordează în mod diferit măsurile de securitate. Câteodată programatorii au responsabilitatea pentru toate aspectele legate de securitate. În alte cazuri, persoana care gestionează sistemul se ocupă şi de securitatea lui. Dacă nu sunteţi sigur cum să atribuiţi responsabilităţile în companie, iată o abordare sugestivă:

- Determinaţi o metodă de planificare a securităţii resurselor în funcţie de următoarele situaţii: compania cumpără sau dezvoltă aplicaţii. Dacă dezvoltaţi propriile aplicaţii, comunicaţi nevoile de securitate a resurselor în timpul procesului de dezvoltare. Dacă aplicaţiile sunt cumpărate, înţelegeţi-vă şi colaboraţi cu proiectantul aplicaţiei. În ambele cazuri, persoana care proiectează aplicaţiile ar trebui să considere securitatea ca parte a proiectării.
- Setarea securităţii ar trebui să fie responsabilitatea ofiţerului de securitate. Ofiţerul de securitate defineşte utilizatorii sistemului şi nivelul lor de acces la sistem. Ofiţerul de securitate este adesea responsabil pentru alte lucruri din sistem, cum ar fi salvarea de siguranţă şi recuperarea informaţiilor.
- Ofiţerul de securitate ar trebui de asemenea să personalizeze sistemul, cât timp multe elemente de securitate joacă un rol important în personalizarea sistemului.

Nu contează ce metodă folosiţi pentru a atribui responsabilităţi de securitate, **comunicate printr-o politică de securitate**. Un director din companie ar trebui să le spună tuturor, de preferat în scris, ce informaţii din calculator sunt considerate importante. Ar trebui să protejaţi acele informaţii, aşa cum este protejat orice altceva de preţ din companie. Vedeţi ″Exemplu: Politica de securitate a Companiei JKL Toy″ pentru un exemplu de politică de securitate.

Acum, după ce aţi înţeles nevoia securităţii sistemului, aţi dori să revedeţi o privire generală a considerentelor privind securitatea sistemului.

O privire generală asupra securităţii de bază a sistemului

Pentru o planificare eficace, e nevoie să înţelegeţi cum viziunea dumneavoastră asupra a ceea ce vreţi să realizaţi se leagă de uneltele furnizate de sistem. Trebuie să ştiţi cum opţiunile utilizatorului şi sistemului lucrează împreună pentru a vă ajuta în realizarea obiectivelor.

Urmatoarele subiecte introduc părţi importante de securitate şi personalizare şi arată cum se potrivesc ele. Aceste subiecte intenţionează să vă dea o privire generală înainte de începerea planificării. Toate conceptele introduse aici sunt explicate în detaliu pe măsură ce sunt necesare în procesul de planificare.

- Securitatea de sistem încorporată
- Terminologia de bază
- Viziunea userului asupra securităţii
- Uneltele sistemului pentru securitate şi personalizare

Securitatea încorporată a sistemului

Toate componentele ce ţin de securitatea sistemului sunt încorporate în sistem. Ele nu sunt un produs separat pe care să îl cumpăraţi. Această abordare integrată are mai multe avantaje:

- Securitatea este consistentă cu restul sistemului de operare. Foloseşte aceleaşi ecrane, comenzi şi terminologie.
- Utilizatorii nu pot ocoli securitatea pentru că ea nu e o piesă software separată.
- Securitatea proiectată aşa cum trebuie are efecte minime la nivelul perfomanţei.
- Securitatea ţine întotdeauna pasul cu noile dezvoltări software. Când noi funcţiuni devin disponibile, securitatea acestor funcţiuni devine disponibilă.

iSeries este livrat cu nivelul de securitate 40, care împiedică utilizatorii neautorizaţi să semneze pe sistem. De asemenea, impiedică apariţia riscurilor de securitate din partea unor programe ce ar putea ocoli măsurile de securitate. Însă puteţi personaliza anumite setări de securitate sau puteţi schimba nivelurile de securitate. Nivelurile de securitate sunt descrise în subiectul Alegerea nivelului de securitate.″

Acum vă este mai clar cum funcţionează securitatea încorporată şi ar fi bine să vă familiarizaţi cu terminologia iSeries.

Terminologia de bază

Acest set de termeni generali este foarte important pentru a înţelege securitatea iSeries:

Obiect Un obiect este un spaţiu din sistem care poate fi manevrat. Cele mai obişnuite exemple de obiecte sunt fişierele şi programele. Alte tipuri de obiecte includ comenzi, cozi, biblioteci şi foldere. Obiectele din sistem sunt identificate după numele obiectului, tipul obiectului şi biblioteca în care obiectul se află. Fiecare obiect din sistem poate fi securizat.

Bibliotecă
O bibliotecă este un tip special de obiect folosit pentru a grupa alte obiecte. Multe obiecte din sistem se găsesc într-o bibliotecă.

Director.
Un director este un alt mod de a grupa obiecte din sistem. Obiectele se pot afla într-un director. Un director se poate afla într-un alt director formând o structură ierarhică.

Acum vă este mai clară terminologia generală iSeries privind securitatea şi ar fi bine să revedeţi ce înseamnă securitatea pentru utilizator.

Viziunea utilizatorului asupra securităţii

Din punctul de vedere al utilizatorului, securitatea afectează modul cum el foloseşte şi completează operaţiunile din sistem. De asemenea include modul în care el interacţionează cu sistemul pentru a completa acele operaţiuni. Este important să se ia în considerare felul în care un utilizator vede securitatea. De exemplu, setând parolele să expire la fiecare 5 zile se produce frustrare iar asta va interfera cu abilitatea utilizatorului de a-şi completa jobul. Pe de altă parte, o politică de securitate prea permisivă poate cauza probleme de securitate.

Pentru a furniza securitatea corectă sistemului dumneavoastră aveţi nevoie să divizaţi securitatea în părţi specifice pe care să le puteţi plănui, gestiona şi monitoriza. Din punctul de vedere al utilizatorului, puteţi divide securitatea sistemului dumneavoastră în mai multe părţi:

Accesul fizic la sistem

Securitatea fizică protejează sistemul, toate dispozitivele sistemului şi mediile de stocare ale back-up-urilor, precum dischete, benzi sau CD-uri, de pierderi sau stricăciuni accidentale sau intenţionate.

Cele mai multe măsuri pe care le luaţi pentru a asigura securitatea fizică a sistemului sunt externe sistemului. Totuşi, sistemul este livrat cu o cheie IPL sau o cartela electronică ce împiedică folosirea neautorizată a funcţiilor la nivelul unităţii de sistem.

Subiectul, ″Planificarea securităţii fizice,″ furnizează informaţii detaliate care să vă ajute la plănuierea securităţii fizice a sistemului dumneavoastră.

Cum semnează utilizatorii

Securitatea semnării împiedică o persoană care nu e identificată în sistem să facă acest lucru. Pentru a semna, un individ trebuie să introducă o combinaţie validă de ID utilizator şi parolă.

Puteţi folosi şi valorile de sistem şi profilurile de utilizator individuale de utilizatori pentru a fi sigur că nu este violată securitatea la semnare. De exemplu, puteţi cere ca parolele să fie schimbate la intervale regulate. Puteţi de asemenea împiedica folosirea parolelor uşor de ghicit.

Ce le este permis utilizatorilor să facă

Un rol important în securitatea şi personalizarea sistemului este definirea a ceea ce utilizatorii pot face. Din perspectiva securităţii, aceasta este cel mai adesea**o limitare**, cum ar fi să se impiedice accesul anumitor persoane la anumite informaţii. Din perspectiva personalizării sistemului, aceasta este o **întărire în** funcţionare. O personalizare corectă a sistemului face posibilă executarea joburilor prin eliminarea informaţiilor şi a operaţiilor nenecesare.

Unele metode de definire a ceea ce utilizatorii pot face sunt corespunzătoare responsabilului de securitate pe când altele sunt responsabilitatea programatorilor. Aceste informaţii se concentrează în special pe acele lucruri pe care un responsabil de securitate le face de obicei. Puteţi găsi descrierile tuturor valorilor sistem în Capitolul 3, ″Valorile sistem de securitate″ din *Security-Reference* (SC41-5302).

Sunt valabili parametri în profilurile de utilizator individuale, descrierile de job şi clase pentru a controla ce poate face utilizatorul în sistem. Lista de mai jos descrie pe scurt tehnicile disponibile:

Limitarea utilizatorilor la câteva funcţii
Puteţi limita accesul utilizatorilor doar la un anumit program, meniu sau set de meniuri precum şi la câteva comenzi de sistem, corespunzător profilului utilizator. De obicei, responsabilul cu securitatea creează şi controlează profilurile de utilizator.

Restricţionarea funcţiilor de sistem
Funcţiile de sistem vă permit să salvaţi şi să restauraţi informaţiile, să gestionaţi ieşirea de imprimantă şi să setaţi noi utilizatori în sistem. Fiecare profil de utilizator specifică funcţiile de sistem obişnuite pe care le poate folosi utilizatorul.

Pe iSeries, executaţi funcţii de sistem folosind comenzile CL (command language - limbajul de comandă) şi API-urile (application arogramming interface - interfeţele de programarea a aplicaţiilor). Fiecare comandă şi API fiind un obiect, puteţi folosi autorizarea la nivel de obiect pentru a controla cine le poate folosi şi efectua funcţii de sistem.

Determinaţi cine poate folosi fişiere şi programe
Resursele de securitate furnizează capabilitatea de a controla folosirea fiecărui obiect din sistem. Pentru orice obiect, puteţi specifica cine îl poate folosi şi cum îl poate folosi. De exemplu, puteţi specifica că un utilizator poate doar privi informaţia dintr-un fişier, un altul poate schimba date în acest fişier iar un al treilea poate schimba fişierul sau chiar îl poate şterge.

Prevenirea abuzului de resurse de sistem
Puterea de procesare a sistemului Dvs poate deveni la fel de importantă pentru afacere ca şi datele ce sunt stocate în el. Responsabilul de securitate ajută la asigurarea că utilizatorii nu folosesc greşit resursele sistemului prin rularea joburilor lor la o prioritate mare, printarea mai întai a rapoartelor lor sau prin folosirea a prea mult spaţiu pe disc.

Cum comunică sistemul dumneavoastră cu celelalte calculatoare

Măsuri de securitate suplimentare pot fi necesare dacă sistemul dumneavoastră comunică cu alte calculatoare sau cu staţii de lucru programabile. Daca nu aveţi un control corespunzător al securităţii, cineva poate porni un job pe alt calculator din reţeaua dumneavoastră sau poate accesa informaţii de pe calculatorul dumneavoastră fără a mai trece prin procesul de semnare.

Puteţi folosi valorile sistem şi atributele reţelei pentru a controla dacă permiteţi joburi la distanţă, accesarea de la distantă a datelor sau accesul de la distanţa pe sistemul dumneavoastră. Dacă permiteţi accesul de la distanţa, puteţi specifica ce securitate să impuneţi. Pueţi găsi descrieri pentru toate valorile sistem în Capitolul 3, ″Valorile sistem de securitate,″ din *Security-Reference* (SC41-5302).

Cum să salvaţi informaţiile dumneavoastră de securitate

Aveţi nevoie să faceţi regulat copii de rezervă ale informaţiilor din sistemul dumneavoastră. Pe lângă datele pe sistemul dumneavoastră, trebuie să salvaţi şi informaţiile de securitate. Dacă are loc un dezastru, trebuie să fiţi capabil să recuperaţi informaţiile despre utilizatorii sistemului, informaţiile de autorizare şi informaţiile propriu-zise.

Subiectul ″Salvarea informaţiilor de securitate″ explică cum se salvează informaţiile de securitate. SubiectulSalvarea de rezervă şi recuperarea din Centrul de informare furnizează mai multe informaţii detaliate despre salvarea de rezervă şi recuperarea datelor de securitate

Cum să monitorizaţi planul de securitate

Sistemul furnizează mai multe unelte pentru monitorizarea efectivităţii măsurilor de securitate:

- Mesajele sunt trimise către operatorul de sistem când au loc anumite violări de securitate.
- Diverse tranzacţii legate de securitate pot fi înregistrate într-un jurnal special de auditare.

Subiectul, ″Monitorizarea securităţii″ pune în discuţie folosirea acestor unelte, în termeni generali. Puteţi găsi mai multe detalii despre auditarea securităţii în Capitolul 9, ″Auditarea securităţii pe sistem″, din *Security-Reference* (SC41-5302).

Pentru a înţelege mai bine cum să vă personalizaţi sistemul trebuie să înţelegeţi personalizarea din punctul de vedere al utilizatorului.

Punctul de vedere al utilizatorului asupra personalizării sistemului: Vă puteţi personaliza sistemul astfel încât să ajutaţi utilizatorii în relizarea muncii lor de fiecare zi. Pentru cea mai buna personalizare a sistemului, gândiţi-vă la ce nevoi au utilizatorii pentru realizarea cu succes a muncii lor. Puteţi personaliza sistemul să arate meniuri şi aplicaţii în mai multe moduri:

Arătaţi utilizatorilor ceea ce doresc ei să vadă

Cei mai mulţi dintre noi îşi aranjeaza birourile astfel încât să poată ajunge uşor la lucrurile de care au nevoie. Gândiţi-vă la accesul utilizatorilor în sistem în acelaşi fel. Dupa ce a semnat, un utilizator trebuie să vadă mai întâi meniul sau ecranul pe care acea persoana îl foloseşte cel mai des. Puteţi foarte uşor proiecta profiluri utilizator pentru a realiza acest lucru.

Eliminaţi ceea ce nu este necesar

Cele mai multe sisteme au aplicaţii diferite pe ele. Cei mai mulţi utilizatori vor doar să vadă lucrurile de care ei au nevoie pentru a-şi face joburile. Limitându-le la cât mai puţine funcţii din sistem le vom face munca mai uşoara. Cu profilurile de utilizator, descrierile de joburi şi alte meniuri corespunzătoare, puteţi da fiecarui utilizator o viziune specifică a sistemului.

Trimiteţi ceva către locul corect

Utilizatorii trebuie să nu-şi facă griji despre cum să-şi trimită rapoartele la imprimanta corectă sau cum să-şi ruleze ″job batch″-urile. Valorile de sistem, profilurile utilizatorilor şi descrierile de joburi fac astfel de lucruri.

Furnizarea asistenţei

Oricât de bine reuşiţi să personalizaţi sistemul, utilizatorii se vor întreba în continuare ″Unde e raportul meu?″ sau ″Jobul meu a rulat deja?″ **Ecranele Asistentului Operaţional**furnizează o interfaţă simplă pentru funcţiile sistemului dând utilizatorului răspunsuri la aceste întrebări. Diferitele versiuni ale ecranelor sistemului,numite **niveluri de ajutor**, furnizează ajutor utilizatorilor cu diferite niveluri de experienţa tehnică. Atunci când sistemul soseşte, Ecranele Asistentului Operaţional sunt în mod automat disponibile pentru toţi utilizatorii. Totuşi, ″design″-ul aplicaţiei dumneavoastră poate necesita schimbări ale modului în care utilizatorii primesc acces la meniul Asistentului Operaţional.

iSeries oferă unelte de sistem care vă ajută să personalizaţi securitatea sistemului, ca să vă protejaţi resursele şi, în acelaşi timp, să permiteţi utilizatorilor accesul la ele.

Unelte de sistem pentru securizare şi personalizare

Pentru o planificare eficace, aveţi nevoie să înţelegeţi cum viziunea dumneavoastră asupra scopului securităţii se leagă de uneltele furnizate de sistem. Puteţi folosi aceste unelte de sistem pentru a personaliza sistemul dumneavoastră.

Nivel de securitate

IBM livrează toate noile servere iSeries cu nivelul de securitate 40. Acest nivel de securitate furnizează parole, securitatea resurselor şi integritatea sistemului. Dacă doriţi să schimbaţi nivelul activ de securitate în sistemul dumneavoastră, puteţi modifica valoarea de sistem QSECURITY. Însă IBM vă recomandă cu insistenţă să lăsaţi nivelul de securitate setat la 40. Pentru a putea schimba nivelul de securitate, un utilizator are nevoie de următoarele: clasa utilizator *SECOFR sau *ALLOBJ şi autorizarea specială *SECADM.

Sistemul oferă patru niveluri de securitate aşa cum se arată în acest tabel:

Tabela 1. Niveluri de securitate disponibile în sistem

Nivel de securitate	Descriere
Nivel de securitate 20	Furnizează doar securitatea parolei
Nivel de securitate 30	Furnizează securitatea parolei şi a resurselor
Nivel de securitate 40	Furnizează securitatea parolei şi resurselor, integritate şi securitate.
Nivel de securitate 50	Furnizează securitatea parolei şi resurselor, protecţia îmbunătăţită a integrităţii.

Subiectul ″Alegeţi nivelul Dvs de securitate″ furnizează detalii despre cum să determinaţi ce nivel de securitate îndeplineşte cel mai bine nevoile dumneavoastră.

Valorile de sistem

Puteţi seta valori de sistem pentru a controla modul în care funcţionează pe iSeries anumite caracteristici ale sistemului de operarare. Puteţi privi valorile de sistem ca pe o politică a companiei. Valorile de sistem sunt valabile pentru oricine foloseşte sistemul, exceptând cazul în care sunt înlocuite de anumite specificaţii, cum ar fi un profil de utilizator.

Valorile de sistem determină lucruri precum imprimanta principală, cum afişează sistemul data şi cât de des aveţi nevoie să schimbaţi parola.

Atribute de reţea

Atributele de reţea definesc unele caracteristici despre cum comunică sistemul cu alte computere, inclusiv calculatoare personale. Atributele de reţea se aplică întregului sistem.

Profiluri de grup

Un profil de grup defineşte un grup de utilizatori. Gândiţi profilurile de grup ca pe o politică de departament. Puteţi folosi profiluri de grup ca pe un model pentru crearea de profiluri de utilizatori individuali. Puteţi de asemenea folosi profiluri de grup pentru a defini cum membrii unui grup primesc permisiunea de a accesa obiecte din sistem. Pentru mai multe informaţii despre profilurile de grup vedeţi subiectul Planificarea grupurilor de useri.″

Profiluri de utilizator

Profilul de utilizator este unul din cele mai puternice şi versatile obiecte din sistem. El conţine lucruri precum parola utilizatorului şi ce meniuri vede utilizatorul când semnează. Profilul utilizatorului defineşte ce poate şi ce nu poate face

o persoană în sistem. Determină o vedere unică a utilizatorului asupra sistemului. Subiectul″Planificarea securităţii utilizatorului″ pune în discuţie sugestii pentru planificarea profilurilor de utilizator.

Descrierile de job

O descriere de job lucrează împreună cu valorile de sistem şi profilurile de utilizator pentru a determina felul în care sistemul procesează joburile unui utilizator. O descriere de job setează lista iniţială de biblioteci de utilizator, listă ce determină bibliotecile la care un utilizator obţine acces în mod automat imediat după ce a semnat.

Securitatea resurselor

Responsabilul de securitate protejează reursele (obiectele) din sistem determinând cine are autorizarea să le folosească şi cum poate utilizatorul accesa aceste obiecte. Responsabilul de securitate poate seta autorizări pentru obiecte individuale sau pentru grupuri de obiecte (liste de autorizări). Fişierele, programele şi bibliotecile sunt cele mai comune obiecte care necesită protecţie, însă securitatea sistemului vă permite să setaţi autorizări pentru orice obiect din sistem.

Puteţi gestiona securitatea resurselor simplu şi eficace, dacă plănuiţi în avans o abordare generală şi directă. O schemă de securitatea resurselor creată fără o planificare prealabilă poate deveni complicată şi ineficientă. Subiectul, ″Planificarea securităţii resurselor descrie moduri în care vă puteţi planifica securitatea resurselor.

Sistemul furnizează mai multe unelte pentru a vă ajuta la proiectarea unei scheme de securizare a resurselor cât mai directe.

- **Profilurile de grup:** Puteţi grupa utilizatori similari sub un singur profil de grup. Grupul de utilizatori poate apoi partaja aceeaşi autorizare către obiecte.
- **Liste de autorizare:** Puteţi grupa obiecte cu nevoi de securitate similare într-o listă. Se poate apoi acorda autorizare listei mai degrabă decât obiectelor individuale.
- **Dreptul de proprietate asupra obiectelor:** Fiecare obiect din sistem are un proprietar. Profilurile de grup sau utilizatorii individuali pot fi proprietari de obiecte. Asignare corespunzătoare a drepturilor de proprietate a obiectelor vă ajuta (1) să gestionaţi aplicaţii şi (2) să delegaţi responsabilitatea pentru securitatea informaţiilor dumneavoastră.
- **Grup primar:** Puteţi specifică autorizarea grupului primar pentru un obiect. Sistemul memorează autorizarea grupului primar cu obiectul. Utilizarea autorizării de grup primar poate simplifica gestiunea autorizării şi imbunătăţi verificarea performanţei autorizării.
- **Autorizare bibliotecă:** Puteţi pune fişiere şi programe care necesită protecţie într-o bibliotecă iar apoi puteţi restricţiona accesul la acea bibliotecă. Aceasta este adesea mai simplu decât restricţionarea accesului pentru fiecare obiect individual. Pentru a proteja obiectele critice aţi putea dori să securizaţi atât obiectul cât şi biblioteca.
- **Autorizare obiect:** În cazurile în care accesul la o bibilotecă nu este restricţionat puteţi restricţiona autorizarea la nivel de obiecte individuale precum fişierele.
- **Autorizare publică:** Pentru fiecare obiect puteţi defini ce mod de acces este valabil pentru orice utilizator din sistem care nu are orice altă autorizare la obiect. Autorizarea publică este un mijloc efectiv pentru securizarea obiectelor care nu sunt confidenţiale şi furnizează o perormanţă de sistem bună.
- **Autorizarea de director:** Puteţi folosi autorizarea de director în acelaşi mod în care folosiţi autorizarea de bibliotecă. Puteţi grupa obiecte într-un director şi apoi securiza acest director mai degrabă decât obiecte individuale.
- **Deţinător de autorizare:** Când ştergeţi un obiect, de asemenea ştergeţi şi informaţia de autorizare pentru acel obiect. Deţinătorul de autorizare menţine informaţia de autorizare pentru fişierele definite din program care sunt şterse şi create din nou de o aplicaţie. Puteţi folosi deţinători de autorizare pentru a vă ajuta la migrarea de la System/36.

Unelte de securitate

Puteţi folosi uneltele de securitate ca ajutor la gestionarea şi monitorizarea mediului de securitate pe iSeries. Puteţi de asemenea folosi uneltele de profil utilizator:

- Găsiţi ce profiluri utilizator au parole implicite.
- Planificaţi profilurile de utilizator astfel încât acestea să nu fie disponibile la anumite ore din zi sau din săptămână.

- Planificaţi un profil de utilizator pentru a fi înlăturat atunci când angajatul pleacă.
- Găsiţi ce profiluri utilizator au autorizări speciale.
- Găsiţi pe cei ce adoptă autorizare către obiecte din sistem.

Puteţi folosi obiectele unelte de securitate pentru a urmări autorizările private şi publice care sunt asociate cu obiectele confidenţiale. Puteţi tipări aceste rapoarte regulat (lunar, de exemplu) pentru a vă putea concentra eforturile de securizare asupra problemelor curente. Puteţi rula rapoarte pentru a afisa doar schimbările de la data ultimei rulări a raportului.

Alte unelte furnizează abilitatea de a monitoriza:

- Programe declanşatoare
- Valorile relevante pentru securitate din intrările de comunicare, descrierile de subsistem, valorile de ieşire, cozile de joburi şi descrierile de joburi.
- Programe alterate sau corupte

Acum că aţi înteles importanţa securităţii sistemului, puteţi revedea o descriere a metodei de planificare ce e folosită ca exemplu de acest subiect.

O metodă de planificare a securităţii de bază a sistemului

Planificarea subiectelor în această abordare îşi propune analizarea din exterior în interior şi de la general la particular. De exemplu, pentru a planifica profilurile de utilizator, trebuie mai întâi sa vă gândiţi ce ar trebui să vadă utilizatorul(din exterior) şi apoi să decideţi cum să faceţi acest lucru (din interior). Planificaţi mai întâi valorile sistem şi profilurile grupului (in general), şi apoi decideţi excepţiile pentru utilizatorii individuali (specifice). Paşii de planificare în subiectul Planificarea securităţii utilizator sunt destinaţi pentru a fi efectuaţi în ordine . Ei furnizează o progresie logică pentru descrierea modalităţilor de folosire a sistemului şi deciderea modului de securizare şi personalizare a lui.

Când plănuiţi şi proiectaţi securitatea sistemului, începeţi să construiţi formulare de securitate elementare, continuând apoi cu formulare din ce în ce mai complexe. Începeţi cu securitatea fizică a sistemului, apoi cu descrierea aplicaţiilor şi a valorilor sistem. În final, trebuie să asiguraţi securitatea utilizatorilor şi obiectelor din sistem.

Prin aceste subiecte de planificare, am furnizat exemple de abordare folosind un scenariu al companiei, JKL Toys. Subiectul ″Compania JKL Toy: Prezentarea companiei folosite ca exemplu″ descrie o companie care este folosită în subiectele de planificare.

Vedeţi subiectul ″Paşi în procesul de planificare ″ pentru o descriere corectă a fiecărui pas şi a legaturii dintre ei.

Exemplu: Prezentarea companiei JKL Toy

Exemplele fac lucrurile mai uşor de explicat şi de înţeles. Cu aceasta în minte, aceste subiecte folosesc pentru exemplificare Compania JKL Toy. JKL Toy, o companie mică, dar care se dezvoltă rapid, ce produce jucării, doreşte să seteze securitatea unui sistem iSeries. Preşedintele companiei, John Smith, doreşte ca noul său sistem iSeries să preia din sarcinile de lucru create de dezvoltarea explozivă a companiei JKL Toy.

John îi dă lui Sharon Jones, managerului de conturi, responsabilitatea de administrator de sistem şi responsabil cu securitatea. Ea trebuie să se asigure că întreaga instalare, inclusiv securitatea, va funcţiona corespunzător. Sharon crede în importanţa planificării. Acum compania este mică, şi cei mai mulţi dintre angaţii au acces la aproape toate informaţiile. Însă Sharon ştie că acest lucru se va modifica pe măsură ce compania creşte. Ea doreşte să facă lucrurile corect de prima dată.

Iniţial, Compania JKL Toy planifică să ruleze următoarele aplicaţiipe sistem : Customer Orders, Inventory Control, Contracts and Pricing, şi Accounts Receivable. Aşa cum aţi citit în subiectele de planificare, veţi învăţa mai multe despre cum să manipulaţi securitatea Companiei JKL Toy.

Subiectul ″Paşi în procesul de planificare″ explică fiecare dintre paşii pe care trebuie să îi urmaţi când planificaţi securitatea sistemului.

Paşi în procesul de planificare a securităţii

Următoarea diagramă descrie fiecare pas în procesul de planificare şi cum sunt relaţionaţi paşii referitor la restul procesului.

Tabela 2. Paşi în procesul de planificare a securităţii

Pas	Ce aveţi de făcut la acest pas	Cum sunt relaţionaţi paşii între ei
Planificarea securităţii fizice	Descrie cum puteţi planifica securitatea pentru a proteja sistemul, dispozitivele şi mediul de stocare.	Cele mai multe dintre aceste informaţii sunt independente de restul procesului. Nu puteţi introduce în sistem informaţii de planificare a securităţii fizice; oricum aveţi nevoie de câteva din aceste informaţii pentru a planifica valorile sistem şi securitatea resurselor.
Planificarea aplicatiei	Descrie scopul, meniurile principale, şi bibliotecile tuturor aplicaţiilor.	Furnizează baza procesului de planificare şi alte decizii de securitate. Nu trebuie să introduceţi aceste informaţii în sistem.
Planificarea abordării generale	Deciderea abordării generale care va fi securizată. Alegerea valorile sistem care sunt suportate de acea abordare.	Folosiţi informaţiile de planificare a aplicaţiei pentru a vă ajuta să determinaţi abordarea generală. Valorile sistem pe care le-aţi ales afectează modul de planificare al profilurilor urilizator şi grup.
Planificarea grupurilor utilizator	Deciderea modului de împărţire al utilizatorilor în grupuri. Deciderea caracteristicilor şi modului de definire a acestora pentru fiecare grup în sistem.	Folosirea descrierii aplicaţiei pentru a determina grupurile în sistem. Grupurile utilizator pe care le-aţi definit afectează modul de planificare al utilizatorilor individuali în sistem.
Planificarea profilurilor de utilizator individuale	Asignarea fiecărui utilizator sistem la un grup. Definirea fiecărui utilizator, incluzând caracteristicile care îl diferenţiază de restul grupulu. De exemplu, utilizatorii care au nevoie de niveluri de acces diferite la o aplicaţie sau o bibliotecă decât restul grupului.	Folosirea informaţiilor despre planificarea aplicaţiei şi a grupului utilizator vă ajută să definiţi utilizatorii individuali.
Planficarea securităţii resurselor	Deciderea aplicaţiilor care ar trebui să fie valabile pentru orice utilizator din sistem. Dacă aveţi nevoie să restricţionaţi anumite aplicaţii, decideţi utilizatorii şi grupurile care ar trebui să aibă permisiunea să le folosească.	Folosirea informaţiilor despre planificarea aplicaţiei şi a profilurilor de grup vă ajută la planificarea securităţii resurselor.
Planificarea instalării aplicaţiei	Deciderea modului de stabilire a dreptului de proprietate şi autorităţii publice referitor la bibliotecile aplicaţiei.	Folosirea informaţiilor de planificare a securităţii resurselor la planificarea instalării aplicaţiei.

Ar trebui să începeţi procesul de planificare al securităţii prin planificarea securităţii utilizator.

Planificarea securităţii utilizator

Planificarea securităţii utilizator include planificarea tuturor suprafeţelor unde securitatea afectează utilizatorii din sistem. Este esenţial să descrieţi următoarele suprafeţe:

Securitatea fizică

Securitatea fizică se referă la protejarea serverului iSeries faţă de deteriorările accidentale (sau intenţionate) şi faţă de furturi. În plus, aceasta include toate staţiile locale, imprimantele şi spaţiul de stocare. ″Planificarea securităţii fizice″ conţine informaţii suplimentare despre elaborarea planului pentru securitatea fizică, despre riscuri şi despre recomandările IBM.

Securitatea aplicaţiilor

Securitatea aplicaţiilor se referă la aplicaţiile stocate de sistem şi la modul de protejare a acestora cât timp se permite accesul simultan al utilizatorilor la acestea. ″Planificarea securităţii pentru aplicaţii″ furnizează detalii despre descrierea aplicaţiilor şi a convenţiilor de nume.

Strategia generală de securitate

Planificarea generală a securităţii include dezvoltarea unui plan de securitate care consideră ambele situaţii prezente şi vă planifică viitorul de afaceri. ″Planificarea strategiei generale de securitate ″ vă furnizează mai multe informaţii despre determinarea politicilor de securitate, nivelului de securitate, consideraţii despre parolă şi valorile sistem.

Securitatea grupului utilizator

Un grup utilizator este un grup de utilizatori care utilizează aceleaşi aplicaţii în acelaşi mod. Planificarea securităţii grupului utilizator implică determinarea grupurilor de muncă care sunt planificate să folosească sistemul şi aplicaţiile necesare acelor grupuri. ″Planificarea grupurilor utilizator″ furnizează informaţii detaliate despre identificarea grupurilor utilizator, planificarea profilurilor de grup, alegerea valorilor sistem şi determinarea mediului utilizatorului .

Securitatea individuală a utilizatorului

După ce aţi determinat grupurile utilizator de care aveţi nevoie puteţi planifica profilurile de utilizator individuale de care aveţi nevoie. ″Planificarea profilurilor de utilizator individuale″ furnizează mai multe informaţii despre numirea utilizatorilor în sistem, determinarea responsabilităţii utilizatorilor individuali şi alegerea valorilor sistem.

Veţi găsi legături în aceste subiecte de planificare pentru a planifica formulare pe care să le folosiţi la înregistrarea deciziilor de planificare.

Planificarea securităţii fizice

Când vă pregătiţi pentru instalarea serverului iSeries, trebuie să creaţi un plan pentru securitatea fizică, care să ofere răspunsuri următoarelor întrebări:

- Unde veţi pune unitatea sistem?
- Unde veţi localiza fiecare staţie de afişare?
- Unde veţi localiza imprimantele?
- De ce echipamente suplimentare aveţi nevoie, cum ar fi cablarea, linii telefonice, caracteristici sau spaţii de stocare?
- Ce măsuri veţi lua pentru a vă proteja sistemul în cazuri de urgenţă cum ar fi căderea de tensiune?

Securitatea fizică ar trebui să facă parte din planul general de securitate. Trebuie să vă luaţi măsuri specile de securitate pentru protejarea sistemului în funcţie de locul de amplasare al sistemului şi de dispozitivele ataşate lui.

Puteţi folosi formularul de Planificare a Securităţii Fizice pentru a înregistra deciziile în legătură cu securitatea fizică a sistemului. Pentru a vă asigura că acoperiţi toate aspectele ale securităţii fizice revedeţi aceste subiecte:

- Securitatea fizică pentru unitatea sistem furnizează detalii despre securitatea sistemului în sine.
- Securitatea fizică pentru documentaţia sistem şi spaţiul de stocare conţine informaţii despre securitatea documentelor sistem şi spaţiul de stocare.
- Securitatea fizică pentru staţiile de lucru discută moduri de securitate a staţiilor de lucru.
- Securitatea fizică pentru ieşirile imprimantă furnizează detalii despre protejarea fizică a imprimantelor şi ieşirile lor.
- Planificarea politicii de securitate explică modul de pregătire a ghidului utilizator şi a politicii de securitate.

Fiecare unitate sistem are un panou de control cu operaţii speciale sistem de depanare şi performaţă, cum ar fi punerea sau scoaterea sistemul de sub tensiune. Pentru a împidica utilizarea neautorizată a acestor operaţii sistem, fiecare unitate sistem are fie un comutator cheie IPL fie o cheie IPL electronică. Acestea furnizează o oarecare protejare a unităţii sistem, însă comutatorul cheie IPL sau cheia IPL electronică nu reprezintă un înlocuitor pentru securitatea fizică corespunzătoare.

Securitatea fizică pentru unitatea sistem

iSeries nu necesită o cameră de calculator cu elemente speciale de control al mediului. Adesea veţi găsi unitatea sistem în mijlocul biroului, unde multe persoane pot avea acces la el. Beneficiarilor le place dimensiunea redusă a serverului iSeries şi faptul că poate fi întreţinut cu uşurinţă; însă aceste caracteristici pot introduce şi riscuri de securitate. De exemplu, o persoană poate să fure cu uşurinţă unitatea sistem sau să scoată componente valoroase din ea.

Trebuie să vă asiguraţi că unitatea sistem se află într-un loc protejat. Cea mai bună locaţie este o cameră privată, încuiată. Cel puţin unitatea sistem ar trebui să fie plasată într-un loc care se închide din exterior în afara orelor obişnuite ale programului de lucru.

Riscurile unităţii sistem

Pe lânga posibilitatea furtului unităţii sistem sau a componentelor lui, există câteva alte riscuri care apar datorită securităţii fizice inadecvate a unităţii sistem:

Compromiterea neintenţionată a operaţiilor sistem
: Apariţia problemelor de securitate datorită utilizatorilor neautorizaţi ai sistemului. Presupunem că una din staţiile de afişare a sistemului este blocată. Operatorul sistem este plecat la o întâlnire. Utilizatorul staţiei de afişare blocate merge la unitatea sistem, gândind că, ″Poate dacă apăs acest buton, se va corecta problema.″ Acel buton inchide sau reâncarcă sistemul în timp ce se rulează multe joburi. Aveţi nevoie de câteva ore pentru a recupera fişierele actualizate parţial. Puteţi folosi comutatorul cheie IPL a unităţii sistem pentru a împiedica aceasta.

Folosirea funcţiilor uneltelor de service dedicate (DST) ocoleşte securitatea
: Securitatea nu controlează funcţionarea serviciilor de performanţă ale sistemului, deoarece software-ul sistemului nu poate fi operaţional corespunzător cînd trebuie să executaţi aceste funcţii. O persoană care ştie sau obţine ID-ul utilizatorului uneltelor de service poate produce stricăciuni considerabile sistemului. Pentru a învăţa mai mult despre Unelte Service, vedeţi subiectul Unelte Service în Centrul de Informare.

Recomandări

- Ideal ar fi să păstraţi unitatea sistem într-o cameră blocată. Dacă nu faceţi asta, plasaţi unitatea sistem acolo unde nu au acces cei din exterior. În plus, alegeţi o locaţie unde angajaţii responsabili îl pot monitoriza. Următoarele caracteristici ale securităţii fizice vă pot ajuta să protejaţi sistemul de accidente intenţionate:
- Folosiţi cheia sau cheia electronică:
  - Setaţi modul de operare la Normal dacă vreţi să fiţi capabil să porniţi sistemul fară folosirea cheii.
  - Setaţi modul de operare la Auto dacă planificaţi să folosiţi funcţia Automatic Power On/Off pentru pornirea şi oprirea sistemului.
  - Înlăturaţi cheia şi puneţi-o într-un loc sigur.
- Modificaţi ID-ul utilizator şi parola Uneltelor Service (DST) imediat după ce aţi instalat sistemul şi după ce aţi rulat personal uneltele de service. Subiectul Unelte Service de la Centrul de Informare explică detaliat cum se face aceasta.

Puteţi vedea un exemplu de planificare a securităţii unităţii pentru Compania JKL Toy înainte de a planifica securitatea fizică pentru documentaţia sistemului mediul de stocare.

Exemplu: formularul de planificare securitate fizică la Compania JKL Toy—secţiunea unitate sistem: Mai jos este un exemplu din secţiunea unitate sistem din formularul Planificare securitate fizică pe care-l foloseşte Sharon Jones pentru sistemul ei:

Tabela 3. Formularul Planificare securitate fizică pentru Compania JKL Toy: exemplu unitate sistem

Formularul Planificare securitate fizică	
Pregătit de: Sharon Jones	Data: 9/2/99
Unitate sistem:	

Tabela 3. Formularul Planificare securitate fizică pentru Compania JKL Toy: exemplu unitate sistem (continuare)

Descrie măsurile de securitate pentru a vă proteja unitatea sistem (de ex. camere încuiate):	Unitatea sistem se află în zona de contabilitate. În timpul zilei, persoanele de la contabilitate sunt mereu în zonă şi se pot uita la unitatea sistem. Oamenii de la contabilitate sunt responsabili şi pentru numerar mărunt, şi pentru conturi importante. În afara orelor normale de lucru, zona este încuiată.
Ce poziţie a cheii IPL este folosită de obicei?	Normal
Unde este păstrată cheia?	Un mic seif din biroul lui Sharon.
Alte comentarii legate de unitatea sistem:	Unitatea sistem este accesibilă uşor. Menţionaţi persoanelor de la contabilitate că trebuie să se asigure că nu se strecoară persoane străine.

După ce vă planifiaţi securitatea fizică a unităţii de sistem, puteţi planifica securitatea fizică pentru documentaţia de sistem şi mediul de stocare.

Securitatea fizică pentru documentaţia sistemului şi spaţiul de stocare

Un alt aspect al planificării securităţii fizice se ocupă cu stocara documentaţiei sistem importante şi mediul de stocare. Documentaţia sistemului include informaţii IBM trimise cu sistemul, informaţii despre parolă, planificarea formularelor, şi orice rapoarte pe care le generează sistemul.

În funcţie de sistem, mediul de salvare de siguranţă poate include benzi, CD-ROM-uri, dischete sau spaţiu de stocare DVD. Aţi putea stoca documentaţia sistemului şi mediul de salvare de siguranţă atât la birou cât şi într-o locaţie situată la distanţă. În cazul unui dezastru, veţi avea nevoie de aceste informaţii pentru a recupera sistemul. Următoarele informaţii vă sugerează moduri de stocare a documentaţiei sistem şi a mediilor de stocare. După ce aţi decis ce metodă să urmaţi, înregistraţi-vă alegerile în secţiunea Mediul Salvare de Siguranţă şi Documentaţie a formularului Planificare Securitate Fizică.

Stocarea în siguranţă a documentaţiei sistem

Uneltele service şi parolele ofiţerului de securitate sunt critice în operaţiunile sistemului. Ar trebui să vă notaţi aceste parole şi să le păstraţi într-un seif, într-o locaţie confidenţială. În plus, păstraţi o copie a acestor parole într-o locaţie externă pentru a vă ajuta la recuperare sistemului în cazul unui dezastru.

De asemenea, păstraţi într-o locaţie externă sigură şi alte documentaţii sistem importante cum ar fi setările de configurare şi bibliotecile aplicaţiilor principale pentru a vă ajuta la recuperarea sistemului în cazul unui dezastru .

Depozitarea în siguranţă a mediilor de stocare

Când instalaţi sistemul, planificaţi salvarea tuturor informaţiilor din sistem în mod regular, pe bandă sau alte medii de stocare. Aceste salvări de siguranţă vă permit să recuperaţi sistemul dacă este necesar. Ar trebui să păstraţi aceste salvări de siguranţă într-o locaţie externă sigură.

Riscuri

- Stricăciuni la mediul de stocare a salvării de siguranţă: Dacă un dezastru sau un act de vandalism distruge salvarea de siguranţă, nu puteţi recupera informaţiile care erau în sistem cu excepţia rapoartelor tipărite.
- Furtul salvării de siguranţă sau a parolelor: Puteţi avea informaţii de afaceri confidenţiale salvate pe mediul de stocare a salvării de siguranţă. Un cunoscător poate fi capabil să restaureze aceste informaţii pe un alt calculator şi să le tipărească sau să le proceseze.

Recomandări

- Depozitaţi toate parolele şi mediile de stoacare a salvărilor de siguranţă într-un birou securizat, blocat.

- Pentru a vă asigura duce-ţi copii ale salvărilor de siguranţă într-o locaţie externă în mod regular, de exemplu cel putin săptămânal.

Puteţi vedea un exemplu cu planul de depozitare a documentaţiei de sistem a Companiei JKL Toy înainte de a planifica securitatea fizică pentru staţiile de lucru.

Exemplu: Formularul Planificare securitate fizică al Companiei JKL Toy — secţiunea mediu de stocare de rezervă şi documentaţie: Sharon Jones de la Compania JKL Toy a completat secţiunea Mediu de salvare de rezervă şi documentaţie a formularului Planificare securitate fizică după cum se arată în tabelul de mai jos:

Tabela 4. Formularul Planificare securitate fizică pentru Compania JKL Toy: Exemplu de mediu de stocare pentru copii de rezervă şi documentaţie

Formularul Planificare securitate fizică	
Pregătit de: Sharon Jones	Data: 9/2/99
Mediu de stocare de rezervă şi documentaţie:	
Unde sunt păstrate benzile de rezervă la sediul firmei?	Într-un seif mare, anti-foc.
Unde sunt păstrate benzile de rezervă în afara sediului firmei?	Într-un seif mare anti-foc la biroul contabilului firmei.
Unde sunt păstrate parolele pentru responsabilul cu securitatea, parolele de service şi DST?	Cu cifru secret în biroul lui John Smith.
Unde este păstrată documentaţia importantă de sistem, cum ar fi numărul serial şi configuraţia?	Într-un seif mare din altă locaţie, la biroul contabilului.

După ce vă planificaţi securitatea mediului de stocare şi a documentaţiei, puteţi planifica securitatea fizică a staţiilor de lucru.

Planificarea securităţii fizice pentru staţiile de lucru

În cele mai multe cazuri, vreţi ca toţi utilizatorii să fie capabili să semneze pe orice staţie de lucru disponibilă şi să realizeze toate funcţiile autorizate. Totuşi, dacă aveţi staţii de lucru care sunt fie publice, fie private, puteţi să vă luaţi măsuri de precauţie. De exemplu, staţiile de afişare care pot memora apăsările de taste şi calculatoarele personale necesită consideraţii speciale. Folosiţi aceasta pentru a vă ajuta să completaţi Partea 2 (Securitatea Fizică a Staţiilor de lucru şi a Imprimantelor) a formularului Planificarea Securităţii Fizice.

Riscurile asociate cu staţiile de lucru

Folsirea unei staţii de lucru într-o locaţie publică în scopuri neautorizate

Dacă persoane din exteriorul companiei pot accesa locaţiile uşor, acestea ar putea vedea informaţiile confidenţiale. Dacă un utilizator de sistem părăseşte o staţie de lucru pe care a semnat, o persoană străină poate fi capabilă să acceseze informaţii confidenţiale.

Folosirea unei staţii de lucru într-o locaţie privată în scopuri neautorizate

O staţie de lucru localizată într-o locaţie privată îi oferă unui intrus oportunitatea de a petrece mai multe ore încercând să dejoace securitatea sistemului fără a fi observat.

Folosind funcţiile playback sau un program de semnare pe PC pe o staţie de afişare puteţi dejuca măsurile de securitate

Multe staţii de afişare au funcţii de înregistrare şi playback, care permit utilizatorilor să memoreze tastele folosite frecvent şi să le repete apăsând o singură tastă. Dacă folosiţi un calculator personal ca staţie de lucru a sistemului iSeries, puteţi scrie un program care să automatizeze procesul de semnare. Deoarece utilizatorii folosesc în mod frecvent procesul de semnare, ei pot decide să stocheze propriul ID-ul de utilizator şi parolele, în loc să le tasteze de fiecare dată când semnează.

Recomandări

Consideraţi aceste recomandări când setaţi securitatea fizică pe staţiile de lucru:

- Dacă este posibil, evitaţi plasarea staţiilor de lucru în locaţii publice sau private.

- Subliniaţi utilizatorilor sistemului importanţa de a face signoff înainte de a părăsi staţia de lucru. Procedura de signoff ar trebui cuprinsă în politica de securitate a sistemului.
- Subliniaţi că înregistrarea unei parole într-o staţie de afişare sau într-un program PC încalcă securitatea sistemului. Ar trebui să cuprindeţi informaţii despre înregistrarea parolei în politica de securitate a sistemului.
- Luaţi-vă măsuri pentru a împiedica utilizatorii să părăsească staţiile de lucru aflate în locaţii publice fără a face signoff, utilizând valorile de sistem pentru cronometru de inactivitate (QINACTITV şi QINACTMSGQ).
- Limitaţi funcţiile pe care utilizatorii le pot realiza la staţiile de lucru publice prin atribuirea utilizatorilor autorizare limitată la acele staţii de lucru.
- Împiedicaţi utilizatorii cu autorizare de securitate sau service să semneze pe staţii de lucru private. Utilizaţi valoarea de sistem QLMTSECOFR pentru a controla unde semnează un utilizator cu aceste autorizări .
- Restricţionaţi posibilitatea utilizatorilor de a semna pe mai multe staţii de lucru în acelaşi timp. Puteţi utiliza valoarea de sistem QLMTDEVSSN, care limitează sesiunile dispozitivelor pentru a controla unde semnează utilizatorii.

Pentru a avea efect aceste recomandări, vedeţi subiectele ″Alegerea valorilor de sistem care afectează semnarea″ şi ″Planificarea securităţii resurselor pentru staţiile de lucru″ pentru amănunte.

Pentru formularul Planificarea Securităţii Fizice, aveţi nevoie să identificaţi care staţii de lucru sunt predispuse la risc datorită localizării lor fizice. Puteţi să revedeţi exemplul despre cum a planificat securitatea fizică a staţiilor de lucru Sharon Jones, de la Compania JKL Toy.

După planificarea securităţii staţiilor de lucru, puteţi planifica securitatea fizică pentru imprimante şi ieşiri imprimantă.

Securitatea fizică pentru imprimante şi ieşiri imprimantă

O dată pornite informaţiile la tipărire, securitatea sistemului nu poate urmări cine le vede. Pentru a minimiza pericolul de a fi vazute informaţii sensibile de afaceri puteţi securiza imprimantele şi ieşirile imprimantă. De asemena ar trebui să creaţi o politică de securitate care să se potrivească cu tipărirea informaţiilor confidenţiale de afaceri.

Riscurile asociate cu imprimantele şi ieşirile imprimantă

Următoarele riscuri pot fi aplicate situaţiei dumneavoastraă de afaceri. Există riscuri de securitate comune care sunt asociate cu imprimanta şi ieşirea imprimantă. Totuşi, ar trebui investigate şi alte riscuri care se pot aplica situaţiilor specifice afacerii dumneavoastră.

- O imprimantă localizată într-un loc public poate oferi accesul utilizatorilor neautorizaţi la informaţii confidenţiale.
- Ieşirea imprimantă rămasă pe suprafaţa de lucru poate dezvălui informaţii.
- Sistemul poate avea ataşate numai una sau două imprimante. Puteţi tipări informaţii de valoare sau confidenţiale, cum ar fi ordine de plată pe care angajaţii companiei ar trebui să le vadă.

Recomandări

Următoarele recomandări vă pot ajuta să diminuaţi riscurile de securitate asociate cu imprimantele şi ieşirile lor.

- Subliniaţi utilizatorilor sistemului importanţa protejării confidenţialităţii ieşirilor. Includeţi deciziile de securitate fizică cu privire la imprimante în politica de securitate.
- Evitaţi localizarea imprimantelor în locuri publice.
- Programaţi tipărirea ieşirilor de inaltă confidenţialitate şi să aveţi la imprimantă o persoană autorizată cât timp sunt printate aceste ieşiri.

″Planificarea securităţii pentru imprimante şi ieşiri imprimantă″ discută sugestii pentru tratarea ieşirilor imprimantă confidenţiale.

Puteţi să vedeţi un exemplu de planificare a securităţii imprimantei al Companiei JKL Toy înainte de a începe să planificaţi propria politică de securitate.

Exemplu: Formularul Planificare securitate fizică al Companiei JKL Toy — secţiunea staţii de lucru şi imprimante: Mai jos este un exemplu din Partea 2 din Planul de securitate fizică pe care îl foloseşte Sharon Jones pentru Compania JKL Toy:

Tabela 5. Exemplu Formular securitate fizică la Compania JKL Toy: Staţii de lucru şi imprimante

Formularul Planificare securitate fizică			Partea 2 din 2
Securitatea fizică pentru staţii de lucru şi imprimante			
Nume staţie de lucru sau imprimantă	Locaţie sau descriere	Expunere de securitate	Măsuri de protecţie de luat
DSP06	Docuri de încărcare	Prea public	Anulare automată semnare. Limitaţi funcţiile care pot fi efectuate de la staţia de lucru.
DSP09	Biroul de serviciu clienţi	Prea public	Anulare automată semnare. Limitaţi funcţiile care pot fi efectuate de la staţia de lucru.
RMT12	Birou de vânzare la distnaţă	Prea privat	Nu permiteţi semnarea responsabilului cu securitatea de acolo.
PRT02	Contabilitate, lângă unitatea sistem	Informaţii sensibile, cum ar fi listele cu preţuri, ar putea fi văzute	Desemnaţi pe cineva să monitorizeze ieşirea de la imprimantă

După ce aţi terminat formularul Planificare securitate fizică, continuaţi cu subiectul″Planificare politică de securitate.

Planificarea politicii de securitate

Este folositor să trimiteţi indicaţii despre securitatea tuturor angajaţilor pentru a asigura politicile de securitate privind securitatea fizică şi securitatea sistemului. Puteţi obţine aceleaşi indicaţii pentru noii utilizatori care sunt adăugaţi la sistem mai târziu.

În aceste indicaţii, puteţi include câteva instrucţiuni generale despre modul de protejare a securităţii sistemului, cum ar fi facerea de signoff pe staţiile de lucru şi nepartajarea parolelor. De asemenea indicaţiile ar putea include informaţii despre anumite decizii pe care le-aţi luat în legătură cu securitatea.

Aşa cum aţi citit în aceste informaţii de planificare, notaţi-vă ce indicaţii de securitate ar trebui incluse. De asemenea, dacă doriţi luaţi notiţe pentru politica de securitate.

De exemplu, Sharon Jones de la Compania JKL Toy a făcut notificări în lăgătură cu planificarea securităţii fizice a sistemului în aceste informaţii de securitate:

```
Aveţi grijă să subliniaţi cât este de important să se facă signoff pentru
compartimentele rampă de aprovizionare, service beneficiari
şi birourile de vînzări la distanţă. Personalul de la contabilitate poate privi unitatea
sistem.
```

După ce aţi completat formularulPlanificarea Securităţii Fizice, sunteţi pregătit să planificaţi securitatea aplicaţiilor.

Planificarea securităţii aplicaţiilor

Pentru a planifica securitatea aplicaţiilor corect, trebuie să ştiţi:

- Ce informaţii planificaţi să stocaţi în sistem?
- Cine trebuie să acceseze acele informaţii?
- Care este tipul de acces de care au nevoie persoanele? Trebuie să modifice informaţii sau doar să le vizualizeze?

Parcurgând aceste subiecte de planificare a aplicaţiilor, răspundeţi la prima întrebare despre tipul informaţiilor pe care planificaţi să le stocaţi în sistem. În subiectele următoare, puteţi decide persoanele care au nevoie de acele informaţii şi tipul de acces necesar. Nu introduceţi în sistem informaţii de planificare a aplicaţiilor; totuşi, veţi avea nevoie de ele când setaţi securitatea utilizatorilor şi a resurselor.

Ce este o aplicaţie?

În primul pas de planificare a securităţii aplicaţiilor, trebuie să descrieţi aplicaţiile care vor rula pe sistem. O aplicaţie este un grup de funcţii grupate logic împreună. De exemplu, la Compania JKL Toy, introducerea ordinelor, expedierea ordinelor şi tipărirea facturilor fac parte dintr-o aplicaţie numită Procesarea Ordinelor.

De obicei, pe iSeries pot rula două tipuri diferite de aplicaţii:

- **Aplicaţii de afaceri**: Aplicaţii pe care le cumpăraţi sau le dezvoltaţi pentru a realiza diferite funcţii de afaceri, cum ar fi procesarea ordinelor sau gestiunea inventarului.
- **Aplicaţii speciale**: Aplicaţii furnizate să fie folosite în companie pentru a realiza o varietate de activităţi care nu sunt specifice procesului de afaceri.

De ce formulare aveţi nevoie?

Folosirea următoarelor formulare vă ajută să planificaţi securitatea aplicaţiilor:

- Formular Descriere Aplicaţie
- Formular Descriere Bibliotecă
- Formular Conventie de Nume

Pentru a tipări aceste formulare, apăsaţi legătura, selectaţi cadrul din dreapta şi apoi apăsaţi iconiţa **Tipărire** în browser.

Citiţi următoarele informaţii pentru a vă ajuta să completaţi aceste formulare de planificare.

- Descrierea aplicaţiilor
- Descrierea convenţiilor de nume
- Descrierea informaţiilor bibliotecii
- Trasarea diagramei unei aplicaţii

Descrierea aplicaţiilor

La acest pas, trebuie să obţineţi informaţii generale despre fiecare dintre aplicaţiile de afaceri. Aăugaţi informaţiile despre aplicaţie în câmpurile corespunzătoare din formularul Descriere Aplicaţie aşa cum este descris mai jos. Mai târziu puteţi folosi aceste informaţii pentru a vă ajuta la planificarea securităţii grupurilor utilizator şi a aplicaţiilor:

Nume aplicaţie şi abrevieri
: Daţi aplicaţiilor nume scurte şi o abreviere pe care să o folosiţi ca prescurtare în formulare şi la numirea obiectelor pe care le foloseşte aplicaţia.

Descriere informaţii
: Descriererea pe scurt a aplicaţiei.

Meniul şi biblioteca primară
: Identificaţi meniul primar pentru accesarea aplicaţiei. Indicaţi biblioteca în care apare meniul. De obicei meniul primar încarcă alte meniuri cu funcţii specifice ale aplicaţiei. Utilizatorii preferă să vadă meniul primar pentru aplicaţia principală imediat după semnarea pe sistem.

Programul iniţial şi biblioteca
: Câteva aplicaţii rulează un program iniţial care setează informaţii de fundal pentru utilizator sau verifică securitatea. Dacă o aplicaţie are un program iniţial sau un program de setare, treceţi-l în formular.

Bibliotecile aplicaţiei
: Fiecare aplicaţie are de obicei o bibliotecă principală pentru fişiere. Include-ţi toate bibliotecile pe care

aplicaţia le utilizează, incluzând bibliotecile de programe şi bibliotecile proprii altor aplicaţii. De exemplu, aplicaţia comenzi clienţi a Companiei JKL Toy foloseşte o bibliotecă inventar pentru a obţine elemente de bilanţ şi de prezentare.

Puteţi folosi relaţionările între biblioteci şi aplicaţii pentru a determina cine are nevoie de acces la fiecare bibliotecă.

Găsirea informaţiilor despre aplicaţii

Dacă încă nu ştiţi informaţiile despre aplicaţii de care aveţi nevoie, puteţi contacta programatorul sau furnizorul aplicaţiei.

Urmărirea este metoda de obţinere a informaţiilor personal, dacă nu aveţi acces la aceste informaţii despre o aplicaţie care rulează pe sistem.

- Utilizatorii unei aplicaţii vă pot spune probabil numele bibliotecii şi al meniului primar sau îi puteţi asista la semnarea pe sistem.
- Dacă utilizatorii văd aplicaţia imediat după semnare, uitaţi-vă în câmpul **Program iniţial** în profilul de utilizator. Acest câmp conţine programul iniţial al aplicaţiei. Puteţi folosi comanda DSPUSRPRF pentru a obţine programul iniţial.
- Puteţi afişa numele şi descrierile tuturor bibliotecilor din sistem. Folosiţi DSPOBJD *ALL *LIB. Aceasta afişează toate bibliotecile din sistem.
- Puteţi observa joburile active cât timp utilizatorii rulează aplicaţia. Utilizaţi comanda WRKACTJOB (Work with Active Job) cu nivel de ajutorare intermediar pentru a obţine informaţii detaliate despre joburile interactive. Puteţi afişa joburile şi arunca o privire la bibliotecile cu obiectele lor listate pentru a găsi bibliotecile care sunt utilizate.
- Puteţi afişa joburile batch într-o aplicaţie folosind comanda WRKUSRJOB (Gestionare joburi utilizator).

Pentru a vă asigura că aţi obţinut toate informaţiile de care aveţi nevoie pentru a planifica securitatea aplicaţiilor, ar trebui să completaţi aceste operaţii înainte de a continuare:

- Completaţi un formular Descriere Aplicaţie pentru fiecare dintre aplicaţiile de afaceri. Completaţi întregul formular, cu excepţia secţiunii cerinţelor de securitate. Veţi utiliza această secţiune pentru a planifica securitatea resurselor pentru aplicaţie aşa cum a fost descrisă în subiectul ″Planificarea securităţii resurselor″.
- Pregătirea unui formular Descriere Aplicaţie pentru fiecare aplicaţie specială, dacă este posibil. Utilizarea formularului vă ajută să determinaţi modul de furnizare al accesului la aplicaţie.

Notă: Pregătirea formularelor Descriere aplicaţie pentru aplicaţii IBM speciale, cum ar fi IBM Query pentru iSeries, este opţională. Accesul la bibliotecile folosite de aceste aplicaţii nu necesită nici o planificare specială. Totuşi, puteţi găsi folositor să obţineţi informaţii şi să pregătiţi formularele.

Puteţi să vedeţi un exemplu de formular Descriere Aplicaţie al Companiei JKL Toy înainte de trece la descrierea convenţiilor de nume.

Exemplu: Formular descriere aplicaţie la Compania JKL Toy: Sharon Jones a listat toate aplicaţiei companiei şi abreviaţiile lor în formularul Descriere aplicaţie. De asemenea, ea a descris pe scurt modul în care utilizatorii lucrează cu aceste aplicaţii.

Customer Orders (CO)
Introduce, urmăreşte şi livrează comenzi. Tipăreşte facturi.

Inventory Control (IC)
Administrează inventarul pentru produsele finite şi materiale. Procesează toate tranzacţiile de inventar.

Contract and Pricing (CP)
Administrează preţurile speciale şi contractele cu clienţii.

Accounts Receivable (AC)
Ţine balanţele curente. Tipăreşte declaraţiile lunare.

Tabelul de mai jos conţine descrierea lui Sharon Jones a aplicaţiei Customer Order. Ea şi-a pregătit formularele sistematic, începând cu o aplicaţie, apoi continuând cu restul.

Tabela 6. Formular descriere aplicaţie la Compania JKL Toy: exemplu

formular Descriere aplicaţie	
Pregătit de: Sharon Jones	Data: 9/3/99
Nume aplicaţie: Customer Orders	Abreviaţe: CO
Scurtă descriere a aplicaţiei:	Introduce comenzi client, le urmăreşte înainte de livrare, livrează comanda şi tipăreşte facturile şi hârtiile de livrare.
Nume meniu principal: COMAIN	Bibliotecă: COPGMLIB
Nume program iniţial: NA	Bibliotecă: NA
Listare biblioteci utilizate de aplicaţie pentru fişiere şi programe: • CUSTLIB • ITEMLIB • CONTRACTS • COPGMLIB	
Definire obiective de securitate pentru aplicaţie, cum ar fi dacă vreo informaţie este confidenţială:	

În plus faţă de aplicaţia Customer Order, Sharon Jones a pregătit de asemenea formulare descriere aplicaţie pentru următoarele aplicaţii de pe sistemul Companiei JKL Toy:

- Inventory Control
- Contracts and Pricing
- Accounts Receivable.

În continuare, puteţi descrie convenţiile de nume pentru obiectele din sistem.

Descrierea convenţiilor de nume

Când cunoaşteţi modul în care sistemul numeşte obiectele, puteţi planifica şi monitoriza securitatea, rezolva probleme, şi planifica salvările de siguranţă şi recuperare. Cele mai multe aplicaţii au reguli pentru asignarea numelor obiectelor cum ar fi biblioteci, fişiere şi programe. Dacă aplicaţiile vin din surse diferite, probabil fiecare aplicaţie are propriul sistem de nume.

Asiguraţi-vă că aţi înregistrat toate convenţiile de nume ale aplicaţiilor şi obiectelor în formularulConvenţii de Nume. În formularul Convenţii de Nume, treceţi regulile folosite de aplicaţii pentru numirea bibiliotecilor şi fişierelor. Puteţi să folosiţi spaţiul pentru alte convenţii de nume, cum ar fi programe şi meniuri. Dacă aplicaţiile vin din surse diferite, probabil fiecare are o convenţie unică de nume. Descrierea convenţiilor de nume pentru fiecare aplicaţie. Trebuie să pregătiţi mai mult de un formular Convenţii de nume.

Puteţi vedea un exemplu despre modul în care Sharon foloseşte convenţiile de nume pentru obiecte în sistemul Companiei JKL Toy înainte de a trece la informaţii descriere bibliotecă.

Exemplu: Formular convenţie de nume la Compania JKL Toy: Tabelul de mai jos arată numai convenţiile de nume pentru biblioteci şi fişiere. Va trebui să descrieţi convenţiile de nume şi pentru alte tipuri de obiecte din sistem. Formularul convenţii de nume conţine câteva obiecte obişnuite; totuşi, este posibil să mai aveţi şi alte tipuri de obiecte pe care trebuie să le pregătiţi.

Tabela 7. Formular convenţii nume la Compania JKL Toy: exemplu

Formular convenţii nume	
Pregătit de: Sharon Jones	Data: 9/3/99
Tip obiect	**Convenţe nume**

Tabela 7. Formular convenţii nume la Compania JKL Toy: exemplu (continuare)

Biblioteci	Bibliotecile care conţin fişiere au nume sugestive, cum ar fi CONTRACTS sau ITEMLIB. Bibliotecile program folosesc abreviaţia aplicaţiei urmat de PGMLIB, de exemplu ICPGMLIB.
Fişiere	Fişierele importante au nume sugestive, cum ar fi CUSTMAST pentru fişierul Customer Master sau ITEMMAST pentru fişierul Item Master. Alte fişiere de aplicaţie (folosite pentru motive cunoscute numai de programatori) au numele de forma abreviaţia aplicaţiei urmată de FILE şi de un număr, de exemplu ICFILE14.

După ce aţi completat Formular convenţie nume, puteţi începe să descrieţi informaţiile din bibliotecă.

Informaţii descriere bibliotecă

După ce aţi descris convenţiile de nume, ar trebui să descrieţi bibliotecile din sistem. Bibliotecile identifică şi organizează obiectele din sistem. Punerea fişierelor asemănătoare împreună într-o bibliotecă permite utilizatorilor accesul mai uşor la fişierele şi aplicaţiile critice. De asemenea puteţi personaliza autorizările utilizatorilor, astfel încât aceştia să poată accesa doar unele biblioteci. Descrierea bibliotecilor care sunt în sistem pentru fiecare aplicaţie. Puteţi avea nevoie să pregătiţi mai mult de un formular Descriere Bibliotecă

Notă: Completaţi numai informaţiile de descriere despre bibliotecă. Când planificaţi securitatea resurselor pentru bibliotecă veţi completa ceea ce a rămas din formularul Descriere bibliotecă. Veţi avea nevoie să adăugaţi informaţii despre autorizări bibliotecă mai târziu. Vedeţi ″Planificarea securităţii pentru bibliotecile aplicaţiei″ pentru detalii despre completarea a ceea ce a rămas din formularul Descriere Bibliotecă.

Înainte de a continua, asiguraţivă că aţi completat următoarele:

- Completaţi părţile fişier şi bibliotecă a formularului Convenţii de nume.
- Completaţi informaţii descriptive în formularul Descriere Bibliotecă pentru fiecare bibliotecă aplicaţie.

Puteţi vedea un exemplu despre modul cum Sharon Jones de la Compania JKL Toy a descris bibliotecile înainte de a trasa diagrama aplicaţiei.

Exemplu: Formular descriere bibliotecă la Compania JKL Toy: Cele două tabele de mai jos descriu două biblioteci folosite de aplicaţia Customer Orders la Compania JKL Toy. Primul tabel descrie o bibliotecă cu fişiere, al doilea descrie o bibliotecă cu programe.

Tabela 8. Exemplu Formular descriere bibliotecă la Compania JKL Toy: bibliotecă cu fişiere

formular Descriere bibliotecă	
Pregătit de: Sharon Jones	Data: 9/3/99
Nume bibliotecă: CUSTLIB	Nume descriptiv (text): Biblioteca înregistrări client
Descriere pe scurt a funcţiei acestei biblioteci:	Păstrează toate fişierele clienţi, inclusiv comenzi şi date cont.

Tabela 9. Exemplu Formular descriere bibliotecă la Compania JKL Toy: bibliotecă cu programe

formular Descriere bibliotecă	
Pregătit de: Sharon Jones	Data: 9/3/99
Nume bibliotecă: COPGMLIB	Nume descriptiv (text): Bibliotecă programe Customer Order
Descriere pe scurt a funcţiei acestei biblioteci:	Păstrează toate programele pentru aplicaţia de comenzi clienţi.

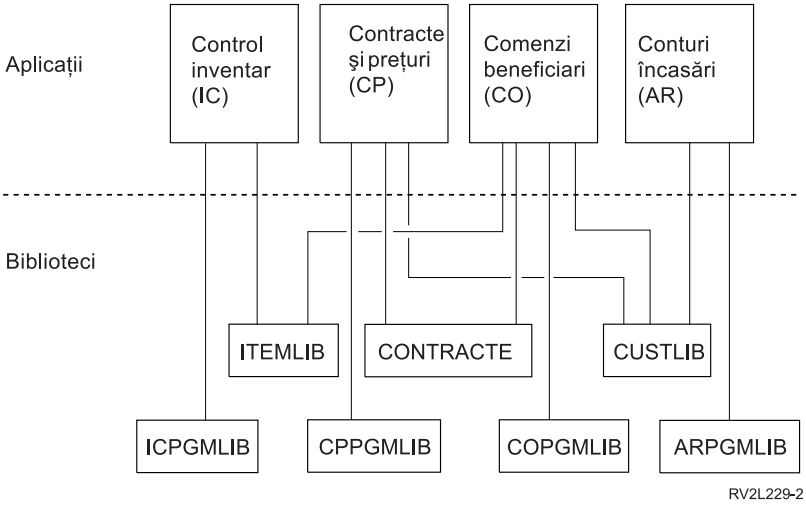
După ce vă descrieţi bibliotecile, ar trebui să desenaţi diagrama aplicaţiilor pentru sistemul dumneavoastră.

Trasarea diagramei unei aplicaţii

Când pregătiţi formularele de Descriere Aplicaţie şi Descriere Bibliotecă, puteţi găsi folositor să trasaţi o diagramă care să arate relaţia dintre aplicaţii şi biblioteci. O diagramă vă va ajuta să planificaţi grupurile utilizator şi şi securitatea resurselor.

Figura de mai jos arată diagrama aplicaţiilor şi bibliotecilor pe care a trasat-o Sharon Jones de la Compania JKL Toy:

Diagrama aplicaţiilor şi bibliotecilor companiei JKL Toy



Colectarea câtorva informaţii despre aplicaţiile şi bibliotecile dumneavoastră vă va ajuta în multe decizii de securitate pe care le veţi lua. Priviţi aceasta ca o şansă de a deveni mai informaţi despre aplicaţiile şi sistemul dumneavoastră.

Pentru a vă asigura că aţi obţinut informaţiile despre aplicaţie de care aveţi nevoie, ar trebui:
- Să completaţi un formular de Descriere Aplicaţie pentru fiecare aplicaţie de afaceri din sistem.
- Opţional, pregătiţi un formular Descriere Aplicaţie pentru fiecare aplicaţie specială din sistem.
- Completaţi secţiunile fişier şi bibliotecă ale formularului Convenţii de Nume.
- Pregătiţi un formular Descriere Bibliotecă pentru fiecare bibliotecă aplicaţie.
- Trasaţi o diagramă a relaţiilor dintre aplicaţii şi biblioteci.

Când aţi completat aceste formulare, puteţi începe planificarea generală a strategiei de securitate.

Planificarea generală a strategiei de securitate

După ce aţi planificat securitatea pentru aplicaţii, sunteţi pregătit să stabiliţi strategia generală de securitate. Mai întâi, trebuie să luaţi decizii în legătură cu abordarea generală a securităţii în sistem. După ce aţi luat aceste decizii, echilibraţi nevoile companiei de azi cu nevoile companiei în viitor.

Folosiţi aceste informaţii pentru a vă ajuta în procesul de planificare să determinaţi obiectivele şi politica de securitate. De asemenea, puteţi folosi aceste informaţii pentru a vă ajuta la alegerea valorilor sistem elementare care afectează toţi utilizatorii din sistem.

De ce formulare aveţi nevoie?

Pentru a efectua planificarea aplicaţiilor, folosiţi formularul Selecţia valorilor sistem.

Ar trebui să revedeţi subiectele din formularele terminate Planificare Securitate Fizică şi Descriere Aplicaţie pentru a lua deciziile în legătură cu valorile sistem.

Revedeţi aceste subiecte pentru a planifica strategia de securitate:

- Scrierea politicii de securitate
- Alegerea nivelului de securitate
- Alegera valorilor sistem care afectează semnarea
- Alegera valorilor sistem care afectează parolele
- Utilizarea valorilor sistem pentru a personaliza sistemul

Scrierea politicilor de securitate

Înainte de a începe planificarea, pregătiţi o declaraţie cu politicile companiei cu privire la securitatea sistemului. Această declaraţie este un angajament între dumneavoastră şi oficialii companiei. Ea vă ajută să luaţi decizii şi să determinaţi ceea ce este important. Politica de securitate ar trebui să arate care este abordarea generală şi ce informaţii necesită protecţie.

Fiecare sistem trebuie să aibă securitate. Puteţi adopta una din aceste abordări pentru stabilirea securităţii:

- **Strict**: Unele persoane numesc aceasta nevoia de a şti schema de securitate. Într-un mediu strict de securitate, oferiţi utilizatorilor acces doar la acele informaţii şi funcţii de care au nevoie în munca lor. Accesul este exclus la alte informaţii. Mulţi auditori recomandă o adordare strictă.
- **Medie**: O abordare medie a securităţii oferă utilizatorilor accesul la obiecte, bazat pe autorizările pe care i le-aţi asignat.
- **Relaxată**: O abordare relaxată a securităţii, vă permite să autorizaţi accesul utilizatorilor la cele mai multe obiecte din sistem. Restricţionaţi accesul în cazurile unor resurse critice şi confidenţiale, departamentele sau companiile mici folosesc abordarea relaxată pentru sistemele lor.

Abordarea generală vă ajută la luarea deciziilor în legătură cu nevoile speciale de securitate. Abordarea securităţii pentru sistem ar trebui să se potrivească cu filozofia accesului la informaţii în companie. Dacă nu sunteţi sigur ce abordare să folosiţi, încercaţi aceasta:

- Folosiţi formularul completat Descriere Aplicaţie pentru a determina cine ar trebui sau nu ar trebui să aibă acces la acele aplicaţii.
- Examinaţi tehnologiile folosite în companie. De exemplu, dacă planificaţi să conectaţi sistemul sau reţeaua la Internet, veţi dori un mediu de securitate mult mai restrictiv pentru a proteja sistemul de utilizatori Internet externi.
- Discutaţi cu alţi membrii ai organizaţiei, cum ar fi auditorii de securitate, pentru a determina cât mai bine nevoile de securitate.

Amintiţi-vă că puteţi modifica oricând politica de securitate. Cele mai multe companii observă că nevoile de securitate devin din ce în ce mai stricte pe măsură ce se dezvoltă. Aceste informaţii vă ajută să setaţi o schemă de securitate care să vă permită să adăugaţi noi restricţii fără a face multe modificări sau a testa din nou toate aplicaţiile.

Ce aveţi de asigurat

În plus la abordarea generală a securităţii în politica de securitate, trebuie să identificaţi informaţiile de preţ ale companiei. Sistemul de securitate ar trebui să fie proiectat pentru a proteja aceste informaţii. Puteţi folosi mai multe cerinţe pentru a determina informaţiile preţioase:

- **Confidenţialitate**: Informaţii care nu sunt în general valabile persoanelor din companie. Ordinul de plată este un exemplu de informaţie confidenţială.
- **Competitivitate**: Informaţii care vă oferă avantaj într-o competiţie, cum ar fi formule şi specificaţii de produs.
- **Operaţionale**: Informaţii de pe calculatorul destinat operaţiunilor zilnice ale afacerii, cum ar fi înregistrări client şi balanţa inventarului.

Sharon Jones, ofiţerul de securitate, şi John Smith, preşedintele companiei, muncesc împreună pentru a pregăti o declaraţie a politicilor de securitate. John Smith foloseşte aceste notiţe pentru a proiecta politica de securitate a Companiei JKL Toy. Puteţi revedea politica de securitate pe care Compania JKL Toy o trimite tuturor angajaţilor după efectuarea planificării şi setării securităţii. Revizuiţi aceste subiecte ale planificării, luaţi-vă notiţe despre ceea ce vreţi să adăugaţi politicii de securitate.

Tabela 10. Politica de securitate a Companiei JKL Toy: exemplu

Abordare generală Relaxată: Cele mai multe persoane au nevoie de acces la cele mai multe informaţii.
Informaţii critice • Contracte şi preţuri speciale • Ordine de plată • Înregistrările client şi inventar sunt valabile numai angajaţilor companiei.
Reguli generale • Fiecare utilizator sistem va avea un profil utilizator. Utilizatorii nu pot partaja profilurile sau parolele. • Utilizatorii trebuie să-şi modifice parolele la fiecare 60 de zile.

După ce aţi luat notiţe cu privire la politica de securitate, puteţi alege nivelul de securitate.

Alegerea nivelului de securitate

Valoarea sistem QSECURITY vă permite să controlaţi nivelul de securitate dorit în sistem. Pentru a înţelege modul de funcţionare al nivelurilor de securitate gândiţi-vă la modul în care a fost construit sistemul, şi unde încearcă persoanele să intre.

Nivelul 20: Securitate parolă

Dacă selectaţi nivelul 20, aveţi o oarecare protejare. Paznicul de la intrare cere identificarea şi parola secretă. Numai persoanele care îndeplinesc ambele condiţii sunt admise în sistem. Însă o dată intraţi în sistem, utilizatorii pot naviga oriunde şi face orice.

Dacă cineva aude o parolă secretă şi o foloseşte pentru a intra în sistem, nu sunteţi protejaţi deloc.

Nivelul 30: Securitatea parolei şi a resurselor

Nivelul 30 vă oferă tot ce aveţi la nivelul 20, putând controla în plus accesul utilizatorilor la anumite părţi din sistem. Puteţi restricţiona prin parolare unele părţi a sistemului.

Puteţi permite persoanelor care au acces la secţiuni restricţionate să facă ce vor, sau le puteţi cere să facă cereri de informaţii de la programele cu informaţii autorizate. Un intrus care a pătruns folosind parola altcuiva trebuie să treacă peste paznicii din interior pentru a ajunge la secţiunile protejate.

Nivelul 40: Protejarea integrităţii

La nivelul 40, se păstrează protejarea de la nivelul 30, însă sistemul verifică accesul utilizatorilor. Paznicul de la intrare verifică parolele şi înregistrează toţi utilizatorii care intră în cameră.

Nivelul 50: Protejarea avansată a integrităţii

La nivelul 50, paznicul impune un set strict de reguli pentru a preveni cunoscătorii să obţină acces în zone restricţionate prin validarea identităţii tuturor celor care semnează.

Recomandări

iSeries este livrat cu nivelul de securitate 40. Nivelul de securitate 40 este alegerea cea mai bună pentru cele mai multe instalări, chiar dacă politica de securitate este strictă, medie sau relaxată. Dacă alegeţi o abordare relaxată, puteţi seta acces public la cele mai multe resurse din sistem. Utilizând nivelul 40 de securitate de la început, aveţi posibilitatea de a face sistemul mult mai sigur în viitor fără multe modificări.

Dacă aţi cumpărat programe de aplicaţii, verificaţi cu furnizorul aplicaţiei dacă programele au fost testate la nivelul 40. Câteva aplicaţii utilizează operaţii care produc erori la nivelul de securitate 40. Dacă aplicaţiile nu au fost testate la nivelul de securitate 40 sau 50, porniţi-le cu nivelul 30. Folosiţi funcţia jurnal auditare pentru a vedea dacă în istoricul aplicaţiilor apar eşuări. Dacă nu apar, puteţi modifica nivelul de securitate la 40 sau 50.

Nivelul de securitate 50 împiedică să apară pe cele mai multe sisteme evenimentele care nu sunt normale. Sistemul face verificări suplimentare chiar dacă programele rulează pe sistem. Aceste verificări suplimentare pot avea efect negativ asupra performanţei.

După introducerea alegerii nivelului de securitate în formularul Selecţie valori sistem, puteţi alege valori de sistem care afectează semnarea.

Alegerea valorilor de sistem care afectează semnarea

După ce aţi ales nivelul de securitate, puteţi alege ce utilizatori să fie vazuţi pe staţia de afişare şi modul de interacţionare cu sistemul folosind valorile sistem. Veţi avea nevoie să planificaţi aceste valori sistem şi să folosiţi formularul Selectare valori sistem pentru a vă înregistra alegerile.

Tabelul de mai jos descrie valorile sistem utilizate în acest subiect.

Tabela 11. Valorile de sistem iSeries şi descrierile lor

Valoare sistem	**Descriere**
QMAXSIGN	Limitează numărul de încercări consecutive de semnare.
QMAXSGNACN	Specifică acţiunea pe care o întreprinde sistemul dacă se atinge numărul de încercări consecutive de semnare.
QLMTDEVSSN	Determinaţi dacă un utilizator poate semna pe mai multe staţii de lucru cu acelaşi profil de utilizator.
QINACTITV	Determinaţi când sistemul să întreprină o acţiune asupra joburilor inactive.
QINACTMSGQ	Determinarea acţiunilor pe care sistemul să le ia când un job interactiv a devenit inactiv pentru o perioadă de timp specificată de valoarea de sistem QINACTITV.
QDSCJOBITV	Controlaţi dacă şi când sistemul opreşte un job care a fost deconectat temporar.
QLMTSECOFR	Restricţionaţi accesul la anumite dispozitive al responsabilului cu securitatea, cel care are autorizare asupra tuturor obiectelor din sistem.

Limitarea numărului de încercări de semnare (QMAXSIGN şi QMAXSGNACN): Două valori sistem determină de câte ori poate cineva încearca să semneze pe sistem şi acţiunea pe care o ia sistemul în momentul în care s-a atins numărul de încercări permise.

Valoarea de sistem QMAXSIGN reprezintă numărul maxim de încercări de semanre şi limitează numărul de încercări consecutive de semnare eşuate pe care sistemul le permite înainte de a executa o acţiune. O încercare incorectă de semnare înseamnă că cineva încearcă să folosească un profil de utilizator specific fie cu o parolă invalidă, fie cu autorizare necorespunzătoare pentru staţia de lucru.

Valoarea de sistem QMAXSGNACN determină numărul maxim de acţiuni de semnare şi specifică cum să reacţioneze sistemul dacă cineva încearcă de prea multe ori la rând să semneze. Valorile posibile sunt:

1 Împiedicarea oricăror încercări de semnare pentru dispozitive. Aceasta se numeşte dezactivarea dispozitivului. Nimeni nu poate să semneze la un dispozitiv până când o persoană autorizată nu activează dispozitivul folosind comanda WRKCFGSTS. Această opţiune de obicei nu oferă protecţie suficientă, în special când încercările de semnare sunt făcute de la un calculator personal sau de la un calculator aflat la distanţă.

Un operator de sistem sau orice altă persoană cu autorizarea *USE pentru dispozitiv poate face dispozitivul disponibil din nou.

2 Împidicarea oricăror încercări de semnare pentru profilul de utilizator. Aceasta reprezintă dezactivarea profilului de utilizator. Nimeni nu poate semna cu acel profiul de utilizator decât după ce o persoană autorizată activează profilul folosind comanda CHGUSRPRF.

Pentru a activa un profil de utilizator (a-i modifica starea), trebuie să fiţi administrator de securitate cu autorizarea de a folosi profilul de utilizator.

3 Dezactivarea profilului utilizator şi a dispozitivului.

Riscuri şi recomandări

Există persoane rău intenţionate care se distrează ghicind parolele şi pătrunzând în sistem. Limitând numărul încercărilor de semnare permise, limitaţi posibilitatea de a ghici parola.

Valoarea de sistem QMAXSIGN reprezintă numărul maxim de încercări de semnare şi determină câte încercări de semnare permiteţi. Setaţi o valoare destul de mare pentru a evita frustrarea utilizatorilor. Setaţi o valoare mai mică pentru a descuraja introducerile neatente de parolă şi a împiedica un potenţial intrus să încerce ghicirea parolei de prea multe ori. Ar trebui să setaţi valoarea pentru numărul maxim de încercări de semnare pe sistem între 3 şi 5.

Valoarea recomandată pentru numărul maxim de acţiuni de semnare (QMAXSGNACN) este 3, chiar dacă dezactivarea dispozitivului sau a profilului utilizator îi poate incomoda pe utilizatori. O staţie de lucru aflată într-un spaţiu privat poate oferi unui intrus posibilitatea de a încerca mai multe profiluri de utilizator şi diferite combinaţii de parole. Dacă sistemul nu are staţii de lucru expuse riscului din cauza localizării lor, atunci probabil că dezactivarea numai a profilului de utilizator este o protecţie suficientă.

Verificaţi formularul Securitate fizică realizat. Dacă aveţi staţii de lucru în locaţii aflate la distanţă sau utilizatori la distanţă (utilizatori care accesează sistemul printr-o linie telefonică sau conexiuni VPN), atunci puteţi limita încercările de semnare cât mai strict. Asiguraţi-vă că aţi adăugat alegerile pentru QMAXSIGN şi QMAXSGNACN în partea a doua a formularului Selecţie valori sistem.

Puteţi găsi folositor să revedeţi un exemplul care ilustrază modul în care aceste valori de sistem funcţionează împreună pentru a limita încercările de semnare înainte de a alege valorile de sistem care limitează accesul utilizatorilor la o staţie de lucru la un moment dat.

Exemplu: Limitarea încercărilor de semnare: Sharon Jones a limitat încercările de semnare la 3 (QMAXSIGN este 3) şi a ales să dezactiveze atât profilul cât şi dispozitivul dacă limita este depăşită (QMAXSGNACN is 3). Iată ce se poate întâmpla când aceste valori sunt atinse:

1. Roger introduce parola incorect de două ori.
2. După a doua încercare el primeşte un mesaj care îl avertizează că dacă încercarea de semnare eşuează încă o dată îi va fi dezactivat profilul de utilizator.
3. El face o nouă greşeală.
4. Sistemul îi dezactivează profilul de utilizator şi staţia de lucru nu mai afişează un ecran de semnare. Dacă Roger încearcă să semneze pe un alt calculator, el primeşte un mesaj de eroare.
5. Acum este nevoit să îi ceară lui Sharon să îi activeze profilul de utilizator pentru a încerca din nou. De asemenea, Sharon sau operatorul de sistem trebuie să facă disponibilă staţia de lucru a lui Roger. Dacă Roger nu îşi aminteşte parola, Sharon îi poate da o parolă temporar, pe care el trebuie să o modifice când semnează din nou.

În continuare puteţi revedea valoarea de sistem care limitează utilizatorii la o staţie de lucru la un moment dat.

Limitarea utilizatorilor la o staţie de lucru la un moment dat: Valoarea de sistem QLMTDEVSSN (de limitare a sesiunilor de dispozitiv) determină dacă acelaşi utilizator poate să semneze pe mai multe staţii de lucru în acelaşi timp. Valorile posibile sunt:

0 Sistemul permite unui număr nelimitat de utilizatori să semneze în acelaşi timp cu acelaşi profil de utilizator.

1 Un profil de utilizator poate fi folosit doar la un singur dispozitiv la un moment dat. Utilizatorii pot avea mai mult de o sesiune pe acelaşi dispozitiv.

Riscuri şi recomandări

Permiţând utilizatorilor să semneze doar pe o staţie de lucru la un moment dat, promovaţi un comportament corect în ceea ce priveşte securitatea. Comportamentul neglijent creează riscuri de securitate:

- Dacă limitaţi utilizatorii la un singur dispozitiv, descurajaţi partajarea ID-ului de utilizator şi a parolelor. Dacă persoanele partajează ID-ul de utilizator, controlul şi responsabilitatea au de suferit. Nu mai puteţi spune cine ce funcţii îndeplineşte cu adevărat în sistem.
- Utilizatorii trebuie să-şi amintească să anuleze semnarea (să facă signoff) pe o staţie de lucru înainte de a se muta la altă staţie. Staţiile de lucru rămase semnate şi nefolosite reprezintă un risc de securitate.

Setarea recomandată pentru valoarea sistem QLMTDEVSSN este 1, care limitează utilizatorii la un singur dispozitiv. Daţi fiecărui utilizator sistem un ID utilizator şi o parolă unice cu autorizările corespunzătoare, apoi restricţionaţi-i să folosească doar o staţie de lucru la un moment dat. Asiguraţi-vă că aţi completat alegerile pentru QLMTDEVSSN în partea a doua a formularului Selecţii Valori Sistem.

Puteţi începe să planificaţi valorile sistem pentru joburile inactive next.

Planificarea valorilor sistem pentru joburi inactive: Trei valori de sistem funcţionează împreună pentru a determina modul în care acţionează sistemul când un utilizator uită să facă signoff pe o staţie de lucru.

Intervalul de timeout pentru job inactiv (QINACTITV)
Valoarea sistem QINACTITV determină dacă sistemul acţionează în vreun fel când un ecran de semnare este inactiv pentru o anumită perioadă de timp.

Notă: **Inactiv** înseamnă că utilizatorul nu a apăsat tasta Enter sau o tastă funcţională în timpul unui interval specificat.

Coada de mesaje a joburilor inactive (QINACTMSGQ)
Setarea pentru valoarea sistem QINACTMSGQ determină ce să facă sistemul când timpul limită pe care l-aţi specificat în valoarea sistem QINACTITV expiră. Dacă selectaţi ENDJOB, sistemul opreşte orice job care a fost inactiv mai mult timp decât intervalul timeout pe care l-aţi ales pentru QINACTITV. Dacă selectaţi DSCJOB, sistemul deconectează un job inactiv. Dacă specificaţi numele unei cozi de mesaje, sistemul trimite un mesaj de avertizare la aceea coadă când un job a fost inactiv mai mult timp.

Când sistemul **deconectează** un job la o staţie de lucru, el suspendă jobul temporar. Staţia de lucru se întoarce la ecranul de semnare. Joburile deconectate continuă cînd acelaşi utilizator semnează din nou pe aceeaşi staţie de lucru.

Intervalul timeout pentru job deconectat (QDSCJOBITV)
Controlaţi dacă şi când sistemul opreşte un job care a fost deconectat temporar. Joburile pot fi deconectate automat de sistem, ca rezultat a valorilor sistem QINACTITV şi QINACTMSGQ. De asemenea, utilizatorii pot cere ca joburile să fie temporar deconectate folosind o opţiune în meniul Asistent Operaţional sau comanda Deconectare Job (DSCJOB).

Riscuri şi recomandări

Dacă Sharon uită să facă signoff la staţia de lucru înainte de a pleca, John poate să ajungă la staţia de lucru şi să realizeze orice funcţie care îi este permisă ei în sistem.

Ar trebui în mod regulat să faceţi inactive ecranele particulare pentru două motive:
- Aveţi un mediu de securizare strict cu informaţii confidenţiale stocate în sistem.
- Aveţi staţiile de lucru localizate în locuri unde persoanele din exteriorul companiei le pot accesa foarte uşor.

Adesea utilizatorii întrerup normal joburile la staţiile de lucru. Obţineţi avantaje despre modul în care aceste trei valori sistem funcţionează împreună pentru a permite întreruperi normale astfel încât să nu fie afectată securizarea sistemului.

Pentru a elimina aceste riscuri, IBM recomandă folosirea valorilor de sistem QINACTITV, QINACTMSGQ şi QDSCJOBITV împreună, pentru a permite întreruperile activităţii normale şi, în acelaşi timp, protejarea securităţii sistemului.

Joburile inactive interval time-out (QINACTITV): Stabiliţi intervalul suficient de scurt pentru a descuraja părăsirea neanunţată, a staţiilor de lucru, însă nu atât de scurt încât să incomodeze utilizatorii. Este recomandat să setaţi la 30 minute. Când un job a fost inactiv pentru 30 minute, sistemul acţionează aşa cum este specificat în coada de mesaje a joburilor inactive.

Coada de mesaje a joburilor inactive (QINACTMSGQ): Alegeţi deconectare job. Sistemul deconectează orice job care a fost inactiv pentru o perioadă de timp specificată în intervalul timeout pentru joburi inactive. Sistemul supendă jobul şi face signoff pentru ecran. Când acelaşi utilizator semnează din nou, jobul va continua de unde a rămas.

Aceasta este incomod pentru utilizatori, deoarece mai degrabă sistemul suspendă joburile decât să le oprească. Deconectarea unui job inactiv furnizează mai multă protecţie pentru sistem decât oprirea unui job.

Notă: Sistemul nu poate deconecta unele joburi. Dacă sistemul nu poate deconecta un job inactiv, atunci acest job va fi oprit. Aceasta poate cauza pierderea informaţiilor. Setaţi QINACTMSGQ pentru a trimite mesaje cozii de mesaje operator sistem.

Intervalul timeout pentru joburile deconectate (QDSCJOBITV): Încurajaţi utilizatorii sistemului să facă signoff temporar când trebuie să plece de la staţia de lucru pentru o scurtă perioadă de timp şi să-şi termine munca şi să facă signoff pentru o întrerupere mai îndelungată.

Folosiţi QDSCJOBITV pentru a opri joburile deconectate înainte ca sistemul să pornească procesarea de noapte, cum ar fi Curăţare Automată. Setaţi o valoare suficient de mare având în vedere posibilitatea întoarcerii utilizatorului la staţia de lucru, însă destul de scurtă pentru a opri jobul înainte de pornirea procesării de noapte. Alegeţi 300 de minute (5 ore) care oderă destul timp procesării de noapte să se efectueaze fără a interfera cu joburile utilizator.

Notă: Pentru a împiedica doi utilizatori să încerce să modifice aceleaşi informaţii în acelaşi timp, sistemul **blochează** o înregistrare înainte de a o actualiza. Orice blocare de resurse rămâne activă când sistemul deconecatează un job utilizator. În funcţie de proiectarea aplicaţiei şi de numărul de utilizatori din sistem, blocarea poate cauza probleme de performanţă în sistem. Verificaţi cu programatorul sau furnizorul aplicaţiei dacă blocarea poate avea impact asupra performanţelor.

Puteţi să revedeţi un exempludespre cum funcţionează împreună aceste valori sistem pentru a manipula joburile inactive din sistem.

După ce aţi înregistrat deciziile dumneavoastră referitor la joburile inactive în formularul Selecţie Valori Sistem, puteţi decide cum limitaţi locurile unde responsabilul cu securizarea poate semna.

Exemplu: Tratarea joburilor inactive cu valorile de sistem QINACTITV, QINACTMSGQ şi QDSCJOBITV: Să presupunem că aţi setat intervalul de timeout job inactiv (QINACTITV) la 30 minute. Sistemul deconectează joburile inactive (QINACTMSGQ este DSCJOB). Intervalul de timeout job deconectat (QDSCJOBITV) este 300 minute (5 ore). De exemplu, dacă Sharon uită să anuleze semnarea la 9:30 a.m., sistemul îi deconectează jobul la 10:00 a.m. şi va opri jobul al 3:00 p.m.

Adăugaţi opţiunile dumneavoastră pentru valorile sistem QINACTITV, QINACTMSGQ şi QDSCJOBITV în Partea 2 din formularul Selecţie valori sistem.

După ce aţi notat deciziile pentru joburile inactive în formularul Selecţie valori sistem, puteţi decide cum să limitaţi locurile de unde responsabilul cu securtatea poate semna.

Limitarea locurilor unde responsabilul cu securitatea poate semna: Puteţi restricţiona utilizatorii autorizaţi să modifice securitatea controlului şi obiectelor la anumite staţii de lucru. Aceasta împiedică utilizatorii să semneze pe staţii de lucru aflate în locaţii la distanţă fără acordul dumneavoastră. Valoarea de sistem QLMTSECOFR (limitarea responsabilului de securitate) vă permite să faceţi acest lucru. Dacă setaţi QLMTSECOFR la 1, utilizatorii cu autorizarea specială asupra tuturor obiectelor din sistem (*ALLOBJ) sau service (*SERVICE) pot semna doar pe consolele sau staţiile de lucru specificate de dumneavoastră.

QLMTSECOFR restricţionează responsabilul de securitate, utilizatorii cu autorizare asupra tuturor obiectelor din sistem, şi persoanele de service la consolă. Puteţi folosi comanda Acordare Autorizare Obiect (GRTOBJAUT) pentru a da acestor utilizatori acces la alte dispozitive.

Notă: Pentru ca valoarea sistem QLMTSECOFR să funcţioneze, nivelul de securitate al sistemului trebuie să fie 30 sau mai mare.

Riscuri şi Recomandări

Valoarea sistem QLMTSECOFR ar trebui setată la 1. Dacă cineva aude sau ghiceşte parola cuiva cu profil responsabil de securitate, poate să obţină acces la un dispozitiv care să-i permită să deschidă sesiune.

După ce aţi completat alegerile pentru QLMTSECOFR în partea a doua a formularului Selecţie Valori Sistem, puteţi alege valori sistem care afectează parolele.

Alegerea valorilor sistem care afectează parolele

Ar trebui să permiteţi utilizatorilor să-şi asigneze parole, mai degrabă decât să le fie asignate de către ofiţerul de securitate. Când utilizatorii îşi stabilesc parolele de obicei, nu au nevoie să le noteze. Parolele care sunt notate se păstrează de obicei în locuri expuse, apărând riscuri pentru securitatea sistemului.

Sugestie pentru crearea parolelor

Utilizatorii ar putea avea probleme crezând că au parole bune. Sugeraţi această tehnică: Folosiţi o secvenţă uşor de memorat pentru a creea o parolă greu de ghicit. De exemplu, după eliberare puteţi folosi propoziţia ″Pescuitul în 4 Iulie a fost sărac″ pentru a creea parolaJ4FWP.

Mai multe valori sistem reglementează parolele. Puteţi controla cât de des utilizatorii sunt nevoiţi să-şi modifice parolele. De asemenea, puteţi stabili mai multe reguli pentru a împiedica utilizarea parolelor uşor de ghicit. Multe din aceste valori sunt importante pentru organizaţiile mari. Câteva sunt importante pentru oricine.

Folosind o opţiune în meniul ASSIST sau comanda Modificare Parolă (CHGPWD), utilizatorii îşi pot asigna propriile parole. Când utilizatorii îşi modifică parolele, sistemul verifică noua parolă în ciuda valorilor sistem referitoare la parolă. Dacă un utilizator îşi modifică parola folosind comanda CHGUSRPRF, sistemul nu verifică noua parolă în ciuda valorilor sistem referitoare la securitate.

Notă: Dacă aveţi setate valori sistem referitoare la parolă, sistemul nu permite ca noua parolă să aibă acelaşi nume cu a profilului utilizator, chiar dacă folosiţi comanda CHGUSRPRF pentru a seta parola.

Tabelul de mai jos descrie valorile sistem care afectează parolele şi definţiile lor:

Tabela 12. Valorile de sistem iSeries referitoare la parolă

Valoare sistem	Descriere
QPWDEXPITV	Necesită modificarea perolei de către utilizatori după o perioadă specificată.
QPWDMAXLEN	Vă permite să specificaţi lungimea maximă a parolelor.
QPWDMINLEN	Vă permite să specificaţi lungimea minimă a parolelor.
QPWDRQDDIF	Împiedică utilizatorii de a alterna între două parole diferite.

Aceste subiecte furnizează mai multe detalii despre aceste valori sistem referitor la parolă:

- Determinarea duratei de valabilitate a parolei
- Determinarea lungimii parolelor
- Restricţionarea duplicării parolelor

Tipăriţi WRKSYSVAL *SEC la linia de comandă CL şi vizualizaţi informaţii online pentru valori sistem începând cu caracterele QPWD.

Determinarea duratei parolei: Valoarea sistem QPWDEXPITV determină cât de des utilizatorii sunt nevoiţi să-şi modifice parolele.

Sistemul avertizează utilizatorii când parolele se apropie de data de expirare. Dacă o parolă expiră, sistemul anunţă prompt utilizatorul să-şi modifice parola la următoarea semnare.

Recomandări

Utilizatorii ar trebui să-şi modifice periodic parolele. Aceasta descurajează partajarea parolelor cu alţi utilizatori sistem. De asemenea, dacă un utilizator neautorizat învaţă parola cuiva, aceea parolă va funcţiona numai pentru o scurtă de timp. Setaţi lungimea intervalului de timp pentru parolă suficient pentru a evita iritarea utilizatorilor, însă nu prea scurt pentru a furniza o bună securitate. Pentru a evita aceste probleme setaţi intervalul între 45 şi 60 de zile.

După ce aţi introdus alegerea pentru valoarea sistem QPWDEXPITV în partea a doua a formularului Selecţie Valori Sistem, puteţi determina lungimea parolelor.

Determinarea lungimii parolelor: Unor utilizatori nu le place să introducă parola. Dacă îi lăsaţi, ei vor alege o parolă dintr-o literă sau iniţiala numelui. Din nefericire, o parolă scurtă poate fi uşor ghicită de un intrus. Valoarea sistem QPWDMINLEN vă permite să setaţi o valoare minimă a lungimii tuturor parolelor din sistem.

Dacă sistemul comunică cu alte sisteme, utilizatorii pot schimba parolele între două calculatoare. Unele metode de comunicaţie restricţionează parola la maxim 8 caractere. Valoarea sistem QPWDMAXLEN vă permite să specificaţi o lungime maximă pentru parole.

Recomandări

Setaţi lungimea minimă a parolei la 6. Aceasta elimină utilizarea iniţialelor şi încurajează utilizatorii de a fi puţin mai creativi în alegerea parolelor. Setaţi lungimea maximă a parolei la 8 dacă sistemul comunică cu alte sisteme.

După ce aţi introdus valorile sistem alese pentru QPWDMINLEN şi QPWDMAXLEN în partea a doua a formularului Selecţie Valori Sistem, puteţi decide cât de tare să restricţionaţi duplicarea parolelor.

Restricţionarea duplicării parolelor: Comanda Modificare Parolă (CHGPWD) cere ca noua parolă să fie diferită de vechea parolă. Totuşi, utilizatorii pot alterna înainte şi înapoi între două parole diferite în afară de cazul în care folosiţi valoarea sistem QPWDRQDDIF pentru a-i împiedica. Tabela de mai jos arată alegerile pentru valoarea sistem QPWDRQDDIF:

Tabela 13. Valorile pentru valoarea sistem QPDRQDDIF

Valoare	Numărul de parole verificate pentru duplicare
0	0 Duplicarea parolelor este permisă.
1	32
2	24
3	18
4	12
5	10
6	8
7	6
8	4

Recomandări

Folosiţi intervalul de expirare parole şi valorile duplicate pentru parolă pentru a cere ca parolele să fie unice pentru un an. De exemplu, dacă parolele expiră în 60 de zile, selectaţi 7 pentru valoarea sistem QPWDRQDDIF.

După ce aţi introdus alegerea pentru valoarea sistem QPWDRQDDIF în partea a doua a formularului Selecţie Valori Sistem, puteţi decide modul în care să folosiţi valorile sistem pentru a personaliza sistemul.

Folosirea valorilor sistem pentru personalizarea sistemului

iSeries foloseşte valorile de sistem şi atributele de reţea pentru a controla multe alte lucruri în afară de securitate. Sistemul şi programele de aplicaţie folosesc cele mai multe dintre aceste valori sistem şi atribute. Ofiţerul de securitate ar trebui să seteze câteva valori sistem şi atribute de reţea pentru a personaliza sistemul.

Obţinerea unui nume sistem

Folosirea atributului de reţea SYSNAME la asignarea unui nume sistemului. Numele de sistem apare în colţul din dreapta-sus al ecranului de semnare şi în rapoartele de sistem. De asemenea, este folosit la comunicarea sistemului cu alt sistem sau cu calculatoarele personale prin iSeries Access pentru Windows.

Când sistemul comunică cu alte sisteme sau calculatoare personale, numele sistemului identifică şi distinge sistemul în reţea. Calculatoarele schimbă între ele numele sistem ori de câte ori ele comunică. O dată ce aţi asignat un nume sistem, nu ar trebui să îl schimbaţi, deoarece modificarea lui afectează alte sisteme din reţea.

Recomandări

Alegeţi un nume semnificativ şi unic pentru sistem. Chiar dacă momentan nu comunicaţi cu alte calculatoare, puteţi face asta în viitor. Dacă sistemul face parte dintr-o reţea, managerul reţelei vă va spune probabil ce nume sistem să folosiţi.

De exemplu, Sharon Jones la Compania JKL Toy a decis să numească sistemul JKLTOY.

Afişarea orei şi a datei sistemului

Puteţi seta ordinea în care să apară anul, luna, ziua când sistemul tipăreşte sau afişează date. Puteţi de asemenea specifica ce caracter să folosească sistemul între an (A), lună (L) şi zi (Z).

Valoarea sistem QDATFMT determină formatul de dată. Următorul caracter vă arată cum tipăreşte sistemul data, 16 Inunie 2000, pentru fiecare din alegerile posibile:

Tabela 14. QDATFMT (format Dată sistem)

Alegerea dumneavoastră	Descriere	Rezultat
YMD	An, Lună, Zi	00/06/16
MDY	Lună, Zi, An	06/16/00
DZY	Zi, Lună, An	16/06/00
JUL	Dată iuliană	00/168

Notă: Aceste exemple folosesc ca şi separator de dată slash-ul (/).

Valoarea sistem QDATSEP determină ce caracter foloseşte sistemul între an, lună şi zi. Tabela de mai jos vă arată posibilităţile. Folosiţi un număr pentru a specifica alegerea dumneavoastră:

Tabela 15. QDATSEP (separator dată sistem)

Separator caracter	Valoarea QDATSEP	Rezultat
/ (slash)	1	16/06/00
- (liniuţă de despărţire)	2	16-06-00

Tabela 15. QDATSEP (separator dată sistem) (continuare)

Separator caracter	Valoarea QDATSEP	Rezultat
. (punct)	3	16.06.00
, (virgulă)	4	16,06,00
(blanc)	5	16 06 00

Notă: Exemplele de mai sus folosesc formatul DMY.

Valoarea sistem QTIMSEP determină caracterul pe care să-l folosească sistemul pentru a separa orele, minutele şi secundele la afişarea orei. Folosiţi un număr pentru a vă specifica alegerea. Tabela de mai jos vă arată cum poate fi formatată ora 10:30 dimineaţa folosind fiecare valoare:

Tabela 16. QTIMSEP (Separator System Time)

Caracter separator	QTIMSEP	Rezultat
: (două puncte)	1	10:30:00
. (punct)	2	10.30.00
, (virgulă)	3	10,30,00
(blanc)	4	10 30 00

Deciderea numelor dispozitivelor sistem

Sistemul configurează automat orice staţii de afişare sau imprimante pe care le ataşaţi. Sistemul obţine un nume pentru fiecare dispozitiv nou. Valoarea sistem QDEVNAMING determină modul în care numele sunt asignate. Diagrama de mai jos arată modul în care sistemul denumeşte o a treia staţie de afişare şi a doua imprimantă ataşată lui:

Tabela 17. Nume Dispozitiv Sistem

Alegerea dumneavoastră	Format nume	Nume staţie de afişare	Nume imprimantă
1	iSeries	DSP03	PRT02
2	S/36	W3	P2
3	Adresa dispozitivului	DSP010003	PRT010002

Notă: În exemplul de mai sus, staţia de afişare şi imprimanta sunt ataşate de primul cablu.

Recomandări

Folosiţi convenţiile de numire iSeries, exceptând cazurile în care software-ul pe care îl rulaţi necesită numirea S/36. Numele iSeries folosite pentru staţiile de afişare şi imprimante sunt mai uşor de folosit decât numele bazate pe adresa dispozitivului. Numele de staţie de afişare şi de imprimantă apar în câteva ecrane ale Asistentului Operaţional. Numele imprimantei este folosit de asemenea la gestionarea ieşirilor de imprimantă.

După ce sistemul a configurat un nou dispozitiv, folosiţi comanda Change Display Device (CHGDEVDSP) sau comanda Modificare Dispozitiv Imprimantă (CHGDEVPRT) pentru a introduce o descriere semnificativă a dispozitivului. Includeţi în descriere adresa fizică a dispozitivului şi locaţia, cum ar fi *Biroul lui John Smith, linia 1 adresa 6*.

Alegerea imprimantei sistem

Folosiţi valoarea sistem QPRTDEV pentru a asigna imprimanta sistem. Această valoare sistem, profilul utilizatorului, şi descrierea jobului determină imprimantă care foloseşte un job. Jobul foloseşte imprimanta sistem chiar dacă profilul utilizatorului sau descrierea jobului specifică o altă imprimantă.

Recomandări

În mod normal, imprimanta sistem ar trebui să fie cea mai rapidă dintre cele ataşate sistemului. Folosiţi imprimanta sistem pentru rapoarte lungi şi ieşiri sistem.

Notă: Nu veţi şti numele imprimantei până când nu instalaţi şi configuraţi sistemul. Notaţi acum locaţia imprimantei sistem. Completaţi numele imprimantei mai târziu.

Permiteţi afişarea completă a ieşirilor imprimantă

Sistemul furnizează utilizatorilor abilitatea de a găsi propriile ieşiri imprimantă. Ecranul Ieşire Imprimantă vă arată toate imprimările curente sau care sunt în aşteptare. Puteţi de asemenea permite utilizatorilor să vadă o listă completă a ieşirilor imprimantă. Aceste ecran arată când ieşirea este tipărită şi la care imprimantă. Aceasta poate fi folositor la localizarea rapoartelor pierdute.

Funcţia de numărare a joburilor şi valoarea sistem QACGLVL vă permite afişarea completă a ieşirilor imprimantă. Opţiunea *PRINT pentru valoarea sistem QACGLVL vă oferă informaţii despre ieşirile imprimantă terminate şi salvate.

Recomandări

Informaţii despre spaţiul ocupat în sistem de ieşirile imprimantă terminate. Chiar dacă credeţi că utilizatorii vor printa multe rapoarte, probabil nu veţi avea nevoie să furnizaţi această funcţie. Introduceţi NO în formularul Selectare Valori Sistem. Această valoare setează nivelul de numărare al jobului la *NONE.

- Asiguraţi-vă că aveţi declarată o politică de securitate pentru propria companie similară cu a Companiei JKL Toy exemplu pe care l-au pregătit Sharon Jones şi John Smith.
- Asiguraţi-vă ca aţi introdus alegerile pentru valorile sistem în formularul Selectare Valori Sistem.
- Notaţi-vă ce ar fi necesar să includeţi în memoriul de securitate.

După ce aţi introdus toate opţiunile sistem în formularul Selectare Valori Sistem şi aţi scris o politică de securitate, puteţi planifica grupurile utilizator.

Exemplu: Politica de securitate la Compania JKL Toy: Memo-ul de mai jos ilustrează politica de securitate pe care John Smith, preşedintele Companiei JKL Toy, o trimite angajaţilor săi. El foloseşte notele pe care el şi Sharon le-au creat pentru a dezvolta acest memo de securitate.

Tabela 18. Exemplu: Memo de securitate la Compania JKL Toy

De la: John Smith, Preşedinte

Tabela 18. Exemplu: Memo de securitate la Compania JKL Toy (continuare)

Compania JKL Toy

Către: Toţi angajaţii Compania JKL Toy

Subiect: Securitatea noului sistem

Aţi participat cu toţii la o întâlnire informativă despre noul nostru sistem. Cei care vor utiliza sistemul au început şcolarizarea şi vor începe procesarea comenzilor de la clienţi săptămâna următoare. Anticipăm că acest sistem va deveni în curând critic pentru succesul afacerii noastre.

Doresc să recapitulez deciziile şi politicile noastre de securitate şi să le subliniez importanţa. Aceste politici au fost proiectate pentru a proteja informaţiile critice pentru afacerea noastră.

- Sharon Jones este responsabilă de securitatea noului sistem. Ken Harrison o va ajuta. Contactaţi-i dacă aveţi vreo întrebare sau suspectaţi vreo problemă de securitate.
- Deciziile noastre despre cine poate efectua operaţii în sistem se bazează pe politicile noastre curente care se referă la informaţii. De exemplu:
  - Informaţiile despre contracte şi preţuri speciale sunt considerate confidenţiale. Nu trebuie divulgate niciodată nimănui din afara companiei.
  - Numai Contabilitatea poate seta şi modifica limitele de credit pentru clienţii noştri.
- Orice persoană care are nevoie să folosească sistemul va primi un ID utilizator şi o parolă. Vi se va cere să vă modificaţi parola la prima semnare pe sistem şi la fiecare 60 de zile după aceea. Alegeţi o parolă pe care să o puteţi ţine minte, însă nu una care să fie evidentă. Formularul pe care îl primiţi cu ID-ul dumneavoastră de utilizator conţine câteva sugestii pentru crearea de parole.
- *Nu divulgaţi nimănui parola dumneavoastră.*. Am intenţionat ca dumneavoastră să puteţi fi în stare să faceţi pe sistem orice este necesar pentru munca duneavoastră. Dacă aveţi nevoie de informaţii, contactaţi pe Sharon sau pe Ken. Dacă v-aţi uitat parola, Sharon sau Ken pot imediat seta una nouă. Nu ar trebui să existe nici un motiv pentru ca cineva să semneze cu ID-ul utilizator şi parola altcuiva.
- Este posibil să fi învăţat cum se utilizează funcţiile de înregistrare şi playback pe staţiile de lucru penru a tasta mai puţin. *Nu* folosiţi aceasta pentru a păstra parola.
- Nu vă lăsaţi staţiile de lucru semnate când sunteţi departe de birou. În timpul şcolarizării aţi învăţat cum să anulaţi temporar semnarea pe staţia de lucru. Folosiţi această funcţie dacă trebuie să plecaţi de la birou pentru o perioadă scurtă de timp. Dacă veţi fi plecaţi pentru mai mult timp, terminaţi-vă lucrul şi folosiţi anularea obişnuită a semnării.

  Anularea semnării când părăsiţi staţia de lucru este importantă mai ales în locaţiile care sunt accesibile publicului, cum ar fi docurile de încărcare, zona de servicii clienţi şi birourile de vânzare de la distanţă.
- Deşi unitatea de sistem este robustă, vă rog să încercaţi să nu o loviţi sau să puneţi lucruri pe ea. Panourile de control de pe unitate vor fi în mod obişnuit dezactivate, dar vă rog să nu le atingeţi. Membrii departamentului de Contabilitate sunt responsabili cu asigurarea faptului că nimeni străin nu se apropie de sistem.

Reţineţi, scopul noului sistem este să ne facă tuturor munca mai uşoară şi să ne imbunătăţească performanţele. Politicile noastre de securitate ar trebui să vă ajute, nu să vă împiedice. Dacă aveţi întrebări sau suspiciuni, nu ezitaţi să-i contactaţi pe Sharon, Ken sau pe mine.

După ce aţi creat o schiţă a politicii de securitate, puteţi începe să planificaţi grupurile utilizator.

Planificarea grupurilor utilizator

Primul pas în procesul planificare, deciderea strategiei de securitate, este aseamănător cu setarea politicilor companiei. Acum sunteţi pregătiţi să planificaţi grupurile de utilizatori, asemănător cu deciderea politicilor departamentului.

Ce este un grup utilizator?

Un grup utilizator este exact ceea ce implică numele: un grup de persoane care au nevoie să folosească aceleaşi aplicaţii în acelaşi mod. Tipic, un grup conţine persoane care muncesc în acelaşi departament şi au responsabilităţi de muncă similare. Puteţi defini un grup utilizator creând un profil de grup.

Ce reprezintă un profil de grup?

Un profil de grup serveşte două scopuri în sistem:

- **Unealtă de securitate**: Un profil de grup furnizează un mod simplu de a organiza cine poate folosi anumite obiecte din sistem (obiecte autorizate). Puteţi defini obiecte autorizate pentru un grup întreg mai degrabă decât pentru fiecare membru individual al grupului.
- **Unealtă de personalizare**: Puteţi folosi un profil de grup ca un model pentru crearea profilurilor de utilizator individuale. Cele mai multe persoane care fac parte din acelaşi grup au nevoie de aceleaşi personalizări, cum ar fi meniul iniţial şi imprimanta implicită. Puteţi defini acestea în profilul grup şi să le copiaţi în profilurile de utilizator individual.

Profilurile de grup sunt mult mai uşor de întreţinut, fiind o schemă compatibilă cu securizarea şi personalizarea sistemului.

Care sunt formularele de care aveţi nevoie?

Pentru a planifica grupurile utilizator, aveţi nevoie de aceste formulare:

- Formular de Identificare Grup Utilizator
- Formular Descriere Grup Utilizator

Notă: Veţi avea nevoie de un formular Descriere Grup Utilizator pentru fiecare grup utilizator care va fi în sistem.

Revedeţi aceste subiecte pentru a vă ajuta să completaţi aceste formulare:

- Identificarea grupurilor utilizator.
- Planificarea profilurilor de grup.
- Alegerea valorilor care afectează semnarea.
- Alegerea valorilor care limitează ceea ce poate face un utilizator
- Alegerea valorilor care setează mediul utilizatorului.

Identificarea grupurilor utilizatori

Când planificaţi grupurile utilizator, trebuie mai întâi să identificaţi grupurile de utilizatori din din sistem. Aceasta vă permite să planificaţi accesul la resursele de care au nevoie aceste grupuri. Încercaţi să folosiţi o metodă simplă pentru a identifica grupurile utilizatori. Gândiţi-vă la departamentele sau grupurile de muncă pe care plănuiţi să le folosiţi în sistem. Aruncaţi o privire la diagrama aplicaţiilor pentru a trasa aplicaţiile. Vedeţi dacă există o relaţie naturală între grupurile de muncă şi aplicaţii:

- Puteţi identifica o aplicaţie primară pentru fiecare grup de muncă?
- Ştiţi care sunt aplicaţiile de care au nevoie fiecare grup? De care aplicaţii au nevoie?
- Ştiţi care grup ar trebui să aibă drept de proprietate asupra informaţiilor din fiecare bibliotecă aplicaţiei?

Dacă puteţi răspunde ″Da″ la aceste întrebări, atunci puteţi începe să planificaţi grupurile utilizator. Totuşi, dacă răspundeţi cu ″câteodată″ sau ″poate″, atunci aţi putea găsi folositor să utilizaţi o abordare sistematică pentru a identifica grupurile utilizatori.

Puteţi să revedeţi un exemplu despre utilizarea acestei abordări pentru a identifica grupurile utilizator.

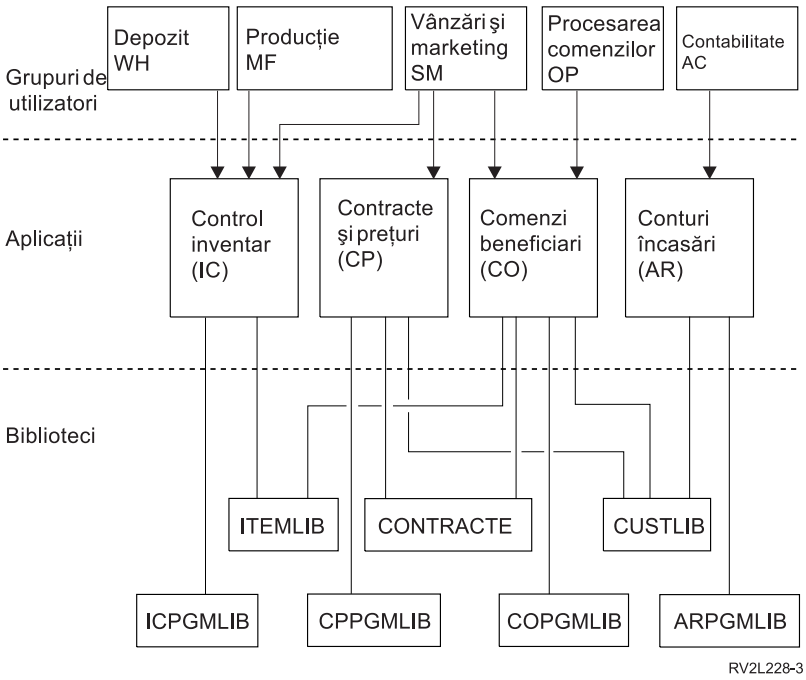
Notă: Aparţinerea utilizatorilor unui singur grup simplifică securitatea gestiunii. Totuşi, există situaţii în care faptul că utilizatorii aparţin mai multor grupuri este de folos.

Este mai uşor de gestionat dacă utilizatori aparţin mai multor profiluri de grup decât să obţii mai multe autorizări private pentru profiluri utilizator individuale.

Exemplu: Identificarea grupurilor utilizator: Dacă relaţiile între grupurile de muncă şi aplicaţii sunt complicate sau vagi, folosind o tehnică matriceală cum ar fi formularul Identificare Grup Utilizator aţi putea clarifica lucrurile. Când proiectaţi utilizatorii sistem şi aplicaţiile de care au nevoie într-o matrice, trebuie să vedeţi modele similare. În plus

pentru a completa în formularul Identificare Grup Utilizator, Sharon Jones a folosit diagrama aplicaţiilor pentru a identifica grupurile de utilizatori care au nevoie de acces la aplicaţii.

Ilustraţia de mai jos arată diagrama aplicaţiilor Companiei JKL Toy.



Dacă abordarea dumneavoastră referitor la securizare este relaxată, folosiţi un X pentru a indica utilizatorul care are nevoie de o aplicaţie. Dacă abordarea dumneavoastră referitor la securitate este restrictivă, trebuie să luaţi în considerare modul în care persoanele folosesc aplicaţiile. Decât să puneţi un X în matrice, folosiţi un V (vizualizare) dacă cineva trebuie doar să vadă informaţiile dintr-o aplicaţie. Folosiţi un C (modificare) dacă cineva trebuie să facă modificări informaţiilor. Folosiţi un O (proprietar) dacă cineva are responsabilitate primară asupra informaţiilor.

De exemplu, la Compania JKL Toy, diferite grupuri au nevoie de aplicaţiile Preţuri şi Contacte:

- Departamentele Vânzări şi Marketing setează preţurile şi creează contractele cu clienţii. Ei au *drept de proprietate*asupra informaţiilor referitoare la preţ şi contracte.
- Departamentul comandă clienţi modifică indirect informaţiile despre contracte. Când ei procesează comenzile, cantităţile din contracte se modifică. Ei trebuie să *modifice*informaţiile despre preţuri şi contracte.
- Persoanele care procesează comenzile trebuie să arunce o privire asupra informaţiilor despre limita creditului pentru a-şi planifica munca, însă nu au permisiunea de a le modifica. Ei trebuie să *vizualizeze* fişierul de limitare credit.

Tabela 19. Formularul Identificare Grup Utilizator al Companiei JKL Toy : exemplu

Formularul Identificare Grup Utilizator					
Pregătit de : Sharon Jones		Data: 9/2/99			
		Accesul Necesar pentru Aplicaţii			
Nume utilizator	Departament	APP: CO	APP: IC	APP: PC	APP: AR
Ken H.	Procesare Comandă (OP)	O	C	C	C
Karen R.	Procesare Comandă (OP)	O	C	C	C
Kris T.	Cont (AC)	V		V	O
Sandy J.	Cont (AC)	V	C	V	O
Peter D.	Cont (AC)	C		V	O

Tabela 19. Formularul Identificare Grup Utilizator al Companiei JKL Toy : exemplu (continuare)

Ray W.	Depozit (WH)	V	O	V	
Rose Q.	Depozit (WH)	V	O	V	
Roger T.	Vânzări şi marketing (SM)	C	C	O	C
Sharon J.	Mangeri (MG)	C	C	C	C

Notă:

- Dacă securizarea mediului este *Relaxată*, folosiţi un X pentru a marca aplicaţiile de care au nevoie utilizatorii.
- Dacă securizarea mediului este *Medie*, folosiţi A pentru a marca ce utilizatori vor avea autorizare la ce aplicaţii.
- Dacă securizarea mediului este *Strictă*, trebuie să folosiţiC (modificare), V (vizualizare), şi O pentru a specifica *cum* sunt folosite aplicaţiile.

Sharon Jones a făcut câteva notiţe despre deciziile ei când şi-a pregătit matricea:

- Procesând comenzile şi conturile furnizaţi o copie de siguranţă pentru fiecare. Astăzi, sunt necesare aplicaţii similare. Totuşi, grupurile ar trebui separate deoarece ele devin mult mai specializate în viitor, prin adăugarea mai multor persoane.
- Deşi procesarea comenzilor nu permite modificarea inventarului sau a contractelor în mod direct, elementul şi contractul echilibrează modificările automat când se creează şi completează comenzile. Acesta va deveni mai târziu un element de securitate?
- Persoanele de la Vânzări şi Marketing sunt implicate în toate segmentele unei afaceri şi în fiecare aplicaţie. Ele setează preţurile şi descrierile pentru elemente. Ele aleg noii clienţi, deşi conturile setează limitele creditului. Acestea sunt responsabile cu stabilirea preţurilor şi a tuturor termenilor din contract.

Decideţi ce ar trebui să fie grupurile utilizator. Completaţi în formularul Identificarea Grupului Utilizator, dacă aveţi nevoie de ajutor pentru a decide.

După ce aţi adăugat utilizatorii în formularul Identificare Grupului Utilizator, puteţiplanifica un profil de grup.

Planificarea unui profil de grup

O dată identificate grupurile de utilizatori, sunteţi pregătiţi să planificaţi un profil pentru fiecare grup. Multe dintre deciziile pe care trebuie să le luaţi afectează securizarea şi personalizarea sistemului. De exemplu, când specificaţi un meniu iniţial, puteţi restricţiona un utilizator să folosească doar acel meniu. De asemenea, trebuie să vă asiguraţi că utilizatorul vede meniul corect după semnare.

Pregătiţi un Formular Descriere Grup Utilizator pentru un grup utilizator ca şi exemplu. După ce aţi terminat primul formular, întoarceţi-vă şi completaţi formularele pentru alte grupuri de care aveţi nevoie.

iSeries a fost proiectat astfel încât securitatea şi personalizarea să fie foarte flexibile. Metoda de planificare din acest subiect oferă o modalitate bună de proiectare a profilurile de grup şi a descrierile joburilor, însă programatorul sau furnizorul aplicaţiei poate recomanda altă metodă.

Numirea profilurilor de grup

Din cauză că profilurile de grup acţionează ca un tip special de profil utilizator, puteţi să identificaţi profilurile de grup uşor în liste şi ecrane. Trebuie să le asignaţi nume speciale. Pentru a apărea împreună în liste, profilurile de grup ar trebui să înceapă cu aceleaşi caractere, cum ar fi GRP (pentru grup) sau DPT (pentru departament). Utilizaţi aceste indicaţii când numiţi grupurile utilizator:

- Numele grupului utilizator poate avea mai mult de 10 caractere lungime.
- Numele poate include litere, numere, şi caractere speciale: liră sterlină (#), dolar ($), liniuţă de subliniere (_), şi semnul (@).
- Numele nu poate să înceapă cu un număr.

Notă: Pentru fiecare profil de grup, sistemul asignează un număr de identificarea a grupului. (*gid*). În mod normal, puteţi lăsa sistemul să genereze un *gid*. Dacă folosiţi sistemul, trebuie să asgnaţi un identificator de grup specific pentru profilurile de grup. Verificaţi cu administratorul de reţea dacă trebuie să asignaţi identificatori de grup.

Ar trebui să adăugaţi sistemului numele profilurilor de grup în câmpul corespunzător al Formularului Convenţii de Nume. De exemplu, Sharon Jones alege DPT ca şi convenţie de nume pentru profilurile de grup. Ea completează în secţiunea corespunzătoare a Formularului Convenţii de Nume.

Tabela 20. Formularul Convenţii de Nume al Companiei JKL Toy: Exemplu de profil de grup

Introducerea unui obiect	Convenţie de nume
Profilurile de grup	Utilizarea caracterelor DPT urmate de prescurtările de departament. Textul de descriere al profilului de grup ar trebui să fie numele departamentului.

Determinarea aplicaţiilor şi bibliotecilor de care are nevoie un grup utilizator

Dacă încă nu aţi făcut lucrul acesta, adăugaţi grupurile utilizator la diagrama aplicaţiilor şi bibliotecilor pe care le-aţi trasat mai devreme. Această imagine vizuală vă va ajuta să decideţi resursele şi aplicaţiile de care are nevoie fiecare grup.

În partea 1 a Formularului Descriere Grup Utilizator indicaţi aplicaţiile primare ale grupurilor, adică aplicaţiile folosite cel mai des. Listaţi alte aplicaţii de care are nevoie grupul.

Aruncaţi o privire la Formularul Descriere Aplicaţii şi la diagrama aplicaţiilor pentru a vedea bibliotecile de care au nevoie fiecare grup. Verificaţi cu programatorul sau furnizorul aplicaţiei cea mai bună metodă pentru furnizarea accesului la aceste biblioteci. Cele mai multe aplicaţii folosesc une din aceste tehnici:

- Aplicaţia include bibliotecile din lista iniţială de biblioteci utilizator.
- Aplicaţia rulează un program de setare care plasează bibliotecile în lista biblitecă utilizator.
- Bibliotecile nu trebuie să fie în lista de biblioteci. Programele aplicaţiei specifică întotdeauna biblioteca.

Sistemul foloseşte o listă de biblioteci pentru a găsi fişierele şi programele de care aveţi nevoie când rulaţi aplicaţiile. **Lista de biblioteci** este o listă de biblioteci în care caută sistemul obiectele de care are nevoie utilizatorul. Are două părţi:

1. **Porţiunea de sistem**: Specificată în valoarea de sistem QSYSLIBL, porţiunea de sistem este folosită pentru bibliotecile OS/400. Valoarea implicită pentru această valoare sistem nu trebuie schimbată.
2. **Partea utilizator**: Valoarea sistem QUSRLIBL furnizează partea utilizator a listei de biblioteci. Descrierea jobului utilizator specifică lista de biblioteci iniţială sau comenzile după ce utilizatorul a semnat. Dacă nu aveţi o listă de biblioteci iniţială, valoarea sistem QUSRLIBL se înlocuieşte. Bibliotecile aplicaţiei ar trebui să fie incluse în partea utilizator a listei de biblioteci.

Folosirea unei descrieri job

Când un utilizator semnează pe sistem, descrierea jobului de utilizator defineşte multe caracteristici ale acestuia, inclusiv modul în care jobul tipăreşte, în care se rulează joburile batch şi lista de biblioteci iniţială. Sistemul este primit cu o descriere job, numită QDFTJOBD, pe care o puteţi folosi când creaţi profilurile de utilizator. Totuşi, QDFTJOBD specifică valoarea sistem QUSRLIBL ca o listă de biblioteci iniţială. Dacă vreţi ca grupuri diferite de utilizatori să aibă acces la anumite biblioteci la semnare, ar trebui creată câte o dscriere de job unică pentru fiecare grup.

Listaţi fiecare bibliotecă de care are nevoie un grup în Formularul Descriere Grup. Dacă biblioteca ar trebui inclusă în lista de biblioteci a descrierii job a grupului, însemnaţi numele fiecărei biblioteci în formular.

Puteţi revedea un exemplu despre modul în care Sharon Jones a descris grupurile utilizator la Compania JKL Toy, înainte de a începe alegerea valorilor care afectează semnarea.

Exemplu: Formular descriere grup utilizator la Compania JKL Toy: Primul tabel arată Partea 1 a formularului Descriere grup utilizatori pe care Sharon Jones l-a pregătit pentru departamentul de Vânzări şi Marketing. Observaţi că nu a inclus bibliotecile CONTRACTS şi CPPGMLIB în lista de biblioteci iniţială a grupului. Aplicaţia le adaugă automat la lista de biblioteci în loc să le adăugăm la lista iniţială de bibloioteci DPTSM. Când un utilizator iese din aplicaţie, sistemul înlătură aceste biblioteci din lista de biblioteci. Acest lucru oferă securitate suplimentară pentru aceste biblioteci, pentru că le accesaţi numai prin programele aplicaţiei.

Tabela 21. Formular de descriere grup de utilizatori în JKL Toy Company: exemplu de informaţii descriptive

formular Descriere grup utiizatori	Partea 1 din 2
Pregătit de: Sharon Jones	Data: 9/5/99
Nume profil grup: DPTSM Descrierea grupului: Departament Vânzări şi Marketing	
Aplicaţia primară pentru grup: Contracts and Pricing Listă cu alte aplicaţii necesare grupului: Inventory (pentru a introduce descrieri articole şi preţuri), Customer Orders	
Listare biblioteci necesare grupului. Bifaţi (✓) fiecare bibliotecă ce ar trebui să facă parte din lista iniţială de biblioteci pentru grup: • ✓CUSTLIB • ✓ITEMLIB • ✓COPGMLIB • ✓ICPGMLIB • CPPGMLIB • CONTRACTS	

În plus, Sharon a început de asemenea un formular Descriere grup utilizatori pentru Departamentul Depozit.

Tabela 22. Formular Descriere grup de utilizatori: informaţii descriptive

formular Descriere grup utilizatori	Partea 1 din 2
Pregătit de: Sharon Jones	Data: 9/5/99
Nume profil grup: DPTWH Descrierea grupului: Departament Depozit	
Aplicaţia primară pentru grup: Inventory control Listă cu alte aplicaţii necesare grupului: none	
Listaţi fiecare bibliotecă de care are nevoie grupul. Puneţi o bifă (✓) în faţa fiecărei biblioteci care ar trebui să fie în lista iniţială de biblioteci pentru grup: • ✓ITEMLIB • ✓ICPGMLIB	

După ce aţi completat Partea 1 din formularul Desriere grup utilizatori, puteţi începe să alegeţi valorile care afectează semnarea.

Alegerea valorilor care afectează semnarea

După ce aţi planificat profilurile de grup în sistem, trebuie să alegeţi valorile sistem care afectează semnarea. Introduceţi alegerile în partea a doua a formularului de Descriere Grup Utilizator. Aminitiţi-vă că, valorile alese trebuie să fie copiate pentru a creea profiluri individuale pentru membrii grupului. Începeţi prin introducerea numelui profilului de grup pe care l-aţi selectat şi o descriere pe scurt (Text) a grupului.

Dacă personalizaţi sistemul corespunzător, utilizatorii pot semna numai cu propriul ID utilizator şi parola. Profilurile lor de utilizator furnizează celelalte valori de semnare.

Parola

Setaţi parola pentru un profil de grup la *NONE. Aceasta împiedică pe oricine să semneze folosind un profil de grup. Mai târziu, când copiaţi profilul de grup pentru a crea profiluri de utilizator individual, setaţi o parolă pentru fiecare utilizator.

Programul şi procedura iniţiale

Un program de utilizator iniţial, numit şi **programul de deschidere**, rulează înainte de a afişa sistemul primul meniu. Puneţi numele programului şi bibliotecii în profilul de grup, chiar dacă biblioteca face parte din lista de biblioteci iniţială. Specificând acestea, vă asiguraţi că sistemul rulează programul corect, şi nu aveţi de ce să vă faceţi griji în legătură cu modificările din lista de biblioteci.

Un program sau o procedură iniţială sunt folosite pentru unul din aceste motive :

- Unele aplicaţii folosesc un program iniţial pentru a seta mediul aplicaţiei.
- Vreţi ca un utilizator să ruleze doar un program şi să nu vadă vreodată meniul. De exemplu, la Compania JKL Toy, persoanele care folosesc staţiile de lucru în platforma de încărcare pot să ruleze numai programul pentru trimiterea inventarului. Aceasta împidică expunerea securităţii staţiei de lucru aflată într-o locaţie publică.

Setarea câmpului**Limitare capabilităţi** pentru un utilizator la *YES sau *PARTIAL împiedică utilizatorii să modifice programele iniţiale în ecranul de semnare.

Verificaţi cu programatorul dacă aplicaţiile necesită un program sau procedură iniţiale.

Meniul Iniţial şi Meniul Bibliotecă Iniţial

Meniul iniţial, numit şi **primul meniu**, este primul meniu pe care îl vede utilizatorul după semnare. Programul iniţial rulează înainte ca meniul iniţial să apară. Dacă programul iniţial arată unele ecrane, utilizatorul vede acele ecrane înainte ca sistemul să arate meniul iniţial.

În mod normal, meniul iniţial pentru un grup ar trebui să fie meniul primar al aplicaţiei principale a grupului. Specificaţi numele meniului şi al bibliotecilor lui.

Dacă setaţi câmpul **Limitare capabilităţi** pentru un utilizator la *YES, utilizatorului nu îi este permis să modifice meniul iniţial din ecranul de semnare. Dacă setaţi câmpul *limitare capabilităţi* pentru un utilizator la *PARTIAL, permiteţi utilizatorului să modifice meniul iniţial din ecranul de semnare.

Biblioteca curentă

Biblioteca curentă este numită **biblioteca implicită**. Se întâmplă mai multe lucruri când specificaţi o bibliotecă curentă pentru un utilizator:

- Dacă utilizatorul creează diferite obiecte, cum ar fi programe interogare, sistemul plasează acele obiecte în biblioteca curentă, cu excepţia situaţiei în care utilizatorul specifică o altă bibliotecă.
- Sistemul adaugă automat biblioteca curentă la partea utilizator a listei de biblioteci. Poate fi inclusă pe o listă de biblioteci iniţială în descrirea job, dar nu este obligatoriu.
- Biblioteca curentă devine prima bibliotecă în partea utilizator a listei de biblioteci. Sistemul caută în biblioteca curentă după fişiere şi programe înainte de a căuta în bibliotecile din lista de biblioteci utilizator.
- Dacă nu asignaţi o bibliotecă curentă pentru un utilizator, sistemul atribuie biblioteca QGPL (scop general).

Recomandări

Biblioteca curentă este importantă în special tunci când intenţionaţi să folosiţi prograamul licenţiat IBM Query pentru iSeries sau alt program similar. Folosiţi una dintre următoarele abordări:

- Creaţi o bibliotecă pentru toţi din grup pentru a o partaja. Puneţi toate programele interogare şi fişierele pentru grup în aceea bibliotecă. Daţi numele bibliotecii acelaşi cu al profilului de grup şi setaţi biblioteca ca fiind biblioteca curentă pentru grup.
- Daţi fiecărui utilizator care îşi planifică să folosească Query o bibliotecă personală. Daţi bibliotecii acelaşi nume ca şi al profilului de grup. Specificaţi care este biblioteca curentă în profilurile individuale ale membrilor grupului, nu în profilul de grup.

În Partea 2 a formularului Descriere Utilizator, completaţi alegerile dumneavoastră în câmpurile care afectează semnarea.

După ce aţi ales valorile care afectează semnarea, puteţi alege valorile care limitează ceea ce poate face un utilizator.

Alegerea valorilor care limitează ceea ce poate face un utilizator

După ce aţi introdus alegerile dumneavoastră pentru valorile care afectează semnarea în Partea 2 a Formularului Descriere Utilizator, ar trebui să consideraţi limitarea a ceea ce utilizatorii pot să facă în sistem. Ar trebui să limitaţi ceea ce pot să facă utilizatorii din câteva motive:

- Pentru a împiedica persoanele să folosească comenzi CL. Acestea pot incerca să experimenteze şi să facă stricăciuni din neatenţie.
- Pentru a restricţiona utilizatorii la anumite aplicaţii şi funcţii.
- Pentru a furniza un mediu simplu unde utilizatorii să nu se încurce în alegeri nenecesare.

Mulţi factori determină cât de multe pot să facă utilizatorii:

- Proiectarea Aplicaţiei
- Valorile Sistem
- Securitatea resurselor
- Profilurile de grup
- Profilurile utilizator
- Descriere Job

Două câmpuri în profilul de grup sau utilizator, **Limitarea capabilităţilor** şi **Clasa utilizator**, determină cât de multe poate să facă un utilizator peste deciziile pe care le-aţi luat.

Limitarea Capabilităţilor

Câmpul **Limitare capabilităţi** este numit **Restricţionarea utilizării liniei de comandă**. Puteţi limita posibilitatea utilizatorilor de a modifica valori în ecranul de semnare, de a introduce comenzi şi de a schimba programul lor de tratare a tastei Attn. Puteţi alege limite stricte (*YES), limite medii (*PARTIAL) sau nici o limită (*NO). Următoarea tabelă arată fiecare dintre aceste valori permise:

Tabela 23. Valorile funcţiilor permise pentru limitarea capabilităţilor

Valoarea Limitare capabilităţi	Modificare program iniţial	Modificare meniu iniţial	Modificare bibliotecă curentă	Modificare program de atenţionare	Introducere comenzi
*YES	Nu	Nu	Nu	Nu	Câteva[1]
*PARTIAL	Nu	Da	Nu	Nu	Da
*NO	Da	Da	Da	Da	Da

1 Sunt permise comenzile: SIGNOFF, SNDMSG, DSPMSG, DSPJOB, DSPJOBLOG, şi STRPCO. Utilizatorul nu poate folosi F9 pentru a afişa o linie de comandă de la nici un meniu Asistent Operaţional sau ecran.

Clasa utilizator

Clasa utilizator, numită şi **introducere utilizator**, determină care sunt opţiunile pe care le vede un utilizator meniu Asistent Operaţional şi meniu sistem. De asemenea determină ce funcţii sistem sunt permise unui utilizator, cu excepţia listei de autorizări din câmpul **Autorizare specială**.

Recomandări pentru limitarea capabilităţilor şi clasei utilizator

Cei mai mulţi utilizatori nu au nevoie de acces la comenzi CL sau funcţii de sistem. Ecranele Asistent Operaţional oferă utilizatorilor suficiente informaţii despre controlul muncii lor. Aceste recomandări permit utilizatorilor să acceseze numai acele resurse sistem de care au nevoie pentru a-şi efectua operaţiile:

- În fiecare profil de grup, setaţi câmpul **Limitare capabilităţi** la *YES. Setaţi câmpul *Clasa utilizator* la *USER.
- Înlocuiţi aceste specificaţii pentru utilizatorii individuali care au nevoie de funcţii sistem.
- Asiguraţi-vă că meniurile furnizează un mijloc de mutare între aplicaţii, dacă utilizatorii au nevoie de aceasta.

După ce aţi introdus alegerile dumneavoastră pentru clasa utilizator şi limitarea capabilităţilor în Partea 2 a formularului de Descriere Grup Utilizator, puteţi alege valori prin care să setaţi mediul utilizator.

Alegerea valorilor care setează mediul utilizator

După ce aţi introdus alegerile dumneavoastră pentru limitarea a ceea ce pot face utilizatorii în sistem în Partea 2 a formularului Descriere Grup Utilizator, puteţi alege valori pentru a determina mediul de operare al utilizatorului. Multe câmpuri în profilul utilizator determină mediul de operare al utilizatorului: ce imprimantă să folosească, unde să trimită mesajele, cu ce prioritate ar trebui să ruleze joburile. Pentru multe din aceste câmpuri, este recomandată setarea implicită. Puţine câmpuri sunt descrise în următoarele paragrafe.

- **Descriere job şi biblioteca descriere job**: Aceste câmpuri din profil îi spun sistemului ce descrire job să folosească când utilizatorul semnează. Descriere job conţine lista de biblioteci iniţială. Fiecare grup utilizator ar trebui să aibă o descriere job cu acelaşi nume ca şi profilul de grup. Descrierile job sunt puse de obicei în biblioteca QGPL.
- **Dispozitivul imprimantă şi coada de ieşiri**: Orice ieşire imprimantă creată de un utilizator merge la dispozitivul imprimantă listat în profil, cu excepţia situaţiei în care un anumit job de tipărire o trimite la o altă imprimantă. Membrii unui grup utilizator sunt de obicei localizaţi împreună şi împart aceeaşi imprimantă. Puteţi specifica imprimanta în profilul de grup şi să o copiaţi în fiecare profil utilizator individual. Dispozitivul imprimantă al utilizatorilor este numit şi **imprimanta implicită**.

  O coadă de ieşiri imprimantă conţine ieşirile imprimantă înainte de a fi tipărite. De obicei, fiecare dispozitiv imprimantă are propria coadă de ieşiri imprimantă cu acelaşi nume. Puteţi specifica *DEV pentru coada de ieşiri imprimantă pentru a-i spune sistemului să folosească coada de ieşiri a dispizitivului imprimantă.

  Completaţi câmpurile nume ale descrierii job, descrierii bibliotecă, imprimantă implicită şi coada de ieşiri imprimantă în formularul Descriere Grup Utilizator.
- **Setarea interfeţei Asistentului Operaţional**: Când este livrat sistemul, meniul Asistent Operaţional este programul de manipulare a tastei atenţionare pentru fiecare utilizator. Când utilizatorii apasă tasta Atenţionare, ei văd meniul Asistent Operaţional (ASSIST). Dacă programele de aplicaţie folosesc deja un alt program de manipulare a tastei atenţionare, ar trebui să furnizaţi o metodă diferită pentru utilizatori pentru a ajunge la meniul Asistent Operaţional:
  - Adăugarea meniul Asistent Operaţional ca opţiune din meniul aplicaţiei principale, utilizând fie GO ASSIST fie CALL QEZAST.
  - Utilizatorii trebuie să introducă GO ASSIST de la linia de comandă.

Dacă câmpul **Limitare capabilităţi** este setat la *YES în profilul utilizator, utilizatorul nu poate folosi comanda GO pentru a afişa un meniu. Trebuie să furnizaţi o metodă pentru Asistentul Operaţional utilizatorilor ca să poată accesa meniul ASSIST.

Puteţi revedea un exemplu cu valorile pe care Sharon Jones le-a ales pentru formularul Descriere Grup Utilizator de la Compania JKL Toy.

Pentru a completa aceşti paşi din planificare, ar trebui:

- Să completaţi un formularDescriere Grup Utilizator pentru fiecare grup utilizator din compania dumneavoastră.
- Descrieţi modul în care numiţi grupurile utilizator în formularulConvenţii de Nume.

- Adăgaţi grupurile utilizator la diagrama aplicaţiilor şi bibliotecilor.

După ce aţi completat aceste operaţii, puteţi începe planificarea profilurilor de utilizator individuale.

Exemplu: formular descriere grup utilizatori la Compania JKL Toy—partea 2: Sharon Jones a făcut câteva note despre departamentele de Vânzare şi Marketing şi cel de Depozit în timp ce a pregătit formularul Descriere grup utilizatori pentru personalul de la Vânzări şi Marketing.

- Personalul de la Vânzări şi marketing vor folosi mult IBM Query for iSeries. Fiecare utilizator ar trebui să aibă o bibliotecă privată. Departamentul Depozit poate avea o bibliotecă de grup.
- Oamenii de la depozit care lucrează la docurile de recepţie vor avea nevoie de un program iniţial în loc de un meniu iniţial.

Sharon a pregătit Partea 2 din formularul Descriere grup utilizatori pentru cele două departamente.

Tabela 24. Exemplu Formular descriere grup utilizatori la Compania JKL Toy - Departament Vânzări şi marketing

Nume câmp	Valoare recomandată	Alegerea dumneavoastră
Nume profil grup (Utilizator)		DSTSM
Parolă	*NONE	*NONE
Clasă utilizator (tipul de utilizator)	*USER	*USER
Biblioteca curentă (biblioteca implicită)	*la fel cu numele profilului de grup*	(lăsaţi spaţiu pentru grupuri; completaţi pentru profilurile individuale)
Programul iniţial de apelat (program de semnare)		
Bibliotecă program iniţial		
Meniu iniţial (primul meniu)		CPMAIN
Bibliotecă meniu iniţial		CPMAINLIB
Facilităţi limitate (restricţionare utilizare linie comandă)	*YES	*PARTIAL
Text (descriere utilizator)		Vânzări şi marketing
Descriere de job	*la fel cu numele profilului de grup*	DPTSM
Bibliotecă descriere job		QGPL
Nume profil grup (grup utilizatori)	*NONE[1]	*NONE
Dispozitiv tipărire (imprianta implicită)		PRT03
Coadă ieşire	*DEV	*DEV

Tabela 25. Exemplu Formular descriere grup utilizatori la Compania JKL Toy - Departament Depozit

Nume câmp	Valoare recomandată	Alegerea dumneavoastră
Nume profil grup (Utilizator)		DPTWH
Parolă	*NONE	*NONE
Clasă utilizator (tipul de utilizator)	*USER	*USER
Mediu special		
Biblioteca curentă (biblioteca implicită)	*la fel cu numele profilului de grup*	DPTWH
Programul iniţial de apelat (program de semnare)		
Bibliotecă program iniţial		
Meniu iniţial (primul meniu)		ICMAIN

Tabela 25. Exemplu Formular descriere grup utilizatori la Compania JKL Toy - Departament Depozit (continuare)

Nume câmp	Valoare recomandată	Alegerea dumneavoastră
Bibliotecă meniu iniţial		ICPGMLIB
Facilităţi limitate (restricţionare utilizare linie comandă)	*YES	*YES
Text (descriere utilizator)		Departament Depozit
Descriere de job	*la fel cu numele profilului de grup*	DPTWH
Bibliotecă descriere job		QGPL
Nume profil grup (grup utilizatori)	*NONE[1]	*NONE
Dispozitiv tipărire (imprianta implicită)		PRT04
Coadă ieşire	*DEV	*DEV

1 Numele profilului de grup trebuie să fie *NONE pentru un profil de grup. Un profil de grup nu poate fi membru al altui grup.

Puteţi începe acum să planificaţi profilurile de utilizator individuale.

Planificarea profilurilor de utilizator individuale

Acum după ce v-aţi decis asupra strategiei generale de securitate şi aţi planificat grupurile utilizator, sunteţi pregătit să planificaţi profilurile de utilizator individual.

Care sunt formularele de care aveţi nevoie?

Folosiţi aceste formulare pentru a planifica profilurile de utilizator individual:

- Formularul Profil Utilizator Individual
- Formularul Responsabilităţi Sistem

Veţi avea nevoie să folosiţi informaţiile din aceste formulare:

- Formularul Definire Grup Utilizator
- Formularul Convenţii de Nume
- Diagrama Aplicaţiei

Numirea profilurilor de utilizator

Numele profilului de utilizator reprezintă modul în care sunteţi identificat în sistem. Introduceţi numele profilului de utilizator în câmpul **ID Utilizator** al ecranului de semnare. Tot ceea ce lucraţi şi ieşirile de imprimantă pe care le creaţi sunt asociate cu numele de profil de utilizator.

Luaţi în considerare acest lucru când decideţi modul în care să numiţi profilul de utilizator:

- Un nume de profil de utilizator poate fi mai lung de 10 caractere. Unele metode de comunicaţie limitează ID-ul de utilizator la 8 caractere.
- Un nume de profil de utilizator poate să includă litere, numere, şi caractere speciale: liră sterlină (#), dolar ($), liniuţă de subliniere (_), şi semnul (@). El nu poate să înceapă cu un număr sau liniuţă de subliniere (_).
- Sistemul nu face deosebire între literele mari şi literele mici într-un nume profil utilizator. Dacă aţi introdus caractere alfabetice mici, sistemul le transformă în caractere mari.
- Ecranele şi listele pe care le folosiţi pentru a gestiona profilurile de utilizator le arată în ordine alfabetică, ordonate după numele de profil de utilizator.
- Toate profilurile livrate de IBM încep cu litera Q. Pentru a păstra profilurile dumneavoastră separat de cele livrate de IBM, evitaţi asignarea începerea numelui profil utilizator cu caracterul Q.

Recomandări

O tehnică pentru asignarea numelor profil utilizator este de a folosi primele 7 caractere ale prenumelui urmate de primul caracter al numelui. Mai jos este convenţia de nume pe care a folosit-o Sharon pentru profilurile de utilizator de la Compania JKL Toy:

Tabela 26. Formular Convenţii de Nume al Companiei JKL Toy: Exemplu profil utilizator

Nume utilizator	Nume profil utilizator
Anderson, George	ANDERSOG
Anderson, Roger	ANDERSOR
Jones, Sharon	JONESS

Această metodă face numele de profiluri mai uşor de reţinut. De asemenea, listele şi ecranele sunt împărţite alfabetic după nume.

De exemplu, Sharon Jones de la Compania JKL Toy planifică să folosească această tehnică de numire. Ea completează în secţiunea corespunzătoare a formularului Convenţii de Nume.

Tabela 27. Formular Convenţii de Nume al Companiei JKL Toy : Exemplu de profil utilizator

Tipuri de obiecte	Convenţie de nume
Profiluri utilizator	Folosiţi primele 7 caractere ale prenumelor utilizatorilor, urmate de primul caracter al numelui. Descrierea unui profil utilizator va fi prenume, nume.

Descrieţi cum aţi planificat să numiţi profilurile de utilizator în formularul Convenţii de Nume şi apoi puteţi determina cine ar trebui să fie responsabil pentru funcţionarea sistemului şi să alegeţi valori pentru fiecare utilizator.

Determinarea responsabilului cu funcţionarea sistemului

Când planificaţi profiluri utilizator individual, trebuie mai întâi să determinaţi responsabilităţile utilizatorilor din sistem. Pentru a pastra funcţionarea eficientă a sistemului de operare, este nevoie ca utilizatorii să realizeze în mod regulat diferite funcţii de gestiune şi întreţinere. Utilizatorii care realizează aceste operaţii trebuie să fie autorizaţi să ruleze comenzi şi să realizeze funcţii sistem.

Alegerea valorilor care limitează ce poate executa un utilizator şi discutat despre cum poate accesa un utilizator câmpurile **Clasa Utilizator** şi **Limitarea capabilităţii** care controlează funcţiile sistemului. În mod normal, nu ar trebui să permiteţi multor utilizatori să realizeze funcţii de sistem (setaţi clasa utilizator la *USER şi limitaţi capabilităţile la *PARTIAL sau *YES). Oricum, câţiva utilizatori au nevoie de autorizări suplimentare pentru a putea păstra funcţionarea eficientă a sistemului de operare.

Tabelul de mai jos listează câteva dintre cele mai importante operaţii de gestionare a sistemului. Este indicat de asemenea, să asignaţi clasa utilizator şi autorizări speciale utilizatorilor cu acele responsabilităţi. Această listă vă ajută să determinaţi care utilizatori din sistem au nevoie de autorizări speciale. Oricum, aceasta nu intenţionează a fi o unealtă de planificare aplicată pentru întreţinerea şi operaţionalitatea sistemului. Acest tabel furnizează clasa utilizator şi autorizari speciale care funcţionează cu cele mai multe sisteme. Puteţi avea nevoie să asignaţi diferite autorizări în funcţie de sistem.

Când asignaţi în profil o clasă utilizator alta decât *USER, utilizatorul primeşte automat un anumit set de autorizări speciale pentru a realiza funcţii de sistem. Puteţi asigna unui utilizator autorizări speciale diferite de cele pe cale le-aţi specificat în câmpul clasa utilizator, însă nu ar fi necesar.

Tabela 28. Responsabilităţi de sistem, Clasa Utilizator, Autorizări Speciale

Funcţie de sistem[1]	**Descriere**	**Clasa Utilizator necesară** [2]	**Autorizare specială necesară** [3]
Operaţii de sistem	Gestionarea ieşirilor imprimantă, pentru a reacţiona la mesajele de sistem, monitoriza operaţiile obişnuite, realiza încărcarea programului iniţial (IPL).	*SYSOPR	*JOBCTL
Întreţinerea sistemului	Realizarea funcţiilor de întreţineri a sistemului, cum ar fi fi planificarea a curăţării şi monitorizării spaţiului pe disc.	*SYSOPR	*JOBCTL
Salvare de rezervă	Salvarea regulată a bibliotecilor aplicaţiei, bibliotecilor sistem, şi a informaţiilor de securitate. Vedeţi Salvare de rezervă şi recuperare subiect din Centrul de Informare pentru detalii despre aceste funcţii.	*SYSOPR	*SAVSYS
Profilul administrare	Adăugarea de noi profiluri utilizator, întreţinerea profilurilor existente.	*SECADM	*SECADM
Administrarea securităţii resurselor	Întreţinerea autorităţilor la obiecte în sistem.	*SECOFR	*ALLOBJ
Întreţinerea programelor	Aplicarea periodică a modificărilor de program (PTFs) la bibliotecile livrate de IBM. Efectuarea modificărilor la bibliotecile aplicaţiei.	*SECOFR	*ALLOBJ
Auditarea securităţii	Setarea funcţiilor de auditare a securităţii. Determinarea evenimentelor, utilizatorilor, şi obiectelor care ar trebui auditate.		*AUDIT [4]
Configurarea sistemului	Adăugarea, modificarea, şi înlăturarea dispozitivelor din sistem.		*IOSYSCFG[5]

1 Setarea câmpului Limitare capabilităţi la *NO pentru utilizatorii aceste responsabilităţi.

2 Acesta este minimul necesar clasei utilizator. Clasa utilizator furnizează autoritatea de a folosi comenzi şi opţiuni de meniu care sunt necesare la executarea unei funcţii. În funcţie de securitatea resurselor, pot fi necesare autorităţi obiect suplimentare.

3 Această autoritate particulară este necesară pentru responsabilităţi de joburi. Clasa utilizator poate obţine autorităţi suplimentare.

4 Autorizarea specială *AUDIT nu are corespondenţă în clasa utilizator. Clasa utilizator *SECOFR include autorizarea specială *AUDIT. Oricum, probabil auditorul nu are nevoie de alte capabilităţi ale clasei utilizator *SECOFR. Trebuie să specificaţi autorizarea specială *AUDIT pentru fiecare utilizator individual care este nevoit să controleze auditarea în sistem.

5 Autorizarea specială *IOSYSCFG nu are corespondenţă în clasa utilizator. Clasa utilizator *SECOFR include autorizarea specială *IOSYSCFG. Trebuie să specificaţi autorizarea specială *IOSYSCFG numai pentru utilizatorii care trebuie să configureze sistemul. Utilizatorii ar putea creea linii, controlere şi dispozitive, sau configura TCP/IP. Oricum, pentru a configura sistemul utilizatorul nu are nevoie de alte capabilităţi ale clasei utilizator *SECOFR.

Recomandări

Folosiţi tabela de mai sus pentru a planifica cine să realizeze funcţii de sistem. Minimal, ar trebui să asignaţi două persoane pentru a gestiona securitatea sistemului, şi alte două pentru a gestiona operaţiile şi salvarea de siguranţă.

Folosiţi formularul de responsabilităţi sistem ca şi unealtă pentru gestionarea şi auditarea sistemului. Păstraţi informaţii despre oricine are autorizări speciale în sistem şi de ce au nevoie de acele autorizări speciale.

Puteţi să revedeţi un exemplu despre cum determină Sharon Jones responsabilităţile utilizatorilor înainte de a alege valori pentru fiecare utilizator.

Exemplu: formular Responsabilităţi sistem la Compania JKL Toy: Mai jos este un exemplu al formularului Responsabilităţi sistem pe care l-a completat Sharon Jones:

Tabela 29. Formular responsabilităţi sistem la Compania JKL Toy: exemplu

Cine este responsabilul principal cu securitatea? Sharon Jones Cine este responsabil cu securitea de rezervă?Ken Harrison			
Nume profil	Nume utilizator	Clasa	Comentarii
JONESS	Sharon Jones	*SECOFR	Sharon este principalul responsabil cu securitatea şi administratorul de sistem.
HARRISOK	Ken Harrison	*SECOFR	Ken este rezerva lui Sharon ca administrator general de sistem.
JOHNSONS	Sandy Johnson	*SYSOPR	Sandy are ca principală responsabilitate operaţiile şi salvările de sistem.
ROGERSK	Karen Rogers	*SYSOPR	Karen o va ajuta pe Sandy la operarea şi salvarea sistemului.
WILLISR	Rose Willis	*SYSOPR	Rose va opera sistemul în schimbul doi.

După ce aţi terminat formularul Responsabilitate sistem, puteţi începe să alegeţi valori pentru fiecare utilizator.

Alegerea valorilor pentru fiecare utilizator

După ce aţi determinat responsabilităţile utilizatorilor din sistem, puteţi începe să alegeţi valori pentru fiecare utilizator. Plănuind profilurile de grup ca modele pentru profilurile de utilizator individual, aproape v-aţi terminat munca. Folosiţi formularul Profil Utilizator Individual pentru a asigna fiecare utilizator la grupul corect şi pentru a defini diferenţele între utilizatorii care aparţin aceluiaşi grup. Ar trebui să completaţi un formular Profil Utilizator Individual pentru un grup de utilizatori ca şi exemplu, apoi să vă întoarceţi şi să pregătiţi formularele Profil Utilizator Individual pentru orice grupuri utilizatori suplimentare.

Completaţi nume profil grup şi alte informaţii descriptive în partea de sus a formularului Profil Utilizator Individual.

Exemplu: formularul Profil Utilizator Individual al Companiei JKL Toy informaţii descriptive

Aici este prezentat modul în care Sharon Jones a completat partea de sus a formularului Profil Utilizator Individual.

Tabela 30. Formularul Utilizator Individual al Companiei JKL Toy : Exemplu descriere informaţii

Formular Profil Utilizator Individual	
Pregătit de: Sharon Jones	Data: 9/5/99
Numele profil grup : DPTOP	
Proprietar al obiectelor create:	Autorizare grup pentru obiectele create:
Tipul autorizare grup:	

Determinarea valorilor pentru membrii grupului

În formularul Profil Utilizator Individual notaţi numele profilului şi informaţii descriptive (nume utilizator) despre fiecare membru al grupului. Paragrafele de mai jos descriu modul în care să determinaţi alte valori pentru fiecare membru al grupului.

Amintiţi-vă, profilul de grup este un model pentru profilurile de utilizator individuale. În formularul Profil de utilizator individual trebuie să specificaţi numai lucrurile care sunt diferite de la un grup la altul.

- **Asignarea parolelor**: Cel mai uşor mod de a asigna iniţial parole utilizatorilor este de a alege parola aceeaşi cu numele profilului. Puteţi apoi cere ca parola să fie modificată la prima semnare a utilizatorului prin setarea parolei să

expire. În subiectul Setarea parolei să expire aţi învăţat modul în care se face aceasta automat cînd copiaţi profilul grupului. Dacă planificaţi să faceţi aceasta, nu este necesar să listaţi parolele în formularul Profil Utilizator Individual.

- **Clasa utilizator şi limitarea capabilităţilor**: Priviţi formularul Responsabilitate Sistem pentru a vedea care membrii din fiecare grup are nevoie de valori diferite pentru câmpurile **clasa Utilizator** şi **Limitarea capabilităţilor**. Completaţi informaţiile corespunzătoare în formularul Profil Utilizator Individual pentru oricine are nevoie de valori diferite de acelea ale profilului de grup.
- **Specificarea altor valori**: Verificaţi pentru a vedea dacă un utilizator particular are nevoie de valori diferite de valorile specificate în formularul de Descriere Grup Utilizator al grupului. În formularul Descriere Grup Utilizator, câmpurile **clasa Utilizator** şi **Limitare capabilităţi** sunt listate în partea de sus, deoarece valorile lor adesea diferă de la un membru al grupului la altul. Listaţi orice alte câmpuri care se modifică pentru membrii grupului cu care lucraţi.

Pentru a termina paşii de planificare, asiguraţi-vă că:

- Aţi completat formularul Selecţie valori sistem.
- Descrieţi modul în care aţi planificat numirea profilurilor de utilizator în formularul Convenţii de numire.
- Pregătirea unui formular Profil utilizator individual pentru fiecare grup de utilizatori din companie.

Puteţi să revedeţi un exemplu de informaţii pe care Sharon le foloseşte pentru utilizatorii individuali înainte de a planifica securizarea resurselor

Exemplu: Formular profil utilizator individual la Compania JKL Toy: La Compania JKL Toy, oamenii care lucrează la docul de încărcare pot rula numai un program. Sharon a limitat aceşti utilizatori la câteva fucţii pentru că lucrează într-o zonă în care publicul poate accesa uşor staţiile de lucru. Aceşti membri ai departamentului Depozit au un program iniţial şi nu au nici un meniu iniţial. Departamentul Procesare comenzi are două imprimante locale şi o imprimantă într-un birou de vânzări de la distanţă. De aceea, Sharon a asignat câtorva utilizatori o altă imprimantă decât cea a grupului.

Mai jos este formularul Profiluri individuale de utilizatori pe care l-a completat Sharon pentru Departamentul Procesare comenzi şi Depozit la Compania JKL Toy. Observaţi că ea a completat câmpurile numai când acestea erau diferite de valorile setate pentru profilul de grup.

Tabela 31. Exemplu: Formular profil utilizator individual la Compania JKL Toy: Departament Depozit

Nume profiluri grup: DPTWH					
Faceţi o înregistrare pentru fiecare membru al grupului:					
Profil utilizator	**Text (descriere)**	**Clasă utilizator**	**Facilităţi limitate**	**Program iniţial / Bibliotecă**	**Meniu iniţial / Bibliotecă**
WILLISR	Willis, Rose	*SYSOPR	*NO		
WAGNERR	Wagner, Ray			ICRCPT/ICPGMLIB	none
AMESJ	Ames, Janice			ICRCPT/ICPGMLIB	none
FOSSJ	Foss, Julie				
WOODBURC	Woodburt, Carol				

Tabela 32. Exemplu formular Profil individual utilizator: Departament Procesare comenzi

Nume profiluri grup: DPTOP				
Faceţi o înregistrare pentru fiecare membru al grupului:				
Profil utilizator	**Text (descriere)**	**Clasă utilizator**	**Facilităţi limitate**	**Dispozitiv imprimantă**
HARRISOK	Harrison, Ken	*SECOFR	*NO	PRT05
RICHARDK	Richards, Karen			
UNGERJ	Unger, Jeff			PRT04

Tabela 32. Exemplu formular Profil individual utilizator: Departament Procesare comenzi (continuare)

BELLB	Bell, Brad			PRT04

Apoi puteţi începe să planificaţi securitatea resurselor.

Planficarea securităţii resurselor

Acum după ce aţi terminat procesul de planificare utilizatori din sistem, puteţi planifica securitatea resurselor care protejează obiectele din sistem. În ″Setarea securităţii resurselor,″ învăţaţi cum să setaţi securitatea resurselor din sistem.

Valorile sistem şi profilurile de utilizator controlează cine are acces la sistem şi împiedică utilizatorii neautorizaţi să folosească sistemul. Securitatea resurselor controlează actiunile pe care utilizatorii autorizaţi ai sistemului le pot realiza după ce au semnat cu succes. Securitatea resurselor are ca scop principal securitatea sistemului şi protejează:

- Confidenţialitatea informaţiilor
- Precizia informaţiilor pentru a împiedica modificarea neautorizată
- Disponibilitatea informaţiilor pentru a împiedica stricăciunile accidentale sau intenţionate.

Puteţi planifica în mod diferenţiat planificarea securităţii resurselor, în funcţie de companie dacă dezvoltă aplicaţii sau le cumpără. Pentru aplicaţiile pe care le dezvoltaţi, puteţi comunica cerinţele pentru securitatea informaţiilor programatorului în timpul procesului de proiectare a aplicaţiei. Când cumpăraţi, aplicaţii trebuie să determinaţi gradul de securitate de care aveţi nevoie şi să-l potriviţi cu acela pe care l-a destinat furnizorul aplicaţiilor. Tehnicile descrise aici ar trebui să vă ajute în ambele cazuri.

Acest subiect oferă o abordare de bază de planificare a securităţii resurselor. Introduce tehnicile principale şi arată cum le puteţi folosi. Metodele descrise aici nu este obligatoriu să funcţioneze pentru fiecare companie şi aplicaţie. Consultaţi programatorul sau furnizorul aplicaţiei când planificaţi securitatea resurselor.

Revederea acestor subiecte vă ajută să planificaţi securitatea resurselor:

- Determinarea obiectivelor pentru securitatea resurselor
- Înţelegerea tipurilor de autorizări
- Planificarea securităţii bibliotecilor aplicaţiilor
- Determinarea dreptului de propietatea a bibliotecilor şi obiectelor
- Gruparea obiectelor
- Protejarea ieşirilor imprimantă
- Protejarea staţiilor de lucru
- Sumarizarea recomandărilor securităţii resurselor
- Planificarea instalării aplicaţiei

De ce formulare aveţi nevoie?

Faceţi copii următoarelor formulare şi completaţi-le în timp ce citiţi acest subiect. Testaţi întregul proces pentru o aplicaţie şi apoi repetaţi procesul pentru fiecare aplicaţie suplimentară.

Tabela 33. Planificarea formularelor necesită planificarea securităţii resurselor

Numele formularului	Numărul de copii necesare
Formularul Lista de autorizări	Mai multe
Ieşire imprimantă şi staţia de lucru Securitate formular	Unu

Adăugarea informaţiilor la următoarele formulare, cu care aţi lucrat anterior:

Tabela 34. Planificarea formularelor care vor fi modificate

Numele formularului	Pregătit pentru
Formularul de descriere a bibliotecii	Descrierea informaţiilor bibliotecii
Formularul de descriere a grupului utilizator	Planificarea profilurilor de grup

Referiţi-vă la aceste formulare, pe care le-aţi pregătit anterior:

Tabela 35. Planificarea formularelor necesară pentru a efectua securitatea resurselor

Numele formularului	Pregătit pentru:
Formularul de descriere a bibliotecii	Trasarea diagramei unei aplicaţii şi Identificarea grupurilor utilizator
Formular pentru Descriere Aplicaţie	Descrierea informaţiilor aplicaţie
Formular Profil Utilizator Individual	Alegerea valorilor pentru fiecare utilizator
Formular Identificare Grup Utilizator	Identificarea grupurilor utilizator
Formular Responsabilităţi Sistem	Determinarea responsabilului pentru funcţionarea sistemului
Formular de Planificare a Securităţii Fizice	Planificarea securităţii fizice

Determinarea obiectivelor pentru securitatea resurselor

Pentru a începe să planificaţi securitatea resurselor ,trebuie mai întâi să înţelegeţi obiectivele. iSeries permite o implementare flexibilă a securităţii resurselor. Vă oferă puterea de a proteja resursele exact aşa cum doriţi. Însă securitatea resurselor poate avea impact asupra performanţelor aplicaţiilor. De exemplu, chiar dacă o aplicaţie are nevoie de un obiect, sistemul trebuie mai întâi să verifice autorizarea utilizatorului la acel obiect. Trebuie să balansaţi nevoia de confidenţialitate cu costurile performanţei. Când luaţi decizii de securitate a resurselor, potriviţi valoarea securităţii cu costurile pe care le implică.

Pentru a împiedica degradarea performanţei aplicaţiilor datorită securităţii resurselor urmaţi aceste îndrumări.

- Păstraţi o schemă simplă pentru securitatea resurselor
- Securizaţi doar obiectele care necesită securitate.
- Folosiţi securitatea resurselor pentru completarea, nu înlocuirea, altor unelte pentru protejarea informaţiilor, cum ar fi:
  - Limitarea utilizatorilor la anumite meniuri şi aplicaţii.
  - Împiedicarea utilizatorilor de a introduce comenzi (facilităţi limitate în profilurile de utilizator).

Începeţi planificarea securităţii resurselor prin definirea obiectivelor. Puteţi defini obiectivele de securitate fie prin formularul de Descriere Aplicaţii fie prinformularul Descriere Biblioteci.

Formularul pe care îl folosiţi depinde de modul de organizare a informaţiilor în biblioteci.

Puteţi revedea un exemplu de obiective de securitate al Companiei JKL Toy înainte de a revedea tipurile de autorizări pe care le puteţi folosi pentru securitatea resurselor.

Exemplu: Obiective de securitate la Compania JKL Toy

Sharon Jones de la Compania JKL Toy a utilizat formularul Descriere bibliotecă pentru a descrie cerinţele de securitate pentru biblioteca Customer Records (CUSTLIB):

Tabela 36. Exemplu Formular descriere bibliotcă la Compania JKL Toy: obiective de securitate

Formular Descriere bibliotecă	Partea 1 din 2

Tabela 36. Exemplu Formular descriere bibliotcă la Compania JKL Toy: obiective de securitate (continuare)

Definiţi obiectivele de securitate pentru bibliotecă, cum ar fi dacă vreo informaţie este confidenţială:	Astăzi, oricui din companie i se permite să se uite la informaţiile despre clienţi şi la comenzile de la clienţi. Pentru a proteja acurateţea informaţiilor, ar trebui să controlăm cine are dreptul să le modifice.

Sharon a utilizat formularul Descriere aplicaţie pentru aplicaţia Contracts and Pricing pentru a descrie obiectivele de securitate pentru întreaga aplicaţie.

Tabela 37. Exemplu Formular descriere aplicaţie la Compania JKL Toy: obiective de securitate

Formular Descriere aplicaţie	Partea 1 din 2
Definiţi obiectivele de securitate pentru bibliotecă, cum ar fi dacă vreo informaţie este confidenţială:	Informaţiile despre contracte şi preţuri speciale sunt considerate confidenţiale. Numai câteva persoane sunt autorizate să le vadă şi să le modifice: • Personalul Vânzări şi Marketing şi toţi directorii trebuie să creeze, să modifice şi să analizeze contracte. Ei trebuie să utilizeze atât fişierele, cât şi programele. • Personalul de la Procesare comenzi modifică contracte şi indirect văd preţurile când introduc şi livrează comenzi. Lor nu le este permis să se uite la contracte şi preţuri decât atunci când introduc sau modifică o comandă.

Scrieţi-vă obiectivele de securitate pentru aplicaţie fie în formularul Descriere aplicaţie, fie în formularul Descriere bibliotecă. Puteţi apoi să revedeţi tipurile de autorizări pe care le puteţi utiliza pentru planificarea securităţii resurselor.

Înţelegerea tipurilor de autorizări

După ce aţi determinat obiectivele pentru securitatea resurselor şi aţi înregistrat deciziile în formularul Descriere Bibliotecă, puteţi începe să planificaţi tipurile de autorizare. Securitatea resurselor defineşte modul în care utilizatorii au acces la obiectele din sistem.

Autorizarea se referă la modul în care persoanele sunt autorizate să folosească un obiect. De exemplu, puteţi avea autorizare să vedeţi informaţii sau să modificaţi informaţii din sistem. Sistemul pune la dispoziţie câteva tipuri de autorizări. IBM grupează aceste tipuri de autorizări în categorii, numite **autorizări definite de sistem**, care corespund necesităţilor obişnuite. Tabelul de mai jos listează categoriile şi vă arată cum se aplică la securitatea fişierelor şi programelor.

Notă: Consultaţi tabelul de mai jos când planificaţi autorizările.

Tabela 38. Autorizări definite de sistem

Nume autorizare	Operaţii permise pentru fişiere	Operaţii interzise pentru fişiere	Operaţii permise pentru programe	Operaţii interzise pentru programe
*USE	Vizualizarea informaţiilor din fişier.	Modificarea sau ştergerea oricărei informaţii din fişier. Ştergerea fişierului.	Rularea programului.	Modificarea sau ştergerea programului.
*CHANGE	Vizualizarea, modificarea şi ştergerea înregistrărilor din fişier.	Ştergerea sau curăţarea intrărilor fişier.	Modificarea descrierii unui program.	Modificarea sau ştergerea programului.

Tabela 38. Autorizări definite de sistem (continuare)

Nume autorizare	Operaţii permise pentru fişiere	Operaţii interzise pentru fişiere	Operaţii permise pentru programe	Operaţii interzise pentru programe
*ALL	Crearea sau ştergerea fişierului. Adăugarea, modificare şi ştergerea înregistrărilor din fişier. Autotizarea altora să folosească fişierul.	Nimic	Crearea, modificarea, şi ştergerea programului. Autorizarea altora să folosească programul.	Modificarea proprietarului unui program, dacă programul are autoritate adoptată.
*EXCLUDE[1]	Nimic	Accesul la fişier.	Nimic	Accesul la program.
1 *EXCLUDE suprascrie orice autorizare publică sau de profil de grup pe care aţi obţinut-o .				

Înţelegerea modul în care autorizăre obiect şi autorizare bibilotecă funcţionează împreună

Pentru a proiecta o securitate a resurselor elementară, încercaţi să planificaţi securitatea pentru întreaga bibliotecă. Pentru a face aceasta, trebuie să înţelegeţi modul în care sunt aplicate bibliotecilor autorizările definite de sistem, descrise în tabelul de mai jos:

Tabela 39. Autorizări definite de sistem pentru biblioteci

Nume autorizare	Operaţii permise	Operaţii interzise
*USE	• Pentru obiectele din bibliotecă, autorizarea permite orice operaţie asupra unui anumit obiect. • Vizualizaţi informaţii descriptive, pentru bibliotecă.	• Adăugaţi noi obiecte bibliotecii. • Modificaţi descrierea bibliotecii. • Ştergerea bibliotecii.
*CHANGE	• Pentru obiectele din bibliotecă, autorizarea permite orice operaţie asupra unui anumit obiect. • Adăugaţi noi obiecte bibliotecii. • Modificaţi descrierea bibliotecii.	• Stergerea bibliotecii.
*ALL	• Orice se poate modifica. • Ştergerea bibliotecii. • Autorizarea altora să folosească biblioteca.	• Nimic

De asemenea, trebuie să înţelegeţi modul în care funcţionează împreună autorizare obiect şi autorizare bibliotecă. Tabela de mai jos vă oferă exemple de autorizări care sunt necesare pentru obiecte şi biblioteci:

Tabela 40. Modul în care funcţionează împreună autorizare bibliotecă şi autorizare obiect

Tipul obiect	Operaţii	Autorizare obiect necesară	Autorizare bibliotecă necesară
Fişier	Modificarea datelor	*CHANGE	*USE
Fişier	Ştergerea fişierului.	*ALL	*USE
Fişier	Crearea unui fişier	*ALL	*CHANGE
Program	Rularea unui program.	*USE	*USE
Program	Modificarea (recompilarea) unui program	*ALL	*CHANGE
Program	Ştergerea unui program	*ALL	*USE

Autorizare director este similară cu autorizare bibliotecă. Aveţi nevoie de autorizare pentru toate directoarele aflate în numele cale, în ordine, pentru a putea accesa obiectul.

Acum sunteţi pregătiţi să planificaţi securitatea bibliotecilor aplicaţiilor.

Planificarea securităţii pentru bibliotecile aplicaţiei

După ce aţi determinat obiectivele pentru securitatea resurselor, puteţi începe planificarea securităţii pentru bibliotecile aplicaţiilor. Alegeţi una din bibliotecile aplicaţiilor pentru a lucra urmând procesul descris aici. Dacă sistemul stochează fişiere şi programe în biblioteci separate, alegeţi o bibliotecă ce conţine fişierele. Când ajungeţi la sfârşitul subiectului, repetaţi aceşti paşi pentru bibliotecile aplicaţiilor rămase.

Revedeţi informaţiile pe care le-aţi obţinut despre aplicaţii şi biblioteci:

- Formular Descriere Aplicaţii
- Formular Descriere Bibliotecă
- Formular Descriere Grup Utilizator pentru oricare grup care are nevoie de bibliotecă
- Diagrama aplicaţiilor, bibliotecilor şi grupurilor utilizator

Reflectaţi asupra grupurilor care au nevoie de informaţii într-o bibliotecă, de ce au nevoie de acele informaţii şi ce vor să facă cu ele.

Determinarea conţinutului unei biblioteci

Bibliotecile aplicaţiei conţin fişiere importante ale aplicaţiei. Pot de asemenea să conţină alte obiecte, cele mai multe fiind unelte de programare pentru a face aplicaţia să funcţioneze corespunzător, cum ar fi:

- Fişiere de lucru
- Zona de date şi cozi de mesaje
- Programe
- Fişiere de mesaje
- Comenzi
- Cozi de ieşire

Cele mai multe dintre obiecte, altele decât fişierele şi cozile de ieşire, nu expun securitatea. De obicei ele conţin cantităţi mici de date ale aplicaţiei adesea într-un format care nu este uşor de înţeles înafara programului. Puteţi lista numele şi descrierile tuturor obiectelor dintr-o bibliotecă folosind comanda Afişare Bibliotecă. De exemplu, pentru a lista conţinuturile bibliotecii CONTRACTS folosiţi comanda: DSPLIB LB(CONTRACTS) OUTPUT(*PRINT)

Apoi decideţi ce autorizare publică vreţi să aveţi pentru bibliotecile aplicaţiei şi bibliotecile programelor.

Deciderea autorizării publice pentru bibliotecile aplicaţiei

Referitor la securitatea resurselor, **public** înseamnă orice persoană autorizată să semneze pe sistem. **Autorizarea publică** permite unui utilizator accesul la un obiect dacă nu are orice alt nivel de acces mai mare. În plus la deciderea autorizării publice pentru obiectele deja adăugate în bibliotecă, puteţi specifica autorizare publică pentru orice nou obiect adăugat mai târziu în bibliotecă. Pentru a face aceasta, folosiţi parametrul **Creare Autorizare (CRTAUT)**. De obicei, autorizarea publică la obiectele bibliotecii şi la bibliotecă ar trebui să creeze acelaşi tip de autorizare asupra noilor obiecte.

Valoarea sistem QCRTAUT (Creare Autoritate) determină domeniul sistem de autorizare publică pentru noile obiecte. IBM livrează valoarea de sistem QCRTAUT setată la *CHANGE. Evitaţi modificarea QCRTAUT, pentru că funcţionarea multor sisteme foloseşte această valoare. Dacă specificaţi valoarea sistem *SYSVAL pentru Creare Autorizare (CRTAUT) a unei biblioteci aplicaţie, aceasta foloseşte pentru QCRTAUT valoarea sistem(*CHANGE).

Folosiţi autorizarea publică cât de mult este posibil, pentru îmbunătăţirea performanţei. Pentru a determnina ce autorizare publică ar trebui să se aplice asupra unei biblioteci, puneţi-vă aceste întrebări:

- Ar trebui oricine din companie să aibă acces la cele mai multe informaţii din această bibliptecă?
- Ce tip ce acces ar trebui să aibă persoanele la majoritatea informaţiilor din această bibliotecă?

Concentraţi-vă asupra deciziilor pentru majoritatea persoanelor şi majoritatea informaţiilor. Mai târziu, veţi învăţa cum să trataţi excepţiile. Planificarea securităţii resurselor este adesea un proces circular. Puteţi descoperi că trebuie să faceţi modificări la autorizarea publică după analizarea necesităţilor pentru anumite obiecte. Încercaţi mai multe combinaţii de autorizări publice şi private pentru obiecte şi biblioteci înainte de a o alege pe cea care se potriveşte cu nevoile de performanţă şi securitate.

Asigurarea autorizării adecvate

Autorizarea *CHANGE pentru obiecte şi autorizarea *USE pentru o bibliotecă se potrivesc cu cele mai multe funcţii aplicaţie. Totuşi, aveţi nevoie să întrebaţi programatorul sau furnizorul aplicaţiei dacă funcţiile aplicaţie necesită autorizare mai mare:

- Este şters vreun fişier sau obiect din bibliotecă în timpul procesării? Sunt fişierele curăţate? Sunt adăugaţi membrii la fişiere? Ştergerea unui obiect, curăţarea unui fişier, sau adăugarea unui membru fişier necesită autorizarea *ALL pentru obiect.
- Sunt fişierele sau alte obiecte create în bibliotecă în timpul procesării? Crearea unui obiect necesită autorizarea *CHANGE pentru bibliotecă.

Puteţi revedea un exemplu despre autorizările asupra obiectelor pe care Sharon le-a făcut, înainte de deciderea autorizării publice la bibliotecile unui program.

Exemplu: Formular descriere bibliotecă la Compania JKL Toy:

Sharon Jones a revăzut obiectivele de securitate pentru biblioteca Înregistrări clienţi, ca şi informaţiile despre aplicaţii şi departamentele care utilizează informaţiile despre clienţi. Ea şi-a notat concluziile:

- Fiecare departament, cu excepţia celor de Depozit şi Producţie, trebuie să schimbe informaţii despre clienţi.
- Toţi utilizatorii din departamentele Depozit şi Producţie au profiluri utilizator cu Facilităţi limitate (Yes) şi sunt restricţionaţi la anumite meniuri sau programe. Meniurile lor le permit să vadă informaţii despre clienţi, dar nu şi să le modifice.
- Autorizarea publică pentru obiectele din biblioteca Înregistrări clienţi poate fi setată la *CHANGE. Restricţiile la meniuri împiedică persoanele neautorizate să modifice informaţiile despre clienţi. Totuşi, acest lucru trebuie reevaluat dacă mai târziu alte departamente sunt adăugate în sistem.

Acesta este un exemplu de abordare relaxată la informaţii. În acest caz, excepţiile sunt tratate prin profilurile de utilizator, mai degrabă decât prin folosirea restricţiilor de autorizare. Sharon a completat partea despre autorizarea publică din formularul Descriere bibliotecă pentru biblioteca Înregistrări clienţi (CUSTLIB).

Tabela 41. Exemplu formular descriere bibliotecă la Compania JKL Toy—Partea 1: Înregistrări clienţi

Nume bibliotecă: CUSTLIB	Nume descriptiv (text): Înregistrări clienţi
Autorizare publică la bibliotecă:	*USE
Autorizare publică şi obiectele din bibliotecă:	*CHANGE
Autorizare publică pentru obiecte noi (CRTAUT):	*CHANGE

Sharon Jones a descoperit că unele fişiere temporare din biblioteca Înregistrări clienţi sunt curăţate în timpul procesării de sfârşit de luna a aplicaţiei Accounts Receivable. Ea a ales să trateze autorizarea pentru aceste filiere individual, decât să-şi asume riscul ca alte obiecte din bibliotecă să fie şterse accidental. Pentru toate celelalte activităţi de procesare, autorizarea *CHANGE este suficientă.

Deşi numai puţine persoane rulează procesarea de sfârşit de lună, Sharon a considerat că fişierele temporare nu expun la nici un risc de securitate. Ea a decis să acorde autorizarea publică *ALL pentru aceste fişiere, decât să acorde

autorizare numai persoanelor care rulează procesarea de sfârşit de lună. Tabelul de mai jos arată partea a doua a formularului Descriere bibliotecă pentru biblioteca Înregistrări clienţi:

Tabela 42. Exemplu formular Descriere bibliotecă la Compania JKL Toy—Partea 2: Înregistrări clienţi

Listare autorizări specifice pentru obiecte biblioteci				
Profil grup sau profil utilizator	Nume obiect	Tip obiect	Autorizare necesară	Listă de autorizaţii
PUBLIC	ARFILE01	*FILE	*ALL	
PUBLIC	ARFILE02	*FILE	*ALL	
PUBLIC	ARFILE03	*FILE	*ALL	

Puteţi acum să decideţi autorizarea publică la bibliotecile program pe care le doriţi.

Deciderea autorizării publice pentru bibliotecile programului

Des, programele aplicaţiei sunt păstrate în biblioteci separat de fişiere şi alte obiecte. Nu este necesar să folosiţi biblioteci separate pentru aplicaţii, însă mulţi programatori folosesc această tehnică când proiectează aplicaţiile. Dacă aplicaţiile au bibliotecile programelor separat, trebuie să decideţi autoritatea publică la acele biblioteci. S-ar putea să ajungă folosirea autorizării *USE la ambele, la bibliotecă şi la programele din bibliotecă, pentru a rula, dar bibliotecile de programe pot avea alte obiecte care necesită autorizare suplimentară. Puneţi câteva întrebări programatorului:

- Foloseşte aplicaţia zone de date sau cozi de mesaje pentru a comunica între programe? Sunt ele în biblioteca programului? Este necesară autorizarea *CHANGE la un obiect pentru a manipula zonele de date şi cozile de mesaje.
- Există obiecte în biblioteca programului, cum ar fi zone de date, şterse în timpul procesării? Este necesară autorizarea *ALL la un obiect pentru a fi şters.
- Este vreun obiect, cum ar fi o zonă de date, creeat în biblioteca programului în, timpul procesării? Trebuie să aveţi autorizare *CHANGE la o bibliotecă pentru a creea un nou obiect în bibliotecă.

Completaţi toate informaţiile de securitate resurse pe ambele părţi ale formularului Descriere bibliotecă cu excepţia proprietarului şi a coloanei cu liste de autorizări. Apoi puteţi determina proprietarul bibliotecii şi obiectelor.

Puteţi să revedeţi următoarele două exemple care arată modul în care Sharon Jones determină autorizarea la bibliotecile unui program. În primul exemplu, Sharon decide dacă o abordare non-restrictivă este corespunzătoare pentru biblioteca programului Comenzi Clienţi. Al doilea exemplu arată o abordare mult mai restrictivă pe care Sharon o utilizează pentru biblioteca programului Primire Conturi.

Exemplu: Formular descriere bibliotecă la Compania JKL Toy—abordare nerestrictivă: Sharon Jones a investigat biblioteca program Comenzi clienţi şi a făcut aceste observaţii:

- O coadă de mesaje, COMSGQ01, este utilizată pentru a comunica între programe.
- Coada de mesaje este curăţată, dar niciodată ştearsă. Autorizarea *CHANGE la coada de mesaje este suficientă.

Sharon a decis să acorde autorizarea *USE tuturor obiectelor din biblioteca program şi să definească coada de mesaje COMSGQ01 separat. Cele două tabele de mai jos arată formularul Descriere bibliotecă pentru biblioteca COPGMLIB:

Tabela 43. Exemplu Formular descriere bibliotcă la Compania JKL Toy: biblioteca cu programe

Formular descriere bibliotecă	**Partea 1 din 2**
Nume bibliotecă: COPGMLIB	Nume descriptiv (text): Bibliotecă programe Customer Order

Tabela 43. Exemplu Formular descriere bibliotcă la Compania JKL Toy: biblioteca cu programe (continuare)

Autorizarea publică la bibliotecă: *USE Autorizarea publică la obiectele din bibliotecă: *USE Autorizarea publică pentru obiectele noi (CRTAUT): *USE Proprietar bibliotecă:

Tabela 44. Exemplu Formular descriere bibliotcă la Compania JKL Toy: biblioteca cu programe

Formular descriere bibliotecă				**Partea 2 din 2**
Listare autorizări la obiecte individuale din bibliotecă				
Profil grup sau profil utilizator	Nume obiect	Tip obiect	Autorizare necesară	Liste de autorizaţii
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

Utilizarea autorizării la un program pentru a controla accesul

Deşi majoritatea persoanelor de la Compania JKL Toy au dreptul să modifice informaţii despre clienţi, numai câtorva persoane li se permite să seteze limitele de credit pentru clienţi. Limitele de credit sunt stocate în fişierul principal de clienţi (CUSTMAS), dar sunt modificate cu program separat numit ARPGM12 din ARPGMLIB. Sharon poate restricţiona accesul la program pentru a împiedica persoanele neautorizate să modifice limitele de credit. Teblele de mai jos arată formularul Descriere bibliotecă pentru ARPGMLIB:

Tabela 45. Exemplu Formular descriere bibliotcă la Compania JKL Toy: autorizare individuală

Formular Descriere bibliotecă	**Partea 1 din 2**
Nume bibliotecă: ARPGMLIB	Nume descriptiv (text): Bibliotecă programe Accounts Receivable
Autorizarea publică la bibliotecă: *USE Autorizarea publică la obiectele din bibliotecă: *USE Autorizarea publică pentru obiectele noi (CRTAUT): *USE Proprietar bibliotecă:	

Tabela 46. Exemplu Formular descriere bibliotcă la Compania JKL Toy: autorizare individuală

Formular Descriere bibliotecă				**Partea 2 din 2**
Listare autorizări la obiecte individuale din bibliotecă				
Profil grup sau profil utilizator	Nume obiect	Tip obiect	Autorizare necesară	Liste de autorizaţii
PUBLIC	ARPGM12	*PGM	*EXCLUDE	
JACOBS	ARPGM12	*PGM	*USE	
DAVISP	ARPGM12	*PGM	*USE	
SMITHJ	ARPGM12	*PGM	*USE	

Poate doriţi să revedeţi un exemplu restrictiv care utilizează autorizarea adoptată înainte de a începe să determinaţi dreptul de proprietate la biblioteci şi obiecte.

Exemplu: Formular descriere bibliotecă la Compania JKL Toy—abordare restrictivă: Exemplele de până acum au arătat o abordare relaxată a securităţii, în care cele mai multe persoane au acces la informaţiile dintr-o bibliotecă.

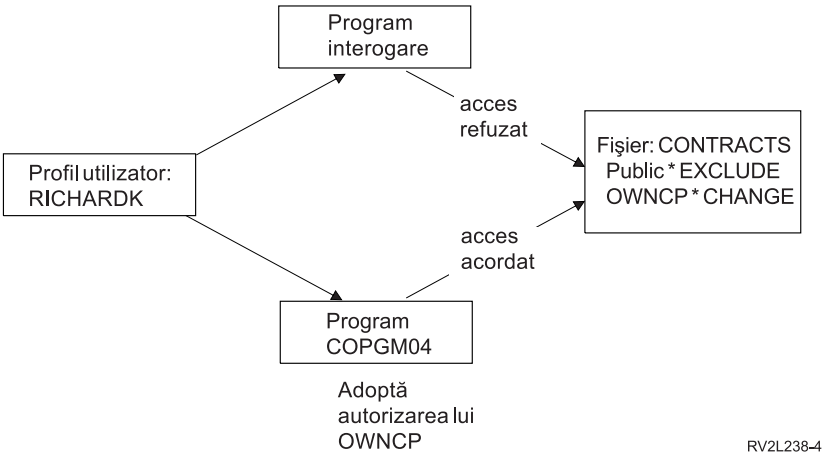
Informaţiile despre contracte şi preţuri sunt considerate confidenţiale la Compania JKL Toy şi necesită o abordare restrictivă. Din fericire, toate aceste informaţii sunt păstrate într-o bibliotecă separată. Programele care actualizează informaţiile despre preţ şi contracte sunt de asemenea într-o bibliotecă specială.

Sharon a revăzut obiectivele de securitate pentru aplicaţiile Contracts şi Pricing (vedeţi Determinarea obiectivelor pentru securitatea resurselor). Ea a revăzut de asemenea formularul Descriere aplicaţie şi formularele Descriere bibliotecă. Sharon a simţit că va fi dificil să îndeplinească obiectivele de securitate pentru aplicaţie. Ea a făcut câteva observaţii şi a discutat problema cu furnizorul lor de aplicaţie:

- Personalul Vânzări şi Marketing şi directorii trebuie să creeze şi să modifice contracte. Ei trebuie să utilizeze atât fişierele, cât şi programele.
- Personalul de la Procesare comenzi modifică contrace şi indirect văd preţurile când introduc şi livrează comenzi, dar nu le este permis să vadă contractele şi preţurile pe altă cale. Totuşi, vor utiliza Query pentru a-şi crea propriile rapoarte despre clienţi şi comenzi. Dacă li se dă autorizare la fişierele Contracte şi Preţuri, ar putea crea programe Query pentru a le vizualiza şi tipări.

Furnizorul de aplicaţie pentru Compania JKL Toy a sugerat folosirea autorizării adoptate pentru a rezolva această problemă. **Autorizarea adoptată** permite unui utilizator să adopte autorizarea proprietarului în timpul rulării programului. Utilizatorul nu are nevoie de autorizare la obiect.

Diagrama de mai jos arată un exemplu a modului în care funcţionează autorizarea adoptată. Karen Richards (RICHARDK) din departamentul Procesare comenzi nu are în mod normal autorizare să folosească fişierul Contracte. Totuşi, când introduce comenzi, ea trebuie să verifice şi să actualizeze balanţele de contract. Programul de introducere comenzi care lucrează cu cel de balanţe contracte (COPGM04) adoptă autorizarea profilului OWNCP. În timp ce Karen rulează programul COPGM04, ea are autorizare să utilizeze fişietul de contracte:



Consultaţi subiectul ″Determinarea dreptului de proprietate pentru biblioteci şi obiecte″ pentru detalii despre dreptul de proprietate asupra obiectelor. Furnizorul sau dezvoltatorul de aplicaţie poate specifica că programul adoptă autorizarea proprietarului la crearea (compliarea) progamului sau un programator poate specifica autorizare adoptată pentru un program cu comanda Change Program (CHGPGM). Asiguraţi-vă că înţelegeţi toate funcţiile programului înainte de a utiliza această tehnică.

Sharon a decis să utilizeze funcţia de autorizare adoptată pentru a acorda persoanelor din afara departamentului de Vânzare ş Marketing acces la fişierele de contracte şi preţuri. Ea a determinat de asemenea că accesul *CHANGE a fost suficient pentru toate obiectele utilizate de aplicaţia Contracte şi preţuri. Tabelul de mai jos arată formularul Descriere bibliotecă pentru biblioteca Contracte:

Tabela 47. Exemplu Formular descriere bibliotecă la Compania JKL Toy: autorizare restrictivă

Formular Descriere bibliotecă	**Partea 1 din 2**
Nume bibliotecă: CONTRACTS	Nume descriptiv (text): Bibliotecă Contracte şi preţuri

Tabela 47. Exemplu Formular descriere bibliotecă la Compania JKL Toy: autorizare restrictivă (continuare)

Autorizarea publică la bibliotecă: *EXCLUDE
Autorizarea publică la obiectele din bibliotecă: *CHANGE
Autorizarea publică pentru obiectele noi (CRTAUT): *CHANGE
Proprietar bibliotecă:

Tabela 48. Exemplu Formular descriere bibliotecă la Compania JKL Toy: autorizare restrictivă

Formular Descriere bibliotecă				**Partea 2 din 2**
Listare autorizări la obiecte individuale din bibliotecă				
Profil grup sau profil utilizator	Nume obiect	Tip obiect	Autorizare necesară	Liste de autorizaţii
DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

Nu este nevoie să restricţionaţi autorizarea la obiectele dintr-o bibliotecă, pentru că restricţionaţi la bibliotecă. De asemenea, Sharon a acordat autorizare directorilor şi departamentului de Vânzări şi Marketing. Ea a utilizat autorizarea de grup, în loc să acorde autorizare la fiecare persoană din departamente.

Notă: Un programator cu destule cunoştinţe care are acces la o bibliotecă poate fi în stare să recâştige accesul la obiectele dintr-o bibliotecă chiar şi după ce aţi revocat autorizarea la bibliotecă. Dacă o bibliotecă are obiecte cu necesităţi sporite de securitate, restricţionaţi şi obictele şi biblioteca pentru o protecţie totală.

Poate doriţi să revedeţi un exemplu restrictiv care utilizează autorizarea publică înainte să începeţi să determinaţi dreptul de proprietate pentru biblioteci şi obiecte.

Determinarea proprietarului bibliotecilor şi obiectelor

După ce aţi planificat securitatea pentru bibliotecile aplicaţiilor, puteţi decide proprietarul bibliotecilor şi obiectelor. Fiecare obiect este asignat unui proprietar când este creeat. Proprietarul unui obiect automat are întreaga autorizare asupra obiectului, care include autorizarea altora pentru a folosi obiectul, modificarea obiectului, şi ştergerea lui. Responsabilul cu securitatea poate realiza aceste funcţii pentru orice obiect din sistem.

Sistemul foloseşte profilul proprietarului obiectului pentru a urmări cine are autorizare la obiect. Sistemul efectuază intern aceste funcţii. Aceasta nu afectează profilul utilizator în mod direct. Totuşi, dacă nu planificaţi corespunzător proprietarul unui obiect, unele profiluri utilizator pot deveni foarte mari.

Când sistemul salvează un obiect, se salvează şi numele profilului proprietarului o dată cu acesta. Sistemul foloseşte aceste informaţii dacă restaurează obiectul. Dacă profilul cu drept de proprietate pentru a restaura un obiect nu este în sistem, sistemul transferă dreptul de proprietate unui profil furnizat de IBM numit QDFTOWN.

Recomandări

Recomandările de mai jos se aplică în multe situaţii însă nu în toate. După ce aţi revăzut recomandările, discutaţi ideile referitoare la proprietarul obiectului cu programatorul sau furnizorul aplicaţiei. Dacă aţi cumpărat aplicaţiile, nu veţi putea să controlaţi care profil are drept de proprietate asupra bibliotecilor şi obiectelor. Aplicaţiile pot fi proiectate să împiedice modificarea dreptului de proprietate.

- Evitaţi folosirea unui profil furnizat de IBM, cum ar fi QSECOFR sau QPGMR, ca profil cu drept de proprietate asupra aplicaţiei. Aceste profiluri deţin multe obiecte în bibliotecile furnizate de IBM şi sunt deja foarte mari.
- În mod normal,un profil de grup nu ar trebui să aibă drept de proprietate asupra unei aplicaţii. Fiecare menbru al grupului are aceeaşi autorizare ca şi profilul de grup, chiar dacă asignaţi în mod special o autorizare mai joasă. De fapt, ar trebui să-i daţi fiecărui membru al grupului autorizare completă asupra aplicaţiei.

- Dacă planificaţi să delegaţi responsabilitatea pentru controlul aplicaţiilor managerilor din departamente diferite, acei manageri ar putea avea drept de proprietate asupra tuturor obiectelor aplicaţiei. Totuşi, managerul unei aplicaţii poate modifica responsabilităţile. În cazul acesta, puteţi transfera dreptul de proprietate asupra tuturor obiectelor aplicaţiei unui nou manager.
- Multe persoane folosesc tehnica de creare a profilului cu drept special de proprietate pentru fiecare aplicaţie cu parola setată la *NONE. Profilul cu drept de proprietate este folosit de sistem pentru a gestiona autorizările pentru aplicaţie. Responsabilul de securitate (sau cineva cu aceeaşi autorizare) realizează gestiunea actuală a aplicaţiei sau este delegat să gestioneze cu autorizarea *ALL anumite aplicaţii.

Decideţi care profiluri ar trebui să aibă drept de proprietate asupra aplicaţiilor. Introduceţi informaţiile despre profilul cu drept de proprietate în fiecare formular Descriere Bibliotecă.

Puteţi să revedeţi un exemplu despre modul în care Compania JKL Toy determinbă dreptul de proprietate asupra aplicaţiilor înainte de a decide dreptul de proprietate şi accesul utilizatorilor la biblioteci.

Exemplu: dreptul de proprietate la aplicaţie la Compania JKL Toy

Sharon Jones a decis să creeze un profil special cu drept de proprietate pentru fiecare aplicaţie. Ea şi Ken Harrison, responsabilul cu securitatea de rezervă, vor prelua responsabilitatea pentru administrarea securităţii aplicaţiei. Mai târziu, dacă cerinţele de securitate ale companiei vor deveni mai complexe, Sharon poate delega unele responsabilităţi pentru administrarea securităţii şefilor de departamente.

Sharon a adăugat o nouă intrare în formularul ei de Convenţii nume:

Tabela 49. Exemplu Formular conveţie nume la Compania JKL Toy: Profil cu drept de proprietate

Tip obiect	Convenţie nume
Profil proprietar	Un profil cu drept de proprietate se va crea pentru fiecare aplicaţie. Acesta va deţine toate bibliotecile de aplicaţii şi obiectele din ele. Profilul proprietar va fi numit OWN plus abreviaţia aplicaţiei. Profilul proprietar Control inventar va fi OWNIC.

Sharon a decis să înceapă numele de profil proprietar cu OWN pentru ca toate profilurile proprietar să apară împreună pe ecrane şi liste.

Sharon a asignat proprietarii tuturor bibliotecilor de aplicaţie şi a introdus această informaţie în formularul Convenţii nume. Singura aplicaţie care avea mai mulţi proprietari posibili a fost biblioteca Înregistrări clienţi. Pentru că aplicaţia Accounts Receivable este utilizată pentru a crea noi clienţi şi pentru a seta limite de credit, Sharon a decis că ar trebui să fie proprietarul fişierelor clienţi. Aceştia sunt proprietarii asignaţi de ea:

Nume bibliotecă	Nume proprietar
ICPGMLIB	OWNIC
ITEMLIB	OWNIC
CONTRACTS	OWNCP
CPPGMLIB	OWNCP
COPGMLIB	OWNCO
CUSTLIB	OWNAR
ARPGMLIB	OWNAR

Puteţi acum să decideţi dreptul de proprietate şi accesul la bibliotecile utilizator.

Deciderea dreptului de proprietate şi accesul pentru utilizarea bibliotecilor

Dacă pe sistemul dumneavoatră rulează programul licenţiat IBM Query pentru iSeries sau alt program de suport pentru decizii, utilizatorii au nevoie de o bibliotecă în care să-şi stocheze programele de le creează. În mod normal, această bibliotecă este **biblioteca curentă** din profilul de utilizator. Pentru mai multe informaţii despre crearea unei biblioteci

curente pentru fiecare utilizator, vedeţi ″Alegere valorilor care afectează semnarea.″ Sharon Jones planifică să folosească bibliotecile curente pentru departamentul Vânzări şi Marketing şi bibliotecile de grup pentru alte departamente:

- Persoanele de la Vânzări şi Marketing vor fi utilizatori din greu ai interogărilor. Fiecare utilizator ar trebui să aibă o bibliotecă privată. Altfel, ar trebui să se îngrijoreze în legătură cu numele interogărilor, pentru că ar putea şterge accidental orice alte programe.
- pentru început, alte departamente vor avea biblioteci de grup. Dacă ei au creeat mai multe programe Interogare, putem considera bibliotecile individuale.

Dacă un utilizator aparţine unui grup, folosiţi un câmp în profilul utilizator pentru a specifica dacă utilizatorul sau grupul are drept de proprietate asupra oricăror obiecte create de utilizator. Dacă utilizatorul are drept de proprietate asupra obiectelor, puteţi specifica ce autorizare au membrii grupului să folosească obiectele. De asemenea, puteţi specifica dacă autorizarea grupului este primară sau privată. Autorizarea de grup primară poate furniza o mai bună performanţă a sistemului. Sharon face câteva însemnări suplimentare despre utilizarea bibliotecilor:

- Persoanele de la Vânzări şi Marketing ar trebui să aibă drept de proprietate asupra obiectelor pe care le-au creat, mai degrabă decât să aibă grupul drept de proprietate asupra lor. Ei nu trebuie să modifice fiecare dintre programele de interogare.
- Oricine din grup ar trebui să fie capabil să ruleze programele Interogări ale altora, ceea ce înseamnă că grupul obţine autorizare *USE asupra oricăror obiecte create de un membru al grupului.
- Autorizarea grupului ar trebui să fie autorizare grup primară.
- Persoanele publice nu ar trebui să aibă acces la aceste biblioteci. Persoanele de la Vânzări şi Marketing pot avea fişiere de ieşire de la interogările lor. Acele fişiere pot conţine date confidenţiale.
- Pentru alte departamente, grupul va avea drept de proprietate asupra bibliotecilor de grup şi asupra a tot ce este creat în bibliotecă. Aceasta înseamnă că orice membru al grupului poate modifica sau şterge orice din bibliotecă. Dacă aceasta cauzează probleme, trebuie să încercaţi altă metodă.

Tabela de mai jos arată Formularul Profil Utilizator Individual pentru departamentul vânzări şi Marketing care foloseşte obiecte cu drept de proprietate pentru utilizatori:

Tabela 50. Formular Profil Utilizator Individual al Companiei JKL Toy: Exemplu de drepturi de proprietate a utilizatorilor asupra obiectelor

Numele profil grup: DPTSM	
Dreptul de proprietate asupra obiectelor create: *USRPRF	Autorizare grup asupra obiectelor create: *USE
Tipul autorizare grup: *PGP	

Tabela de mai jos arată Formularul Profil Utilizator Individual pentru un departament care are obiecte cu drept de proprietate pentru grup:

Tabela 51. Formularul Profil Utilizator Individual al Companiei JKL Toy: Exemple de obiecte cu drept de proprietate pentru grup

Numele profil grup: DPTxx	
Proprietar al obiectelor create: *GRPPRF	Autorizare grup pentru obiectele create:

Câmpul Autorizare **Grup la obiectele create** nu este folosit dacă dreptul de proprietate asupra obiectelor create îl are grupul. Membrii grupului automat au autorizarea *ALL la orice obiect creat.

Decideţi cine ar trebui să aibă drept de proprietate şi acces să folosească bibliotecile. Introduceţi alegerile în câmpurile**Drept de Proprietate a obiectelor create** şi **Autorizare Grup peste obiecte** în formularul Profil Utilizator Individual. Acum sunteţi pregătit să începeţi gruparea obiectelor .

Gruparea obiectelor

După ce aţi determinat dreptul de proprietate asupra bibliotecilor şi obiectelor, puteţi începe gruparea obiectelor în sistem. Pentru a simplifica gestionarea autorizărilor, folosiţi o listă de autorizare pentru a grupa obiectele cu aceleaşi cerinţe Puteţi da apoi autorizarea publică, de profiluri de grup şi de profiluri de utilizator în lista de autorizări, decât obiectelor individuale din listă. Sistemul tratează la fel în lista de autorizări fiecare obiect pe care l-aţi securizat, însă puteţi da diferiţilor utilizatori anumite autorizări pentru întreaga listă.

O listă de autorizări vă permite să restabiliţi autorizările mai uşor când restauraţi obiecte. Dacă securizaţi obiecte cu o listă de autorizare, procesul de restaurare automat leagă obiectele de listă.

Puteţi da unui grup sau utilizator autorizarea de a gestiona o listă de autorizări (*AUTLMGT). Gestionarea listei de autorizări pemite utilizatorilor să adauge sau să înlăture alţi utilizatori din listă şi să modifice autorizările pentru acei utilizatori.

Recomandări

- Folosiţi liste de autorizări pentru obiecte care necesită protecţie de securitate şi care au cerinţe de securitate similare. Folsind listele de autorizaţii încurajaţi modul de gândire relativ la categoriile de autorităţii mai degrabă decât la autorităţi individuale. De asemenea, listele de autorizaţii fac mai uşoară restaurarea obiectelor şi auditarea autorizaţiilor în sistem.
- Evitaţi schemele complicate care combină listele de autorizaţii, autorizaţie grup, şi autorizaţie individuală. Alegeţi metoda care se potriveşte cel mai bine cerinţelor dumneavoastră, mai degrabă decât să folosiţi toate metodele în acelaşi moment.

De asemenea, veţi avea nevoie să adăugaţi convenţia de nume pentru listele de autorizaţii în formularul Covenţii de Nume.

O dată ce aţi pregătit un formular Lista de Autorizaţii, întoarceţi-vă şi adăugaţi acele informaţii formularului Descriere Bibliotecă. Programatorul sau furnizorul aplicaţiei pot avea deja create listele de autorizaţii. Aveţi grijă să-i consultaţi.

Puteţi găsi folositor să revedeţi un exemplu despre modul în care Sharon Jones de la Compania JKL Toy a planificat listele de autorizaţii înainte de aplanifica securizarea pentru imprimante şi ieşiri imprimantă.

Exemplu:Formularul listă autorizaţii la Compania JKL Toy

Sharon a revăzut Descrierea bibliotecă pentru biblioteca Înregistrări clienţi şi a decis să creeze o listă de autorizaţii pentru fişierele care sunt curăţate la sfârşitul fiecărei luni. Deşi sunt curăţate numai trei fişiere, Sharon a decis să utilizeze o listă de autorizaţii pentru a simplifica gestiunea autorizărilor. Dacă mai târziu sunt adăugate alte fişiere la procesarea de sfârşit de lună, ea poate apoi pur şi simplu să securizeze acele fişiere cu lista de autorizaţii. Sharon a decis să excludă publicul de la fişiere, pentru a împiedica problemele neintenţionate în timpul procesării de sfârşit de lună. Ea a acordat autorizare *ALL numai acelor utilizatori care rulează procesarea. Rose Willis, operatorul sistem în timpul serii, poate avea nevoie să vadă informaţiile despre fişiere pentru a verifica procesarea de sfârşit de lună. Ea are nevoie de autorizare *USE.

Tabelul de mai jos ilustrează convenţia de nume pe care a utilizat-o Sharon pentru listele de autorizaţii:

Tabela 52. Exemplu Formular Convenţie nume la Comapnia JKL Toy: Listă autorizaţii

Formular convenţii nume	
Pregătit de: Sharon Jones	Data: 9/5/99
Tip obiect	**Convenţe nume**
Liste de autorizaţii	Pentru listele care securizează obictele dintr-o bibliotecă, utilizaţi o parte din numele bibliotecii şi un număr. O listă pentru obiectele din CUSTLIB ar fi CUSTLST1. Pentru o listă care securizează obiectele din mai multe biblioteci, utilizaţi dacă este posibil o abreviaţie de aplicaţie: ARLST1. Dacă lista se aplică mai multor aplicaţii, alegeţi orice nume cu sens. Descrierea pentru listă ar trebui să reflecte scopul ei principal.

Tabelul de mai jos arată formularul Listă de autorizaţii pentru biblioteca CUSTLIB. Sharon a pregătit acest formular utilizând informaţia din formularul Descriere bibliotecă:

Tabela 53. Plan Listă de autorizaţii la Compania JKL Toy: exemplu

Formular Listă de autorizaţii					
Nume listă de autorizaţii: CUSTLST1					
Descriere: Fişierele curăţate în timpul procesării de sfârşit de lună.					
Listaţi obiectele securizate de listă					
Nume obiect	Tip obiect	Bibliotecă obiect	Nume obiect	Tip obiect	Bibliotecă obiect
ARFILE01	*FILE	CUSTLIB	ARFFILE02	*FILE	CUSTLIB
ARFILE03	*FILE	CUSTLIB			
Listaţi grupurile şi utilizatorii care au acces la listă					
Grup sau utilizator	Tipul de acces permis	Administrare listă?	Grup sau utilizator	Tipul de acces permis	Administrare listă?
PUBLIC	*EXCLUDE	no	ROSSG	*ALL	no
SMITHJ	*ALL	no	JONESS	*ALL	yes
WILLISR	*USE	no			

Sharon a adăugat de asemenea informaţiile despre lista de autorizaţii în formularul Descriere bibliotecă pentru biblioteca CUSTLIB:

Formular Descriere bibliotecă				Partea 2 din 2
Pregătit de: Sharon Jones			Data: 9/9/99	
Nume bibliotecă: CUSTLIB				
Listare autorizări specifice pentru obiectele bibliotecii				
Profil grup sau profil utilizator	Nume obiect	Tip obiect	Autorizare necesară	Listă de autorizaţii
PUBLIC	ARFILE01	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE02	*FILE	*AUTL	CUSTLST1
PUBLIC	ARFILE03	*FILE	*AUTL	CUSTLST1

Observaţi că autorizarea publică pentru fiecare fişier trebuie modificată la *AUTL pentru ca sistemul să utilizeze lista de autorizaţii pentru determinarea autorizării publice.

Uitaţi-vă la autorizările de grup sau individuale din formularele dumneavoastră de Descriere bibliotecă. Decideţi dacă este potrivită utilizarea listelor de autorizaţii. Dacă da, pregătiţi formulare Listă de autorizaţii şi actualizaţi formularele Descriere bibliotecă cu informaţiile despre lista de autorizaţii. Puteţi apoi să planificaţi securitatea pentru imprimante şi ieşire imprimante.

Planificarea securităţii imprimantei şi ieşirii de imprimantă

După ce vă grupaţi obiectele, aveţi nevoie să plănuiţi cum să protejaţi ieşirea imprimantei. Va trebuie să dezvoltaţi planuri pentru a proteja informaţia memorată pe sistemul vostru. De asemenea aveţi nevoie de un plan de protecţie a informaţiilor confidenţiale în timp ce acestea sunt tipărite sau aşteaptă să fie tipărite. Verificaţi în Planul de securitate fizică ce imprimante foloseşte compania dumneavoastră pentru ieşirile confidenţiale.

Atunci când rulaţi un program care tipăreşte un raport, de obicei raportul nu ajunge direct la imprimantă. Programul creează o copie a raportului, numită **fişier spool** sau **ieşire de imprimantă**. Sistemul memorează fişierul spool într-un

obiect numit **coadă de ieşire** până când o imprimantă e valabilă. Când coada de ieşire conţine o ieşire de imprimantă, puteţi vedea raportul la staţia dumneavoastră. De asemenea îl puteţi reţine sau redirecta la o anumită imprimantă.

Spooling-ul face mai uşoară planificarea joburilor de printare şi partajarea imprimantelor. Spooling-ul de asemenea vă ajută să protejaţi confidenţialitatea ieşirii. Puteţi crea una sau mai multe cozi de ieşire speciale care să păstreze confidenţialitatea ieşirii şi să restricţioneze cine poate vizualiza şi gestiona aceste cozi de ieşire. Deasementea puteţi controla când o ieşire confidenţială este trimisă din coadă către imprimantă.

Completaţi formularul Securitatea ieşirilor de imprimantă şi a staţiei de lucru pe măsură ce treceţi prin acest subiect.

Când creaţi o coadă de ieşire specială, puteţi specifică mai mulţi parametri care au legatură cu securitatea:

- **Parametrul Afişare Data (DSPDTA)**: Parametrul DSPDTA al unei cozi de ieşire determină dacă un utilizator poate vedea, trimite sau copia un fişier spool aparţinând altui utilizator.
- **Parametrul Authority to Check (AUTCHK)**: Parametrul AUTCHK determină dacă un utilizator poate schimba sau şterge un fişier spool aparţinând altui utilizator.
- **Parametrul Operator Control (OPRCTL)**: Parametrul OPRCTL determină dacă utilizatorii care au autoritatea speciala *JOBCTL (sau cei din clasa *SYSOPR) au permisiunea de a controla coada de ieşire.

Parametrii cozii de ieşire, autorizarea utilizatorului asupra cozii de ieşire, şi autorizarea specială a utilizatorului lucrează împreună la determinarea funcţiilor pe care un utilizator le-ar putea realiza asupra unui fişier spool dintr-o coadă de ieşire. Tabelul de mai jos arată ce combinaţii permit utilizatorilor realizarea de diferite funcţii:

Funcţii de printare	Parametrul Coadă de Ieşires			Autorizare coadă de ieşire	Autorizare specială
	DSPDTA	AUTCHK	OPRCTL		
Adaugă fişier de spool în coadă[1]	Oricare	Oricare	Oricare	*READ	Nimic
	Oricare	Oricare	*Yes	Oricare	*JOBCTL
Vizualizare lista de fişiere spool (comanda WRKOUTQ)[2]	Oricare	Oricare	Oricare	*READ	Nimic
	Oricare	Oricare	*Yes	Oricare	*JOBCTL
Afişează, copie sau trimite fişiere de spool (DSPSPLF, CPYSPFL, SNDNETSPLF, SNTCPSPLF)[2]	*YES	Oricare	Oricare	*READ	Nimic
	*NO	*DTAAUT	Oricare	*CHANGE	Nimic
	*NO	*OWNER	Oricare	Proprietar[3]	Nimic
	*YES	Oricare	*Yes	Oricare	*JOBCTL
	*NO	Oricare	*Yes	Oricare	*JOBCTL
	*OWNER	Oricare	Oricare	Oricare[5]	Oricare
Modifică, şterge, reţine, eliberează fişiere de spool (CHGSPLFA, DLTSPLF, HLDSPLF, RLSSPLF)[2]	Oricare	*DTAAUT	Oricare	*CHANGE	Nimic
	Oricare	*OWNER	Oricare	Proprietar[3]	Nimic
Modifică, curăţă, reţine şi eliberează ieşirea cozii (CHGOUTQ, CLROUTO, HLDOUTQ, RLSOUT)[2]	Oricare	*DTAAUT	Oricare	*CHANGE	Nimic
	Oricare	*OWNER	Oricare	Proprietar[3]	Nimic
	Oricare	Oricare	*YES	Oricare	*JOBCTL
Porniţi un program de scriere pentru coadă (STRPRTWTR, STRRMTWTR)[2]	Oricare	*DTAAUT	*Any	*CHANGE[4]	Nimic
	Oricare	Oricare	*YES	Oricare[4]	*JOBCTL

1 Aceasta este autorizarea necesară pentru a directa ieşirea dumneavoastră către coada de ieşire.

2 Folosind aceste comenzi sau opţiunile echivalente dintr-un ecran.

3 Trebuie să fiţi proprietarul cozii de ieşire.

4 De asemenea necesită autorizarea *USE la descrierea dispozitivului de printare.

5 Trebuie să fiţi proprietarul fişierului de spool sau să aveţi autorizarea specială *SPLCTL pentru a folosi această comandă.

Revedeţi secţiunea imprimantă din Planul dumneavoastră de Securitate Fizică. Completaţi în secţiunea coadă de ieşire din formularul Printer Output and Workstation Security pe măsura ce parcurgeţi acest topic.

Puteţi găsi folositoare revederea unui exemplu despre cum Sharon Jones, de la Compania JKL Toy, a determinat valorile pentru aceşti parametri ai cozii de ieşire înainte să planuiască securitatea resurselor pentru staţiile de lucru.

Exemplu: Formular securitate coadă de ieşire şi staţie de lucru la Compania JKL Toy—secţiunea coadă de ieşire

Departamentul Vânzări şi Marketing de la Comania JKL Toy are două cerinţe pentru tipărirea confidenţială:

- Listele de preţuri preliminarii sunt tipărite când se planifică modificări de preţuri. Nimeni din afara departamentului de Vânzări şi Marketing nu poate vedea această informaţie, cu excepţia directorilor companiei.
- Contractele sunt confidenţiale pe timpul negocierilor. O schiţă a contractului poate fi văzută numai de persoana care negociază contractul, nu şi de ceilalţi membrii ai departamentului de Vânzări şi Marketing.

Sharon a decis să creeze două cozi de tipărire speciale:

PRICEQ
: Pentru a fi utilizată pentru listele preliminare de preţuri. Oricine din departamentul de Vânzări şi Marketing poate efectua orice funcţie în această coadă de ieşire. Nimeni din afara departamentului nu poate utiliza această coadă, inclusiv operatorii de sistem. PRICEQ este în biblioteca CONTRACTS.

NEWCP
: Penru a fi utilizată la tipărirea contractelor care sunt negociate. Coada de ieşire este partajată de membrii departamentului Vânzări şi Marketing, dar numai persoana care creează un fişier spool în coada de ieşire poate controla acel fişier. NEWCP este în biblioteca CONTRACTS.

Tabelul de mai jos ilustrează formularul Securitate coadă de ieşire şi staţie de lucru pe care Sharon l-a pregătit pentru aceste cozi de ieşire:

Tabela 54. Exemplu formular Securitate coadă de ieşire şi staţie de lucru la Compania JKL Toy: Coadă de ieşire imprimantă

Listaţi parametrii pentru cozile de ieşire restricţionate:				
Nume coadă ieşire	Bibliotecă coadă de ieşire	Afişare orice fişier (DSPDTA)	Autorizări de verificat (AUTCHK)	Control operator (OPRCTL)
PRICEQ	CONTRACTS	*YES	*DTAAUT	*NO
NEWCP	CONTRACTS	*NO	*OWNER	*NO

Subiectul Decidere autorizare publică la bibliotecile program conţine un exemplu care ilustrează autorizarea pentru biblioteca CONTRACTS de la Compania JKL Toy. Numai directorii şi membrii departamentului Vânzări şi Marketing au acces la bibliotecă. Autorizarea publică pentru obiectele din bibliotecă (incluzând aceste cozi de ieşire) este *CHANGE.

Pentru că parametrul AUTCHK pentru coada de ieşire NEWCP este *OWNER, numai proprietarul unui fişier spool poate lucra cu acel fişier (vedeţi tabelul Autorizare necesară pentru efectuarea funcţiilor de tipărire de mai sus). Aceasta împiedică membrii departamentului de Vânzări şi Marketing să-şi tipărească unii altora contractele noi sau să le vadă în coada de ieşire.

După ce planificaţi securitatea cozilor de ieşire, puteţi să planificaţi securitatea staţiilor de lucru.

Planificarea securităţii pentru staţiile de lucru

După planificarea securitaţii resurselor pentru imprimante şi a ieşirilor de imprimantă puteţi începe să planificaţi securitatea staţiei de lucru În Planul dumneavoastră de Securitate Fizică listaţi staţiile de lucru ce reprezintă un risc de securitate prin locaţia lor. Folosiţi aceste informaţii pentru a determina ce staţii de lucru trebuie să fie restricţionate.

Îi puteţi încuraja pe cei care folosesc aceste staţii de lucru să acorde o atenţie specială securităţii. Ei ar trebui să facă signoff de fiecare dată când părăsesc staţia de lucru. Aţi putea înregistra în politica de securitate decizia dumneavoastră despre procedura de anulare a semnării pentru staţiile vulnerabile. Puteţi de asemenea limita funcţiile ce pot fi realizate pe aceste staţii pentru a minimiza riscul.

Cea mai uşoară metodă de a limita funcţionalitatea la o staţie de lucru este de a folosi profiluri de utilizator cu funcţii limitate. Sharon Jones foloseşte această tehnică pentru departamentul Depozite la compania JKL Toy. Sharon a permis lui Ray Wagner şi lui Janice Ames, ce lucrează la rampa de încarcare, să ruleze doar programul de inventar de recepţie. De asemenea, Sharon a făcut din ei singurii utilizatori care au permisiunea să semneze pe staţia de lucru de la rampa de încărcare.

Puteţi alege să împiedicaţi persoane cu autorizare de responsabil cu securitatea sau de service să semneze la orice staţie de lucru. Dacă folosiţi valoarea de sistem QLMTSECOFR pentru a face asta, persoanele cu autorizare de responsabil cu securitatea pot semna doar pe staţiile de lucru specificate.

Pregătiţi porţiunea staţie de lucru dinformularul securitatea Cozilor de Ieşire şi a staţiilor de lucru

Aţi putea dori să revedeţi un exemplu de cum a plănuit Sharon securitatea pentru staţiile de lucru, pe măsura ce pregătiţi porţiunea staţii de lucru din formularul securitatea cozilor de Ieşire şi a Staţiilor de lucru. Ar trebui să revedeţi de asemenea o listă cu recomandări pentru securitatea resurselor pentru a fi siguri că planul Dvs de securitatea resurselor este simplu şi complet. După ce aţi revăzut exemplul şi recomandările puteţi începe planificarea instalării aplicaţiei dumneavoastră..

Exemplu: Formular securitate coadă de ieşire şi staţie de lucru la Compania JKL Toy — secţiunea staţie de lucru

Sharon Jones şi-a revăzut Planul de securitate fizică pentru a determina ce staţii de lucru sunt expuse unor riscuri de securitate. La Compania JKL Toy, de exemplu, persoane din afara companiei pot uşor să acceseze staţiile de lucru de pe docul de încărcare şi de la birourile de vânzare de la distanţă. Sharon a indicat în Planul de securitate fizică faptul că aceste staţii de lucru expun la riscuri de securitate.

Cea mai uşoară metodă pentru limitarea funcţiilor unei staţii de lucru este de a o restricţiona la profiluri utilizator cu funcţii limitate. Sharon Jones a utilizat această tehnică pentru departamentul Depozit la Compania JKL Toy. Sharon a permis lui Ray Wagner şi Janice Ames, care lucrează la docul de încărcare, să ruleze numai programul de primire inventar. De asemenea, Sharon a făcut din ei singurii utilizatori care au permisiunea să semneze pe staţia de lucru de la rampa de încărcare.

Sharon şi-a reevaluat alegerea pentru valoarea de sistem QLMTSECOFR. Ea a decis ă ar trebui să o seteze pe 1 (Da) ca protecţie suplimentară pentru staţiile de lucru vulnerabile de la docul de încărcare şi birourile de vânzare de la distanţă.

Tabelul de mai jos ilustrează secţiunea staţie de lucru a formularului Securitate coadă de ieşire şi staţie de lucru pregătit de Sharon.

Tabela 55. Exemplu formular Securitate coadă de ieşire şi staţie de lucru la Comania JKL Toy: Staţie de lucru

Staţii de lucru responsabil cu securitatea: Dacă limitaţi accesul responsabilului cu securitatea la anumite staţii de lucru (valoarea de sistem QLMTSECOFT este yes), listaţi mai jos staţiile de lucru autorizate pentru responsabilul cu securitatea şi oricine cu autorizarea *ALLOBJ: Toate staţiile cu excepţia celor listate mai jos.	
Listaţi mai jos autorizările pentru staţiile de lucru restricţionate:	
Nume staţie de lucru	Grupuri de utilizatori autorizate (autorizare *CHANGE)
DSP10	AMESJ, WAGNERR
DSP11	AMESJ, WAGNERR
RMT01	UNGERJ, BELLB
RMT02	UNGERJ, BELLB

Poate doriţi să revedeţi un rezumat al recomandărilor de securitate resurse înainte de a planifica instalarea aplicaţiei dumneavoastră.

Rezumatul recomandărilor pentru securitatea resurselor

După ce aţi terminat planificarea securităţii staţiilor de lucru, puteţi revedea următoarele recomandări referitoare la securitatea resurselor. Sistemele iSeries oferă multe opţiuni pentru protejarea informaţiilor de pe sistem. Aceasta vă dă flexibilitatea să proiectaţi planul de securitate a resurselor care e cel mai bun pentru compania dumneavoastră. Dar această mulţime de opţiuni poate fi în egală măsură derutantă.

Folosind ca exemplu Compania JKL Toy, acest subiect a încercat să demonstreze o abordare elementară a planificării securităţii resurselor care foloseşte aceste principii:

- Treceţi de la general către specific:
  - Plănuiţi securitatea bibliotecilor. Lucraţi cu obiecte individuale doar când e nevoie.
  - Plănuiţi autorizarea publică mai întâi, apoi autorizarea de grup şi autorizarea individuală.
- Pentru a îmbunătăţi perfomanţele şi a simplifica salvarea şi recuperarea, definiţi securitate specifică doar pentru obiectele cu cerinţe de securitate ce nu pot fi satisfăcute folosind autorizarea publică.
- Faceţi autorizarea publică pentru obiectele noi dintr-o bibliotecă (CRTAUT) la fel cu autorizarea publică definită pentru majoritatea obiectelor existente în bibliotecă.
- Încercaţi să nu daţi autorizări individuale sau de grup mai puţine decât are autorizarea publică. Aceasta diminuează performanţa şi poate conduce mai târziu la greşeli făcând auditarea dificilă. Dacă ştiţi că toată lumea are cel puţin aceeaşi autorizare pentru un obiect ca şi cea publică atunci planificarea şi auditarea securităţii va fi mai uşoara.
- Folosiţi listele de autorizare pentru a grupa obiectele cu aceleaşi cerinţe de securitate. Listele de autorizare sunt mai simplu de gestionat decât autorizările individuale şi ajută la recuperarea informaţiilor de securitate.
- Creaţi profiluri de utilizator special ca proprietari de aplicaţie. Setaţi parola proprietarului în *NONE.
- Evitaţi să aveţi aplicaţii deţinute de profiluri furnizate de IBM precum QSECOFR sau QPGMR.
- Folosiţi cozile speciale de ieşire pentru rapoartele confidenţiale. Puneţi cozile de ieşire în aceeaşi bibliotecă cu informaţiile confidenţiale.
- Limitaţi numărul de persoane ce au autorizarea de responsabil cu securitatea.
- Fiţi atenţi când acordaţi autorizarea *ALL pentru obiecte şi biblioteci. Persoanele cu autorizarea *ALL pot accidental şterge anumite lucruri.

Pentru a fi siguri că aţi plănuit cu succes configurarea securităţii resurselor verificaţi dacă aţi adunat următoarele informaţii:

- Completaţi Partea 1 şi 2 din formularele de Descriere de bibliotecă pentru toate bibliotecile de aplicaţie.
- În formularele Profil Utilizator Individual completaţi câmpurile **Proprietarul obiectelor create** şi **Autorizarea de grup pentru obiectele create**.
- În formularul Convenţii de nume descrieţi cum plănuiţi să denumiţi listele de autorizări.
- Pregătiţi formularele de Liste de Autorizare.
- Adăugaţi informaţii despre lista de autorizare la formularele de Descriere de Bibliotecă.
- Pregătiţi un formular pentru securitatea cozilor de ieşire şi a staţiilor de lucru.

Acum sunteţi gata să planificaţi instalarea aplicaţiei dumneavoastră..

Planificarea instalării aplicaţiei Dvs

Pentru a terminaplanificarea securităţii resurselor, aveţi nevoie să vă pregătiţi pentru instalarea aplicaţiei dumneavoastră. Următoarele subiecte vă vor ajuta să vă planificaţi dreptul de proprietate şi autorizarea aplicaţiilor Dvs după ce le-aţi instalat. Metodele descrise aici ar putea să nu funcţioneze pentru toate aplicaţiile. Consultaţi programatorul dumneavoastră sau furnizorul aplicaţiei pentru a vă ajuta la dezvoltarea unui plan de instalare bun.

Dacă plănuiţi să obţineţi o aplicaţie de la un furnizor de aplicaţii, folosiţi aceste informaţii pentru a plănui activităţile de securitate pe care trebuie să le faceţi înainte şi după ce încărcaţi bibliotecile aplicaţiei.

Dacă planuiţi să instalaţi o aplicaţie pe care programatorii au dezvoltat-o pe sistemul Dvs, folosiţi aceste informaţii pentru a planifica activităţile de securitate necesare pentru a muta aplicaţia din starea de test în cea de producţie.

Treceţi prin aceşti paşi pentru o aplicaţie. Apoi mergeţi înapoi şi pregătiţi formularele de instalare a aplicaţiei pentru orice aplicaţii suplimentare.

Ce formulare sunt necesare?

Faceţi o copie a următoarelor formulare şi completaţile pe măsură ce parcurgeţi acest subiect:

Tabela 56. Planificarea formularelor necesare în planificarea instalării unei aplicaţii

Nume formular	Număr de copii necesare
Formularul de instalare a aplicaţiei	Unul pentru fiecare aplicaţie

Folosiţi aceste formulare pe care le-aţi folosit anterior la strângerea informaţiilor necesare planificării instalării aplicaţiei.

Nume formular	Pregătit în:
Formularul de descriere a bibliotecii	Descrierea informaţiilor despre bibliotecă
Formularul Listă de autorizare	Gruparea obiectelor

În subiectulÎncărcarea aplicaţiilor dumneavoastră veţi învăţa cum să realizaţi paşii necesari pentru a instala aplicaţiile dumneavoastră.

Pentru a plănui instalarea aplicaţiei dumneavoastră vedeţi următoarele subiecte:

- Determinarea profilurilor de utilizator şi a valorilor de instalare pentru aplicaţii.
- Schimbarea valorilor de instalare.

Determinarea profilurilor de utilizator şi a valorilor de instalare pentru aplicaţii

Atunci când planificaţi instalarea aplicaţiei dumneavoastră, trebuie mai întâi să decideţi profilurile de utilizator şi valorile de instalare pentru fiecare aplicaţie. Înainte de a instala o aplicaţie ce a fost creată pe un alt sistem, aţi putea avea nevoie să creaţi unul sau mai multe profiluri utilizator. Profilul utilizator care deţine bibliotecile aplicaţiei şi obiectele trebuie să existe pe sistemul dumneavoastră înainte de a încărca bibliotecile în sistem. Înregistraţi în formularul Instalarea Aplicaţiei profilurile pe care aveţi nevoie să le creaţi pentru fiecare bibliotecă şi ce parametri sunt necesari profilurilor.

Pentru a determina valorile de instalare necesare, cereţi de la programatorul sau furnizorul aplicaţiei răspunsurile la urmatoarele întrebări şi înregistraţi răspunsurile în formularul Instalarea Aplicaţiei:

- Ce profil deţine biblioteca aplicaţiei?
- Ce profil deţine obiectele din bibliotecă?
- Care este autorizarea publică pentru bibliotecă (AUT) ?
- Care este autorizarea publică pentru noile obiecte (CRTAUT)?
- Care este autorizarea publică pentru obiectele din bibliotecă?
- Ce programe, dacă există vreunul, adoptă autorizarea proprietarului?

Aflaţi dacă programatorii dumneavoastră sau furnizorul aplicaţiei au creat vreo listă de autorizare pentru aplicaţie. Pregătiţi un formular listă de Autorizare pentru fiecare listă de autorizare creată sau cereţi programatorului informaţii despre listă.

Puteţi determina dacă trebuie să schimbaţi valorile de instalare..

Schimbarea valorilor de instalare pentru aplicaţie

Comparaţi informaţia din formularul Instalarea Aplicaţiei cu planul de securitatea resurselor pentru biblioteca din formularul Descrierea Bibliotecii. Dacă sunt diferite trebuie să decideţi ce schimbări trebuie să faceţi după ce aplicaţia a fost instalată.

Schimbarea dreptului de proprietate al aplicaţiei

Dacă programatorul sau furnizorul aplicaţiei a creat un profil special pentru a deţine bibliotecile şi obiectele aplicaţiei, gânditi-vă şi la utilizarea acestui profil chiar dacă nu se potriveşte convenţiei dumneavoastră de nume. Transferarea dreptului de proprietate a obiectelor poate lua mult timp şi ar trebui evitată.

Dacă unul din profilurile de grup furnizate de IBM, cum ar fi QSECOFR sau QPMGR, deţine aplicaţia, ar trebui să transferaţi dreptul de proprietate către alt profil după ce aţi instalat aplicaţia.

Uneori programatorii proiectează aplicaţiile astel încât să prevină modificarea dreptului de proprietate asupra obiectului. Încercaţi să lucraţi cu aceste restricţii şi în acelaşi timp să îndepliniţi cerinţele Dvs de securitate pentru gestionarea securităţii. Totuşi, dacă un profil furnizat de IBM, QSECOFR de ex, deţine aplicaţia, Dvs şi programatorul sau furnizorul trebuie să dezvoltaţi un plan de schimbare a dreptului de proprietate. În mod ideal, ar trebui să schimbaţi dreptul de proprietate înainte să instalaţi aplicaţia.

Schimbarea autorizării publice.

Atunci când salvaţi obiecte, salvaţi odată cu ele şi autorizarea lor publică. Când restauraţi o bibliotecă de aplicaţie pe sistem, biblioteca şi toate obiectele sale vor avea aceeiaşi autorizare publică pe care au avut-o când au fost salvate. Asceasta este adevarată chiar dacă aţi salvat biblioteca pe un alt sistem.

Valoarea CRTAUT pentru o bibliotecă (autorizarea publică pentru obiecte noi) nu afectează obiectele care sunt restaurate. Ele sunt restaurate cu autorizarea lor publică salvată, indiferent de CRTAUT pentru acea bibliotecă.

Trebuie să schimbaţi autorizarea publică a bibliotecii şi a obiectelor pentru a potrivi planul Dvs cu formularul Descrierea Bibliotecii.

Aţi putea dori să revedeţi unexemplu care arată cum Sharon Jones de la JKL Toy a plănuit instalarea aplicaţiei pe măsură ce plănuiţi instalarea aplicaţiei dumneavoastră.

Pentru a fi siguri că aţi plănuit până la capăt instalarea aplicaţiei dumneavoastră, ar trebui să:

- Terminaţi de completat formularuliniţial de Instalare a Aplicaţiei. Apoi mergeţi înapoi şi pregatiţi formularele pentru aplicaţiile suplimentare.
- Revedeţi toate formularele dumneavoastră şi asiguraţi-vă că sunt completate. Faceţi copii după toate formularele şi păstraţi-le într-o locaţie sigură până când aţi instalat sistemul şi programele licenţiate.

După ce aţi terminat aceste operaţii de planificare, sunteţi gata săsetaţi securitate userilor.

Exemplu: Formular instalare apliaţie la Compania JKL Toy: Compania JKL Toy şi-a cumpărat aplicaţiile Customer Orders şi Accounts Receivable de la un furnizor de aplicaţie. Ei au angajat un programator din afară pentru a le dezvolta aplicaţia de Contracts and Princing şi să o lege la aplicaţia Customer Orders.

Sharon Jones a utilizat informaţiile din formularele Descriere bibliotecă pentru a pregăti un formular Instalare aplicaţie. Tabelul de mai jos arată o copie a formularului Descriere bibliotecă pentru CUSTLIB: (Vedeţi subiectul ″Descriere informaţii bibliotecă.″)

Tabela 57. Formular Descriere bibliotecă la Compania JKL Toy: exemplu

Formular Descriere ibliotecă	**Partea 1 din 2**

Tabela 57. Formular Descriere bibliotecă la Compania JKL Toy: exemplu (continuare)

Pregătit de: Sharon Jones	Data: 9/9/99
Nume bibliotecă: CUSTLIB	Nume descriptiv (text): Biblioteca înregistrări client
Descrieţi pe scurt funcţia acestei biblioteci: Păstrează toate fişierele clienţi, inclusiv comenzi şi conturi.	

Definiţi obiectivele de securitate pentru bibliotecă, cum ar fi dacă vreo informaţie este confidenţială:
`Astăzi, permitem oricui din companie să se uite la comenzile clienţi.`
`Pentru a proteja acurateţea informaţiilor, ar trebui să limităm persoanele`
`cărora li se permite să le modifice.`	

Autorizarea publică la bibliotecă: *USE Autorizarea publică şi obiectele din bibliotecă: *CHANGE Autorizarea publică pentru obiecte noi (CRTAUT): *CHANGE Proprietar bibliotecă: OWNAR	

Tabelul de mai jos ilustrează formularul Instalare aplicaţie pe care l-a pregătit Sharon penru aplicaţia Customer Orders. Observaţi că Sharon a decis să utilizeze profilul proprietar creat de furnizorul de aplicaţie. Profilul COWNER va deţine atât bibliotecile cu fişiere, cât şi cele cu programe.

După instalarea aplicaţiei, Sharon ar trebui să facă următoarele:

- Să modifice autorizarea publică pentru bblioteci pentru a corespunde planului de securitate resurse în formularele Descriere bibliotecă.
- Să modifice clasa utilizator pentru profilul COWNER la *USER şi să înlăture orice autorizări speciale.
- Să modifice parola profilului COWNER la *NONE.

Tabela 58. Formular Instalare aplicaţie la Compania JKL Toy: exemplu

Nume aplicaţie: Customer Orders (CO)		Descriere: Introduce, urmăreşte şi livrează comenzi.
Listaţi şi explicaţi fiecare profil care trebuie creat pentru instalarea aplicaţiei: Biblioteca cu fişiere este deţinută de un profil numit COWNER. Biblioteca cu programe este deţinută de QPGMR.		
Nume bibliotecă: CUSTLIB		
	Înainte de instalare	**După instalare**
Proprietar bibliotecă	COWNER	COWNER
Proprietar obiect	COWNER	COWNER
Autorizare publică bibliotecă	*EXCLUDE	*USE
Autorizare publică bibliotecă	*ALL	*CHANGE
Autorizare publică pentru obiecte noi	*CHANGE	*CHANGE
Nume bibliotecă: COPGMLIB		
	Înainte de instalare	**După instalare**
Proprietar bibliotecă	QPGMR	COWNER
Proprietar obiect	QPGMR	COWNER
Autorizare publică bibliotecă	*EXCLUDE	*USE
Autorizare publică bibliotecă	*ALL	*CHANGE
Autorizare publică pentru obiecte noi	*CHANGE	*CHANGE

Acum că aţi terminat operaţiile de planificare, puteţi să setaţi securitatea utilizator.

Setarea securităţii utilizatorului

Acest subiect vă ghidează prin operaţiile necesare pentru a seta securitatea utilizatorilor în sistemul dumneavoastră prin folosirea interfeţei linie de comandă. Dacă configuraţi un sistem nou, trebuie să completaţi, în ordine, următorii paşi. Sistemul foloseşte informaţiile din fiecare pas pe măsură ce treceţi la pasul următor. Pentru a seta securitatea elementară a sistemului trebuie să efectuaţi două seturi de task-uri. Trebuie mai întâi să definiţi securitatea utlizatorului şi apoi trebuie ss protejaţi resursele din sistem. Cele două tabele de mai jos evidenţiază fiecare pas ce trebuie urmat pentru a seta securitatea unui utilizator şi a resurselor.

Notă: TREBUIE **să** completaţi toţi paşii pentru a seta mai întâi securitatea utilizatorului, apoi începeţi să setaţi securitatea resurselor.

Tabela 59. Paşi în setarea securităţii utilizatorului

Pas	Ce faceţi în acest pas	Ce formulare folosiţi
Setarea mediului general	Setaţi valorile de sistem iniţiale şi atributele de reţea. Creaţi un profil de utilizator responsabil cu securitatea.	Formularul de Selecţie Valori de Sistem
Setarea valorilor de sistem pentru securitate	Setaţi valorile de sistem adiţionale	Formularul de selecţie valori de sistem
Pregătirea paşilor pentru securitatea elementară pentru încărcarea aplicaţiilor	Creaţi profiluri de proprietar. Încărcaţi aplicaţiile dumneavoastră Bibliotecile de aplicaţie şi obiectele trebuie să fie în sistem înainte de a completa paşii rămaşi.	Formularul de instalare a aplicaţiei
Setarea grupurilor de utilizatori	Creaţi descrierile de joburi, grupaţi bibliotecile şi profilurile.	Formularul de descriere a grupului de utilizatori
Setare utilizatori individuali	Creaţi biblioteci individuale şi profiluri de utilizator.	Formular de profil utilizator individual

Tabela 60. Paşi în setarea securităţii resurselor

Pas	Ce faceţi în acest pas	Ce formulare folosiţi
Setarea dreptului de proprietate şi a autorizării publice.	Stabiliţi dreptul de proprietate şi autorizarea publică pentru biblioteci şi obiecte.	Formularul de instalare a aplicaţiei
Crearea unei liste de autorizare	Creaţi liste de autorizare.	Formularul Listă de Autorizare
Setarea autorizărilor specifice	Setaţi accesul la biblioteci şi obiecte individuale.	Formularul de descriere a Bibliotecii
Securizarea ieşirii de imprimantă	Protejarea ieşirii de imprimantă prin crearea cozilor de ieşire şi alocarea de ieşiri.	Formularul pentru Cozi de Ieşire şi securitatea Staţiei de Lucru
Securizarea staţiilor de lucru	Protejarea staţiilor de lucru.	Formularul pentru Cozi de Ieşire şi securitatea Staţiei de Lucru

În plus faţă de subiectele menţionate în tabelul de mai sus, vedeţi următoarele subiecte pentru gestionarea securităţii sistemului dumneavoastră:

- Testarea securităţii.
- Modificarea informaţiilor de securitate.
- Salvarea informaţiilor de securitate.
- Monitorizarea securităţii.

Înainte de a începe

Dacă instalaţi un sistem nou faceţi următoarele lucruri înainte de a începe setarea securităţii:

- Asiguraţi-vă că sistemul şi dispozitivele dumneavoastră sunt instalate şi funcţionează corect. Dacă intenţionaţi să folosiţi pentru dispozitive convenţiile iSeries de numire, nu ataşaţi staţiile de lucru şi imprimantele decât după ce aţi modificat valoarea de sistem care determină modul în care sunt denumite dispozitivele (QDEVNAMING). Aplicarea noilor valori de sistem vă spune când să ataşaţi dispozitivele.
- Încărcaţi programele licenţiate pe care planuiţi să le folosiţi.

Setarea mediului general

Pentru a începe setarea securităţii utilizatorilor, aveţi nevoie să setaţi mediul general pentru utilizatorii dumneavoastră. În acest subiect, folosiţi meniul SETUP pentru a seta valorile de sistem şi a crea propriul profil de utilizator. De asemenea, veţi schimba ID-urile de utilizatori şi parolele pentru profiluri (DST) Uneltele de service Dedicat.

În procedurile următoare veţi găsi exemple de ecrane linie de comanda ce ilustrează aceşti paşi. Totuşi, acestea nu vă arată întreg ecranul. Ele arată doar informaţia necesară pentru a completa task-ul.

Ce formulare sunt necesare?

Introduceţi informaţia din formularul de selecţie a valorilor de sistem pe care l-aţi pregătit în ″Planuirea strategiei generale de securitate.″

Pentru a seta mediul general aveţi nevoie de completarea următoarelor task-uri:

1. Semnarea pe sistem.
2. Selectarea nivelului corect de asistenţă.
3. Împiedicarea celorlalţi să semneze.
4. Introducerea valorilor sistem pentru securitate.
5. Aplicarea noilor valori de sistem.
6. Crearea unui profil de responsabil cu securitatea

După ce aţi completat paşii de mai sus, trebuie să schimbaţi parolele de Unelte de Service pentru a împiedica folosirea lor incorectă de către cineva. Vedeţi Unelte de Service pentru detalii

Semnarea pe sistem

Pentru a începesetarea mediului dumneavoastră de sistem , trebuie să semnaţi pe sistem.

1. La consolă, iniţiaţi o conexiune ca responsabil cu securitatea (QSECOFR). Dacă e prima oară când deschideţi o conexiune, folosiţi parola QSECOFR. Întrucât sistemul livrează această parolă expirată, vi se va cere să o schimbaţi. Trebuie să schimbaţi această parolă pentru a semna cu succes.
2. Introduceţi SETUP în *câmpul de meniu* al ecranului Semnare.

Notă: meniul SETUP este numită Personalizaţi meniul Sistem, utilizatori şi dispozitive. Acest text se referă la el ca meniul SETUP peste tot.

```
                Semnare
                            Sistem  . . . . .
                            Subsistem . . . .
                            Ecran . . . . . .

Utilizator. . . . . . . . . . .   QSECOFR
Parola. . . . . . . . . . . . .   __________
Program/procedură . . . . . . .   __________
Meniu . . . . . . . . . . . . .   SETUP
Biblioteca curentă. . . . . . .   __________
```

După ce aţi semnat trebuie să selectaţi nivelul de asistenţă corespunzător.

Selectarea nivelului corect de asistenţă

După ce aţi semnat pe sistem, puteţi alege nivelul de asistenţă corespunzător pentru utilizatori. **Nivelul de asistenţă** determină ce versiune a ecranului veţi vedea. Multe ecrane sistem au doua versiuni diferite:

- O versiune nivel de ajutorare de bază, ce conţine mai puţine informaţii şi nu foloseşte terminologie tehnică.
- O versiune nivel de ajutorare intermediar, ce afişează mai multe informaţii şi foloseşte termeni tehnici.

Unele câmpuri sau funcţii sunt valabile doar pentru o anumită versiune de ecran. Instrucţiunile vă spun ce versiune să folosiţi. Pentru a schimba dintr-un nivel de asistenţă în altul folosiţi**F21** (Selectaţi nivelul de asistenţă). **F21** nu este valabilă din toate ecranele.

După ce aţi selectat nivelul de asistenţă trebuie să împiedicaţi deschiderea de alte conexiuni în sistem în timp ce faceţi setări de securitate

Împiedicarea deschiderii de alte conexiuni

După ce aţi selectat nivelul de asistenţă corespunzător, trebuie să-i împiedicaţi pe ceilalţi să semneze pe sistem. Dacă sunteţi îngrijorat că anumite persoane vor încerca penetrarea sistemului dumneavoastră înainte să reuşiţi să-l securizaţi, puteţi împiedica pe oricine să semneze de pe o altă staţie de lucru. Aceast lucru este opţional. Faceţi-l numai dacă simţiţi că e necesară o securitate temporară:

1. Din meniul SETUP, apăsaţi **F9** pentru a afişa o linie de comandă
2. In linia de comandă, introduceţi GO DEVICESTS.
3. Ecranul vă arată meniul Task-uri Stare Dispozitiv. Dacă vedeţi meniul Gestionare Stare Configuraţii, folosiţi**F21** (Selectare nivel de asistenţă) pentru a schimba în nivel de ajutorare de bază.
4. Selectaţi opţiunea **1** (Gestionare dispozitive de afişare).
5. În ecranul Gestionare dispozitive de afişare, faceţi indisponibile toate staţiile de lucru cu excepţia celei pe care o folosiţi dumneavoastră. Realizaţi asta prin tastarea**2** înaintea numelui fiecărei staţii de lucru şi prin apăsarea tastei**Enter** .
6. Întoarceţi-vă la meniul SETUP prin apăsarea de doua ori a lui**F3** (Exit).
7. Apăsaţi **F12** (Cancel) pentru a anula linia de comandă.

```
                          Gestionarea dispozitivelor de afişare

Introduceţi opţiunile de mai jos şi apoi apăsaţi Enter
  1=Activare    2=Dezactivare   5=Afişare
  7=Afişare mesaj   8=Gestionare controler şi linie
  13=Modificare descriere

Opt  Device      Type    Status
__   DSP01       3196    QSECOFR
2_   DSP02       3196    Disponibil pentru folosire
2_   DSP03       3196    Disponibil pentru folosire
2_   DSP04       3196    Disponibil pentru folosire
```

Când faceţi indisponibil un dispozitiv, el nu va avea ecranul Semnare, chiar dacă este alimentat. Staţiile de lucru rămân indisponibile până la oprirea şi repornirea sistemului. S-ar putea să fiţi nevoiţi să repetaţi acest pas.

După ce i-aţi împiedicat pe ceilalţi să semneze, puteţi introduce valorile de sistem pentru securitate.

Introducerea valorile de sistem pentru securitate

După ce aţi împiedicat ceilalţi utilizatori să semneze, trebuie să introduceţi valorile de sistem.

Folosiţi această procedură pentru a introduce informaţiile din Partea 1 a formularului Selectare valori sistem:

1. Din meniul SETUP, alegeţi opţiunea **1** (modificare opţiuni de sistem)
2. Introduceţi informaţiie din formularul Selectare valori sistem în ecranul Opţiuni sistem. Dacă nu vreţi să schimbaţi una din aceste alegeri din ecran puteţi folosi tasta TAB pentru a sări peste ele.

3. Introduceţi data şi ora corectă în acest ecran, dacă nu au fost setate atunci când aţi pornit sistemul.
4. După ce aţi introdus informaţia în această pagină treceţi la pagina următoare. Dacă apare *Continuare...* în colţul din dreapta-jos al ecranului înseamnă că ecranul mai are cel puţin încă o pagină.

```
                          Schimbaţi opţiunile sistemului
Sistem:
Introduceţi opţiunile de mai jos şi apoi apăsati Enter

Nume sistem . . . . . .   JKLTOY     Name

Opţiuni de dată şi timp:
  Data sistemului . . . . . .   09/21/99     MM/DD/YY
  Ora sistemului. . . . . .   10:52:57     HH:MM:SS
  Separator de dată. . . . . .   1           1=/
                                             2=-
                                             3=.
                                             4=,
                                             5=blank
  Formatul datei. . . . . .   MDY           YMD, MDY, DMY, JUL
  Separator de timp . . . . . .   1           1=:
                                             2=.
                                             3=,
                                             4=blank


                                                                 Mai mult..
F1=Ajuor F3=Ieşire F5=Reîmprospătare   F12=Anulare
```

5. Tastaţi alegerile dumneavoastră în a doua pagină a ecranului şi treceţi mai departe

```
                          Schimbaţi opţiunile sistemului

Introduceţi opţiunile de mai jos şi apoi apăsati Enter

Opţiuni de securitate:
  Nivel de securitate . . . . .   40
   :
  Permite responsabilului cu securitatea să
    semneze pe orice staţie de
    afişare. . . . . .   N
```

6. Tastaţi alegerile dumneavoastră în a treia pagină a ecranului şi apăsaţi**tasta Enter**.

```
                          Schimbaţi opţiunile sistemului

Introduceţi opţiunile de mai jos şi apoi apăsati Enter

Opţiuni dispozitiv
  Formatul denumirii dispozitivelor pentru noile
  dispozitive. . . . . .   1


  Imprimantă de sistem implicită.   PRT01

Opţiuni suplimentare
  Pune utilizatorii intr-un mediu S/36
    la semnare nouă. . .   N
  Salvează contabilizare job
    Informaţii despre ieşirea
    de imprimantă terminată  . . . . . .   Y
```

7. Trebuie să vedeţi din nou meniul SETUP. Observaţi mesajul din partea de jos a ecranului dumneavoastră: **Opţiuni de sistem modificate cu succes. Este necesar IPL**.

Notă: Sistemul cere un IPL doar dacă aţi schimbat nivelul de securitate.

La sfârşitul celor mai multe subiecte despre operaţii sistem veţi găsi un tabel ce descrie erori posibile şi paşii de recuperare. Folosiţi aceste tabele pentru asistenţă dacă rezultatele dumneavoastră sunt diferite de cele descrise. Aceste tabele nu anticipează chiar orice problemă. Scopul tabelelor este să vă dea câteva idei în rezolvarea problemelor şi să vă facă să vă simţiţi mai confortabil la folosirea sistemului dumneavoastră.

Erori posibile	Recuperare
Meniul principal este afişat.	Apăsaţi **F3** (Exit) sau **F12** (Cancel). Apăsaţi GO SETUP şi încercaţi din nou.
Veţi vedea un alt ecran, cum ar fi ecranul Modificare opţiuni curăţare.	Aţi selectat opţiunea greşită din meniul SETUP. Apăsaţi **F3** (Exit) pentru a vă intoarce la meniu şi încercaţi din nou.
Meniul Modificare opţiuni sistem este arătat din nou după ce aţi apăsat tasta **Enter**.	Uitaţi-vă după un mesaj de eroare în partea de jos a ecranului. Probabil aţi introdus o valoare ce nu e permisă. Amintiţi-vă să folosiţi **F1** (Ajutor) dacă aveţi nevoie de informaţii suplimentare. Folosiţi **F5** (Reîmprospătare) dacă doriţi ca sistemul să restaureze toate valorile la cele de dinainte de a începe introducerea. Încercaţi din nou.
Aţi apăsat **tasta Enter** înainte de a introduce în ecran toate alegerile dumneavoastră.	Puteţi folosi acest ecran de câte ori veţi avea nevoie să schimbaţi valorile sistem. Selectaţi opţiunea **1** din meniul SETUP şi introduceţi valorile pe care le-aţi omis prima dată. **Atenţie: După ce sistemul este operaţional, nu mai schimbaţi nivelul de securitate fără să consultaţi un programator. De asemenea, nu modificaţi numele de sistem dacă folosiţi iSeries Access sau în cazul comunicării cu alt calculator.**
Aţi apăsat tasta**Enter** în loc de pagină jos.	Selectaţi opţiunea **1** din meniul SETUP din nou şi treceţi o pagină mai jos pentru următorul ecran. Tastaţi-vă alegerile şi apăsaţi tasta**Enter**.

După ce aţi introdus valorile de sistem, trebuie apoi săaplicaţi noile valori de sistem..

Aplicarea noilor valori de sistem

După ce aţi introdus valorile de sistem, aveţi nevoie să aplicaţi câteva din aceste valori. Cele mai multe schimbări ale valorilor de sistem au efect imediat. Totuşi, când schimbaţi nivelul de securitate în sistemul dumneavoastră schimbarea nu are efect până nu opriţi şi reporniţi sistemul. După ce verificaţi că aţi introdus corect toate valorile în ecranul de Schimbare opţiuni de Sistem, sunteţi gata să aplicaţi noile valori.

Notă: Ataşaţi staţiile dumneavoastră de lucru la sistem, dacă nu aţi făcut-o deja. Când veţi porni sistemul, el va configura automat acele dispozitive folosind fomatul de denumire ales în ecranul de Schimbare Opţiuni de sistem.

Folosiţi următoarea procedură pentru a opri sistemul şi a-l reporni. Când sistemul porneşte, valorile pe care le-aţi introdus în ecranul de Schimbare a opţiunilor de sistem işi vor face efectul.

1. Asiguraţi-vă că aţi semnat pe consolă şi că nu s-a semnat pe altă staţie de lucru.
2. Asiguraţi-vă ca poziţia cheii IPL a unităţii de procesare este Normal.
3. Din meniul SETUP, selectaţi opţiunea pentru operaţia de oprire pornire Alimentare.
4. Selectaţi opţiunea de oprire imediată a alimentării sistemului şi apoi de pornire aliemntare. Apăsaţi tasta**Enter**.
5. Sistemul vă arată un ecran ce vă cere să confirmaţi cererea de oprire a alimentării. Apăsaţi **F16** (Confirmare).

Asta duce la oprirea şi apoi pornirea automată a sistemului. Ecranul dumneavoastră devine blanc pentru câteva minute. Apoi trebuie să vedeţi din nou ecranul de semnare nouă.

După ce aţi aplicat noile Dvs valori de sistem, trebuie săcreaţi un profil de responsabil cu securitatea. pentru dumneavoastră.

Crearea unui profil de responsabil cu securitatea

Un **responsabil cu securitatea** într-un sistem este un utilizator cu clasa de utilizator *SECOFR sau autorizările speciale *ALLOBJ şi *SECADM.

După ce aţi aplicat valorile de sistem din ecranul de schimbare opţiuni de sistem, creaţi un profil de utilizator pentru dumneavoastră sau pentru alţi responsabili cu securitatea. În viitor, folosiţi-vă profilul mai degrabă decât profilul QSECOFR, atunci când realizaţi funcţii de responsabil cu securitatea.

1. Semnaţi pe sistem ca QSECOFR şi cereţi meniul SETUP.

   Observaţi că numele sistemului ales de dumneavoastră apare în dreapta sus a ecranului de semnare.

```
                  Semnare
                            Sistem  . . . . .
                            Subsistem . . . .
                            Ecran . . . . . .

Utilizator. . . . . . . . . . .   QSECOFR
Parola. . . . . . . . . . . . .   _________
Program/procedură . . . . . . .   _________
Meniu . . . . . . . . . . . . .   SETUP
Biblioteca curentă. . . . . . .   _________
```

2. Din meniul SETUP, selectaţi *Gestionare opţiuni înrolare utilizatori*. Ecranul de Gestionare Opţiuni de înrolare utilizatori listeaza profilurile curente din sistemul dumneavoastra

   Notă: Dacă vedeţi ecranul de Gestionare Profiluri Utilizatori, apăsaţi**F21** (Selectare nivel de asistenţă) şi schimbaţi în nivel de ajutorare de bază.

3. Pentru a crea un profil nou tastaţi**1** (Adaugă) în coloana*Opt* (opţiune) şi numele profilului dumneavoastra în coloana*Utilizator* . Apăsaţi tasta**Enter.**

```
                          Gestionare înrolare utilizatori

Introduceţi opţiunile de mai jos şi apoi apăsaţi Enter
  1=Adaugă   2=Schimbă  3=Copiază  4=Înlătură 5=Afişează

Opt     Utilizator        Descriere
1       JONESS
QDOC                           Document profil utilizator
QSECOFR                        profil utilizator responsabil cu securitatea
```

4. În ecranul Adaugă Utilizator alocaţi-vă o parolă.
5. Completaţi câmpurile arătate în ecranul eşantion cu propriile dumneavoastră informaţii.
6. Treceţi o pagină mai jos în ecranul dumneavoastra

```
                          Adaugă utilizator

Introduceţi opţiunile de mai jos şi apoi apăsati Enter

Utilizator. . . . . .   JONESS
Descriere utilizator. . .   Jones, Sharon
Parolă . . . . . .  secret
Tipul utilizatorului. . .   *SECOFR
Grupul utilizatorului . .   *NONE

Restricţionează folosirea liniei de comandă
Bibliotecă implicită. . .
Imprimantă implicită. . .   *WRKSTN
Program de semanre . .*NONE
Bibliotecă. . . . . .

Primul meniu  . . . . . .
Bibliotecă. . . . . .
```

7. Umpleţi şi a doua pagină a ecranului şi apăsaţi tasta**Enter** .
8. Verificaţi pentru mesaje de confirmare în partea de jos a ecranului Gestionare înrolare utilizatori.
9. Apăsaţi **F3** (Ieşire) pentru a vă intoarce lameniul SETUP.

```
                          Adaugă utlizator

Introduceţi opţiunile de mai jos şi apoi apăsati Enter

Program de tasta Attn. .   *SYSVAL
  Bibliotecă. . . . . .
```

Erori posibile	Recuperare
Aţi apăsat **tasta Enter** înainte de a introduce în ecran toate alegerile dumneavoastra	Folosiţi opţiunea *Modifică* din ecranul de Gestionare înrolare utilizatori pentru a schimba profilul pe care tocmai l-aţi creat. Dacă profilul nu apare în listă, apăsaţi **F5** (Reîmprospătare) şi treceţi o pagină mai jos pentru a-l găsi.

După ce aţi creat pentru dumneavoastra un profil de responsabil cu securitatea, aveţi nevoie să schimbaţi ID-ul de utilizator şi parola pentru utilizatorii de unelte de service. Vedeţi şi subiectul Unelte de Servicedin Centrul de informare.

Setarea valorilor de sistem pentru securitate

În acest subiect, utilizaţi comanda de Gestionare a valorilor de sistem (WRKSZSVAL) pentru a schimba şi a afişa valorile de sistem.

Ce formulare sunt necesare?

Introduceţi informaţia din formularul de selecţie a valorilor de sistem pe care l-aţi pregătit în ″Plănuirea strategiei generale de securitate.″

Pentru a seta valorile de sistem parcurgeţi următoarele operaţii:

1. Schimbarea valorilor de sistem de securitate.
2. Schimbarea valorilor individuale de sistem.

Semnarea în interfaţa liniei de comandă

Folosiţi aceste informaţii pentru a semna pe sistem:

Profil Profilul propriu (sunt necesare autorizările *SECADM şi *ALLOBJ)

Meniu Principal

După ce aţi semnat puteţi începe să schimbaţi valorile de sistem de securitate.

Schimbarea valorilor de sistem de securitate

După ce aţi semnat, folosiţi această procedură pentru a intrdoduce valorile de sistem de securitate ce apar în Partea a 2-a a formularului Selectarea valorilor de sistem.

1. În linia de comandă introduceţi WRKSYSVAL *SEC şi apăsaţi tasta **Enter**. Parametrul *SEC de după numele comenzii semnifică faptul că doriţi să vedeţi doar valorile de sistem ce au legătură cu securitatea.
2. În ecranul de gestiune a valorilor de sistem tastaţi **2** (Modificare) în coloana *Opţiune* din faţa valorii de sistem pe care doriţi să o modificaţi. Dacă valoarea de sistem pe care doriţi s-o modificaţi nu apare pe ecran derulaţi în jos până o gasiţi.

```
                          Gestionare valori de sistem

Poziţie la. . . . .               Caracter de început
Subset după tip . . . . .   *SEC         F4 pentru listă

Introduceţi opţiunile, apăsaţi Enter
  2=Modificare   5=Afişare

        Sistem
Opţiune Valoare     Tip         Descriere
        QINACTMSGQ  *SEC        Coada de mesaje a joburilor inactive
2       QLMTDEVSSN  *SEC        Limitare sesiuni dispozitiv
        QLMTSECOFR  *SEC        Limitare access la dispozitive pentru responsabilul cu securitatea
        QMAXSGNACN  *SEC        Acţiune încercări nereuşite de semnare
   ⋮
```

3. Tastaţi alegerea dumneavoastră pentru valoarea de sistem şi apăsaţi tasta **Enter**. Este afişat din nou ecranul Gestionare valori de sistem.

```
                          Schimbă valoarea de sistem
Valoare sistem . . . . :    QLMTDEVSSN
Descriere. . . . . . . :    Limitează sesiunile dispozitiv


Introduceţi opţiunile, apăsaţi Enter

  Limitează sesiunile dispozitiv. . . 0          0=Nu
                                              1=Limitează
```

4. Uitaţi-vă după un mesaj de confirmare în partea de jos a ecranului.

Erori posibile	Recuperare
Veţi vedea valori de sistem diferite de cele arătate în exemplul de ecran de Gestionare a Valorilor de sistem.	Aţi uitat sa tastaţi *SEC. Comparaţi câmpul *Subset după tip* în partea de sus a ecranului cu exemplu. Deplasaţi cursorul până la câmpul *Subset după câmp*. Tastaţi *SEC şi apăsaţi tasta**Enter**.
Sistemul nu a procesat comanda dumneavoastra Înca mai vedeţi un meniu.	Verificaţi după mesaje de eroare în partea de jos a ecranului dumneavoastra Probabil aţi tastat greşit numele comenzii. Încercaţi din nou. Dacă mesajul spune că nu sunteţi autorizat, anulaţi semnarea şi semnaţi din nou folosind un profil cu autorizare responsabil cu securitatea.

Erori posibile	Recuperare
Ecranul Modificare valori de sistem este arătat din nou după ce aţi apăsat tasta **Enter**.	Verificaţi partea de jos a ecranului pentru mesaje de eroare. Probabil aţi tastat incorect alegerile dumneavoastra sau aţi ales o valoare ce era în afara intervalului permis. Folosiţi tasta**F1** (Ajutor) pentru informaţii suplimentare.
În locul ecranului de gestiune a valorilor de sistem vedeţi un meniu.	Probabol aţi apăsat tasta**Enter** de două ori. Tastaţi WRKSYSVAL *SEC.
Aţi selectat o valoare de sistem pe care nu doriţi să o schimbaţi.	Apăsaţi **F12** (Anulare) pentru a vă întoarce la ecranul de Gestionare a valorilor de sistem.

Ce rol are * (Asteriscul)?

Probabil că aţi observat ca unele valori au înaintea lor un asterisc (*). Sistemul foloseşte asteriscul pentru arăta diferenţa dintre valorile speciale şi cuvintele obişnuite. De exemplu, când specificaţi că o parolă a unui profil de utilizator este *NONE, înseamnă că sistemul nu va permite nimănui să semneze folosind acel profil. Dacă specificaţi că o parolă este NONE, utilizatorul trebuie să tasteze caracterele NONE pentru parolă.

Cât timp setaţi securitatea în sistemul dumneavoastra fiţi atenţi la folosirea asteriscului în instrucţiuni şi în formulare.

După ce aţi schimbat valorile de sistem de securitate puteţischimba valorile de sistem individuale.

Schimbarea valorilor individuale de sistem

După ce aţi schimbat valorile de sistem de securitate, puteţi schimba valorile de sistem individuale.

De exemplu, valoarea de sistem Interval de timeout pentru joburile deconectate (QDSCJOBITV) nu este inclusă ca şi valoare de sistem de securitate. Ea nu apare în subsetul *SEC din ecranul de Gestionare Valori de sistem. Folosiţi aceasta procedură pentru a schimba valoarea de sistem QDSCJOBITV sau orice altă valoare de sistem individuală:

1. Tastaţi *QDSCJOBITV şi apăsaţi tasta**Enter**.
2. În ecranul de gestiune a valorilor de sistem tastaţi **2** (Modificare) în coloana *Opţiune* din faţa valorii QDSCJOBITV.
3. Tastaţi alegerea dumneavoastra pentru QDSCJOBITV.
4. Verificaţi mesajul de confirmare.

```
                          Schimbă valoarea de sistem
Valoare sistem . . . . :   QDSCJOBITV
Descriere    . . . . . :   Interval de timeout pentru joburi deconectate


Introduceţi opţiunile, apăsaţi Enter

  Interval de timeout pentru joburi deconectate300
```

Listarea valorilor dumneavoastra de securitate.

După ce aţi introdus toate informaţiile din formularul de Selectare a Valorilor de sistem puteţi printa o listă a tuturor valorilor de sistem de securitate. Tastaţi WRKSYSVAL *SEC OUTPUT(*PRINT). Păstraţi într-un fişier o copie a listei cu formularul Selectare Valori de sistem. Retipăriţi lista ori de câte ori schimbaţi o valoare de sistem de securitate.

După ce aţi introdus toate alegerile pentru valorile de sistem din formularul de Selectare a Valorilor de sistem, puteţi pregătiîncărcarea aplicaţiilor dumneavoastra.

Realizarea paşilor de securitate pentru încărcarea aplicaţiilor

După ce aţi setat valorile dumneavoastra de sistem, puteţi face pregătiri pentru încărcarea aplicaţiilor dumneavoastra Acest subiect acoperă paşii de securitate necesari pentru încărcarea bibliotecilor de aplicaţii în sistemul dumneavoastra După ce aţi creat profiluri şi alte obiecte de securitateSetarea dreptului de proprietate şi a autorizării publice″ şi ″Setarea securităţii resurselor″ vă arată cum să stabiliţi dreptul de proprietate şi autorizare pentru aplicaţiile dumneavoastra

Dacă e posibil ar trebui să incărcaţi în sistem bibliotecile aplicaţiei înainte să setaţi grupurile de utilizatori şi profilurile individuale. Aveţi nevoie să faceţi referire la obiectele aplicaţiei atunci când creaţi descrierile de job şi profilurile.

Dacă nu puteţi incărca aplicaţiile înainte de a crea grupul şi profilurile individuale, puteţi primi mesaje de avertizare cum ar fi:

- Sistemul nu găseşte bibliotecile iniţiale la crearea descrierilor de job.
- Sistemul nu găseşte programul sau meniul iniţial la crearea profilurilor.

Nu puteţi testa cu succes profilurile şi descrierile de job până nu încărcaţi bibliotecile aplicaţiei dumneavoastra

Folosiţi formularele de instalare a aplicaţiei pe care le-aţi pregătit înPlanificarea instalării aplicaţiei dumneavoastra.″

Pentru a încărca fiecare aplicaţie completaţi aceste operaţii.

1. Creaţi un profil de proprietar.
2. Încărcaţi aplicaţia.

Semnarea pe sistem

- Pentru a crea profiluri de proprietar:

  Profil Proprietar (e necesară autorizarea *SECADM)

  Meniu Principal
- Pentru a încărca bibliotecile de aplicaţie:

  Consultaţi furnizorul aplicaţiei pentru a vedea dacă trebuie să semnaţi ca responsabil cu securitatea sau ca proprietarul aplicaţiei atunci când incărcaţi bibliotecile aplicaţiei.

După ce aţi semnat, puteţi crea un profil de proprietar pentru aplicaţia dumneavoastra

Crearea unui profil de proprietar

După ce aţi semnat pe sistem, verificaţi Plan instalare aplicaţie ca să vedeţi dacă aveţi nevoie să creaţi profiluri înainte de a încărca aplicaţia. Pentru a crea un profil:

1. Tastaţi CRTUSRPRF (Creare Profil Utilizator) şi apăsaţi tasta **F4** (Prompt).
2. În ecranul Creare profil utilizator, completaţi câmpurile aşa cum aţi primit instrucţiuni de la programatorul sau furnizorul aplicaţiei dumneavoastra
3. Folosiţi **F10** (Mai multe câmpuri) şi derulaţi pagina pentru a afişa câmpurile suplimentare.

```
                      Creare Profil Utilizator (CRTUSRPRF)

Introduceţi opţiunile, apăsaţi Enter

Profil utilizator. . . . . >
Parola Utilizator. . . . . .   *USRPRF
Setează parola să expire . . . .   *NO
Stare. . . . . .   *ENABLED
Clasa Utilizator . . . . . .   *USER
Nivel de Asistenţă . . . . . .   *SYSVAL
Biblioteca curentă. . . . . .   *CRTDFT
Programul iniţial de apelat . .   *NONE
  Biblioteca . . . . . .
Meniul Iniţial . . . . . .   MAIN
  Biblioteca . . . . . .     *LIBL
Limitează capabilităţile. . . . . .   *NO
Text 'descriere' . . . . . .   Proprietarul lui xxxxxx
```

4. Verificaţi partea de jos a ecranului pentru mesaje.

Notă: Crearea unui profil de grup descrie în detaliu crearea de profiluri.

După ce aţi creat un proprietar al aplicaţiei puteţi începe săîncărcaţi aplicaţia.

Încărcarea aplicaţiei

Urmăriţi instrucţiunile furnizorului aplicaţiei pentru încarcarea bibliotecilor aplicaţiei. În ″Setarea dreptului de proprietate şi a autorizării,″ aţi învăţat să setaţi dreptul de proprietate şi autorizarea publică pentru aplicaţii.

După ce încărcaţi toate aplicaţiile, puteţi să setaţi grupurile de utilizatori.

Setarea grupurilor de utilizatori

Dupa ce realizaţi paşii de securitate pentru încărcarea aplicaţiilor Dvs puteţi seta grupurile de utilizatori. Veţi crea biblioteci de grupuri, descriere de job şi profiluri de grupuri. Parcurgeţi întreg subiectul cu unul din grupurile Dvs de utilizatori şi apoi, pentru orice grup suplimentar, repetaţi de la capăt toţi paşii. Ecranele exemplu vă arată informaţia din formularul Descriere de Grup de Utilizatori pentru Departamentul de vânzări şi marketing şi pentru Departamentul de Depozite al Compania JKL Toy.

Folosiţi fomularele de Descriere de Grup de Utilizatori pe care le-aţi pregătit în ″Planificare grupurilor de utilizatori.″

Efectuaţi aceste operaţii pentru a seta grupuri de utilizatori:

1. Creaţi o bibliotecă pentru grupul de utilizatori..
2. Creaţi o descriere de job..
3. Creaţi un profil de grup..

Semnarea pe sistem

Profil Proprietar (e necesară autorizarea *SECADM)

Meniu Principal

După ce aţi semnat, puteţi crea o bibliotecă pentru grupul de utilizatori.

Crearea unei biblioteci pentru grup

După ce aţi semnat pe sistem, trebuie să creaţi o bibliotecă pentru grupul de utilizatori. Dacă plănuiţi ca grupul să partajeze o bibliotecă pentru obiectele pe care le creează, cum ar fi programe de interogare, creaţi biblioteca înainte de a crea profilul de grup:

1. Tastaţi CRTLIB (Creare Bibliotecă) şi apăsaţi**F4** (Prompt).
2. Completaţi ecranul. Numele bibliotecii trebuie să fie numele profilului de grup.

3. Apăsaţi **F10** (Parametrii suplimentari).
4. Completaţi autorizarea publică pentru biblioteca şi obiectele noi ce sunt create în bibliotecă.
5. Apăsaţi tasta **Enter**. Verificaţi mesajul de confirmare.

```
                          Creare bibliotecă

Introduceţi opţiunile, apăsaţi Enter

Biblioteca . . . . . .   DPTWH
Tipul bibliotecii . . . . . .   *PROD
Text 'Descriere' . . . . . .   Warehouse Library

                          Parametrii suplimentari

Autorizare . . . . . .   *USE
ID pool de stocare auxiliar . . .   1
Creare autorizare. . . . . .   *CHANGE
Creare auditare obiect . . . . . .   *SYSVAL
```

Erori posibile	Recuperare
Aţi apăsat tasta **Enter** înainte de a introduce o descriere pentru bibliotecă.	Tastaţi **CHGLIB** şi apăsaţi**F4** (Prompt). Tastaţi numele bibliotecii în ecranul de prompt şi apăsaţi tasta **Enter**. Tastaţi descrierea în ecranul de Modificare Bibliotecă.
Aţi dat bibliotecii un nume greşit.	Folosiţi comanda Redenumire Obiect(RNMOBJ).

După ce aţi creat o bibliotecă pentru grup, puteţicrea o descriere de job.

Crearea unei descrieri de job

După ce aţi creat o bibliotecă pentru grup,puteţi crea o descriere de job pentru fiecare grup.

Dacă bibliotecile necesare listei iniţiale de biblioteci nu sunt încă în sistem, puteţi primi un mesaj de avertizare atunci când creaţi o descriere de job.

1. Tastaţi**CRTJOBD** (Creare descriere de job) şi apăsaţi**F4** (prompt).
2. Completaţi aceste câmpuri:

   Descriere de job:
   Acelaşi ca numele profilului de grup.

   Numele bibliotecii:
   QGPL

   Text: Descriere grup
3. Apăsaţi **F10** (Parametrii suplimentari).
4. Derulaţi în jos până la *câmpul Lista Iniţială de biblioteci*.

```
                  Creare Descriere de job

Introduceţi opţiunile, apăsaţi Enter

Descriere de job . . . . . .   DPTSM
  Biblioteca . . . . . .  .   QGPL
Coadă de joburi. . . . . .  .   QBATCH
  Biblioteca . . . . . .  .     *LIBL
Prioritate de job (în JOBQ). . . .   5
Prioritate de ieşire (in OUTQ) . .   5
Dispozitiv de tipărire . . . . . .   *USRPRF
Coadă de ieşire. . . . . .  .   *USRPRF
  Biblioteca . . . . . .  .
Text 'descriere' . . . . . .   Vânzări şi Marketing
```

5. Tastaţi un **+** (plus) peste *SYSVAL în *câmpul lista iniţilă de biblioteci* pentru a specifica că doriţi să introduceţi o listă de valori. Apăsaţi tasta **Enter**.

```
Cod de contabilizare . . . . . .  .   *USRPRF
   ⋮
Verificare sintaxă CL . . . . . .   *NOCHK
Lista iniţială de biblioteci. . . .   +
              + pentru mai multe valori
```

6. În câmpul *lista iniţială de biblioteci* , tastaţi numele bibliotecilor care sunt marcate (✓) din formularul Descriere de Grup Utilizator:
   - Puneţi câte un nume de bibliotecă pe linie.
   - Includeţi QGPL şi QTEMP. Fiecare job foloseşte o bibliotecă numită QTEMP pentru a memora obiectele temporare. **Toate listele iniţiale de biblioteci trebuie să aibă biblioteca QTEMP**. Pentru cele mai multe aplicaţii biblioteca QGPL ar trebui să existe în lista iniţială de biblioteci.
   - Nu e nevoie să includeţi biblioteca curentă (implicită) în lista de biblioteci. Sistemul adaugă automat acea bibliotecă la semnare.
7. Apăsaţi tasta **Enter**. Verificaţi mesajele. (Derulaţi în jos pentru a vedea toate mesajele.)

```
Specificaţi mai multe valori pentru

Introduceţi opţiunile, apăsaţi Enter

Lista iniţială de biblioteci  . .    CUSTLIB
                                     ITEMLIB
                                     COPGMLIB
                                     ICPGMLIB
                                     QGPL
                                     QTEMP
```

Erori posibile	Recuperare
Aţi apăsat tasta**Enter** în loc de **F10**.	Pentru a pune bibliotecile corecte în lista iniţială de biblioteci, tastaţi **CHGJOBD** (Modificare descriere job) şi apăsaţi **F4**.
Aţi primit mesaje de eroare când aţi încercat să creaţi descrierea de job.	Cel mai obişnuit mesaj de eroare apare când încercaţi să includeţi o bibliotecă ce nu e în sistem. Acesta este un mesaj de avertizare. Descrierea de job este totuşi creată cu bibliotecile din lista iniţială de biblioteci. Nu puteţi semna cu un profil ce specifică descrierea de job până când biblioteca nu e în sistem. Dacă biblioteca este în sistem, atunci poate că aţi tastat greşit numele ei. Verificaţi numele bibliotecii şi încercaţi din nou.

După ce aţi creat o descriere de job puteţi crea un profil de grup.

Crearea unui profil de grup

După ce aţi creat o descriere de job, puteţi crea profilul de grup. Pentru a face asta folosiţi informaţia din Partea a 2-a a formularului Descriere Grup Utilizatori.

1. Folosiţi comanda Gestionare profiluri utilizatori. Tastaţi WRKUSRPRF *ALL. Iniţial, ecranul listează profilurile livrate de IBM.

   Notă: Dacă vedeţi ecranul de Gestionare înrolare utilizator, apăsaţi **F21** pentru a modifica în nivel de ajutorare intermediar.

2. Pentru a crea un profil nou, tastaţi **1** în coloana *Opt* (opţiune) şi numele numele profilului în coloana*profil utilizator* . Apăsaţi tasta**Enter**.

```
                        Gestionare profiluri utilizatori

Introduceţi opţiunile, apăsaţi Enter
  1=Creare   2=Modificare 3=Copiază  4=Şterge   5=Afişează
  12=Gestionare obiecte după proprietar

     Utilizator
Opt  Profile     Text
1    DPTSM
     QDOC        Document profil utilizator
     QSECOFR     Profil utilizator responsabil cu securitatea
```

3. Introduceţi informaţia din formularul descriere de grup utilizatori în câmpurile corespunzătoare.
4. Folosiţi tasta**Tab** pentru a sări peste câmpurile la care doriţi să păstraţi valoare implicită.
5. Apăsaţi **F10** (Parametrii suplimentari).
6. Derulaţi în jos.

```
                      Creare Profil Utilizator (CRTUSRPRF)

Introduceţi opţiunile, apăsaţi Enter

Profil utilizator . . . . . > DPTSM
Parola utilizator. . . . . .   *none
Setează parola să expire . . . .   *NO
Stare  . . . . . .   *ENABLED
Clasa Utilizator . . . . . .   *USER
Nivel de asistenţă . . . . . .   *SYSVAL
Biblioteca curentă . . . . . .   *CRTDFT
Programul iniţial de apelat. . .   cpsetup
  Biblioteca . . . . . .   cppgmlib
Meniul iniţial . . . . . .   cpmain
  Biblioteca . . . . . .   cppgmlib
Limitează capabilitaţile . . . .   *yes
Text 'descriere' . . . . . .   Vânzări şi Marketing
```

7. Introduceţi câmpurile rămase din formularul de Descriere Grup Utilizatori în paginile suplimentare ale ecranului şi apăsaţi tasta **Enter** .

```
                        Creare Profil Utilizator

                          Parametrii suplimentari

Autorizare specială. . . . . .   *USRCLS

   :
Descriere job . . . . . .  .   DPTSM
  Biblioteca . . . . . .  . .  QGPL
```

```
                       Creare Profil Utilizator

Autorizare grup . . . . . .   *NONE

   :
Dispozitiv de tipărire . . . . .   PRT03
```

8. Verificaţi mesajele.

Reţineţi

Un profil de grup este doar un tip special de profil de utilizator. Multe mesaje şi ecrane se referă la profilurile de grup ca la utilizatori sau profiluri utilizatori. Sistemul ştie că aţi creat un profil de grup doar dacă adăugaţi membri la el sau îi asignaţi un număr de identificare grup (gid).

Erori posibile	Recuperare
Aţi apăsat **tasta Enter** înainte de a introduce în profilul de grup toate valorile.	Apăsaţi **F5** (Reâmprospătare) pentru a adăuga profilul creat în ecranul Gestionare Profiluri Utilizatori. Folosiţi opţiunea **2** (Modifică) pentru a corecta profilul.
Aţi creat un profil cu un nume greşit.	Nu puteţi modifica numele unui profil. Folosiţi opţiunea de copiere (**3**) pentru a crea un nou profil cu numele corect. Apoi ştergeţi (opţiunea **4**) profilul cu nume greşit.
Unele câmpuri din formularul Descriere Grup utilizatori nu apar pe ecran.	Asiguraţi-vă că folosiţi nivel de ajutorare intermediar. Versiunea nivel de ajutorare de bază de Creare profil utilizator este numită ecranul Adăugare utilizator. Pentru a schimba nivelul de asistenţă, apăsaţi **F12** (Anulare) ca să vă întoarceţi la ecranul de gestionare de înrolare utilizatori. Folosiţi **F21** pentru a schimba nivelul de asistenţă. Vedeţi ″Selectarea nivelului corect de asistenţă. .″
Aţi şters accidental anumite informaţii implicite din ecranul Creare profil utilizator.	Dacă lăsaţi un câmp blanc, sistemul foloseşte valoarea implicită atunci când profilul de utilizator este creat. Dacă doriţi să vedeţi valorile implicite, apăsaţi **F5** (Reîmprospătare) pentru a restaura întregul ecran. Tastaţi din nou informaţia dumneavoastra

Listarea rezultatelor dumneavoastra

Listaţi numele şi descrierile tutoror profilurilor din sistem folosind comanda Afişare utilizatori autorizaţi (DSPAUTUSR). Tastaţi DSPAUTUSR OUTPUT(*PRINT). Verificaţi că toate profilurile de grup au parola *NONE.

Completaţi următoarele înainte de a seta utilizatorii individuali:

- Creaţi o descriere de job pentru fiecare grup de utilizatori.
- Opţional, creaţi o bibliotecă pentru fiecare grup.
- Creaţi un profil de grup pentru fiecare grup de utilizatori.

Setarea utilizatorilor individuali

Atunci cândsetaţi grupurile de utilizatori, parcurgeţi paşii de creare a profilurilor de grup. Acum, creaţi profilurile individuale pentru membrii grupurilor.

Parcurgeţi întreg subiectul cu unul din grupurile Dvs de utilizatori şi apoi, pentru orice grup suplimentar, repetaţi de la capăt toţi paşii. Ecranele exemplu vă arată utilizatorii din Formular profiluri utilizatori individuali acela Sharon Jones pregătiţi pentru Departamentele de Vânzari şi Marketing precum şi pentru Departamentul de Depozite al Compania JKL Toy. Puteţi găsi copii ale acestor formulare în Planificarea profilurilor de utilizatori individuali.″

Folosiţi formularele pentru profiluri de utilizatori individuali pe care le-aţi pregătit înPlanificarea profilurilor de utilizatori individuali.″

Pentru a crea profiluri individuale pentru membrii grupurilor, efectuaţi aceste operaţii:

1. Creaţi o bibliotecă personală.. (opţional)
2. Copiaţi profilul de grup..
3. Setaţi parola să expire.
4. Creaţi utilizatorii suplimentari.. (opţional)

   Notă: Repetaţi Creaţi o bibliotecă personală şi Creaţi utilizatorii suplimentari până când fiecare membru al grupului are un profil de utilizator.
5. Schimbaţi informaţia despre un utilizator, dacă e nevoie.
6. Afişaţi rezultatele voastre.

Semnarea pe sistem

Profil Proprietar (e necesară autorizarea *SECADM)

Meniu SETUP

Crearea unei biblioteci personale

Pentru a începe setarea utilizatorilor individuali, aveţi nevoie să creaţi o bibliotecă personală pentru fiecare membru, pentru obiecte precum programele de interogare. Creaţi bibliotecile personale înaite de a crea profilurile de utilizator individuale.

1. Tastaţi **CRTLIB** şi apăsaţi**F4** (Prompt).
2. Daţi bibliotecii acelaşi nume ca al profilului de utilizator.
3. Apăsaţi**F10** (Parametrii suplimentari).
4. Completaţi autorizarea publică pentru biblioteca şi obiectele noi ce sunt create în bibliotecă.
5. Apăsaţi tasta **Enter**. Verificaţi mesajul de confirmare.

```
                          Creaţi Biblioteca

Introduceţi opţiunile, apăsaţi Enter

Biblioteca . . . . . .   DPTSM
Tipul bibliotecii . . . . . .   *PROD
Text 'Descriere' . . . . . .   Biblioteca Depozit

                         Parametrii suplimentari

Autorizarea. . . . . .   *EXCLUDE
ID pool de stocare auxiliar . . .   1
Creaţi autorizare. . . . . .   *CHANGE
Creaţi obiect de auditare . . .   *SYSVAL
```

După ce aţi creat o bibliotecă personală, puteţi crea profilul individual copiind profilul de grup.

Copierea profilului de grup

Profilul de grup are două roluri:

1. Sistemul îl foloseşte pentru a determina dacă un membru al grupului este autorizat să folosească un obiect.
2. Îl puteţi folosi ca pe un model pentru a crea profiluri de utilizatori pentru membrii individuali ai grupului.

Atunci când setaţi grupurile de utilizatori, creaţi profilurile de grup. Acum, puteţi copia un profil de grup pentru a crea un profil individual şi puteţi copia profilul individual pentru a crea alte profiluri în grup.

1. Alegeţi opţiunea Gestionare Înrolare Utilizator din meniul SETUP.

   Notă: Dacă vedeţi ecranul Gestionare Profiluri Utilizatori, folosiţi **F21** (Selectaţi nivelul de asistenţă) pentru a modifica în nivel de ajutorare de bază.

2. Tastaţi **3** (Copiere) în coloana*Opt* înaintea grupului de utilizatori. Monitorul arată ecranul Copiere Utilizator. (Dacă grupul de utilizatori pe care doriţi să-l copiaţi nu este pe ecranul dumneavoastra derulaţi în jos până îl găsiţi). Sistemul lasă gol câmpul cu numele utilizatorului şi completează câmpurile rămase din profilul de grup pe care l-aţi copiat.

```
                        Gestionare Înrolare Utilizatori

Introduceti opţiunile de mai jos şi apoi apăsaţi Enter
  1=Adaugă   2=Schimbă  3=Copiază  4=Înlătură 5=Afişează

Opt     Utilizator        Descriere

        DPTSM          Departamentul Vânzări şi Marketing
3       DPTWH          Departamentul Depozite
```

3. Tastaţi numele şi descrierea profilului de utilizator pe care îl creaţi.
4. Lăsaţi parola necompletată. Sistemul în mod automat face parola să fie aceeaşi cu numele noului profil de utilizator.
5. Puneţi numele profilului de grup în câmpul *Grup utilizatori* .
6. Verificaţi formularul Profil de Utilizator Individual pentru a vedea dacă acest utilizator are alte valori, diferite de ale grupului. Introduceţi aceste valori.
7. Derulaţi în jos.

```
                              Copiere utilizator

Copiaţi din utilizator . . . :   DPTWH

Introduceţi opţiunile de mai jos şi apoi apăsati Enter

Utilizator. . . . . .   WILLISR
Descriere utilizator. . .   Willis, Rose
Parolă . . . . . .
Tipul de utilizator . . .   *SYSOPR
Grup de utilizatori. . .   DPTWH

Restricţionează folosirea liniei de comandă    N

Biblioteca implicită . . . . .   DPTWH
Imprimanta implicită. . .   PRT04
Program de semnare . .*NONE
  Bibliotecă. . . . . .

Primul meniu. . . . . .   ICMAIN
  Biblioteca. . . . . .      ICPGMLIB
```

8. Faceţi orice schimbări ce sunt necesare în pagina următoare a ecranului şi apăsaţi tasta **Enter**.
9. Verificaţi pentru mesaje de confirmare în partea de jos a ecranului Gestionare Înrolare Utilizatori .

```
                                Copiere utilizator

Copiaţi din utilizator . . . :   DPTWH

Introduceţi opţiunile de mai jos şi apoi apăsati Enter

Program tastă Attn. .   *SYSVAL
  Bibliotecă. . . . . .
```

Erori posibile	Recuperare
Vedeţi ecranul Creaţi Profil Utilizator în loc de ecranul Copiere Utilizator.	Folosiţi **F12** (Anulare) pentru a vă întoarce la ecranul Gestionare Profiluri Utilizatori. Folosiţi **F21** pentru a schimba în nivel de ajutorare de bază. Porniţi din nou operaţia de copiere.
Numele profilului de utilizator pe care l-aţi selectat nu începe în promptul de utilizator.	Deşi numele profilurilor de utilizatori pot avea până la 10 caractere, ecranele de Copiere şi Adăugare Utilizator nu suportă mai mult de 8 caractere pentru nume. Fie alegeţi un nume de utilizator mai scurt fie folosiţi nivel de ajutorare intermediar pentru a crea profiluri de utilizatori individuali.

Testarea Profilului de Utilizator

Atunci când creaţi primul profil individual într-un grup, trebuie să-l testaţi logându-vă în sistem cu acel profil. Verificaţi că vedeţi corect primul meniu şi că programul de semnare rulează.

Dacă nu vă puteţi loga cu succes cu acel profil, probabil că sistemul nu a găsit ceva specificat în profil. Aceasta ar putea fi programul de semnare, descrierea de job sau una din bibliotecile din lista iniţială de biblioteci. Folosiţi ecranul de Gestionare a Ieşirilor de Imprimantă pentru a găsi istoricul jobului ce a fost scris atunci când aţi încercat să semnaţi. Istoricul jobului vă spune ce erori au survenit.

Pentru informaţii despre testarea şi diagnosticarea problemelor ce apar când faceţi schimbări de securitate, vedeţi ″Testarea securităţii.″

După ce aţi testat profilul de utilizator, puteţiseta parola să expire.

Setarea parolei pentru expirare

Setaţi profilurilor individuale să ceară utilizatorilor să-şi schimbe parolele la prima semnare pe sistem. Câmpul *Setare parolă să expire* nu apare în versiunea nivel de ajutorare de bază a ecranului Copiere Utilizator. E nevoie să îl schimbaţi separat, după ce aţi creat profilul de utilizator cu funcţia de copiere. Pentru a schimba câmpul *Setează parola să expire*, tastaţi CHGUSRPRF *nume-profil* PWDEXP(*YES).

Notă: Dacă doriţi sa testaţi un profil de utilizator semnând cu el, faceţi testul *înainte* de a seta parola să expire.

Erori posibile	Recuperare
Aţi testat un profil şi aţi fost forţat să schimbaţi parola.	Tastaţi **CHGUSRPRF** *nume-profil* şi apăsaţi **F4** (Prompt). Setaţi la loc parola cu numele profilului utilizatorului. (Tastaţi numele profilului utilizatorului în câmpul parolă.) Tastaţi ***YES** în câmpul *Setează parola să expire*. E nevoie nivel de ajutorare intermediar să faceţi asta.

După ce aţi creat primul profil de utilizator individual, puteţi crea utilizatori suplimentari.

Crearea utilizatorilor suplimentari

După ce aţi copiat un profil de grup pentru a crea primul profil individual, puteţi crea utilizatori suplimentari. Copiaţi primul profil de utilizator individual pentru a crea membrii suplimentari în grup. Priviţi atent fiecare profil individual atunci când îl creaţi cu metoda de copiere. Verificaţi formularul Profil de Utilizator Individual şi asiguraţi-vă că aţi schimbat fiecare câmp ce e unic pentru noul profil de utilizator.

1. În ecranul Gestionare Înrolare Utilizatori, tastaţi **3** (Copiere) înaintea profilului de utilizator pe care doriţi să-l copiaţi.
2. În ecranul Copiere Utilizator, tastaţi numele profilului şi descrierea.
3. Introduce-ţi informaţia în fiecare câmp ce e unic pentru noul utilizator.

```
                        Gestionare Înrolare Utilizatori

Introduceti opţiunile de mai jos şi apoi apăsaţi Enter
  1=Adaugă   2=Schimbă  3=Copiază  4=Înlătură 5=Afişează

Opt     Utilizator        Descriere

        DPTSM          Departamentul Vânzări şi Marketing
        DPTWH          Departmentul Depozite
3       WILLISR        Willis, Rose
```

Erori posibile	Recuperare
Profilul pe care vreţi să îl copiaţi nu apare în ecranul Gestionare Înrolare Utilizatori.	Apăsaţi **F5** (Refresh). Derulaţi în sus şi în jos. Lista este în ordine alfabetică după numele profilului.

Dacă doriţi să modificaţi informaţia despre un utilizator, vedeţi Modificarea informaţiilor despre un utilizator.

Modificarea informaţiilor despre utilizator

Pentru anumiţi utilizatori, ar putea fi nevoie să setaţi valorile ce nu apar în ecranul Copiere Utilizator. De exemplu, unii utilizatori pot aparţine mai multor profiluri de grup. După ce aţi creat un profil de utilizator folosind metoda de copiere, îl puteţi modifica.

1. În ecranul Gestionare înrolare utilizatori, apăsaţi **F21** pentru a schimba în nivel de ajutorare intermediar.
2. În ecranul Gestionare profiluri utilizatori, tastaţi **2** (Modificare) în coloana *Opt* (opţiune) imediat după profilul pe care doriţi să-l schimbaţi. Apăsaţi tasta **Enter**.

```
                        Gestionare profiluri utilizatori

Introduceţi opţiunile, apăsaţi Enter
  1=Creare   2=Modificare 3=Copiere  4=Şterge   5=Afişează
  12=Gestionare obiecte după proprietar

     Utilizator
Opt  Profile     Text
2    AMESJ       Ames, Janice
     DPTSM          Departamentul Vânzări şi Marketing
     QDOC        Document profil utilizator
     QSECOFR     Profil utilizator responsabil cu securitatea
     WAGNERR     Wagner, Ray
     WILLISR     Willis, Rose
```

3. În ecranul Modifică Profilul Utilizator, apăsaţi **F10** (Parametrii suplimentari).
4. Derulaţi în jos până când găsiţi câmpurile pe care doriţi să le modificaţi. De exemplu, dacă vreţi să faceţi utilizatorul membru al unor profiluri suplimentare, derulaţi în jos până când găsiţi câmpul *grupuri suplimentare* .

5. Tastaţi valorile pe care le doriţi şi apăsaţi tasta **Enter**. Veţi primi mesaje de confirmare şi veţi vedea din nou ecranul de Gestionare a Profilurilor de Utilizatori.

```
                        Modifică Profil Utilizator (CHGUSRPRF)

Introduceţi opţiunile, apăsaţi Enter

Spaţiu de stocare maxim permis . . . .   *NOMAX
Prioritatea de planificare cea mai mare. .   3
Descriere de job . . . . . .   DPTWH
  Bibliotecă . . . . . .     QGPL
Profil de grup . . . . . .   DPTWH
Proprietar . . . . . .   *GRPPRF
Autorizare de grup . . . . . .   *USEE
Tipul autorizării de grup. . . . .   *PGP
Grupuri suplimentare . . . . . .   DPTIC
              + pentru mai multe valori
```

Odată ce aţi schimbat informaţia utilizatorului, puteţi afişa rezultatele pentru a vă verifica profilurile.

Afişarea profilurilor de utilizatori

Pentru a afişa profilurile create sunt disponibile mai multe metode.

Afişarea unui profil
Folosiţi obţiunea **5** (Afişează) fie din ecranul Gestionare Înrolare Utilizatori fie din ecranul Gestionare Profiluri Utilizatori.

Afişarea unui profil
Folosiţi comanda Afişează profilul de Utilizator: DSPUSRPRF *nume-profil* DETAIL(*BASIC) OUTPUT(*PRINT).

Afişare membrii grup
Tastaţi DSPUSRPRF *nume-profil-grup* *GRPMBR. Puteţi folosi OUTPUT(*PRINT) pentru a tipări lista.

Listarea tuturor profilurilor
Pentru a lista numele şi descrierile tuturor profilurilor, sortate după grup, folosiţi comanda Afişează Utilizatorii Autorizaţi DSPAUTUSR SEQ(*GRPPRF) OUTPUT(*PRINT).

Înainte de a seta dreptul de proprietate şi autorizarea publică, asiguraţi-vă că aţi efectuat aceste operaţii:

- Terminaţi crearea tuturor profilurilor de utilizatori individuali.
- Setaţi să expire parola fiecărui profil.
- Tipăriţi o lista a tuturor profilurilor sortate după grup şi ţineţi-o cu formularele de Descriere Grup Utilizatori. Tipăriţi lista din nou când adăugaţi noi utilizatori.

Setarea securităţii resurselor

La acest subiect, stabiliţi dreptul de proprietate şi autorizarea pentru public la obiecte, precum şi autorizări specifice pentru aplicaţia dumneavoastra. Setaţi de asemenea securitate resurse pentru staţii şi imprimante. Parcurgeţi toate etapele pentru o biblioteca, apoi mergeţi înapoi şi repetaţi paşii pentru toate celelalte biblioteci folosite de o aplicaţie. Când aţi terminat de setat securitatea resurselor pentru o aplicaţie, repetaţi paşii pentru alte aplicaţii.

Folosiţi aceste proceduri ori de câte ori instalaţi o aplicaţie noua în sistem sau când setaţi securitatea de resurse pentru o aplicaţie existentă.

Ecranele exemplu din acest subiect afişează formularele Listă autorizaţie, Descriere bibliotecă, Coadă de ieşire şi Securitate staţii de lucru pentru Compania JKL Toy. Puteţi găsi exemple ale acestor formulare în ″ Setare drept proprietate şi autorizare publică.″

Ce formulare sunt necesare?

- Formularele Instalare aplicaţie pe care le-aţi pregătit în ″Planificare instalare aplicaţie.″
- Formularele Listă autorizaţie pe care le-aţi pregătit în ″Grupare obiecte.″
- Formularele Descriere bibliotecă pe care le-aţi pregătit în ″Determinarea dreptului de proprietate asupra bibliotecilor şi obiectelor.″
- Formularele Coadă de ieşire şi Securitate staţie de lucru pe care le puteţi pregăti în″Protejare ieşire imprimantă″ şi ″Protejare staţii de lucru.″
- Formularul Responsabilit[ţi sistem pe care l-aţi pregătit în ″Planificare strategie generală de securitate.″

Puteţi seta securitatea resurselor în mai multe feluri. Ordinea paşilor din acest subiect corespunde ordinii informaţiilor din formularele Instalare aplicaţie, Lista autorizaţie şi Descriere bibliotecă:

1. Setare drept de proprietate şi autorizare publică.
2. Creare listă autorizaţie.
3. Securizare obiecte cu o listă de autorizaţii.
4. Adăugare utilizatori la lista de autorizaţii.
5. Setare autorizări specifice.
6. Securizare ieşire imprimantă.
7. Securizare staţii de lucru.
8. Restricţionare access la coada de mesaje de operator sistem .

Setarea dreptului de proprietate şi a autorizării publice.

În acest subiect veţi stabili dreptul de proprietatea şi autorizarea publică pentru bibliotecile de aplicaţii, bibliotecile de grup şi bibliotecile personale. Parcurgeţi întreg subiectul cu o aplicaţie iar apoi repetaţi de la început toţi paşii pentru fiecare aplicaţie suplimentară. Ecranele exemplu vă arată formularele de Instalare Aplicaţie pe care Sharon Jones le-a preparat pentru aplicaţia Comenzi Clienţi în Planificarea instalării aplicaţiei Dvs.″

Folosiţi procedurile din acest subiect ori de câte ori instalaţi o nouă aplicaţie în sistemul dumneavoastra sau când setaţi securitatea pentru o aplicaţie existentă.

Folosiţi formularele de Instalare Aplicaţie pe care le-aţi pregătit în Planificarea instalării aplicaţiei Dvs.″

Pentru a seta dreptul de proprietate şi autorizarea publică efectuaţi aceste operaţii:

1. Creaţi un profil de proprietar.
2. Modificaţi dreptul de proprietate asupra bibliotecii.
3. Setaţi dreptul de proprietate asupra obiectelor aplicaţiei.
4. Setaţi accesul public la o bibliotecă.
5. Setaţi autorizarea publică pentru toate obiectele dintr-o bibliotecă.
6. Setaţi autorizare publică pentru obiectele noi.
7. Gestionarea bibliotecilor personale şi de grup.

Semnarea pe sistem

Profil Proprietar (e necesară autorizarea *ALLOBJ)

Meniu Principal

Crearea unui profil de proprietar

Dacă profilul de proprietar nu există faceţi următoarele:

- Folosiţi comanda CRTUSRPRF (Creare Profil Utilizator) pentru a-l crea. Setaţi parola în *NONE.

Dacă profilul de proprietar există deja, faceţi următoarele:

- Folosiţi comanda CHGUSRPRF (Modificare Profil de Utilizator) pentru a seta parola în *NONE.

După ce creaţi profilul de proprietar puteţi modifica dreptul de proprietar asupra bibliotecii.

Modificarea dreptului de proprietate al bibliotecii

Acest pas schimbă dreptul de proprietate al unei biblioteci nu al obiectelor din bibliotecă.

Atenţie: Înainte de a schimba dreptul de proprietate al oricărui obiect aplicaţie consultaţi-vă mai întâi cu furnizorul aplicaţiei. Unele aplicaţii folosesc funcţii ce se bazează pe anumite drepturi de proprietate ale obiectelor.

1. TastaţiCHGOBJOWN (Modificare Proprietar Obiect) şi apăsaţi **F4** (Prompt).
2. Completaţi numele bibliotecii, tipul obiectului (*LIB) şi noul proprietar.
3. Verificaţi mesajele de confirmare.

```
                      Modificare Proprietar Obiect (CHGOBJOWN)

Introduceţi opţiunile, apăsaţi Enter

Obiect . . . . . . . . . . . . . > COPGMLIB
  Biblioteca . . . . . . . . . . >   *LIBL       Nume,
Tip Obiect  . . . . . . . . . .> *LIB
Noul proprietar. . . . . . . . .   COWNER
Autorizarea proprietarului curent . .   *REVOKE
```

Erori posibile	Recuperare
Primiţi mesaje de eroare.	Cel mai obişnuit mesaj este fie că biblioteca nu a fost găsită sau noul profil de proprietar nu a fost găsit. Verificaţi ce erori ce aţi tastat şi încercaţi din nou.

După ce schimbaţi dreptul de proprietate al bibliotecii puteţi seta dreptul de proprietate pentru obiectele aplicaţie.

Setarea dreptului de proprietate al obiectelor aplicaţie

Modificarea dreptului de proprietate pentru obiectele aplicaţiei este un task greu de realizat din cauză că trebuie să modificaţi fiecare obiect individual. Dacă e posibil, cereţi programatorului sau furnizorului aplicaţiei să stabilească drepturile de proprietate pentru dumneavoastra

Listarea obiectelor dintr-o bibliotecă

Înainte de a schimba dreptul de proprietate, tipăriţi o listă a tuturor obiectelor dintr-o bibliotecă folosind comanda Afişare Bibliotecă. O puteţi folosi ca pe o listă de verificare. Tastaţi DSPLIB *nume-bibliotecă* *PRINT.

Alegerea celei mai bune metode

Alegeţi una din aceste două metode pentru a schimba dreptul de proprietate al obiectelor din bibliotecile Dvs de aplicaţii:

Tabela 61. Metode de Schimbare a Dreptului de Proprietate al Obiectelor

Metodă	Ce face	Când s-o folosiţi
Comanda Gestionare obiecte după proprietar	Arată un ecran ce listează toate obiectele pe care le deţine un profil. Puteţi folosi o obţiune în ecran pentru a schimba proprietarul unui obiect.	Această metodă este mai uşor de folosit. Însă dacă obiectele sunt deţinute de QPGMR sau QSECOFR, IBM nu recomandă această metodă. Aceste profiluri deţin multe obiecte, iar lista dumneavoastra afişată va fi foarte mare.

Tabela 61. Metode de Schimbare a Dreptului de Proprietate al Obiectelor (continuare)

Metodă	Ce face	Când s-o folosiţi
Comanda Modificare drept de Proprietate Obiect	Necesită folosirea unei comenzi separate pentru fiecare obiect. Totuşi, puteţi folosi *Comenzi anterioare* (**F9**) pentru a repeta comanda anterioară şi a reduce astfel din cantitate de date ce trebuie introdusă.	Această metodă este mai rapidă dacă QPGMR sau QSECOFR deţin obiectele.

Folosirea comenzii Gestionare obiecte după proprietar (WRKOBJOWN): Folosiţi această metodă pentru a modifica dreptul de proprietate al obiectelor dintr-o bibliotecă dacă profilurile livrate de IBM, precum QPGMR sau QSECOFR, *nu* deţin obiectele:

1. Tastaţi WRKOBJOWN *nume-profil-proprietar*. Ecranul dumneavoastra afişează o listă cu toate obiectele pe care le deţine acel profil de utilizator.
2. Tastaţi **9** (Modificare proprietar) în faţa fiecărui obiect din biblioteca cu care lucraţi.
3. Pe linia *Parametrii sau comandă* în partea de jos a ecranului, tastaţi NEWOWN(*nume-profil-proprietar*) şi apăsaţi tasta **Enter**.
4. Sistemul modifică proprietarul fiecărui obiect indicat de dumneavoastra cu noul proprietar pe care l-aţi introdus în partea de jos. Veţi recepţiona mesaje de confirmare în partea de jos a ecranului dumneavoastra Obiectele nu mai apar pe ecranul dumneavoastra pentru că profilul nu le mai deţine.
5. Repetaţi paşii 2 şi 4 până când modificaţi dreptul de proprietate pentru toate obiectele din bibliotecă.

```
                         Gestionare Obiecte după Proprietar

Profil utilizator. . . . . :   OLDOWNER

Introduceţi opţiunile, apăsaţi Enter
  2=Editează autorizarea  4=Şterge  5=Afişează autorul
  8=Afişează descrierea   9=Modifică proprietarul

Opt  Obiect        Bibliotecă    Tip       Atribut
     COPGMMSG      COPGMLIB      *MSGQ
9    CUSTMAS       CUSTLIB       *FILE
9    CUSTMSGQ      CUSTLIB       *MSGQ
     ITEMMSGQ      ITEMLIB       *MSGQ


   ⋮

Parametrii sau comandă
===> NEWOWN(COWNER)
F3=Ieşire F4=Prompt   F5=Reâmprospătare F9=Comenzi Anterioare
F18=Partea de jos
```

Erori posibile	Recuperare
Vedeţi ecranul de Modificare proprietar obiect	Vedeţi acest ecran dacă specificaţi opţiunea **9** (Modificare proprietar) şi nu tastaţi nici un parametru în partea de jos a ecranului Gestionare Obiecte după Proprietar. Vedeţi de asemenea acest ecran dacă tastaţi incorect parametri. Apăsaţi **F12** (Anulare) pentru a vă întoarce la ecranul Gestionare Obiecte după Proprietar. Încercaţi din nou. Asiguraţi-vă că aţi tastat parametrii aşa cum v-a fost arătat în exemplu.

Puteţi folosi comanda de schimbare a proprietarului obiectului pentru a schimba dreptul de proprietate al obiectelor ce sunt deţinute de QPMGR sau QSECOFR.

Folosirea comenzii de schimbare a dreptului de proprietate al obiectelor: Folosiţi această metodă pentru a schimba proprietarul obiectelor dintr-o bibliotecă dacă QPMGR sau QSECOFR deţin acele obiecte.

1. Tastaţi CHGOBJOWN şi apăsaţi**F4** (Prompt).
2. Completaţi pe ecran informaţiile pentru primul obiect din listă şi apăsaţi tasta **Enter**.

```
                      Modificare Proprietar Obiect (CHGOBJOWN)

Introduceţi opţiunile, apăsaţi Enter

Obiect . . . . . . . . . . . . . > CUSTMAS
  Bibliotecă. . . . . . . . . . .   CUSTLIB
Tip obiect . . . . . . . . . . . > *FILE
Noul Proprietar. . . . . . . . .   COWNER
Autorizarea proprietarului curent . .  *REVOKE
```

3. Primiţi un mesaj de confirmare cum că dreptul de proprietate al obiectului a fost modificat. Debifaţi elementul din lista dumneavoastra
4. Apăsaţi **F9** (Comenzi anterioare) pentru a relua comanda pe care aţi introdus-o.
5. Apăsaţi **F4** (Prompt). În ecranul Modificare Proprietar Obiect introduce-ţi informaţia pentru următorul obiect din bibliotecă şi apăsaţi tasta **Enter** .
6. Repetaţi paşii patru şi cinci pentru fiecare obiect din bibliotecă.

Verificarea muncii dumneavoastra

Pentru a fi siguri că aţi schimbat dreptul de proprietate al tuturor obiectelor din bibliotecă, folosiţi comanda Gestionare Obiecte după Proprietar. Tastaţi WRKOBJOWN *noul-profil-proprietar*. Comparaţi acest ecran cu lista dumneavoastra de obiecte din bibliotecă.

După ce modificaţi dreptul de proprietate al obiectelor din bibliotecă puteţi seta accesul public la bibliotecă.

Setarea accesului public la o bibliotecă

După ce setaţi dreptul de proprietate pentru obiectele aplicaţie, puteţi folosi comanda Editare Autorizare Obiect (EDTOBJAUT) pentru a schimba autorizarea publică a bibliotecii:

1. Tastaţi EDTOBJAUT *nume-bibliotecă* *LIB.
2. Mutaţi cursorul în jos la linia ce arată **PUBLIC*.
3. Tastaţi autorizarea pe care doriţi să o aibă publicul pentru bibliotecă şi apăsaţi tasta**Enter**.

```
                          Editare Autorizare Obiect

Obiect . . . . . :   CUSTLIB        Proprietar . . . . . :   COWNER
  Bibliotecă . . . :     QSYS       Grup primar .  . . . :   *NONE
Tip obiect   . . . :   *LIB

Tastaţi modificările pentru autorizările curente şi apăsaţi Enter.

  Obiect securizat de lista de autorizare . . . . . .   *NONE

                         Obiect
Utilizator  Grup        Autorizare
COWNER                   *ALL
*PUBLIC                  *CHANGE
```

4. Ecranul vă arată noua autorizare.

Puteţi acum seta autorizarea publică pentru toate obiectele dintr-o bibliotecă.

Setarea autorizării publice pentru toate obiectele dintr-o bibliotecă

Folosiţi comanda Retragere Autorizare Obiect (RVKOBJAUT) pentru a înlătura autorizarea publică curentă pentru obiectele dintr-o bibliotecă. Folosiţi comanda de Acordare Autorizare Obiect (GRTOBJAUT) pentru a seta autorizarea publică pentru toate obiectele dintr-o bibliotecă.

1. Tastaţi RVKOBJAUT şi apăsaţi **F4** (Prompt).
2. Completaţi ecranul aşa cum s-a arătat, substituind numele biblioteci Dvs de aplicaţie şi apăsând tasta **Enter**.

```
                    Retragere Autorizare Obiect (RVKOBJAUT)

Introduceţi opţiunile, apăsaţi Enter

Obiect . . . . . .   *all
  Biblioteca . . . . . .    custlib
Tip obiect   . . . . . .   *all
Utilizatori. . . . . .   *public
              + pentru mai multe valori
Autorizare . . . . . .   *all
```

Notă: Dacă biblioteca are un număr mare de obiecte, sistemului îi poate lua câteva minute ca să proceseze cererea.

3. Introduceţi GRTOBJAUT şi apăsaţi **F4** (Prompt).
4. Completaţi ecranul aşa cum s-a arătat, substituind numele bibliotecii Dvs de aplicaţie şi autorizarea pe care o doriţi şi apăsând tasta **Enter** .

```
                    Acordare Autorizare Obiect (GRTOBJAUT)

Introduceţi opţiunile, apăsaţi Enter

Obiect . . . . . .   *all
  Biblioteca . . . . . .    custlib
Tip obiect   . . . . . .   *all
Utilizatori. . . . . .   *public
              + pentru mai multe valori
Autorizare . . . . . .   *use
```

Notă: Dacă biblioteca are un număr mare de obiecte, sistemului îi poate lua câteva minute ca să proceseze cererea.

După ce aţi terminat setare autorizării publice pentru toate obiectele dintr-o bibliotecă puteţifolosi logul de joburi ca să verificaţi ce aţi făcut.

Folosire log de joburi pentru verificarea muncii: Când folosiţi comanda GRTOBJAUT pentru a face schimbări multiple la autorizare verificaţi logul de joburi pentru a verifica ce aţi făcut.

1. Tastaţi DSPJOBLOG (Afişare Log de Joburi).
2. Apăsaţi **F10** (Afişare mesaje detaliate).
3. Trebuie să aveţi un mesaj despre schimbările de autorizare pentru fiecare obiect din bibliotecă. Debifaţi în lista dumneavoastra obiectele pe măsură ce parcurgeţi mesajele.

```
                          Afişează toate mesajele
                        Sistem:   RCHASxxx
Job . . :   QPADEV0010    Utilizator   JCHEIDEL      Număr  . . . :   025457

7 > GRTOBJAUT OBJ(CUSTLIB/*ALL) OBJTYPE(*ALL) USER(*PUBLIC) AUT(*USE)
  Autorizarea dată utilizatorului *PUBLIC pentru obiectul CUSTMAS în CUSTLIB
    *FILE.
  Autorizarea dată utilizatorului *PUBLIC pentru obiectul CUSTMSGQ în CUSTLIB
    *MSGQ.
  Autorizarea dată pentru 2 obiecte. Nu dată la 0 obiecte. Parţial dată la 0
    obiecte.
  Autorizarea obiect acordată.
7>> dspjoblog
```

Erori posibile	Recuperare
Logul dumneavoastra de joburi indică cum că autorizarea nu a fost modificată pentru anumite obiecte ale bibliotecii.	Folosiţi Ajutorul**F1**) pentru a primi mai multe informaţii despre mesaj. Folosiţi EDTOBJAUT pentru a seta individual autorizarea acelor obiecte.

Acum puteţi seta autorizarea publică pentru noile obiecte.

Setarea autorizării publice pentru noile obiecte.

Descrierea bibliotecii are un parametru numit creare autorizare (CRTAUT), ce determină autorizarea publică pentru noile obiecte ce sunt create în bibliotecă. Comenzile ce creează obiecte folosesc în mod implicit autorizarea CRTAUT a bibliotecii de obiecte. Trebuie să faceţi CRTAUT pentru o bibliotecă aceeaşi ca autorizarea publică pentru majoritatea obiectelor existente în bibliotecă.

1. Tastaţi CHGLIB *nume-bibliotecă* şi apăsaţi **F4** (Prompt).
2. Apăsaţi **F10** (Parametrii suplimentari).
3. Introduceţi alegerea dorită în câmpul *Creare autorizare*.

```
                     Modifică bibliotecă (CHGLIB)

Introduceţi opţiunile, apăsaţi Enter

Biblioteca . . . . . . . . . . . > CUSTLIB
Tip bibliotecă . . . . . . . . .   *PROD
Text 'descriere' . . . . . . . .   'Customer Records'


                     Parametrii suplimentari

Creare autorizare. . . . . . . .   *CHANGE
Creare auditare obiect . . . . .   *SYSVAL
```

Dacă setaţi CRTAUT cu *SYSVAL, sistemul foloseşte setările curente pentru valoarea de sistem QCRTAUT la crearea de obiecte noi în bibliotecă. Setând o autorizare specifică CRTAUT pentru fiecare bibliotecă protejăm împotriva schimbărilor viitoare a valorii de sistem QCRTAUT.

Puteţi acum lucra cu biblioteci de grup şi personale.

Gestionarea bibliotecilor de grup şi personale

Profilul dumneavoastra deţine bibliotecile personale şi de grup create atunci când aţi setat grupurile de utilizatori şi utilizatorii individuali.

Folosiţi procedurile învăţate pentru a schimba dreptul de proprietate al bibliotecilor de grup la profilul de grup şi pentru a schimba dreptul de proprietate al bibliotecilor personale la profilurile de utilizator individuale. Folosiţi comanda EDTOBJAUT.

Setaţi parametrul Creare Autorizare pentru fiecare bibliotecă de grup şi personală pentru a delimita autorizare publică pentru orice nou obiect în acele biblioteci. Folosiţi comanda CHGLIB.

Înainte de începe să creaţi liste de autorizare , parcurgeţi aceste operaţii:

- Folosiţi formularele dumneavoastra de Instalare de Aplicaţii şi formularele de Descrieri de Biblioteci pentru a fi siguri că aţi stabilit dreptul de proprietate şi autorizarea publică pentru toate bibliotecile de aplicaţii.
- Setaţi dreptul de proprietate şi creaţi autorizare pentru toate bibliotecile de grup şi personale pe care le-aţi creat.

Notă: Puteţi primi o listă cu toate bibliotecile din sistem tastând DSPOBJD *ALL *LIB *PRINT.

Creare listă de autorizaţii

După ce aţi setat dreptul de proprietate şi autorizare publică, sunteţi gata să setaţi listele de autorizaţii. Folosind informaţiile din formularele Listă autorizaţii, creaţi orice listă de autorizaţii necesară pentru a securiza biblioteca. Folosiţi comanda Creare listă autorizaţii (Create Authorization List - CRTAUTL):

1. Introduceţi CRTAUTL şi apăsaţi **F4** (Prompt).
2. Completaţi informaţiile din formularul Listă autorizaţii.
3. Apăsaţi **F10** (Parametrii suplimentari).
4. Folosiţi parametrul autorizare pentru a specifica autorizarea publică pentru obiectele care sunt securizate de listă.
5. Verificaţi dacă sunt mesaje de confirmare.

```
                    Creare listă autorizaţii (CRTAUTL)

Introduceţi opţiuni, apăsaţi Enter.

Listă autorizaţii . . . . . .   custlst1
Descriere text . . . . . .   Fişiere curăţate la

                        Parametrii suplimentari

Autorizare  . . . . . .   *ALL
```

Eroare posibilă	Recuperare
Aţi introdus numele listei incorect.	Nu puteţi modifica numele unei liste, odată creată în sistem. Ştergeţi lista (DLTAUTL) şi încercaţi din nou.
Aţi uitat să specificaţi autorizarea publică pentru listă.	Folosiţi comanda Editare listă autorizaţii (EDTAUTL).

Acum puteţi securiza obiectul cu o listă de autorizaţii.

Securizare obiecte cu o listă de autorizaţii

Odată ce aţi creat o listă de autorizaţii, folosiţi comanda Editare autorizare obiect (EDTOBJAUT) pentru a securiza elementele listate în formularul Listă autorizaţie:

1. Introduceţi EDTOBJAUT şi apăsaţi **F4** (prompt).
2. Completaţi ecranul de prompt şi apăsaţi tasta **Enter**.
3. În ecranul Editare autorizare obiect, introduceţi numele listei de autorizaţii.
4. Dacă autorizarea publică pentru obiect vine din lista de autorizaţii, modificaţi autorizarea publică la *AUTL.
5. Repetaţi aceşti paşi pentru fiecare obiect din formularul Listă autorizaţie.

```
                          Editare autorizare obiect

Obiect . . . . . :   ARFILE01        Proprietar . . . . . :   OWNAR
  Bibliotecă . . . . :     CUSTLIB       Grup primar. . . . . :   *NONE
Tip obiect . . . . . :   *FILE

Introduceţi modificările la autorizările curente, apăsaţi Enter.

  Obiect securizat de listă autorizaţie . . . . . .   CUSTLST1

                          Obiect
Utilizator   Grup         Autorizare
PROPRIETAR               *ALL
*PUBLIC                  *AUTL
```

Acum puteţi adăuga utilizatori la o listă de autorizaţii.

Adăugare utilizatori la o listă de autorizaţii

Odată ce aţi securizat un obiect cu o listă de atorizaţii, folosiţi comanda Editare listă autorizaţii (EDTAUTL) pentru a adăuga utilizatorii listaţi în formularul Listă autorizaţie:

1. Introduceţi EDTAUTL *nume-listă-autorizaţii*.
2. În ecranul Editare listă autorizaţii, apăsaţi F6 **F6** (Adăugare utilizator nou).
3. Introduceţi numele utilizatorilor sau grupurilor şi autorizarea pe care trebuie să o aibă asupra articolelor din listă şi apăsaţi tasta **Enter**.
4. Utilizatorii ar trebui să apară în listă.

```
                           Adăugare noi utilizatori

Obiect . . . . . :   WSLST1          Proprietar
  Bibliotecă . . . . :     QSYS

Introduceţi utilizatorii noi, apăsaţi Enter.

             Obiect    Listă
Utilizator  Autorizare Mgt
QSECOFR     *CHANGE
```

Eroare posibilă	Recuperare
Aţi dat unui utilizator sau grup autorizare greşită la listă.	Puteţi modifica autorizarea în ecranul Editare listă de autorizaţii.
Aţi adăugat un utilizator sau un grup greşit la listă.	Puteţi înlătura un utilizator sau un grup folosind comanda Înlăturare intrare din listă de autorizaţii (RMVAUTLE), sau puteţi tasta spaţii peste autorizarea utilizatorului în ecranul Editare listă de autorizaţii.

Verificare

Folosiţi comanda Aişare listă de autorizaţii (Display Authorization List - DSPAUTL) pentru a lista toate autorizările utilizator la lista de autorizaţii. Folosiţi **F15** pentru a afişa toate obiectele securizate de lista de autorizaţii.

Înainte de a seta autorizări specifice, efectuaţi aceste operaţii:

- Utilizaţi comanda CRTAUTL pentru a crea listele de autorizaţii de care aveţi nevoie pentru aplicaţie.
- Securizaţi obictele cu liste de autorizaţii folosind comanda EDTOBJAUT.

- Adăugaţi utilizatori la listele de autorizaţii folosind comanda EDTAUTL.

Setare autorizări specifice

În ″Setare drept de proprietate şi autorizare publică,″ aţi învăţat cum să utilizaţi comanda GRTOBJAUT pentru a seta autorizarea publică pentru toate obiectele dintr-o bibliotecă, în funcţie de informaţia din Partea 1 a formularului Descriere bibliotecă. Acum, puteţi folosi comanda Editare autorizare obiect (Edit Object Authority - EDTOBJAUT) pentru a seta autorizarea specifică pentru bibliotecă şi obiectele din bibliotecă, în funcţie de informaţia din Partea 2 a formularului Descriere bibliotecă.

Consultaţi aceste subiecte pentru a seta autorizări specifice:

- Setare autorizare specifică pentru o bibiotecă.
- Setare autorizare specifică pentru un obiect.
- Setare autorizare pentru mai multe obiecte simultan.

Setare autorizare specifică pentru o bibiotecă

O bibliotecă este într-adevăr un tip special de obiect. Setaţi autorizarea pentru o bibliotecă exact cum setaţi autorizarea pentru orice alt obiect, folosind comanda EDTOBJAUT. Toate bibliotecile se află într-o bibliotecă furnizată de IBM numită QSYS. Ecranele din următoarele exemple folosesc Partea 2 din formularul Descriere bibliotecă pentru biblioteca CONTRACTS de la Compania JKL Toy:

Listare autorizări specifice pentru obiecte bibliotecă				
Profil grup sau profil utilizator	Nume obiect	Tip obiect	Autorizare necesară	Listă de autorizaţii
DPTSM	CONTRACTS	*LIB	*USE	
DPTMG	CONTRACTS	*LIB	*USE	

1. Introduceţi EDTOBJAUT şi apăsaţi **F4** (Prompt).
2. Completaţi ecranul de prompt şi apăsaţi tasta **Enter**.

```
                    Editare autorizare obiect (Edit Object Authority - EDTOBJAUT)

Introduceţi opţiuni, apăsaţi Enter.

Obiect . . . . . . . . . . . . .   CONTRACTS
  Bibliotecă . . . . . . . . . .     QSYS
Tip obiect  . . . . . . . . . .   *LIB
```

3. În ecranul Editare autorizare obiect, apăsaţi**F6** (Adăugare noi utilizatori) pentru a acorda autorizare utilizatorilor care nu sunt afişaţi pe ecran.
4. Apăsaţi tasta **Enter**.

```
                             Adăugare noi utilizatori

Obiect . . . . . . . :   CONTRACTS       Proprietar . . . . . :   OWNCP
  Bibliotecă . . . . :     QSYS          Grup primar. . . . . :   *NONE
Tip obiect . . . . . :   *LIB


Introduceţi noi utilizatori, apăsaţi Enter.

                   Obiect
Utilizator         Autorizare
DPTSM       *USE
DPTMG       *USE
```

5. Ecranul Editare autorizare obiect ar trebui să corespundă informaţiilor din Partea 1 şi Partea 2 din formularul Descriere bibliotecă.

```
                          Editare autorizare obiect

Obiect . . . . . :   CONTRACTS       Proprietar . . . . . :   OWNCP
  Bibliotecă . . . . :     QSYS          Grup primar. . . . . :   *NONE
Tip obiect . . . . . :   *LIB

Introduceţi modificările la autorizările curente, apăsaţi Enter.

  Obiect securizat de listă de autorizaţii. . . . . .   *NONE

                          Obiect
Utilizator   Grup         Autorizare
OWNCP                    *ALL
DPTSM                    *USE
DPTMG                    *USE
*PUBLIC                  *EXCLUDE
```

Autorizarea publică pentru noile autorizări obiect (CRTAUT) nu apare în ecranul Editare autorizare obiect pentru o bibliotecă. Utilizaţi comanda Afişare bibliotecă (DSPLIB) pentru a vedea CRTAUT pentru o bibliotecă.

Puteţi de asemenea utiliza această procedură pentru a seta o anumită autorizare pentru un obiect din sistem.

Puteţi acum seta o autorizare specifică pentru un obiect.

Setare autorizare specifică pentru un obiect

Procedura pentru setarea unei autorizări specifice pentru un obiect dintr-o bibliotecă de aplicaţie este aceeaşi ca pentru setarea autorizării specifice pentru o bibliotecă. Exemplul foloseşte Partea 2 din formularul Descriere bibliotecă pentru biblioteca COPGMLIB de la Compania JKL Toy:

Tabela 62. Descriere bibliotecă la Compania JKL Toy form

Profil grup sau profil utilizator	Nume obiect	Tip obiect	Autorizare necesară	Listă de autorizaţii
PUBLIC	COMSGQ01	*MSGQ	*CHANGE	

1. Introduceţi EDTOBJAUT şi apăsaţi **F4** (Prompt).
2. Completaţi informaţiile din ecranul de prompt şi apăsaţi tasta **Enter**.
3. Completaţi informaţiile despre autorizări în ecranul Editare autorizare obiect şi apăsaţi tasta **Enter**.

```
                          Editare autorizare obiect

Obiect . . . . . :   COMSGQ01        Proprietar . . . . . :   OWNCO
  Bibliotecă . . . . :     COPGMLIB       Grup primar. . . . . :   *NONE
Tip obiect . . . . . :   *MSGQ

Introduceţi modificările la autorizările curente, apăsaţi Enter.

  Obiect securizat de listă de autorizaţii. . . . . .   *NONE

                          Obiect
Utilizator   Grup         Autorizare
OWNCO                    *ALL
*PUBLIC                   *CHANGE
```

Puteţi acum seta autorizarea pentru mai multe obiecte simultan.

Setarea autorizării pentru mai multe obiecte simultan

Exemplele de până acum au utilizat comanda EDTOBJAUT pentru a seta autorizarea specifică pentru un singur obiect. Utilizaţi comanda acordare autorizare (Grant Authority - GRTOBJAUT) pentru a seta autorizarea pentru mai multe obiecte. Introduceţi GRTOBJAUT şi apăsaţi **F4** (Prompt). În continuare sunt câteva exemple pentru efectuarea de mai multe modificări la autorizare.

- Câmpurile introduse în ecranul următor setează autorizarea publică pentru toate cozile de mesaje din biblioteca CUSTLIB la *CHANGE.

```
                    Acordare autorizare obiect (Grant Object Authority - GRTOBJAUT)

Introduceţi opţiuni, apăsaţi Enter.

Obiect . . . . . .   *all
  Bibliotecă . . . . . .    custlib
Tip obiect . . . . . .   *msgq
Utilizatori. . . . . .   *public
              + pentru mai multe valori
Autorizare. . . . . .   *change
```

- Câmpurile introduse în ecranul următor acordă autorizarea *ALL tuturor fişierelor ale căror nume începe cu caracterele WRK din biblioteca CUSTLIB utilizatorului AMES.

```
                    Acordare autorizare obiect

Introduceţi opţiuni, apăsaţi Enter.

Obiect . . . . . .   WRK*
  Bibliotecă . . . . . .    custlib
Tip obiect. . . . . .   *file
Utilizatori. . . . . .   AMES
              + pentru mai multe valori
Autorizare . . . . . .   *all
```

Acest exemplu foloseşte o tehnică pentru specificarea parametrilor numită nume**generic**. Multe comenzi vă permit să specificaţi primul caracter urmat de un asterisc (*) pentru un parametru. Sistemul efectuează operaţia pe fiecare obiect al cărui nume începe cu acele caractere. Informaţia on-line pentru o comandă spune ce parametrii permit nume generice.

- Va trebui să urmaţi doi paşi pentru a securiza toate fişierele care încep cu caracterele AR utilizând o listă de autorizaţii numită ARLST1 şi ca toate fişierele să-şi ia autorizarea publică din listă. Aceste ecrane arată paşii necesari.

```
                    Acordare autorizare obiect

Introduceţi opţiuni, apăsaţi Enter.

Obiect . . . . . .   AR*
  Bibliotecă . . . . . .    CUSTLIB
Tip obiect   . . . . . .   *FILE

   :
Listă autorizaţii. . . . . .   ARLST1
```

```
                    Acordare autorizare obiect

Introduceţi opţiuni, apăsaţi Enter.

Obiect . . . . . .   AR*
  Bibliotecă . . . . . .     CUSTLIB
Tip obiect   . . . . . .   *FILE
Utilizatori. . . . . .   *PUBLIC
              + pentru mai multe valori
Autorizare  . . . . . .    *AUTL
              + pentru mai multe valori
```

Utilizaţi comanda DSPJOBLOG aşa cum este descrisă în ″Utilizare istoric job pentru verificare″ pentru a verifica dacă sistemul a efectuat modificările de autorizare necesare.

Înainte de a merge la ″Securizare ieşire imprimantă,″ utilizaţi comanda EDTOBJAUT sau GRTOBJAUT pentru a seta autorizări specifice în Partea 2 din formularul Descriere bibliotecă.

Securizare ieşire imprimantă

După ce aţi setat anumite autorizări, vă puteţi proteja ieşirea la imprimantă folosind informaţiile din următoarele subiecte:

- Crearea unei cozi de ieşire şi controlul utilizatorilor care o pot administra.
- Asociere ieşire imprimantă specială la coadă.

Crearea unei cozi de ieşire

1. Introduceţi CRTOUTQ (Creare coadă ieşire) şi apăsaţi **F4** (Prompt).
2. Completaţi numele cozii de ieşire şi a bibliotecii.
3. Apăsaţi **F10** (Parametrii suplimentari).
4. Derulaţi în jos pentru a găsi informaţiile despre securitate pentru coada de ieşire.

```
                  Creare coadă de ieşire (Create Output Queue - CRTOUTQ)

Introduceţi opţiuni, apăsaţi Enter.

Coadă ieşire . . . . . >   NEWCP
  Bibliotecă . . . . . .       CONTRACTS
Dimensiune maximă fişier spool:
  Număr de pagini  . . . . . .   *NONE         Număr, *NONE
  Oră început  . . . . . .                    Ora
  Oră terminare. . . . . .                    Ora
            + pentru mai multe valori
Ordinea fişierelor în coadă . . .   *FIFO
Sistem la distanţă . . . . . .   *NONE

   ⋮
Descriere text     . . . . . .   Coadă contracte noi
```

5. Completaţi informaţiile din formularul Securitate cozi de ieşire şi staţii de lucru pentru a controla cine poate utiliza şi administra coada de ieşire.
6. Apăsaţi tasta **Enter** şi verificaţi dacă sunt mesaje de confirmare.

```
                    Creare coadă de ieşire (Create Output Queue - CRTOUTQ)

Introduceţi opţiuni, apăsaţi Enter.


Parametrii suplimentari

Afişare orice fişier . . . . . .   *NO
Separatori job . . . . . .  . .   0
Controlat de operator  . . . . .   *NO
Coadă de date. . . . . .  . . .   *NONE
  Bibliotecă . . . . . .  . . .
Autorizare de verificat. . . . .   *OWNER
Autorizare. . . . . .  . . . . .  *LIBCRTAUT
```

Eroare posibilă	Recuperare
Aţi apăsat tasta **Enter** în loc de **F10**.	Folosiţi comanda Modificare coadă ieşire (Change Output Queue - CHGOUTQ) pentru a introduce informaţii suplimentare.
Aţi creat coada de ieşire într-o bibliotecă greşită.	Folosiţi comanda Mutare obiect (Move Object - MOVOBJ) pentru a o muta în biblioteca corectă.

Puteţi acum să asignaţi ieşirea de imprimantă la o coadă de ieşire .

Asignare coadă imprimantă la o coadă de ieşire

După ce aţi creat o coadă de ieşire, puteţi asigna ieşirea imprimantă la o coadă de ieşire. Un fişier imprimantă controlează de obicei destinaţia ieşirii imprimantă. Consultaţi furnizorul aplicaţiei pentru a afla numele şi bibliotecile fişierelor de imprimantă pentru raporturi confidenţiale.

Dacă nu aveţi acces la aceste informaţii, tipăriţi raportul şi păstraţi-l în coada de ieşire. Utilizaţi opţiunea de atribut din ecranul Gestionare fişiere spool pentru a afla numele fişierului de imprimantă. Fişierul de imprimantă apare în câmpul *Fişier dispozitiv* în ecranul Gestionare atribute fişier spool.

Pentru a modifica destinaţia (coada de ieşire) a unui fişier imprimantă, folosiţi comanda Mofificare fişier imprimantă (CHGPRTF):

```
CHGPRTF FILE(nume-bibliotecă/nume-fişier-imprimantă)
        OUTQ(nume-bibliotecă/nume-coadă-ieşire)
```

Raportul se duce la noua destinaţie ori de câte ori cineva cere din nou raportul. Pentru a modifica destinaţia pentru un fişier spool care este deja în coada de ieşire, folosiţi opţiunea de modificare din ecranul Gestionare fişiere spool.

De exemplu, Sharon Jones de la Compania JKL Toy vrea să asigneze fişierul de imprimantă listă preţuri PRCLST1 cozii de ieşire PRICEQ. Ea tastează:

```
CHGPRTF FILE(CONTRACTS/PRCLST1) OUTQ(CONTRACTS/PRICEQ)
```

Pentru a asigna toate rapoartele liste de preţuri la coada de ieşire PRICEQ, Sharon ar putea să folosească un nume de fişier de imprimantă generic

```
CHGPRTF FILE(CONTRACTS/PRCLST*) OUTQ(CONTRACTS/PRICEQ)
```

Pentru a directa noile contracte la coada de imprimantă NEWCP, Sharon ar putea să modifice coada de ieşire asociată cu documentul exemplu utilizat pentru crearea de contracte.

Verificare

Cea mai bună cale de a vă verifica strategia de protecţie pentru ieşirea la imprimantă confidenţială este de a tipări. Verificaţi dacă se duce la coada de ieşire corectă. Intraţi ca un operator sistem şi vedeţi dacă puteţi vedea sau manipula fişierele din coadă.

Înainte de a securiza staţiile de lucru, asiuraţi-vă că:

- Aţi creat toate cozile de ieşire listate în formularul Securitate cozi de ieşire şi staţii de lucru folosind comanda CRTOUTQ.
- Asignaţi ieşirea imprimantă la noile cozi de ieşire folosind comanda CHGPRTF.

Securizare staţii de lucru

După ce aţi securizat ieşirea imprimantă, ar trebui să vă securizaţi staţiile de lucru. Autorizaţi staţiile de lucru în acelaşi mod în care autorizaţi alte obiecte din sistem. Folosiţi comanda EDTOBJAUT pentru a acorda utilizatorilor autorizare la staţiile de lucuru.

Utilizatorii trebuie să aibă autorizare *CHANGE pentru a semna de la o staţie de lucru. Dacă valoarea de sistem QLMTSECOFR este setată la 0, responsabilul cu securitatea sau oricine cu autorizarea *ALLOBJ poate semna de la orice staţie de lucru.

Dacă valoarea de sistem QLMTSECOFR este setată pe 1, folosiţi următoarele sugestii pentru a seta autorizarea la staţiile de lucru:

Utilizatori cărora li se permite să semneze de la staţia de lucru	Autorizare publică	Autorizare QSECOFR	Autorizare utilizator individual
Toţi utilizatorii	*CHANGE	*CHANGE	Nu este necesar
Numai utilizatorii selectaţi	*EXCLUDE	Fără autorizare	*CHANGE
Utilizatorii selectaţi şi utilizatorii cu autorizare la toate obiectele	*EXCLUDE	*CHANGE	*CHANGE
Toţi utilizatorii, cu excepţia utilizatorilor cu autorizare la toate obiectele	*CHANGE	Fără autorizare	Nu este necesar

Înainte de a restricţiona accesul la coada de mesaje operator sistem, utilizaţi comanda EDTOBJAUT pentru a securiza staţiile de lucru, bazat pe informaţiile din formularul Securitate cozi de ieşire şi staţii de lucru.

Restricţionare acces la coada de mesaje operator sistem

Vă puteţi îmbunătăţi securitatea securizând ieşirea imprimantă, securizând staţiile de lucru şi restricţionând accesul la coada de mesaje operator sistem.

Opţiunea pentru manipularea mesajelor în meniul ASSIST permite utilizatorilor să folosească o tastă funcţională pentru a afişa coada de mesaje operator sistem (QSYSOPR). Răspunsuri incorecte la mesajele operator sistem pot conduce la probleme în sistem. Utilizatorii au nevoie de autorizarea *CHANGE pentru a răspunde la mesaje şi pentru a şterge mesaje dintr-o coadă de mesaje. Numai operatorii de sistem ar trebui să aibă această autorizare. Consultaţi-vă formularul Responsabilităţi sistem pentru a vedea cine ar trebui să aibă autorizarea *CHANGE la coada de mesaje operator sistem.

Folosiţi comanda EDTOBJAUT:

1. Introduceţi EDTOBJAUT QSYSOPR *MSGQ şi apăsaţi tasta **Enter**.
2. Apăsaţi **F11** pentru a afişa informaţii detaliate despre autorizarea obiect.
3. Acordaţi autorizarea public *OBJOPR, ca în ecranul exemplu, şi apăsaţi tasta **Enter**.

```
                          Editare autorizare obiect

Obiect . . . . . :   QSYSOPR         Proprietar . . . . . :   QSYS
  Bibliotecă . . . . :     QSYS        Grup primar. . . . . :   *NONE
Tip obiect . . . . . :   *MSGQ

Introduceţi modificările la autorizările curente, apăsaţi Enter.

  Obiect securizat de listă de autorizaţii. . . . . .   *NONE

                         Obiect    ----------Obiect-----------
Utilizator Grup        Autoriz.   Opr  Mgt  Exist  Alter  Ref
*PUBLIC                 USER DEF    X
```

4. Sistemul modifică coloana *Autorizare obiect* la USER DEF (User defined).
5. Apăsaţi-o din nou **F11** pentru a afişa informaţii detaliate despre autorizare date.
6. Acordaţi autorizarea publică *ADD, ca în ecranul exemplu, şi apăsaţi tasta **Enter**.

```
                          Editare autorizare obiect

Obiect . . . . . :   QSYSOPR         Proprietar . . . . . :   QSYS
  Bibliotecă . . . . :     QSYS        Grup primar. . . . . :   *NONE
Tip obiect . . . . . :   *MSGQ

Introduceţi modificările la autorizările curente, apăsaţi Enter.

  Obiect securizat de listă de autorizaţii. . . . . .   *NONE

                         Obiect    ---------------Date---------------
Utilizator  Grup        Autoruz.   Read  Add  Update  Delete  Execute
*PUBLIC                 USER DEF          X
```

7. Utilizaţi **F6** (Adăugare utilizatori) pentru a adăuga utilizatorii care trebuie să răspundă la mesajele QSYSOPR. Acordaţi-le autorizarea *CHANGE.

Atenţie: Nu faceţi autorizarea publică *EXCLUDE. Toate joburile (şi utilizatorii) trebuie să poată adăuga mesaje la coada de mesaje QSYSOPR.

Pentru a vă asigura că aţi terminat de setat securitatea resurselor, ar trebui:

- Să utilizaţi formularele Listă autorizaţii şi Descriere biblioteci pentru a fi siguri că aţi stabilit securitatea pentru toate bibliotecile de aplicaţii.
- Să verificaţi formularul Securitate cozi de ieşire şi staţii de lucru pentru a fi siguri că aveţi staţii de lucru protejate şi că aţi creat toate cozile de ieşire speciale.
- Să restricţionaţi accesul la coada de mesaje operator sistem (QSYSOPR).
- Să vă salvaţi bibliotecile de aplicaţii conform instrucţiunilor furnizate de aplicaţii. Sistemul salvează informaţiile despre dreptul de proprietate şi autorizarea publică împreună cu aplicaţia.
- Să utilizaţi comanda Salvare date securitate (Save Security Data - SAVSECDTA) pentru a salva informaţiile de securitate pe care le-aţi creat. Consultaţi ″Salvare informaţii securitate″ pentru mai multe informaţii despre salvarea informaţiilor legate de securitate.

Acum puteţi începe să vă testaţi setările de securitate.

Testarea securităţii

Acest subiect descrie tehnicile pentru testarea securităţii pe care aţi setat-o pe sistem. În acest context, testare înseamnă să vă asiguraţi că setările funcţionează aşa cum aţi intenţionat. Subiectul ″Monitorizarea securităţii″ discută modul de evaluare a eficacităţii securităţii pe sistemul dumneavoastră.

Testaţi securitatea ori de câte ori efectuaţi modificări majore în sistem. Aceasta ar putea fi adăugarea unei noi aplicaţii, setarea securităţii resurselor pentru o aplicaţie existentă, adăugarea unui nou utilizator sau modificarea nivelului de securitate.

Revedeţi aceste subiecte pentru a învăţa despre metodele de testare şi pentru diagnosticarea problemelor când efectuaţi modificări de securitate:

- Testarea profilurilor de utilizator.
- Testarea securităţii resurselor.

Testarea profilurilor de utilizator

Pentru a începe să vă testaţi securitatea, veţi vrea să testaţi un profil de utilizator ori de câte ori setaţi un grup nou în sistem. Testaţi unul dintre profilurile individuale pe care le-aţi copiat din profilul de grup.

- Puteţi semna cu succes cu profilul de utilizator? Dacă nu puteţi semna, verificaţi istoricul jobului care a fost scris pentru încercarea nereuşită de semnare. Utilizaţi opţiunea Gestionare ieşire imprimantă din meniul ASSIST pentru a localiza istoricul jobului pentru mai multe informaţii.

  Cele mai probabile probleme sunt:

  – Unul din obiectele necesare, cum ar fi meniul iniţial, biblioteca curentă sau programul iniţial, nu există.
  – Lista de biblioteci care este specificată în descrierea de job cauzează eroarea. Fie o bibliotecă nu există, fie aţi uitat să includeţi QGPL şi QTEMP în lista de biblioteci.
  – Utilizatorul nu are autorizare la staţia de lucru.
- Când semnaţi, ecranul afişează corect meniul sau programul iniţial?
- Dacă introduceţi un meniu iniţial sau o bibliotecă curentă în ecranul de semnare, ce se întâmplă? Dacă utilizatorul este definit cu Limited Capabilities setată la YES, ar trebui să primiţi un mesaj de eroare.
- Când apăsaţi tasta Attention se afişează ecranul corect?
- Ieşirea se duce la imprimanta corectă? Dacă nu, folosiţi opţiunea Gestionare ieşire imprimantă din meniul ASSIST pentru a afla unde s-a dus. Verificaţi profilul utilizator şi descrierea de job pentru a determina de ce ieşirea s-a dus la altă imprimantă.
- Puteţi obţine o linie de comandă?
- Puteţi executa funcţiile aplicaţiei fără erori de securitate? Consultaţi ″Testarea securităţii resurselor″ pentru mai multe detalii.
- Puteţi executa operaţiile de sistem necesare, cum ar fi administrarea imprimantelor sau salvarea bibliotecilor?

Dacă sistemul v-a cerut să asignaţi o nouă parolă când aţi semnat cu un profil, setaţi parola înapoi la numele profilului de utilizator după ce aţi terminat testarea:

1. Semnaţi cu propriul profil de utilizator (cu autorizare responsabil cu securitatea)
2. Introduceţi CHGUSRPRF *nume-profil* PASSWORD(*nume-profil*) PWDEXP(*YES).

Acum că aţi testat profilurile de utilizator, puteţi testa securitatea resurselor.

Testarea securităţii resurselor

După testarea profilurilor de utilizator, ar trebui să testaţi şi securitatea resurselor. Când testaţi securitatea resurselor, vă uitaţi la următoarele:

- Utilizatori care nu au suficientă autorizare pentru a-şi face treaba.
- Utilizatori care au mai multă autorizare decât aţi intenţionat.

Testare autorizare insuficientă

Testarea funcţiilor interactive şi batch pentru a vedea dacă profilurile de utilizator au suficientă autorizare.

Testare interactivă

Pentru a vă testa securitatea resurselor pentru o aplicaţie, poate fi nevoie să semnaţi de mai multe ori cu diverse profiluri de utilizator. Obiectivul este de a testa eşantioane de utilizatori pentru a vă asigura că autorizarea pe care aţi asignat-o este suficientă.

- Testaţi funcţiile care necesită niveluri de autorizare diferită: vizualizare, modificare şi ştergere.
- Testaţi programele, nu doar meniurile. Selectarea unei opţiuni dintr-un meniu poate să nu fie suficientă pentru a testa autorizarea. Câteodată sistemul nu accesează un fişier până în momentul în care încercaţi efectiv să efectuaţi o operaţie, cum ar fi ştergerea unei înregistrări. Verificarea autorizării se face atunci când sistemul deschide un fişier. Proiectarea aplicaţiei determină când sistemul deschide un fişier.
- Înregistraţi erorile de securitate şi rezolvaţi-le. Dacă apare o eroare de autorizare, ar trebui să vedeţi un mesaj pe ecran care să vă spună că nu aveţi autorizare suficientă pentru operaţie şi ce obiect încercaţi să utilizaţi.

Testare batch

- Rulaţi eşantioane de joburi batch din aplicaţie utilizând profilurile utilizatorilor care vor lansa joburile.
- Testaţi joburi batch care necesită niveluri de autorizare diferită, cum ar fi: tipărire informaţii, modificare informaţii, sau curăţirea fişierelor la sfârşit de lună.
- Verificaţi coada de mesaje QSYSOPR şi istoricul QHST pentru erori de securitate. Folosiţi comanda DSPLOG pentru a vedea istoricul QHST. Mesajele de securitate sunt în aceste intervale: CPF2200, CPI2200, CPC2200, CPD2200, CPF4A00, CPI4A00, CPC4A00 şi CPD4A00.

  Puteţi de asemenea utiliza funcţia de auditare securitate pentru a înregistra eşecurile de securitate sau alte evenimente legate de securitate.

Testare autorizare excesivă

Dacă utilizaţi securitatea resurselor pentru a vă proteja informaţiile confidenţiale, testaţi eşantioane de profiluri utilizator pentru a vă asigura că securitatea funcţionează. Semnaţi cu profilul unui utilizator care nu ar trebui să acceseze fişierul confidenţial.

- Puteţi obţine un meniu care permite accesul la fişier?
- Ce se întâmplă când selectaţi o opţiune meniu care utilizează acest fişer?
- Puteţi obţine o linie de comandă?
- Puteţi rula o comandă pentru a lista fişierul, cum ar fi CPYF FROMFILE(*nume-fişier*) TOFILE(QSYSPRT)?
- Puteţi utiliza o interogare pentru a vă uita la fişier?

Rezultatele testărilor vă pot indica dacă este necesar să vă modificaţi informaţiile de securitate.

Modificarea informaţiilor de securitate

Acum că aţi planificat securitatea sistemului, trebuie să vă asiguraţi că planul dumneavoastră ramâne eficace pe măsură ce afacerea se modifică.

Acest subiect subliniază simplicitatea ca un obiectiv esenţial în proiectarea securităţii. Aţi proiectat grupuri de utilizatori ca modele pentru utilizatori individuali. Aţi încercat să utilizaţi autorizarea publică, listele de autorizare şi autorizarea la nivel bibliotecă în loc de autorizări individuale specifice. Profitaţi de această abordare când gestionaţi securitatea:

- Când adăugaţi un nou grup utilizatori sau o nouă aplicaţie, utilizaţi tehnicile pe care le-aţi folosit la planificarea securităţii.
- Când trebuie să faceţi modificări de securitate, încercaţi să abordaţi problema la modul general, mai degrabă decât să creaţi o excepţie pentru a rezolva o problemă specifică.

Subiectul Comenzi de securitate descrie ce comenzi să utilizaţi pentru a afişa, modifica sau şterge informaţii de securitate.

Consultaţi aceste subiecte despre abordarea diferitelor tipuri de modificări:

- Adăugarea unui nou utilizator în sistem.
- Crearea unui nou grup de utilizatori.
- Modificarea unui nou grup de utilizatori.
- Adăugarea unei noi aplicaţii.
- Adăugarea unei noi staţii de lucru.
- Modificarea responsabilităţilor unui utilizator.
- Înlăturarea unui utilizator din sistem.

Comenzi de securitate

Tabelul de mai jos arată ce comenzi folosiţi pentru a lucra cu obiectele de securitate din sistem. Puteţi utiliza comezile următoare pentru a executa aceste operaţii:

- Vizualizare şi listare informaţii de securitate.
- Modificare informaţii de securitate.
- Şterge informaţii de securitate.

Tabela 63. Comenzi de securitate

Obiect de securitate	Cum se vizualizează	Cum se modifică	Cum se şterge
Valoare sistem	WRKSYSVAL DSPSYSVAL	WRKSYSVAL CHGSYSVAL	Nu poate fi şters
Descriere de job	WRKJOBD DSPJOBD	WRKJOBD CHGJOBD	DLTJOBD
Profil de grup	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF	DLTUSRPRF[1],[2]
Profil utilizator	WRKUSRPRF DSPUSRPRF DSPAUTUSR	WRKUSRPRF CHGUSRPRF CHGUSRAUD	DLTUSRPRF[1]
Autorizări obiect	DSPAUT DSPOBJAUT DSPUSRPRF TYPE(*OBJAUT)	CHGAUT EDTOBJAUT GRTOBJAUT WRKAUT	EDTOBJAUT RVKOBJAUT WRKAUT
Drept de proprietate obiect	WRKOBJOWN DSPOBJAUT DSPUSRPRF TYPE(*OBJOWN)	CHGOBJOWN CHGOWN	CHGOBJOWN CHGOWN vă permite să anulaţi drepturile proprietarului anterior.
Grup primar	DSPOBJAUT WRKOBJPGP DSPUSRPRF TYPE(*OBJPGP)	CHGOBJPGP CHGPGP	CHGOBJPGP CHGPGP setează grupul primar la *NONE
Auditare obiect	DSPOBJD	CHGOBJAUD CHGAUD	CHGOBJAUD (setat la *NONE) CHGAUD
Listă de autorizaţii	DSPAUTL DSPAUTLOBJ	EDTAUTL (autorizarea utilizatorului la o listă) EDTOBJAUT (obiect securizat de listă) ADDAUTLE CHGAUTLE GRTOBJAUT	DLTAUTL (toată lista)[3] RMVAUTLE (înlătură autorizarea utilizatorului la listă) EDTOBJAUT (obiect securizat de listă) RVKOBJAUT

Tabela 63. Comenzi de securitate (continuare)

Obiect de securitate	Cum se vizualizează	Cum se modifică	Cum se şterge

1. IBM recomandă folosirea opţiunii de înlăturare din ecranul Gestionare înrolare utilizator pentru a şterge un profil. Utilizând această opţiune, puteţi şterge orice obiect deţinut de profil sau să-l reasignaţi la un nou proprietar. Anumiţi parametri din comanda DLTUSRPRF vă permit să ştergeţi toate obiectele deţinute de utilizator sau să le asignaţi unui nou proprietar. Nu puteţi şterge un profil decât dacă ştergeţi sau reasignaţi obiectele aflate în proprietate. De asemenea, nu puteţi şterge un profil care este grup primar pentru un obiect.
2. Nu puteţi şterge un profil de grup care are membrii. Folosiţi opţiunea *GRPMBR a comezii DSPUSRPRF pentru a lista membrii grupului. Modificaţi câmpul *profil de grup* în fiecare profil de grup individual înainte de a ştege profilul de grup.
3. Nu puteţi şterge o listă de autorizaţie care este utilizată pentru a securiza obiecte. Utilizaţi comanda DSPAUTLOBJ pentru a lista obiectele securizate de listă. Modificaţi autorizarea oricărui obiect securizat de listă folosind comanda EDTOBJAUT.

Vizualizare şi listare informaţii de securitate

Puteţi lista informaţiile de securitate folosind o comandă de afişare (DSP) cu opţiunea de tipărire (*PRINT). De exemplu, pentru a afişa o listă de autorizaţii numită MYLIST, introduceţi DSPAUTL MYLIST *PRINT.

Unele comeni de afişare oferă opţiuni pentru diferite tipuri de listare. De exemplu, când creaţi profiluri utilizator individuale, adăugaţi opţiunea *GRPMBR la comanda DSPUSRPRF pentru a lista toţi membrii profilului de grup. Folosiţi funcţia de prompt (**F4**) şi informaţiile online pentru a afla ce tipuri de listare sunt disponibile pentru obiectele de securitate.

Puteţi utiliza comenzile de afişare pentru a vedea informaţiile de securitate de la staţia dumneavoastră de lucru. Puteţi de asemena utiliza comenzile Work with... (WRK), care oferă mai multe funcţii. Comenzile Work with... oferă un ecran tip listă. Puteţi utiliza acest ecran pentru a modifica, şterge şi vizualiza informaţii.

Puteţi de asemenea să utilizaţi comenzi de securitate pentru a lista sau vizualiza informaţii folosind nume generice. Dacă introduceţi WRKUSRPRF DPT*, ecranul Gestionare înrolare utilizator (Work with User Enrollment) sau Gestionare profil utilizator (Work with User Profile) arată numai profilurile care încep cu caracterele *DPT*. Folosiţi informaţia online pentru o comandă pentru a afla ce parametrii permit nume generice.

Modificarea informaţiilor de securitate

Puteţi modifica informaţiile de securitate interactiv utilizând o comandă Work with... (WRK) sau Edit... (EDT). Puteţi vizualiza informaţii, să le modificaţi şi să vedeţi din nou informaţiile după modificare.

Puteţi de asemenea să modificaţi informaţiile de securitate fără a le vizualza înainte şi după modificare, folosind o comandă Change... (CHG) sau Grant... (GRT). Această metodă este folositoare în special când se fac modificări pe mai multe obiecte simultan. De exemplu, aţi utilizat comanda GRTOBJAUT pentru a seta autorizarea publică pentru toate obiectele dintr-o bibliotecă (vedeţi “Setarea autorizării publice pentru toate obiectele dintr-o bibliotecă” la pagina 94).

Ştergere informaţii de securitate

Puteţi şterge sau înlătura anumite tipuri de informaţii de securitate interactiv folosind comenzile Work with... (WRK) sau Edit... (EDT). Puteţi de asemenea utiliza comenzile Delete... (DLT), Remove... (RMV) şi Revoke... (RVK) pentru a şterge informaţiile de securitate. Adesea, trebuie să îndepliniţi anumite condiţii înainte ca sistemul să vă permită ştergerea informaţiilor de securitate. Notele de la Comenzi de securitate descriu unele din aceste condiţii.

Adăugarea unui nou utilizator în sistem

Când adăugaţi un utilizator nou în sistem, folosiţi următoarea procedură:

1. Asignaţi persoana unui grup de utilizatori. Folosiţi formularul Descriere grup utilizatori pentru referinţe.
2. Decideţi dacă noul utilizator are nevoie să efectueze funcţii sistem. Dacă da, adăugaţi această informaţie în formularul Responsabilităţi sistem .
3. Adăugaţi persoana în formularul Profiluri utilizator individuale.

4. Revedeţi formularul Responsabilităţi sistem şi formularul Descriere grup de utilizatori pentru a determina dacă noul utilizator are nevoie de valori diferite de cele ale grupului.
5. Creaţi un profil utilizator copiind profilul de grup sau profilul unui membru al grupului. Asiguraţi-vă că parola nu expiră. (vedeţi ″Copiere profil de grup.″)
6. Daţi noului utilizator o copie a politicii de securitate.

Pentru a învăţa cum se creează un grup utilizatori, consultaţi ″Creare grup utilizatori nou.″

Creare grup utilizatori nou

Poate fi nevoie să creaţi noi grupuri de utilizatori pentru următoarele motive:

- Noi departamente au nevoie să utilizeze sistemul.
- Aţi descoperit că trebuie să faceţi grupuri utilizatori pentru a corespunde nevoilor de securizare a resurselor.
- Compania a reorganizat unele departamente.

Pentru a crea un nou grup de utilizatori, faceţi următoarele:

1. Completaţi un Formular descriere grup utilizatori urmând instrucţiunile din ″Planificare grupuri utilizatori.″
2. Adăugare grup utilizatori la diagrama aplicaţiilor, bibliotecilor şi a grupurilor de utilizatori.
3. Evaluaţi dacă vreun membru al grupului trebuie să efectueze funcţii sistem. Actualizaţi formularul Responsabilităţi sistem. (Vedeţi ″Determinarea persoanelor responsabile pentru funcţiile sistemului.″)
4. Utilizaţi informaţia din formularul Descriere grup utilizatori şi din Responsabilităţi sistem pentru a completa formularul Profiluri individuale utilizatori.
5. Creaţi o bibliotecă de grup.
6. Creaţi o desriere de job pentru grup.
7. Creaţi un profil de grup.

   Notă: Consultaţi ″Setare grupuri utilizatori″ pentru instrucţiuni în efectuarea paşilor cinci, şase şi şapte.
8. Creaţi profiluri utilizator individuale pentru membrii grupului. (Consultaţi ″Setare utilizatori individuali.″)
9. Evaluaţi formularul Descriere biblioteci pentru toate aplicaţiile care sunt necesare grupului. Efectuaţi toţi paşii necesari pentru a da grupului acces la obiectele aplicaţiei utilizând tehnicile descrise în ″ Setare securitate resurse.″
10. Daţi tuturor membrilor grupului o copie a memo-ului de securitate.

Pentru a învăţa cum se modifică un grup utilizatori, consultaţi ″Modificarea unui grup de utilizatori.″

Modificarea unui grup de utilizatori

Va trebui să trataţi diferitele tipuri de modificări la caracteristicile unui grup în moduri diferite. În continuare sunt câteva exemple de modificări şi modul lor de abordare:

Modificarea autorizării unui grup

Puteţi descoperi că grupul are nevoie de autorizări la obiecte pe care nu le-aţi anticipat în planificarea iniţială. Faceţi următoarele:

1. Utilizaţi comanda Editare autorizare obiect (Edit Object Authority - EDTOBJAUT) pentru a acorda grupului accesul corect la obiecte sau la o listă de autorizare potrivită. “Setare autorizări specifice” la pagina 98 arată un exemplu pentru asta. Fiecare membru al grupului primeşte autorizarea la obiect când acordaţi autorizare grupului.
2. Dacă daţi gruplui autorizare la o resursă confidenţială, poate doriţi să verificaţi membrii grupului. Utilizaţi comanda Afişare profil utilizator (DSPUSRPRF *nume-profil-grup* *GRPMBR) pentru a obţine membrii grupului.

Modificarea personalizării unui grup

Poate fi nevoie să modificaţi setarea de mediu utilizator pentru membrii unui grup. De exemplu, dacă un departament primeşte propria imprimantă, vreţi ca noua imprimantă să fie cea implicită pentru grupul de utilizatori ai acelui departament. Sau, când pe sistem se instalează o nouă aplicaţie, membrii unui grup de utilizatori pot dori un nou meniu iniţial când semnează.

Profilul de grup oferă un model pe care îl puteţi copia pentru a crea profiluri individuale pentru membrii grupului. Personalizarea valorilor în profilul de grup nu afectează totuşi profilurile de utilizator individuale după ce le creaţi. De exemplu, modificara unui câmp, cum ar fi *Dispozitiv imprimantă* din profilul de grup, nu are efect asupra membrilor grupului. Trebuie să modificaţi câmpul *Dispozitiv imprimantă* în fiecare profil utilizator în parte.

Puteţi utiliza ecranul Gestionare profiluri utilizator pentru a modifica un parametru pentru mai mulţi utilizatori simultan. Exemplul arată modificarea cozii de ieşire pentru toţi membrii unui grup:

1. Tastaţi WRKUSRPRF *ALL şi apăsaţi tasta **Enter**.
2. Dacă vedeţi ecranul Gestionare înrolare utilizatori, folosiţi **F21** (Selectare nivel asistenţă) pentru a ajunge la ecranul Gestionare profiluri utilizator.

```
                         Gestionare profiluri utilizator

Introduceţi opţiuni, apăsaţi Enter.
  1=Creare   2=Modif.   3=Copiere 4=Ştergere 5=Afişare
  12=Gestionare obiecte după proprietar

          Utilizator
Opt       Profil        Text

                HARRISOK         Harrison, Keith
2               HOGANR           Hogan, Richard
                JONESS           Jones, Sharon
2               WILLISR          Willis, Rose

   ⋮
                                                                    Cont...
Parametri pentru opţiunile 1, 2, 3, 4 şi 5 sau comandă
===> PRTDEV(PRT02)
F3=Ieşire F5=Reîmprospătare F12=Anulare F16=Repetare poziţionare  F17=Poziţionare
F21=Selectare nivel asistenţă         F24=Taste suplimentare
```

3. Tastaţi **2** (Modificare) lângă fiecare profil pe care vreţi să-l modificaţi.
4. Pe lina de parametrii din partea de jos a ecranului, introduceţi numele parametrului şi noua valoare. Dacă nu ştiţi numele parametrului, apăsaţi **F4** (Prompt).
5. Apăsaţi tasta **Enter**. Primiţi un mesaj de confirmare pentru fiecare profil care s-a modificat.

   Cu toate că modificarea unui câmp în profilul de grup nu are efect asupra membrilor grupului, poate fi de ajutor în viitor. Profilul de grup oferă un model pentru când veţi vrea să adăugaţi membrii la grup mai târziu. Este de asemenea o înregistrare a valorilor de câmp standard pentru grup.

Acordarea grupului acces la o nouă aplicaţie

Când un grup de utilizatori are nevoie de acces la o nouă aplicaţie, trebuie să analizaţi informaţia despre grup şi despre aplicaţie. În continuare se sugerează o metodă:

1. Uitaţi-vă la formularul Descriere aplicaţie pentru noua aplicaţie şi diagrama aplicaţiilor, bibliotecilor şi a grupurilor de utilizatori pentru a vedea ce biblioteci foloseşte aplicaţia. Adăugaţi acele biblioteci la formularul Descriere grupuri utilizator.
2. Actualizaţi diagrama aplicaţiilor, bibliotecilor şi a grupurilor de utilizatori pentru a reflecta noua relaţie dintre grupul de utilizatori şi aplicaţie.
3. Dacă lista de biblioteci iniţială a grupului ar trebui să includă bibliotecile, modificaţi descrierea de job a grupului cu comanda Modificare descriere job CHGJOBD). Consultaţi “Crearea unei descrieri de job” la pagina 81 dacă aveţi nevoie de ajutor pentru lucrul cu descrierile de job.

Notă: Când adăugaţi biblioteci la lista de biblioteci iniţială într-o descriere de job, nu trebuie să modificaţi profilurile de utilizator care utilizează acea descriere de job. La următoarea semnare, lista de biblioteci iniţială adaugă automat acele biblioteci.

4. Evaluaţi dacă trebuie să modificaţi programul iniţial sau meniul iniţial pentru grup pentru a oferi acces la noua aplicaţie. Trebuie să faceţi modificări individuale la meniul iniţial sau programul iniţial pentru fiecare profil utilizator cu comanda CHGUSRPRF.
5. Revedeţi formularul Descriere bibliotecă pentru toate bibliotecile care sunt utilizate de aplicaţie. Determinaţi dacă accesul public pentru biblioteci este suficient pentru nevoile grupului. Dacă nu, poate fi necesar să acordaţi grupului autorizare la bibliotecă, la anumite obiecte sau la liste de autorizare. Pentru asta utilizaţi comenzile Editare autorizare obiect (Edit Object Authority - EDTOBJAUT) şi Editare listă autorizare (Edit Authorization List - EDTAUTL). (Vedeţi ″Setare securitate resurse″ dacă aveţi nevoie de mai multe informaţii.)

Pentru a adăuga aplicaţii în sistem, consultaţi ″Adăugare aplicaţie nouă.″

Adăugarea unei noi aplicaţii

Ar trebui să planificaţi securitatea unei aplicaţii noi la fel de atent cum aţi planificat aplicaţiile originale. Urmaţi aceleaşi proceduri:

1. Pregătiţi un formular Descriere aplicaţie şi formulare Descriere bibliotecă petru aplicaţie.
2. Actualizare diagrama aplicaţiilor, bibliotecilor şi a grupurilor de utilizatori.
3. Urmaţi procedurile din ″Planificare securitate resurse″ pentru a decide cum să securizaţi noua aplicaţie.
4. Pregătiţi un formular Instalare aplicaţie folosind metoda descrisă în ″Planificare instalare aplicaţie.″
5. Evaluaţi dacă vreo ieşire imprimantă a aplicaţiei este confidenţială şi are nevoie de protecţie. Actualizaţi formularul Securitate cozi ieşire şi staţii de lucru, dacă este necesar.
6. Urmaţi paşii descrişi în ″Setare drept de proprietate şi autorizare publică″ şi ″Setare securitate resurse ″ pentru a instala şi securiza aplicaţia.

Pentru a adăuga o staţie de lucru în sistem, consultaţi Adăugarea unei noi staţii de lucru.″

Adăugarea unei noi staţii de lucru

Când adăugaţi o nouă staţie de lucru în sistem, luaţi în considerare cerinţele de securitate:

1. Locaţia fizică a unei noi staţii de lucru introduce vreun risc de securitate? (Vedeţi ″Planificare securitate fizică″ pentru a vă reîmprospăta memoria.)
2. Dacă staţia de lucru expune securitatea, actualizaţi-vă formularul Securiate cozi de ieşire şi staţii de lucru.
3. În mod normal, ar trebui să creaţi noile staţii de lucru cu autorizarea *CHANGE. Dacă acest lucru nu corespunde cu cerinţele dumneavoastră de securitate pentru staţia de lucru, utilizaţi comanda EDTOBJAUT pentru a specifica o altă autorizare.

Pentru a modifica responsabilitatea unui utilizator în sistem, consultaţi ″Modificarea responsabilităţilor unui utilizator.″

Modificarea responsabilităţilor unui utilizator

Când un nou utilizator sistem primeşte alt post de lucru sau un nou set de responsabilităţi în companie, trebuie să evaluaţi cum afectează acest lucru profilul utilizator.

1. Este necesar ca utilizatorul să aparţină altui grup de utilizatori? Puteţi folosi comanda CHGUSRPRF pentu a modifica grupul utilizatori.
2. Este necesar să modificaţi vreo valoare personalizată în profil, cum ar fi imprimanta sau meniul iniţial? Puteţi utiliza tot comanda CHGUSRPRF pentru a le modifica.
3. Sunt autorizările aplicaţie ale noului grup utilizatori suficiente pentru această persoană?
   - Folosiţi comanda Afişare profil utilizator (Display User Profile - DSPUSRPRF) pentru a vedea autorizările pentru profilurile de grup vechi şi noi.
   - De asemenea, uitaţi-vă la autorizările pentru profiluri individuale de utilizatori.

- Efectuaţi toate modificările necesare folsind comanda EDTOBJAUT.

4. Utilizatorul are vreun obiect în proprietate? Ar trebui să modificaţi dreptul de proprietate pentru aceste obiecte? Folosiţi comanda Gestionare obiecte după proprietar (Work with Objects by Owner - WRKOBJOWN).
5. Utilizatorul efectuează funcţii sistem? Utilizatorul trebuie să efectueze funcţii sistem pentru noul post de lucru? Actualizaţi formularul Responsabilităţi sistem şi modificaţi profilul utilizator dacă este necesar.

Pentru a învăţa cum să înlăturaţi un utilizator din sistem, consultaţi Înlăturarea unui utilizator din sistem.″

Înlăturarea unui utilizator din sistem

Dacă cineva părăseşte compania, ar trebui să înlăturaţi profilul utilizator din sistem imediat. Înainte de a putea şterge un profil utilizator, trebuie fie să ştergeţi, fie să transferaţi dreptul de proprietate asupra tuturor obiectelor al căror proprietar este. Penru asta puteţi folosi comanda WRKOBJOWN sau utiliza opţiunea **4** (Înlăturare) din ecranul Gestionare înrolare utilizator (Work with User Enrollment).

Când selectaţi opţiunea **4** (Înlăturare) pentru un profil din ecranul Gestionare înrolare utilizator, vedeţi ecrane suplimentare care vă permit să manipulaţi orice obiect aflat în proprietatea utilizatorului. Puteţi alege să daţi toate obiectele unui nou proprietar sau să trataţi obiectele individual:

```
                              Înlăturare utilizator

Utilizator . . . . . :   HOGANR
Descriere utilizator . . . :   Departament Vânzări şi Marketing

Pentru a înlătura acest utilizator, introduceţi o opţiune mai jos, apoi apăsaţi Enter.

    1. Daţi toate obiectele aflate în proprietatea acestui utilizator unui nou utilizator
    2. Ştergeţi sau modificaţi proprietarul anumitor obiecte deţinute de acest utilizator
```

Dacă alegeţi să trataţi obiectele individual (opţiunea **2**), ecranul afişează o listă cu toate obiectele care se află în proprietatea utilizatorului:

```
                              Înlăturare utilizator

Utilizator . . . . . :   HOGANR
Descriere utilizator . . . :   Departament Vânzări şi Marketing

Proprietar nou . . . . . .                   Nume, F4 pentru listă

Pentru a înlătura acest utilizator, ştergeţi sau modificaţi proprietarul pentru toate obiectele.
Introduceţi opţiuni, apăsaţi Enter.
  2=Modif. la proprietar nou 4=Ştergere   5=Afişare detalii

Opt  Obiect        Bibliotecă    Descriere
 4   HOGANR        QUSRSYS       Hogan, Richard message queue
 4   QUERY1        DPTWH         Inventory Query
```

Dacă alegeţi să ştergeţi obiectele, puteţi vedea ecranul Confirmare ştergere. Odată ce sistemul şterge obiectele, puteţi înlătura profilul utilizator. Puteţi apoi vedea ecranul Gestionare înrolare utilizator (Work with User Enrollment) din nou cu un mesaj care vă spune că sistemul a înlăturat utilizatorul.

Salvarea informaţiilor de securitate

Acest subiect prezintă o privire generală asupra modului de salvare şi recuperare a informaţiilor de securitate. Când vă planificaţi salvarea şi recuperarea sistemului, trebuie să consideraţi atât securitatea informaţiilor, cât şi înseşi informaţiile. Consultaţi subiectul din Centru de informaţii Salvare, recuperare şi disponibilitate pentru ajutor în proiectarea unui plan complet de salvare şi recuperare.

Subiectele următoare descriu cum să salvaţi şi să restauraţi informaţiile de securitate pe care le creaţi când setaţi securitatea:

- Salvarea valorilor de sistem.
- Salvarea profilurileor de grup şi de utilizatori..
- Salvarea descrierilor de job.
- Salvarea informaţiilor de securitate resurse.
- Folosirea profilului proprietar implicit (QDFTOWN).
- Recuperarea dintr-o listă de autorizaţii deteriorată.

Salvarea valorilor de sistem

Valorile de sistem sunt memorate în biblioteca de sistem QSYS. Salvaţi biblioteca QSYS când faceţi următoarele:

- Folosiţi comanda Salvare sistem (SAVSYS).
- Folosiţi opţiunea de a salva întregul sistem din meniul Save (Salvare).
- Folosiţi opţiunea de a salva informaţiile sistem din meniul Save (Salvare).
- Folosiţi opţiunea de a salva tot sistemul din meniul Run Backup (RUNBCKUP).

Dacă trebuie să vă recuperaţi tot sistemul, restauraţi automat valorile sistem când vă restauraţi sistemul de operare.

Consultaţi apoi ″Salvarea profilurilor de grup şi utilizator″.

Salvarea profilurileor de grup şi de utilizatori.

Profilurile de grup şi utilizator sunt memorate în biblioteca QSYS. Le salvaţi când utilizaţi comanda Salvare sistem (SAVSYS) sau selectaţi opţiunea de meniu de salvare tot sistemul.

Puteţi de asemenea să salvaţi profilurile de grup şi de utilizator folosind comanda Salvare date securitate (SAVSECDTA).

Restauraţi profiluri utilizator folosind comanda Restaurare profil utilizator (RSTUSRPRF). Ordinea normală este:

1. Restauraţi sistemul de operare, ceea ce restaurează biblioteca QSYS.
2. Restauraţi profilurile de utilizator.
3. Restauraţi bibliotecile rămase.
4. Restauraţi autorizarea la obiecte folosind comanda Restaurare autorizare (RSTAUT).

Consultaţi apoi ″Salvare descrieri de joburi″.

Salvarea descrierilor de job

Când creaţi o descriere de job, specificaţi o bibliotecă unde ar trebui să se afle. IBM recomandă crearea descrierilor de job în biblioteca QGPL.

Puteţi salva descrierile de job salvând bibliotecile în care se află. Utilizaţi pentru asta comanda Salvare bibliotecă (SAVLIB). Puteţi de asemenea salva o descriere de job folosind comanda Salvare obiect (SAVOBJ).

Puteţi restaura conţinutul unei biblioteci folosind comanda Restaurare bibliotecă (RSTLIB). Puteţi restaura o descriere de job individuală folosind comanda Restaurare obiect (RSTOBJ).

Consultaţi apoi ″Salvarea informaţiilor de securitate resurse″.

Salvarea informaţiilor de securitate resurse

Securitatea resurselor, care defineşte modul în care utilizatorii pot lucra cu obiectele, constă din diverse tipuri de informaţii stocate în mai multe locuri:

Tabela 64. Salvarea şi restaurarea informaţiilor de securitate resurse

Tip de informaţii	Unde sunt stocate	Cum sunt salvate	Cum sunt restaurate
Autorizare publică	Cu obiectul	comanda SAVxxx [1]	comanda RSTxxx [2]
Valoare auditare obiect	Cu obiectul	comanda SAVxxx [1]	comanda RSTxxx [2]
Drept de proprietate obiect	Cu obiectul	comanda SAVxxx [1]	comanda RSTxxx [2]
Grup primar	Cu obiectul	comanda SAVxxx [1]	comanda RSTxxx [2]
Listă de autorizaţii	Biblioteca QSYS	SAVSYS sau SAVSECDTA	RSTUSRPRF USRPRF(*ALL)
Legătură între obiect şi listă de autorizaţii	Cu obiectul	comanda SAVxxx [1]	comanda RSTxxx [2]
Autorizare privată	Cu profilul utilizator	SAVSYS sau SAVSECDTA	RSTAUT

1. Puteţi salva cele mai multe tipuri de obiecte folosind comezile SAVOBJ sau SAVLIB. Unele tipuri de obiecte, cum ar fi configuraţiile, au comenzi speciale de salvare.
2. Puteţi restaura cele mai multe tipuri de obiecte folosind comenzile RSTOBJ sau RSTLIB. Unele tipuri de obiecte, cum ar fi configuraţiile, au comenzi speciale de restaurare.

Când trebuie să recuperaţi o aplicaţie sau tot sistemul, trebuie să vă planificaţi paşii cu grijă, inclusiv recuperarea autorizării la obiecte. În continuare sunt paşii de bază necesari pentru a recupera informaţiile de securitate resurse pentru o aplicaţie:

1. Dacă este necesar, restauraţi profilurile de utilizator, incluzând profilurile care sunt proprietarele aplicaţiei. Puteţi restaura anumite profiluri sau toate profilurile cu comanda RSTUSRPRF.
2. Restauraţi toate listele de autorizaţii folosite de aplicaţii. Restauraţi listele de autorizaţii când folosiţi RSTUSRPRF USRPRF(*ALL).

   Notă: Aceasta restaureaă toate valorile profilurilor de utilizator, inclusiv parolele, de pe mediul de stocare de rezervă.
3. Restauraţi bibliotecile de aplicaţie folosind comezile RSTLIB sau RSTOBJ. Aceasta recuperează dreptul de proprietate, autorizarea publică şi legătura dintre obiecte şi listele de autorizare.
4. Restauraţi autorizarea privată la obiecte folosind comanda RSTAUT. Comanda RSTAUT restaurează de asemenea autorizările utilizatorilor la listele de autorizaţii. Puteţi restaura autorizarea pentru anumiţi utilizatori sau pentru toţi utilizatorii.

Consultaţi ″Utilizare profil proprietar implicit (QDFTOWN)″ pentru informaţii despre restaurarea unui obiect şi a profilului proprietar care nu este pe sistem.

Folosirea profilului proprietar implicit (QDFTOWN)

Dacă restauraţi un obiect şi profilul proprietar nu este pe sistem, sistemul transferă dreptul de propietate al obiectului la un profil implicit numit QDFTOWN. Odată ce aţi recuperat profilul proprietarului sau l-aţi creat din nou puteţi transfera dreptul de proprietate înapoi folosind comanda Gestionare Obiecte după Utilizator(WRKOBJOWN).

Pentru informaţii despre recuperarea listei de autorizări vedeţiRecuperarea din dezastru a listei de autorizări.″

Recuperarea din dezastru a listei de autorizări

Când o lista de autorizări securizează un obiect şi se deteriorează, doar utilizatorii care au autorizarea specială (*ALLOBJ) au acces la obiect.

Recuperarea din dezastru a unei liste de autorizări necesită doi paşi:

1. Recuperarea utilizatorilor şi a autorizărilor lor în lista de autorizări.
2. Recuperarea asocierii listei de autorizări cu obiectele.

Un utilizator cu autorizarea specială *ALLOBJ poate realiza aceşti paşi.

Pasul 1: Recuperarea listei de autorizări

Dacă ştiţi autorizarea utilizatorului la lista de autorizări, ştergeţi lista de autorizări, creaţi-o din nou şi adăugaţi utilizatori în ea.

Dacă nu ştiţi toate autorizările utilizator la lista de autorizări, reastauraţi-o din ultima bandă cu SAVSYS sau SAVSECDTA folosind următorii paşi:

1. Ştergeţi lista de autorizări deteriorată:
   ```
   DLTAUTL AUTL(nume-listă-autorizări)
   ```
2. Restauraţi lista de autorizări:
   ```
   RSTUSRPRF USRPRF(*ALL)
   ```
3. Adăugaţi utilizatori la listă folosind comanda Restaurare Autorizări (RSTAUT).

Pasul 2: Recuperarea asocierii obiectelor cu lista de autorizări

Dacă aţi restaurat lista de autorizări sau aţi creat-o din nou, aveţi nevoie să stabiliţi o legătură între listă şi obiectele securizate de listă :

1. Folosiţi comanda Pretindere spaţiu de stocare(RCLSTG). RCLSTG alocă la o lista implicită numită QRCLAUTL, obiecte ce sunt securizate de lista de autorizări pierdută sau deteriorată.
2. Listaţi obiectele ce sunt securizate de lista de autorizări QRCLAUTL:
   ```
   DSPAUTLOBJ AUTL(QRCLAUTL)
   ```
3. Folosiţi comanda GRTOBJAUT pentru a securiza obiectele cu lista de autorizare corectă. De exemplu, pentru a securiza fişierul ARWRK01 în biblioteca CUSTLIB cu lista de autorizare ARLST01, tastaţi
   ```
   GRTOBJAUT OBJ(CUSTLIB/ARWRK01) OBJTYPE(*FILE) +
             AUTL(ARLST01)
   ```

Monitorizarea securităţii

Acest subiect oferă sugestii de bază pentru monitorizarea eficacităţii măsurilor de securitate de pe sistemul dumneavoastră.

Monitorizarea regulată a securităţii are două scopuri principale:

- Să vă asiguraţi că protejaţi corespunzător resursele companiei.
- Să detectaţi încercările neautorizate de a accesa sistemul şi informaţiile companiei.

Revedeţi declaraţia de politică de securitate şi memo de securitate către utilizatori pe măsură ce decideţi ce operaţii de monitorizare trebuie să efectuaţi în mod regulat.

Consultaţi subiectele următoare pentru mai multe informaţii despre monitorizarea securităţii:

- Listă de verificare pentru monitorizarea securităţii.
- Auditarea securităţii.

Listă de verificare pentru monitorizarea securităţii

În continuare sunt liste de verificare pentru a revedea diferite aspecte ale securităţii pe sistemul dumneavoastră. Folosiţi-le pentru a vă dezvolta planul.

Monitorizarea resurselor fizice

- Protejaţi mediul de stocare de rezervă de deteriorare şi furt.
- Restricţionaţi accesul la staţiile de lucru din zonele publice. Folosiţi comanda DSPOBJAUT pentru a vedea cine are autorizare *CHANGE la staţiile de lucru.

Monitorizarea valorilor de sistem

- Verificaţi că setările corespund formularului Selecţie valori sistem. Folosiţi comanda Tipărire atribute securitate sistem (Print System Security Attributes - PRTSYSSECA).
- Revedeţi deciziile despre valorile sistem, în special când instalaţi aplicaţii noi.

Monitorizare profiluri grup

- Verificaţi că profilurile de grup nu au nici o parolă. Folosiţi comanda DSPAUTUSR pentru a verifica faptul că toate profilurile de grup au parola *NONE.
- Verificaţi că persoanele corecte sunt membrii grupului. Folosiţi comanda DSPUSRPRF cu opţiunea *GRPMBR pentru a lista membrii unui grup.
- Verificaţi autorizările speciale pentru fiecare profil de grup. Folosiţi comanda DSPUSRPRF. Dacă sunteţi la nivel de securitate 30, 40 sau 50, profilurile de grup ar trebui să nu aibă autorizarea *ALLOBJ.

Monitorizarea profilurilelor utilizator

- Verificaţi că profilurile de utilizator de pe sistem aparţin uneia din categoriile:
  - Profiluri utilizator pentru angajaţii actuali
  - Profiluri de grup
  - Profiluri pentru proprietarii de aplicaţie
  - Profiluri furnizate de IBM (încep cu Q)
- Înlăturaţi profilul utilizator corespunzător unui utilizator care părăseşte compania. Folosiţi comanda Change Expiration Schedule Entry (CHGEXPSCDE) pentru a şterge automat sau pentru a dezactiva profilul imediat ce utilizatorul pleacă.
- Uitaţi-vă după profiluri inactive şi ştergeţi-le. Folosiţi comanda Analiză ativitate profiluri (Analyze Profile Activity - ANZPRFACT) pentru a dezactiva automat un profil după ce a fost inactiv o anumită perioadă de timp.
- Determinaţi ce utilizatori au parola la fel cu numele profilului utilizator. Folosiţi comanda Analiză parole implicite (Analyze Default Passwords - ANZDFTPWD). Utilizaţi opţiunea din această comandă pentru a forţa utilizatorii să-şi modifice parolele la următoarea semnare.

  Atenţie: Nu înlăturaţi nici unul dintre profilurile furnizate IBM din sistem. Profilurile furnizate IBM încep cu litara Q.
- Vedeţi cine are o clasă utilizator alta decât *USER şi de ce. Folosiţi comanda Tipărire profil utilizaqtor (Print User Profile - PRTUSRPRF) pentru a obţine o listă cu toţi utilizatorii, clasele lor de utilizator şi autorizările lor speciale. Comparaţi această informaţie cu formularul Responsabilităţi sistem.
- Controlează ce profil utilizator are câmpul *Facilităţi limitate* setat pe *NO.

Monitorizare obiecte critice

- Revedeţi cine are acces la obiectele critice. Folosiţi comanda Tipărire autorizări private (Print Private Authorities - PRTPVTAUT) şi comanda Tipărire obiecte autorizate public (Print Publicly Authorized Objects - PRTPUBAUT) pentru a monitoriza obiectele. Dacă un grup are acces, verificaţi membrii grupului cu opţiunea *GRPMBR a comenzii DSPUSRPRF.
- Verificaţi cine poate utiliza programe de aplicaţie care oferă acces la obiecte prin altă metodă de securitate, cum ar fi autorizare adoptată. Folosiţi comanda Print Adopting Objects (PRTADPOBJ).

Monitorizare acces neautorizat

- Instruiţi operatorii sistem să se alerteze la mesajele de securitate din coada de mesaje QSYSOPR. În special, spuneţi-le să alerteze responsabilul de securitate despre încercări fără succes repetate de semnare. Mesajele de securitate sunt în intervalul de la 2200 la 22FF şi de la 4A00 la 4AFF. Au prefixele CPF, CPI, CPC şi CPD.
- Setaţi auditarea de securitate să înregistreze încercările neautorizate de a accesa obiecte.

Consultaţi apoi Auditarea securităţii.

Auditarea securităţii

Când monitorizaţi securitatea, sistemul de operare poate înregistra în istoric evenimente de securitate ce apar în sistem. Aceste evenimente sunt înregistrate în obiecte speciale de sistem numite**receptoare jurnal**. Puteţi seta receptoarele jurnal să înregistreze tipuri diferite de evenimente de securitate cum ar fi schimbarea unei valori de sistem sau a profilului utilizator sau o încercare nereuşită de accesare a unui obiect. Următoarele valori controlează ce evenimente sunt înregistrate în istoric:

- Valoarea de sistem controlul auditării (QAUDCTL)
- Valoarea de sistem nivelul auditării (QAUDLVL)
- Valoarea nivel de auditare (AUDLVL) din profilul utilizatorului
- Valoarea auditare de obiect (OBJAUD) din profilul utilizatorului
- Valoarea auditare de obiect (OBJAUD) din obiecte.

Informaţia din jurnalele de auditare este folosită:

- La detectarea încercărilor de violare a securităţii.
- La plănuirea migrării la un nivel de securitate mai ridicat.
- Pentru a monitoriza folosirea obiectelor sensibile, cum ar fi fişierele confidenţiale.

Pentru a vizualiza informaţia din jurnalele de auditare în diferite moduri, sunt disponibile comenzi.

Formulare pentru planificarea primară a securităţii sistemului

Puteţi copia sau tipări aceste formulare dintr-un browser.

Pentru a printa toată informaţia elementară de securitate, selectaţi panoul din dreapta şi apoi faceţi click pe icoana PDF din banner-ul ″Centrul de informare″.

Pentru a printa un singur formular de planificare, faceţi clic pe legătura ce corespunde formularului de planificare pe care doriţi să-l printaţi. Faceţi clic pe panoul din dreapta şi apoi pe icoana Print din browser-ul dumneavoastră. Aceasta va printa formularul selectat de dumneavoastră.

Iată o listare completă a tuturor formularelor de planificare ce sunt necesare pentru a plănui şi folosi cu succes securitatea primară a sistemului:

- Formularul de Planificare a securitaţii Fizice
- Formularul de descriere de aplicaţie
- Formularul de convenţii de nume
- Formularul de descriere de bibliotecă
- Formularul de selecţie a valorilor de sistem
- Formularul de responsabilităţi în sistem
- Formularul de identificare grup de utilizatori
- Formularul de descriere grup de utilizatori
- Formularul de profil utilizator individual
- Formularul listă de autorizare
- Formularul securitatea cozilor de ieşire şi a staţiilor de lucru
- Formularul de instalare a aplicaţiei

Formularul Planificare securitate fizică

Tabela 65. Formularul Planificare securitate fizică

Formularul Planificare securitate fizică	
Pregătit de:	Data:

Tabela 65. Formularul Planificare securitate fizică (continuare)

Instrucţiuni • Învăţaţi despre acest formular în ″Planificare securitate resurse.″ • Utilizaţi acest formular pentru a descrie toate problemele de securitate legate de locaţia fizică a unităţii de sistem şi a dispozitivelor ataşate. • Nu trebuie să introduceţi în sistem informaţia din acest formular.	
Unitate sistem:	
Descrie măsurile de securitate pentru a vă proteja unitatea sistem (de ex. camere încuiate):	
Ce poziţie a cheii IPL este folosită de obicei?	
Unde este păstrată cheia?	
Alte comentarii legate de unitatea sistem:	
Mediu de stocare de rezervă şi documentaţie:	
Unde sunt păstrate benzile de rezervă la sediul firmei?	
Unde sunt păstrate benzile de rezervă în afara sediului firmei?	
Unde sunt păstrate parolele pentru responsabilul cu securitatea, parolele de service şi DST?	
Unde este păstrată documentaţia importantă de sistem, cum ar fi numărul serial şi configuraţia?	

Formularul Planificare securitate fizică			Partea 2 din 2
Instrucţiuni suplimentare pentru Partea 2 • Listaţi mai jos staţiile de lucru şi imprimante a căror locaţie fizică poate expune securitatea. Indicaţi ce măsuri de protecţie veţi lua. Pentru o imprimantă, listaţi exemple de rapoarte confidenţiale în coloana *Expuneri de securitate*. • Dacă permiteţi sistemului să configureze automat dispozitivele locale, este posibil să nu ştiţi numele staţiilor de lucru şi imprimantelor până după instalarea sistemului. Dacă nu ştiţi numele când pregătiţi acest formular, completaţi descrierile (cum ar fi locaţia) şi adăugaţi numele mai târziu.			
Securitatea fizică pentru staţii de lucru şi imprimante			
Nume staţie de lucru sau imprimantă	Locaţie sau descriere	Expunere de securitate	Măsuri de protecţie de luat

Formular descriere aplicaţie

Tabela 66. formular Descriere aplicaţie

formular Descriere aplicaţie	
Pregătit de:	Data:

Tabela 66. formular Descriere aplicaţie (continuare)

Instrucţiuni • Învăţaţi despre acest formular în ″Descrierea aplicaţiei″ şi ″Planificarea securităţii resurselor.″ • Pregătiţi un formular separat pentru fiecare aplicaţie. • Nu trebuie să introduceţi în sistem informaţia din acest formular.	
Nume aplicaţie:	Abreviaţie:
Scurtă descriere de aplicaţiei:	
Nume meniu primar:	Bibliotecă:
Nume program iniţial:	Bibliotecă:
Listare biblioteci utilizate de aplicaţie pentru fişiere şi programe:	
Definire obiective de securitate pentru aplicaţie, cum ar fi dacă vreo informaţie este confidenţială:	

Formular convenţie nume

Tabela 67. Formular convenţii nume

Formular convenţii nume	
Pregătit de:	Data:
Instrucţiuni • Învăţaţi despre acest formular în ″Descrierea aplicaţiilor.″ • Nu trebuie să introduceţi în sistem informaţia din acest formular. • Utilizaţi acest formular pentru a descrie cum veţi asigna numele obiectelor din sistem. Daţi exemple pentru fiecare.	
Tip obiect	**Convenţie nume**
Profiluri de grup	
Profiluri utilizator	
Liste de autorizaţii	
Biblioteci	
Fişiere	
Calendare	
Dispozitive	
Benzi	

Formular descriere bibliotecă

Tabela 68. formular Descriere bibliotecă

formular Descriere bibliotecă	Partea 1 din 2
Pregătit de:	Data:
Instrucţiuni: • Învăţaţi despre acest formular în ″Planificare securitate utilizator″ şi ″Planificare securitate resurse.″ • Utilizaţi acest formular pentru a descrie bibliotecile principale şi pentru a defini cerinţele de securitate a resurselor pentru ele. • Completaţi un formular pentru fiecare bibliotecă importantă de aplicaţie din sistem. • Învăţaţi cum să introduceţi informaţia din acest formular în ″Setare securitate resurse.″	
Nume bibliotecă:	Nume descriptiv (text):
Descriere pe scurt a funcţiei acestei biblioteci:	

Tabela 68. formular Descriere bibliotecă (continuare)

Definiţi obiectivele de securitate pentru bibliotecă, cum ar fi dacă vreo informaţie este confidenţială:	
Autorizare publică la bibliotecă:	
Autorizare publică şa obiectele din bibliotecă:	
Autorizare publică pentru obiecte noi (CRTAUT):	
Proprietar bibliotecă:	

formular Descriere bibliotecă				Partea 2 din 2
Pregătit de:			Data:	
Nume bibliotecă:				
Instrucţiuni suplimentare pentru Partea 2 • În tabelul de mai jos listaţi toate persoanele sau obiectele care au nevoie de autorizări speciale. • Specificaţi tipul de autorizare necesar: *ALL, *CHANGE, *USE sau *EXCLUDE.				
Listaţi autorizările specifice pentru obiecte biblioteci				
Profil grup sau profil utilizator	Nume obiect	Tip obiect	Autorizare necesară	Listă de autorizaţii

Formular Selecţie valori sistem

Tabela 69. Formular Selecţie valori sistem

Formular Selecţie valori sistem		Partea 1 din 2
Pregătit de:		Data:
Instrucţiuni • Învăţaţi mai multe despre acest formular în ″ Planificare abordare generală.″ • Utilizaţi acest formular pentru a înregistra opţiunile pentru valorile sistem care afectează securitatea. • Folosiţi opţiunea **1** din meniul SETUP pentru a intra în Partea 1 din acest formular.		
Valori din ecranul Modificare opţiuni sistem		
Veloare sistem/atribut reţea	**Alegere recomandată**	**Alegerea dumneavoastră**
Nume sistem		
Separator dată (QDATSEP)		
Format dată (QDATFMT)		
Separator oră (QTIMSEP)		
Format nume dispozitive pentru dispozitive noi (QDEVNAMING)	1 (Sistem iSeries)	
Imprimantă sistem (QPRTDEV)		
Nivel securitate (QSECURITY)	40	

Tabela 69. Formular Selecţie valori sistem (continuare)

Permiterea responsabilului cu securitatea să semneze de la orice staţie de afişare (QLMTSECOFR)	N	
Salvare informaţii contabilizare job despre ieşirea imprimantă terminată (QACGLVL)	N (*NONE)	

Formular Selecţie valori sistem		Partea 2 din 2
Instrucţiuni suplimentare pentru Partea 2 • Învăţaţi mai multe despre Partea 2 a acestui formular în ″Setare valori sistem.″ • Utilizaţi comanda Gestionare valori sistem (Work With System Value - WRKSYSVAL) pentru a introduce Partea 2.		
Valori de sistem de securitate		
Valoare sistem	**Alegere recomandată**	**Alegerea dumneavoastră**
Interval timeout job inactiv (QINACTITV)	de la 30 la 60	
Coadă de mesaje job inactiv (QINACTMSGQ)	*DSCJOB	
Limitare sesiuni dispozitive (QLMTDEVSSN)	1 (DA)	
Acţiune în caz de încercări eşuate de semnare (QMAXSGNACN)	3 (Dezactivare ambele)	
Număr maxim de încercări de semnare (QMAXSIGN)	de la 3 la 5	
Interval expirare parolă (QPWDEXPITV)	de la 30 la 60	
Lungime maximă parolă (QPWDMAXLEN)	8	
Lungime minimă parolă (QPWDMINLEN)	6	
Parole diferite (QPWDRQDDIF)	7 (6 parole unice)	
Alte valori sistem		
Valoare sistem	**Alegere recomandată**	**Alegerea dumneavoastră**
Intervalul de timeout job deconectat (QDSCJOBITV)	300	
Notă: Puteţi dori să setaţi alte valori de sistem care afectează securitatea. Consultaţi capitolul trei din *Referinţe Securitate* (SC41-5302-04) penru o listă completă a valorilor de sistem care afectează securitatea şi recomandările pentru ele.		

Formular responsabilităţi sistem

Tabela 70. Formular responsabilităţi sistem

Formular responsabilităţi sistem	
Pregătit de:	Data:
Instrucţiuni: • Învăţaţi despre acest formular în ″Planificare profiluri individuale de utilizatori.″ • Utilizaţi acest formular pentru a lista toate persoanele care au clasa utilizator diferită de *USER. • Transferaţi informaţia din acest formular în coloana *Clasă utilizator* din formularul Profiluri individuale de utilizatori.	

Tabela 70. Formular responsabilităţi sistem (continuare)

Cine este responsabilul principal cu securitatea? Cine este responsabil cu securitea de rezervă?			
Nume profil	Nume utilizator	Clasa	Comentarii

Formular identificare grup utilizatori

Tabela 71. Formular identificare grup utilizatori

Formular identificare grup utilizatori								
Pregătit de:		Data:						
Instrucţiuni: • Învăţaţi despre acest formular în ″Planificare grupuri utilizatori.″ • Acest formular vă ajută să identificaţi grupurile de utlizatori care au nevoi similare de aplicaţie. 1. Listaţi aplicaţiile principale în partea de sus a formularului. 2. Listaţi utilizatorii în coloana din partea stângă. 3. Bifaţi aplicaţiile necesare fiecărui utilizator. • Nu trebuie să introduceţi în sistem informaţia din acest formular.								
		Acces necesar la aplicaţii						
Nume utilizator	Departament	APP:	APP:	APP:	APP:	APP:	APP:	APP:
Notă: • Dacă aveţi un mediu de securitate *slab*, folosiţi un **X** pentru a bifa aplicaţiile de care au nevoie utilizatorii. • Dacă aveţi un mediu de securitate *strict*, poate fi nevoie să utilizaţi **C** (change) şi **V** (view) pentru a specifica *cum* sunt utilizate aplicaţiile.								

Formular Descriere grup utilizatori

Tabela 72. formular Descriere grup utiizatori

Formular Descriere Grup Utilizator	Partea 1 din 2
Pregătit de:	Data:

Tabela 72. formular Descriere grup utiizatori (continuare)

Instrucţiuni pentru Partea 1 • Învăţaţi cum să pregătiţi acest formular în Planificare grupuri utilizatori.″ • Învăţaţi cum să intraţi în acest formuar în Setare securitate utilizator.″ • Pregătiţi un formular separat pentru fiecare grup care va utiliza sistemul. • Utilizaţi comanda Creare descriere job (Create Job Description - CRTJOBD) pentru a crea o descriere de job pentru grup. Descrierea de job conţine lista iniţială de biblioteci pentru grup.
Nume profil grup: Descrierea grupului:
Aplicaţia primară pentru grup: Listaţi alte aplicaţii necesare grupului:
Listaţi fiecare bibliotecă necesară grupului. Bifaţi (✓) fiecare bibliotecă ce ar trebui să fie în lista iniţială de biblioteci a grupului:
Notă: Uitaţi-vă în formularul Descriere aplicaţie pentru fiecare aplicaţie care este listată în secţiunea anterioară pentru a afla ce biblioteci utilizează fiecare aplicaţie.

formular Descriere grup utilizatori		Partea 2 din 2
Instrucţiuni suplimentare pentru Partea 2 • Tabelul de mai jos listează toate câmpurile care apar în ecranul Creare profil utilizator. Câmpurile sunt împărţite în două grupuri: cele pentru care alegerea trebuie să o faceţi dumneavoastră şi cele pentru care IBM recomandă valoarea implicită. • Folosiţi ecranul Gestionare profiluri (Work with User Profiles) sau comanda Creare profil utilizator (Create User Profile (CRTUSRPRF) pentru a introduce informaţiile din această parte a formularului în sistem.		
Alegeţi valori pentru aceste câmpuri în profilul de grup:		
Nume câmp	**Alegere recomandată**	**Alegerea dumneavoastră**
Nume profil grup (Utilizator)		
Parolă	*NONE	
Clasă utilizator (tipul de utilizator)	*USER	
Biblioteca curentă (biblioteca implicită)	*la fel cu numele profilului de grup*	
Programul iniţial de apelat (program de semnare)		
Bibliotecă program iniţial		
Meniu iniţial (primul meniu)		
Bibliotecă meniu iniţial		
Facilităţi limitate (restricţionare utilizare linie comandă)	*YES	
Text (descriere utilizator)		
Descriere de job	*la fel cu numele profilului de grup*	
Bibliotecă desscriere job		
Nume profil grup (grup utilizatori)	*NONE	
Dispozitiv tipărire (imprianta implicită)		
Coadă ieşire	*DEV	
Notă: Aceste câmpuri sunt în ordinea în care apar în ecranul Creare profil utilizator (cu F4).		
Folosiţi valorile furnizate de sistem (implicite) pentru câmpurile de mai jos:		
Cod contabilizare	Punere în buffer tastatură	Autorizare publică
Nivel asistenţă	ID limbă	Setare parolă să expire

Program tasta Attention	Limitare sesiuni dispozitive	Secvenţă sortare
ID set caractere codificate	Spaţiu maxim de stocare	Autorizare specială
ID ţară sau regiune	Coadă mesaje	Mediu special
Afişare informaţii semnare	Interval expirare parolă	Stare
Parolă document	Limită prioritate	Opţiuni utilizator
Notă: Câmpurile din această listă sunt aranjate în ordine alfabetică.		

Formular profil utilizator individual

Tabela 73. Formular profil utilizator individual

Formular profil utilizator individual						
Pregătit de:			Data:			
Instrucţiuni: • Învăţaţi cum să pregătiţi acest formular în ″Planificare profiluri utilizator individuale.″ • Utilizaţi acest formular pentru a înregistra informaţii despre utilizatorii de sistem. Completaţi câte un formular pentru fiecare grup (profil de grup) de pe sistem. • Utilizaţi coloanele libere din dreapta pentru orice alte câmpuri suplimentare pe care doriţi să le specificaţi pentru utilizatori individuali. • Învăţaţi cum să intraţi în acest formular în ″Setare utilizatori individuali.						
Nume profiluri grup:						
Proprietarul obiectelor create:			Autorizarea grupului la obiectele create:			
Tip autorizare grup:						
Faceţi o înregistrare pentru fiecare membru al grupului:						
Profil utilizator	Text (descriere)	Clasă utilizator	Facilităţi limitate			

Formular listă autorizaţii

Tabela 74. Formular Listă de autorizaţii

Formular Listă de autorizaţii	
Pregătit de:	Date:
Instrucţiuni • Învăţaţi despre acest formular în ″Planificare securitate resurse.″ • Pregătiţi câte un formular pentru fiecare listă de autorizaţii. • Utilizaţi formularul pentru a lista obiectele pe care le securizează lista şi grupurile şi persoanele care au acces la listă. • Învăţaţi cum să intraţi în acest formular în Setare securitate resurse.″	

Tabela 74. Formular Listă de autorizaţii (continuare)

Nume listă de autorizaţii:					
Descriere:					
Listaţi obiectele securizate de listă					
Nume obiect	Tip obiect	Bibliotecă obiect	Nume obiect	Tip obiect	Bibliotecă obiect
Listaţi grupurile şi utilizatorii care au acces la listă					
Grup sau utilizator	Tipul de acces permis	Administrare listă?	Grup sau utilizator	Tipul de acces permis	Administrare listă?

Formular securitate ieşire imprimantă şi staţie de lucru

Tabela 75. Formular Securitate coadă de ieşire şi staţie de lucru

Formular Securitate coadă de ieşire şi staţie de lucru				
Pregătit de:		Data:		
Instrucţiuni • Învăţaţi despre acest formular în ″Protejare ieşire imprimantă.″ • Faceţi o înregistrare în acest formular pentru orice staţie de lucru sau coadă de ieşire care are nevoie de protecţie specială. • Învăţaţi cum să intraţi în acest formular în ″Protejarea staţiilor de lucru.″				
Listaţi parametrii pentru cozile de ieşire restricţionate:				
Nume coadă de ieşire	Bibliotecă coadă ieşire	Afişare orice fişier (DSPDTA)	Autorizări de verificat (AUTCHK)	Control operator (OPRCTL)
Staţie de lucru responsabil cu securitatea: Dacă limitaţi accesul responsabilului cu securitatea la anumite staţii de lucru (valoarea sistem QLMTSECOFR este yes), listaţi mai jos staţile de lucru autorizate pentru responsabilul cu securitatea şi oricine cu autorizarea *ALLOBJ:				
Listaţi mai jos autorizările pentru staţiile de lucru restricţionate:				

Tabela 75. Formular Securitate coadă de ieşire şi staţie de lucru (continuare)

Nume staţie de lucru	Grupuri de utilizatori autorizate (autorizare *CHANGE)
Notă: Staţile de lucru restricţionate ar trebui să aibă autorizarea publică setată pe*EXCLUDE.	

Formular instalare aplicaţie

Tabela 76. formular Instalare aplicaţie

formular Instalare aplicaţie		Partea 1 din 2
Pregătit de:		Data:
Instrucţiuni • Învăţaţi despre acest formular în ″Planificare instalare aplicaţie.″ • Pregătiţi câte un formular pentru fiecare aplicaţie pe care o veţi instala. • Utilizaţi formularul pentru a planifica cum veţi stabili dreptul de proprietate şi autorizarea publică pentru aplicaţii după ce le veţi încărca. • Învăţaţi cum să intraţi în acest formular în Setare securitate resurse.″		
Nume aplicaţie:		
Descriere:		
Listaţi şi explicaţi fiecare profil care trebuie creat pentru instalarea aplicaţiei:		
Nume bibliotecă:		
	Înainte de instalare	După instalare
Proprietar bibliotecă		
Proprietar obiect		
Autorizare publică bibliotecă		
Autorizare publică bibliotecă		
Autorizare publică pentru obiecte noi		
Nume bibliotecă:		
	Înainte de instalare	După instalare
Proprietar bibliotecă		
Proprietar obiect		
Autorizare publică bibliotecă		
Autorizare publică bibliotecă		
Autorizare publică pentru obiecte noi		

formular Instalare aplicaţie		Partea 2 din 2
Nume bibliotecă:		
	Înainte de instalare	După instalare
Proprietar bibliotecă		
Proprietar obiect		
Autorizare publică bibliotecă		
Autorizare publică bibliotecă		

Autorizare publică pentru obiecte noi		
Nume bibliotecă:		
	Înainte de instalare	După instalare
Proprietar bibliotecă		
Proprietar obiect		
Autorizare publică bibliotecă		
Autorizare publică bibliotecă		
Autorizare publică pentru obiecte noi		
Nume bibliotecă:		
	Înainte de instalare	După instalare
Proprietar bibliotecă		
Proprietar obiect		
Autorizare publică bibliotecă		
Autorizare publică bibliotecă		
Autorizare publică pentru obiecte noi		

Anexa. Observaţii

Aceste informaţii au fost elaborate pentru produse şi servicii oferite în S.U.A.

Este posibil ca IBM să nu ofere în alte ţări produsele, serviciile sau opţiunile discutate în acest document. Luaţi legătura cu reprezentantul IBM local pentru informaţii despre produsele şi serviciile disponibile în zona dumneavoastră. Referirea la un produs, program sau serviciu IBM nu înseamnă că se afirmă sau că se sugerează faptul că poate fi folosit numai acel produs, program sau serviciu IBM. Poate fi folosit în loc orice produs, program sau serviciu care este echivalent din punct de vedere funcţional şi care nu încalcă dreptul de proprietate intelectuală al IBM. Însă evaluarea şi verificarea modului în care funcţionează un produs, program sau serviciu non-IBM ţine de responsabilitatea utilizatorului.

IBM poate avea brevete sau aplicaţii în curs de brevetare care să acopere subiectele descrise în acest document. Faptul că vi se furnizează acest document nu înseamnă că vi se acordă licenţa pentru aceste brevete. Puteţi trimite întrebări cu privire la licenţe, în scris, la:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594-1785
U.S.A.

Pentru întrebări privind licenţa pentru informaţiile DBCS (double-byte), contactaţi departamentul IBM de proprietate intelectuală din ţara dumneavoastră sau trimiteţi întrebări 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 PENTRU 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 conţine greşeli tehnice sau erori de tipar. Se efectuează modificări periodice la informaţiile incluse aici; aceste modificări vor fi încorporate în noi ediţii ale publicaţiei. IBM poate aduce îmbunătăţiri şi/sau modificări produsului (produselor) descris în această publicaţie în orice moment, fără notificare.

Referirile din aceste informaţii la adrese de situri Web non-IBM sunt făcute numai pentru a vă ajuta, fără ca prezenţa lor să însemne un gir acordat acestor situri Web. Materialele de pe acele situri Web nu fac parte din materialele pentru acest produs IBM şi utilizarea acestor situri Web este pe riscul dumneavoastră.

Posesorii de licenţe pentru acest program care doresc să obţină 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 52 N
Rochester, MN 55901
U.S.A.

Aceste informaţii pot fi disponibile cu respectarea termenilor şi condiţiilor corespunzătoare, iar în unele cazuri cu plata unei taxe.

Programul licenţiat descris în aceste informaţii şi toate materialele licenţiate disponibile pentru el sunt furnizate de IBM conform termenilor din IBM Customer Agreement, IBM International Program License Agreement sau orice acord echivalent încheiat între noi.

Informaţiile privind produsele non-IBM au fost obţinute de la furnizorii acestor produse, din anunţurile lor publicate sau din alte surse disponibile publicului. IBM nu a testat aceste produse şi nu poate confirma acurateţea performanţelor, compatibilitatea sau oricare alte pretenţii legate de produsele non-IBM. Întrebările legate de capacităţile produselor non-IBM le veţi adresa furnizorilor acestor produse.

Aceste informaţii sunt doar în scop de planificare. Informaţiile menţionate aici se pot modifica înainte ca produsele descrise să devină disponibile pe piaţă.

Aceste informaţii conţin exemple de date şi rapoarte folosite în operaţiile comerciale de zi cu zi. Pentru a fi cât mai complete, exemplele includ nume de persoane, de companii, de mărci şi de produse. Toate aceste nume sunt fictive şi orice asemănare cu nume sau adrese folosite de o întreprindere reală este pură coincidenţă.

Mărci comerciale

Următorii termeni sunt mărci comerciale deţinute de International Business Machines Corporation în Statele Unite, în alte ţări sau ambele:

Application System/400
AS/400
e (logo)
IBM
iSeries
Operating System/400
OS/400
400

Lotus, Freelance şi WordPro sunt mărci comerciale deţinute de International Business Machines Corporation şi Lotus Development Corporation în Statele Unite, în alte ţări sau ambele.

C-bus este o marcă comercială deţinută de Corollary, Inc. în Statele Unite, în alte ţări sau ambele.

ActionMedia, LANDesk, MMX, Pentium şi ProShare sunt mărci comerciale sau mărci comerciale înregistrate deţinute de Intel Corporation în Statele Unite, în alte ţări sau ambele.

Microsoft, Windows, Windows NT şi logo-ul Windows sunt mărci comerciale deţinute de Microsoft Corporation în Statele Unite, în alte ţări sau ambele.

SET şi logo-ul SET sunt mărci comerciale deţinute de SET Secure Electronic Transaction LLC.

Java şi toate mărcile comerciale bazate pe Java sunt mărci comerciale deţinute de Sun Microsystems, Inc. în Statele Unite, în alte ţări sau ambele.

UNIX este o marcă comercială înregistrată deţinută de The Open Group în Statele Unite şi în alte ţări.

Alte nume de companii, produse şi servicii pot fi mărci comerciale sau mărci de serviciu ale altora.

Termenii şi condiţiile pentru descărcarea şi tipărirea publicaţiilor

Permisiunile pentru utilizarea publicaţiilor pe care le-aţi selectat pentru descărcare sunt acordate cu respectarea următorilor termeni şi condiţii şi a confirmării dumneavoastră că îi acceptaţi.

Uz personal: Puteţi reproduce aceste publicaţii pentru uzul dumneavoastră personal, noncomercial, cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi distribui, afişa sau realiza obiecte derivate din aceste publicaţii sau dintr-o porţiune a lor fără consimţământul explicit al IBM.

Uz comercial: Puteţi reproduce, distribui şi afişa aceste publicaţii doar în interiorul întreprinderii dumneavoastră cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi să realizaţi lucrări derivate din aceste publicaţii sau să reproduceţi, să distribuiţi sau să afişaţi aceste publicaţii sau o porţiune a lor în afara întreprinderii dumneavoastră fără consimţământul explicit al IBM.

Cu excepţia a ceea ce este acordat explicit în această permisiune, nici o altă permisiune, licenţă sau drept nu vor mai fi acordate, explicit sau implicit, asupra publicaţiilor sau a altor informaţii, date, software sau altă proprietate intelectuală conţină aici.

IBM îşi rezervă dreptul de a retrage permisiunile acordate aici oricând consideră că folosirea informaţiilor este în detrimentul intereselor sale sau când personalul IBM constată că instrucţiunile de mai sus nu sunt urmate corespunzător.

Nu puteţi descărca, exporta sau reexporta aceste informaţii decât în deplină conformitate cu legile şi regulamentele aplicabile, inclusiv toate legile şi regulamentele de export ale Statelor Unite. IBM NU ACORDĂ NICI O GARANŢIE PENTRU CONŢINUTUL ACESTOR PUBLICAŢII. PUBLICAŢIILE SUNT FURNIZATE ″CA ATARE″, FĂRĂ NICI UN FEL DE GARANŢIE, EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANŢIILE IMPLCITE DE VANDABILITATE ŞI DE POTRIVIRE PENTRU UN ANUMIT SCOP.

Prin descărcarea sau tipărirea unei publicaţii de pe acest sit, aţi indicat că sunteţi de acord cu aceşti termeni şi condiţii.

Tipărit în S.U.A.