IBM

eserver

iSeries

Referinţe privind securitatea

Versiunea 5

SA12-6497-08

IBM

@server

iSeries

Referinţe privind securitatea

Versiunea 5

SA12-6497-08

Notă

Înainte de a utiliza aceste informaţii şi produsul la care se referă, aveţi grijă să citiţi Anexa H, “Observaţii”, la pagina 605.

Ediţia a noua (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 ulterioare, până se indică altceva în noile ediţii. Această versiune nu rulează pe toate modelele RISC şi nici pe modelele CISC.

Această ediţie înlocuieşte SC41-5302-07.

Cuprins

Figuri

Tabele

Despre Referinţe privind securitatea (SC41-5302)

Această carte furnizează informaţii despre planificarea, setarea, gestionarea şi auditarea securităţii pe sistemul dumneavoastră iSeries. Ea descrie toate caracteristicile securităţii din sistem şi discută cum se înrudesc caracteristicile securităţii cu alte aspecte ale sistemului, cum ar fi controlul funcţionării, salvarea de rezervă şi recuperarea şi proiectarea aplicaţiilor.

Această carte nu furnizează instrucţiuni operaţionale complete pentru setarea securităţii pe sistemul dumneavoastră. Pentru un exemplu pas-cu-pas de setare a securităţii, consultaţi Centrul de informare iSeries (vedeţi "Cerinţe preliminare şi informaţii înrudite" la pagina xvi) şi cartea *Tips and Tools for Securing Your iSeries*, SC41-5300-07. Informaţii despre Securitatea de bază a sistemului şi planificarea pot fi de asemenea găsite în Centrul de informare (vedeţi "Cerinţe preliminare şi informaţii înrudite" la pagina xvi).

Această carte nu furnizează informaţii complete despre planificare pentru utilizatorii de IBM Lotus Domino. Pentru utilizatorii Lotus Domino, vedeţi the URL http://www.lotus.com/ldd/doc. Acest sit Web oferă informaţii despre IBM Lotus Notes, Lotus Domino şi IBM Lotus Domino for iSeries. De pe acest site Web puteţi descărca informaţii în formatul de bază de date Domino (.NSF) şi în formatul Adobe Acrobat (.PDF), puteţi căuta în baza de date şi puteţi afla cum puteţi obţine manuale tipărite.

Această carte nu conţine informaţii complete despre API-urile (application programming interfaces - interfeţe de programare de aplicaţii) care sunt disponibile pentru a accesa informaţiile de securitate. API-urile sunt descrise în Centrul de informare. Acest subiect nu conţine informaţii despre Internet. Pentru informaţii despre considerentele privind conectarea sistemului dumneavoastră la Internet, vedeţi IBM SecureWay: iSeries şi Internet din Centrul de informare (vedeţi "Cerinţe preliminare şi informaţii înrudite" la pagina xvi). .

Pentru o listă de publicaţii înrudite, vedeţi "Informaţii înrudite" la pagina 609.

Cine ar trebui să citească această carte

Ţinta principală a acestei cărţi este administratorul de securitate.

Capitolul 9, "Auditarea securităţii pe sistemul iSeries", la pagina 223 este intenţionată pentru oricine doreşte să realizeze o auditare de securitate asupra sistemului.

Această carte presupune că sunteţi deja familiarizat cu introducerea de comenzi în sistem. Pentru a folosi câteva dintre exemplele din această carte, trebuie să ştiţi cum se face:

- Editarea şi crearea unui program CL (Control Language).
- Utilizarea unei unelte de interogare, cum ar fi programul cu licenţă Query/400.

Informaţiile din următoarele capitole pot ajuta programatorii de aplicaţii şi de sisteme să înţeleagă relaţia dintre securitate şi aplicaţie şi proiectarea sistemului:

Capitolul 5, "Securitatea resurselor", la pagina 109

Capitolul 6, "Securitate control funcţionare", la pagina 169

Capitolul 7, "Proiectarea securităţii", la pagina 189

Capitolul 8, "Salvarea de rezervă şi recuperarea informaţiilor de securitate", la pagina 213

Convenţiile şi terminologia utilizate în această carte

Ecranele iSeries din această carte pot fi afişate în Navigator iSeries, care face parte din iSeries Access pentru Windows de pe calculatorul personal. Ecranele date ca exemplu în această carte pot fi de asemenea afişate fără ca Navigator iSeries să fie disponibil.

Pentru informaţii suplimentare despre cum se utilizează Navigator iSeries, citiţi Centrul de informare iSeries (vedeţi "Cerinţe preliminare şi informaţii înrudite").

Cerinţe preliminare şi informaţii înrudite

Folosiţi Centrul de informare iSeries drept punct de pornire pentru cerinţele dumneavoastră de informaţii referitoare la iSeries. Informaţiile sunt disponibile în unul dintre următoarele moduri:

- Pe Internet la următoarea adresă URL (uniform resource locator):

  `http://www.ibm.com/eserver/iseries/infocenter`
- Pe CD-ROM: SK3T–4090–00, Centrul de informare iSeries. Acest pachet include de asemenea versiunile PDF ale manualelor iSeries (SK3T–4092–00, Centrul de informare iSeries: Manuale suplimentare), care înlocuiesc CD-ROM-ul Bibliotecă Softcopy.

Centrul de informare iSeries conţine consilieri şi subiecte importante, cum ar fi comenzile CL, API-urile de sistem, partiţiile logice, funcţionarea în cluster, Java, TCP/IP, servirea Web şi reţelele securizate. Include de asemenea legături spre cărţi înrudite IBM din seria Redbooks şi legături Internet spre alte site-uri Web ale IBM, cum ar fi Technical Studio şi pagina de bază IBM.

Cu fiecare nouă comandă de hardware, primiţi următoarele informaţii pe CD-ROM:

- **SK3T-4096-00, Instalare iSeries şi Biblioteca de service.** Acest CD-ROM conţine manuale PDF necesare pentru instalare şi pentru întreţinerea de sistem a unui IBM @server iSeries.
- *CD-ROM-ul Setarea şi operaţiile iSeries*, SK3T-4098-02. Acest CD-ROM conţine IBM iSeries Access pentru Windows şi vrăjitorul EZ-Setup. iSeries Access Express oferă un puternic set de capabilităţi de client şi de server pentru conectarea PC-urilor la servere iSeries. Vrăjitorul EZ-Setup execută automat multe dintre operaţiile de setare iSeries.

Pentru o listă de publicaţii înrudite, vedeţi "Informaţii înrudite" la pagina 609.

Navigator iSeries

Utilizaţi Centrul de informare iSeries drept un punct de pornire pentru obţinerea informaţiilor tehnice referitoare la iSeries.

Puteţi accesa Centrul de informare în două moduri:

- De pe următorul site web:

  `http://www.ibm.com/eserver/iseries/infocenter`
- De pe CD-ROM-ul *Centrul de informare iSeries*, SK3T-4091-04. Acest CD-ROM este trimis o dată cu noua dumneavoastră comandă de actualizare a hardware-ului iSeries sau software-ului IBM i5/OS. Puteţi de asemenea comanda CD-ROM-ul la Centrul de publicaţii IBM:

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

Centrul de informare iSeries conţine informaţii noi şi actualizate referitoare la iSeries, cum ar fi cele despre instalarea software-ului şi hardware-ului, Linux, WebSphere, Java, disponibilitatea înaltă, baza de date, partiţiile logice, comenzile CL şi API-urile de sistem. În plus, el furnizează consilieri şi programe de căutare care să vă ajute la planificarea, depanarea şi configurarea hardware-ului şi software-ului dumneavoastră iSeries.

Cu fiecare nouă comandă de hardware, primiţi *CD-ROM-ul Setarea şi operaţiile iSeries*, SK3T-4098-02. Acest CD-ROM conţine IBM @server iSeries Access pentru Windows şi vrăjitorul EZ-Setup. iSeries Access Family oferă un puternic set de capabilităţi de client şi de server pentru conectarea PC-urilor la servere iSeries. Vrăjitorul EZ-Setup execută automat multe dintre operaţiile de setare iSeries.

Cum să vă trimiteţi comentariile

Răspunsul dumneavoastră este important la furnizarea unor informaţii cât mai exacte şi de calitate înaltă. Dacă aveţi comentarii despre această carte sau despre orice altă documentaţie iSeries, completaţi formularul pentru comentariile cititorului de la sfârşitul acestei cărţi.

- Dacă preferaţi să trimiteţi comentarii prin poştă, utilizaţi formularul pentru comentariile cititorului cu adresa care este tipărită pe spate. Dacă trimiteţi prin poştă un formular cu comentarii de cititor dintr-o ţară sau regiune diferită de Statele Unite, puteţi să lăsaţi formularul la biroul reprezentanţei IBM locale sau la reprezentantul IBM pentru a fi trimis gratuit prin poştă.
- Dacă preferaţi să trimiteţi comentarii prin FAX, utilizaţi oricare dintre numerele următoare:
  - Statele Unite, Canada şi Puerto Rico: 1-800-937-3430
  - Alte ţări sau regiuni: 1-507-253-5192
- Dacă preferaţi să trimiteţi comentarii pe cale electronică, utilizaţi una dintre aceste adrese de e-mail:
  - Comentarii despre cărţi:

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

    RCHINFOC@us.ibm.com

Asiguraţi-vă că includeţi următoarele:

- Numele cărţii sau subiectul din Centrul de informare iSeries.
- Numărul de publicaţie al unei cărţi.
- Numărul de pagină sau subiectul unei cărţi la care se referă comentariile.

Ce este nou pentru V5R3

Două noi valori de sistem generale pentru securitate

Adăugarea a două noi valori de securitate, Scanare sistem de fişiere (QSCANFS) şi Control scanare sistem de fişiere (QSCANFSCTL), vă permite să activaţi uneltele pentru a scana fişierele care se află în sistemul de fişiere integrat. După ce virusul este detectat, puteţi întreprinde acţiunea corespunzătoare pentru a elimina virusul.

Valoarea de sistem Scanare sistem de fişiere (QSCANFS) vă permite să specificaţi sistemul de fişiere integrat în care obiectele vor fi scanate. Scanarea sistemului de fişiere integrat este activată când programele de ieşire sunt înregistrate cu oricare dintre punctele de ieşire referitoare la scanarea sistemului de fişiere integrat.

Valoarea de sistem Control scanare sistem de fişiere (QSCANFSCTL) controlează scanarea sistemului de fişiere integrat care este activată când programele de ieşire sunt înregistrate cu oricare dintre punctele de ieşire referitoare la scanarea sistemului de fişiere integrat.

O valoare de sistem nouă pentru a controla auditarea

Valoarea de sistem Extensie nivel de auditare (QAUDLVL2), împreună cu valoarea de sistem Nivel de auditare (QAUDLVL), determină care evenimente referitoare la securitate sunt înregistrate în jurnalul de auditare a securităţii (QAUDJRN) pentru toţi utilizatorii sistemului. Valoarea de sistem QAUDLVL2 este necesară când sunt necesare mai mult de şaisprezece valori de auditare.

Câmpuri de parametru pentru profil de utilizator nou

Câmpul de parametru Gestionare locală parolă specifică dacă parola profilului de utilizator trebuie să fie gestionată local. Dacă nu vreţi să gestionaţi parola local, valoarea parolei este trimisă altor produse IBM, care realizează sincronizarea parolei. Dacă nu gestionaţi parola local, atunci parola locală este setată la *NONE.

Câmpul de parametru Asociere EIM specifică dacă trebuie să fie adăugată o asociere EIM (Enterprise Identity Mapping) unui identificator EIM pentru utilizator.

Capitolul 1. Introducere în securitatea iSeries

Familia de sisteme **@server** acoperă un interval mare de utilizatori. Un sistem mic poate avea între trei şi cinci utilizatori, iar un sistem mare poate avea câteva mii de utilizatori. Unele instalări îşi au toate staţiile de lucru într-o singură zonă, relativ sigură. Altele au utilizatori răspândiţi pe distanţe mari, inclusiv utilizatori care se conectează prin apel telefonic şi utilizatori indirecţi, conectaţi prin calculatorul personal sau prin reţele de sisteme.

Securitatea sistemului iSeries este destul de flexibilă pentru a îndeplini cerinţele acestei diversităţi de utilizatori şi de situaţii. Trebuie să înţelegeţi caracteristicile şi opţiunile disponibile, astfel încât să le puteţi adapta la cerinţele dumneavoastră de securitate. Acest capitol conţine o privire generală asupra opţiunilor de securitate din sistem.

Securitatea sistemului are trei obiective importante:

Confidenţialitatea:
- Protejarea împotriva dezvăluirii de informaţii persoanelor neautorizate.
- Restricţionarea accesului la informaţiile confidenţiale.
- Protejarea împotriva utilizatorilor de sistem curioşi şi împotriva celor din afară.

Integritatea:
- Protejarea împotriva modificărilor neautorizate ale datelor.
- Restricţionarea manipulării datelor la programele autorizate.
- Furnizarea siguranţei că datele sunt de încredere.

Disponibilitatea:
- Prevenirea modificărilor accidentale sau a distrugerii datelor.
- Protejarea împotriva încercărilor celor din afară de a abuza sau distruge resurse de sistem.

Securitatea sistemului este deseori asociată cu ameninţări externe, cum ar fi hacker-ii sau rivalii în afaceri. Totuşi, protejarea împotriva accidentelor de sistem produse de utilizatori de sistem autorizaţi este deseori cel mai mare beneficiu al unui sistem de securitate bine organizat. Într-un sistem fără bune caracteristici de securitate, apăsarea unei taste greşite ar putea determina ştergerea de informaţii importante. Securitatea sistemului poate împiedica acest tip de accidente.

Cele mai bune funcţii de sistem pentru securitate nu pot duce la rezultate bune fără o bună planificare. Securitatea setată pe bucăţi mici, fără planificare, poate fi derutantă. Este dificil de întreţinut şi de auditat. Planificarea nu implică proiectarea în avans a securităţii pentru fiecare fişier, program şi dispozitiv. Ea implică stabilirea unei abordări generale a securităţii sistemului şi comunicarea acestei abordări dezvoltatorilor de aplicaţii, programatorilor şi utilizatorilor sistemului.

Când planificaţi securitatea sistemului dumneavoastră şi stabiliţi gradul de securitate de care aveţi nevoie, luaţi în considerare aceste întrebări:
- Există o politică a companiei sau un standard care necesită un anumit nivel de securitate?
- Persoanele din companie care realizează auditarea au nevoie de un nivel de securitate?
- Cât de important este pentru afacerea dumneavoastră sistemul împreună cu datele de pe el?
- Cât de importantă este protecţia la eroare furnizată de caracteristicile de securitate?
- Care sunt cerinţele de securitate ale companiei dumneavoastră pentru viitor?

Pentru a uşura instalarea, multe din capabilităţile de securitate din sistemul dumneavoastră nu sunt activate la livrarea sistemului. În această carte sunt furnizate recomandări pentru a aduce sistemul dumneavoastră la un nivel rezonabil de securitate. Luaţi în considerare cerinţele de securitate ale instalării dumneavoastră când evaluaţi recomandările.

Securitatea fizică

Securitatea fizică include protejarea unităţii de sistem, a dispozitivelor de sistem şi a mediilor cu copii de rezervă pentru deteriorări accidentale sau intenţionate. Majoritatea măsurilor pe care le luaţi pentru a asigura securitatea fizică a sistemului dumneavoastră sunt externe sistemului. Totuşi, sistemul este echipat cu o cheie de IPL, care împiedică executarea funcţiilor neautorizate de la unitarea sistem.

Notă: În cazul anumitor modele este necesar să comandaţi caracteristica de cheie IPL.

Securitatea fizică este descrisă în Centrul de informare (vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii).

Securitatea privind cheia IPL

Cheia IPL de pe panoul de control 940x controlează accesul la diverse funcţii ale panoului de control al sistemului. Poziţia cheii IPL poate fi extrasă şi modificată prin control de program utilizând una dintre următoarele:

- API-ul QWCRIPLA (Retrieve IPL Attributes - Extragere atribute IPL)
- Comanda CHGIPLA (Change IPL Attributes - Modificare atribute IPL)

Aceasta permite accesul utilizatorului de la distanţă la funcţiile suplimentare pe care le oferă panoul de control. De exemplu, se poate controla de unde va realiza maşina IPL-ul şi în ce mediu, fie în OS/400, fie în DST (Dedicated Service Tools - Unelte de service dedicate).

Valoarea de sistem OS/400 QRMTSRVATR controlează accesul la distanţă. Această valoare este livrată implicit dezactivată, ceea ce nu va permite înlocuirea cheii IPL. Valoarea de sistem poate fi modificată pentru a permite accesul de la distanţă, dar pentru aceasta este nevoie de autorizările speciale *SECADM şi *ALLOBJ.

Nivelul de securitate

Puteţi alege gradul de securitate pe care doriţi să îl impună sistemul prin setarea valorii de sistem QSECURITY (security level - nivel de securitate). Sistemul oferă cinci niveluri de securitate:

Nivelul 10:
Nivelul 10 nu mai este suportat. Vedeţi Capitolul 2, “Utilizarea valorii de sistem QSecurity (Securitate sistem)”, la pagina 7 pentru informaţii despre nivelurile de securitate (10, 20, 30, 40 şi 50).

Nivelul 20:
Sistemul necesită un ID de utilizator şi o parolă pentru semnare. Toţi utilizatorii primesc acces la toate obiectele.

Nivelul 30:
Sistemul necesită un ID de utilizator şi o parolă pentru semnare. Este impusă securitatea resurselor.

Nivelul 40:
Sistemul necesită un ID de utilizator şi o parolă pentru semnare. Este impusă securitatea resurselor. În plus, sunt impuse caracteristici suplimentare de protecţie a integrităţii.

Nivelul 50:
Sistemul necesită un ID de utilizator şi o parolă pentru semnare. Este impusă securitatea resurselor. Sunt impuse protecţia integrităţii de nivel 40 şi protecţia integrităţii îmbunătăţită. Nivelul de securitate 50 este conceput pentru sisteme iSeries cu cerinţe înalte de securitate, fiind proiectat să îndeplinescă cerinţele de securitate C2.

Nivelurile securităţii sistemului sunt descrise în Capitolul 2, “Utilizarea valorii de sistem QSecurity (Securitate sistem)”, la pagina 7.

Valorile de sistem

Valorile de sistem vă permit să personalizaţi multe dintre caracteristicile sistemului dumneavoastră. Pentru a defini setările de securitate ale întregului sistem, se utilizează un grup de valori de sistem. De exemplu, puteţi specifica:

- Câte încercări de semnare permiteţi la un dispozitiv.
- Dacă un sistem deconectează automat o staţie de lucru inactivă.
- Cât de des este nevoie să fie modificate parolele.
- Lungimea şi formatul parolelor.

Valorile de sistem care se referă la securitate sunt descrise în Capitolul 3, “Valorile de sistem privind securitatea”, la pagina 19.

Semnarea

O componentă cheie a securităţii este integritatea: posibilitatea de a avea încredere că obiectele din sistem nu au fost utilizate sau modificate. Software-ul sistemului dumneavoastră de operare este protejat prin semnături digitale şi acum puteţi consolida integritatea prin semnarea obiectelor software pe care vă bazaţi. (Pentru informaţii suplimentare despre folosirea semnării pentru a vă proteja sistemul, vedeţi *Tips and Tools for Securing Your iSeries*.) Acest lucru este important în special dacă obiectul a fost transmis prin internet sau memorat pe un mediu de stocare despre care credeţi că a fost modificat. Semnătura digitală poate fi folosită pentru a detecta dacă obiectul a fost modificat.

Semnăturile digitale şi utilizarea lor pentru verificarea integrităţii software-ului pot fi gestionate în în conformitate cu politica dumneavoastră de securitate, folosind valoarea de sistem QVFYOBJRST (Verify Object Restore - Verificare restaurare obiecte), comanda CHKOBJITG (Check Object Integrity - Verificare integritate obiect) şi unealta DCM (Digital Certificate Manager - Manager certificate digitale). În plus, puteţi alege să vă semnaţi programele (toate programele cu licenţă livrate împreună cu iSeries sunt semate). DCM este descris în Centrul de informare (vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii).

Începând cu V5R2 puteţi restricţiona adăugarea semnăturilor digitale la un depozit de certificate digitale, folosind API-ul Adăugare verificator şi puteţi restricţiona resetarea parolelor pentru rezerva de certificate digitale. SST (System Service Tools - Unelte de service sistem) furnizează o nouă opţiune de meniu, numită ″Gestionare securitate sistem″, unde puteţi restricţiona adăugarea de certificate digitale.

Activarea pentru semnare unică

În reţele eterogene din prezent, cu servere partiţionate şi cu multiple platforme, administratorii trebuie să facă faţă complexităţii de a gestiona identificarea şi autentificarea utilizatorilor din reţea. Noua infrastructură IBM şi exploatarea ei în iSeries îi ajută pe administratori, utilizatori şi programatorii de aplicaţii să gestioneze mult mai ieftin şi mai uşor aceste identificări şi autentificări.

Pentru a activa un mediu cu semnare unică, IBM furnizează două tehnologii care funcţionează împreună pentru a permite utilizatorilor să semneze cu parola şi numele lor de utilizator Windows şi să fie autentificaţi pe sistemele iSeries din reţea. Serviciul de autentificare în reţea şi EIM (Enterprise Identity Mapping - Maparea identităţii în întreprindere) sunt cele două tehnologii pe care un administrator trebuie să le configureze pentru a activa un mediu cu semnare unică. Windows 2000, XP, AIX şi zSeries folosesc protocolul Kerberos pentru a autentifica utilizatorii în reţea. Un server centralizat, securizat, denumit centru de distribuire a cheilor, autentifică principalii (utilizatorii Kerberos) în reţea.

În timp ce serviciul de autentificare în reţea permite unui sistem iSeries să participe în acea regiune Kerberos, EIM furnizează un mecanism pentru asocierea acestor principali Kerberos la un singur identificator EIM, care reprezintă acel utilizator în întreaga întreprindere. Alte identităţi de utilizator, cum ar fi un nume de utilizator OS/400, pot fi asociate cu acest identificator EIM. Când un utilizator semnează în reţea şi accesează un sistem iSeries, nu i se cere ID-ul de utilizator şi parola. Dacă autentificarea Kerberos a reuşit, aplicaţiile pot căuta asocierile cu identificatorul EIM pentru a găsi numele de utilizator OS/400. Utilizatorul nu mai are nevoie de o parolă pentru aplicaţiile şi funcţiile iSeries, deoarece este deja autentificat prin intermediul protocolului Kerberos. Administratorii pot gestiona central

identităţile de utilizator cu EIM, în timp ce utilizatorii de reţea au nevoie să gestioneze doar o parolă. Puteţi activa semnarea unică prin configurarea serviciului de autentificare în reţea şi prin configurarea EIM (Enterprise Identity Mapping - Mapare de identitate în întreprindere) pe sistemul dumneavoastră iSeries. Pentru a examina un scenariu care ilustrează cum se face setarea unui mediu cu semnare unică, vedeţi în Centrul de informare subiectul Scenariu: Activarea semnării unice. (**Securitate—>Serviciu de autentificare în reţea—>Scenarii serviciu de autentificare în reţea—>Scenariu: Activarea semnării unice**). Vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru informaţii suplimentare despre accesarea Centrului de informare.

Profilurile de utilizator

Fiecare utilizator al sistemului are un profil de utilizator. La nivelul de securitate 10, sistemul creează automat un profil când un utilizator semnează pentru prima dată. La nivelurile de securitate mai înalte, trebuie să creaţi un profil de utilizator înainte ca un utilizator să poată semna.

Profilul de utilizator este o unealtă puternică şi flexibilă. El controlează ce poate face utilizatorul şi personalizează modul în care apare sistemul pentru utilizator. Urmează descrierile câtorva caracteristici importante de securitate ale profilului de utilizator:

Autorizarea specială
: Autorizările speciale stabilesc dacă utilizatorul are permisiunea de a executa funcţii de sistem, cum ar fi crearea de profiluri de utilizator sau modificarea joburilor altor utilizatori.

Meniul iniţial şi programul iniţial
: Meniul iniţial şi programul iniţial stabilesc ce vede utilizatorul după ce semnează pe sistem. Puteţi limita un utilizator la un anumit set de operaţii prin restricţionarea utilizatorului la un meniu iniţial.

Limitarea capabilităţilor
: Câmpul Limitare capabilităţi din profilul de utilizator stabileşte dacă utilizatorul poate introduce comenzi şi dacă poate modifica meniul iniţial sau programul iniţial când semnează.

Profilurile de utilizator sunt discutate în Capitolul 4, “Profilurile de utilizator”, la pagina 55.

Profilurile de grup

Un profil de grup este un tip special de profil de utilizator. Puteţi folosi un profil de grup pentru a defini autorizarea pentru un grup de utilizatori, în loc să acordaţi autorizarea fiecărui utilizator în parte. Un profil de grup poate deţine obiecte din sistem. Puteţi de asemenea utiliza un profil de grup drept model la crearea de profiluri de utilizator individuale, prin utilizarea funcţiei de copiere profil.

“Planificarea profilurilor de grup” la pagina 207 discută utilizarea autorizării de grup. “Dreptul de proprietate al grupului asupra obiectelor” la pagina 118 discută ce obiecte ar trebui deţinute de profilurile de grup. “Grupul primar pentru un obiect” la pagina 119 discută utilizarea grupului primar şi a autorizării de grup primar pentru un obiect. “Copierea profilurilor de utilizator” la pagina 97 descrie cum se face copierea unui profil de grup pentru a crea un profil de utilizator individual.

Securitatea resurselor

Securitatea resurselor sistemului vă permite să definiţi cine poate utiliza obiectele şi cum pot fi utilizate acele obiecte. Capacitatea de a accesa un obiect este numită **autorizare**. Puteţi specifica autorizări detaliate, cum ar fi adăugarea sau modificarea de înregistrări. Sau puteţi folosi subseturile de autorizări definite de sistem: *ALL, *CHANGE, *USE şi *EXCLUDE.

Fişierele, programele şi bibliotecile sunt cele mai obişnuite obiecte care necesită protecţia prin securitate, dar puteţi specifica o autorizare pentru orice obiect din sistem. Urmează descrierile caracteristicilor securităţii de resurse:

Profiluri de grup
: Un grup de utilizatori similari pot partaja aceeaşi autorizare de a folosi obiecte.

Listă de autorizare
Obiectele care au necesităţi similare de securitate pot fi grupate într-o listă; autorizarea poate fi astfel acordată listei, în loc să fie acordată individual obiectelor.

Drept de proprietate obiect
Fiecare obiect din sistem are un proprietar. Obiectele pot fi deţinute de un profil de utilizator individual sau de un profil de grup. Alocarea corespunzătoare a dreptului de proprietate asupra obiectului vă ajută să gestionaţi aplicaţiile şi să delegaţi responsibilitatea pentru securitatea informaţiilor dumneavoastră.

Grup primar
Puteţi specifica un grup primar pentru un obiect. Autorizarea grupului primar este memorată cu obiectul. Utilizarea grupurilor primare poate simplifica administrarea autorizăilor şi poate îmbunătăţi performanţele de verificare a autorizării.

Autorizare de bibliotecă
Puteţi aduna fişiere şi programe care au cerinţe similare de protecţie într-o bibliotecă şi puteţi restricţiona accesul la acea bibliotecă. Aceasta se face de obicei mai uşor decât restricţionarea accesului la fiecare obiect în parte.

Autorizare de director
Puteţi utiliza autorizarea de director în acelaşi mod în care folosiţi autorizarea de bibliotecă. Puteţi grupa obiecte într-un director şi puteţi securiza directorul, nu obiecte individuale.

Autorizare de obiect
În cazurile în care restricţionarea accesului la o bibliotecă sau la un director nu este destul de precisă, puteţi restricţiona autorizarea de accesare a obiectelor individuale.

Autorizare publică
Pentru fiecare obiect, puteţi defini ce fel de acces este disponibil pentru fiecare utilizator de sistem care nu are nici o altă autorizare asupra obiectului. Autorizarea publică este un mijloc efectiv de a securiza informaţiile şi ea furnizează o bună performanţă.

Autorizare adoptată
Autorizarea adoptată adaugă autorizarea proprietarului unui program la autorizarea utilizatorului care rulează programul. Autorizarea adoptată este o unealtă utilă atunci când un utilizator are nevoie de autorizare diferită pentru un obiect, în funcţie de situaţie.

Deţinător de autorizare
Un deţinător de autorizare memorează informaţiile de autorizare pentru un fişier de bază de date descris de program. Informaţiile de autorizare rămân, chiar dacă fişierul este şters. Deţinătorii de autorizare sunt utilizaţi de obicei la convertirea din System/36, deoarece aplicaţiile System/36 şterg de obicei fişierele şi le creează din nou.

Autorizare la nivel de câmp
Autorizările la nivel de câmp sunt acordate câmpurilor individuale dintr-un fişier de bază de date. Această autorizare este gestionată prin SQL.

Securitatea resurselor este descrisă în Capitolul 5, “Securitatea resurselor”, la pagina 109

Jurnalul de auditare a securităţii

Există mai multe funcţii în sistem pentru a vă ajuta la auditarea eficacităţii securităţii. În particular, sistemul furnizează abilitatea de a înregistra într-un jurnal de auditare a securităţii anumite evenimente legate de securitate. Mai multe valori de sistem, valori de profil de utilizator şi valori de obiecte controlează ce evenimente sunt înregistrate în jurnal.

Capitolul 9, “Auditarea securităţii pe sistemul iSeries”, la pagina 223 furnizează informaţii despre auditarea securităţii.

Securitatea C2

Utilizând nivelul de securitate 50 şi urmând instrucţiunile din *Security - Enabling for C2*, SC41-5303-00, puteţi aduce un sistem iSeries Versiunea 4 Ediţia 4 la nivelul C2 de securitate. C2 este un standard de securitate definit de guvernul S.U.A. în *Department of Defense Trusted System Evaluation Criteria* (DoD 5200.28.STD).

În octombrie 1995, Departamentului de Apărare al Statelor Unite a încadrat oficial iSeries în clasa de securitate C2. Clasa C2 se aplică ediţiei V2R3 a OS/400, SEU, Query/400, SQL şi Common Cryptographic Architecture Services/400. În cadrarea în clasa C2 a fost acordată după o perioadă de mai mulţi ani de evaluare riguroasă. iSeries este primul sistem care atinge o rată de securitate C2 pentru un sistem (hardware şi sistem de operare) cu o bază de date integrată, complet funcţională.

În 1999, iSeries a fost clasificat C2 pentru Versiunea 4 Ediţia 4 a OS/400 (cu cod caracteristică 1920), SEU, Query/400, SQL, TCP/IP Utilities, Cryptographic Access Provider şi Advanced Series Hardware. În evaluare a fost inclus un set limitat de funcţii de comunicaţie TCP/IP între servere iSeries, ataşate la o reţea locală (LAN).

Pentru a fi considerat de clasă C2, un sistem trebuie să îndeplinească strict anumite criterii în următoarele domenii:

- Controlul nelimitat al accesului
- Contabilizarea utilizatorilor
- Auditarea securităţii
- Izolarea resurselor

Pool-ul de discuri independent

Pool-urile de discuri independente furnizează abilitatea de a grupa împreună spaţii de stocare care pot fi trecute în starea offline sau pot fi aduse online independent de datele de sistem sau de orice alte date înrudite. Termenii pool de memorie auxiliară (auxiliary storage pool - ASP) independent şi pool de discuri independent sunt sinonimi. Un pool de discuri independent poate fi comutabil între mai multe sisteme dintr-un mediu cu funcţionare în cluster sau conectat la un singur sistem. Pentru V5R2, modificările funcţionale asupra pool-urilor de discuri independente au implicaţii asupra securităţii din sistemul dumneavoastră. De exemplu, când executaţi comanda CRTUSRPRF, nu puteţi crea un profil de utilizator (*USRPRF) într-un pool de discuri independent. Însă când un utilizator este autorizat în particular asupra unui obiect din pool-ul de discuri independent, când este proprietarul unui obiect dintr-un pool de discuri independent sau când este grupul primar al unui obiect dintr-un pool de discuri independent, numele profilului este memorat în pool-ul de discuri independent. Dacă pool-ul de discuri independent este mutat în alt sistem, autorizarea particulară, dreptul de proprietate asupra obiectului şi intrările de grup primar vor fi ataşate la profilul cu acelaşi nume din sistemul destinaţie. Dacă nu există un profil în sistemul destinaţie, este creat un profil. Utilizatorul nu va avea nici o autorizare specială şi parola va fi setată la *NONE.

Pool-urile de discuri independente au fost îmbunătăţite pentru a furniza suport pentru obiecte bazate pe biblioteci. În ediţiile anteriore, pool-urile de discuri independente suportau doar UDFS (user-defined file systems - sisteme de fişiere definite de utilizator). Există însă mai multe obiecte care nu sunt permise pe pool-urile de discuri independente. Pentru o listă completă cu obiectele suportate şi nesuportate, vedeţi în Centrul de informare subiectul Tipurile de obiecte OS/400. (**Administrarea sistemelor—>Pool-urile de discuri independente—>Concepte—>Restricţii şi considerente—>Tipurile de obiecte OS/400 suportate şi nesuportate**)

Capitolul 2. Utilizarea valorii de sistem QSecurity (Securitate sistem)

Acest capitol discută valoarea de sistem pentru nivelul de securitate (QSECURITY) şi problemele asociate cu ea.

Privire generală:

Scop: Specificaţi nivelul de securitate care să fie impus în sistem.

Cum se face:
WRKSYSVAL *SEC (comanda Gestionare valori de sistem) sau meniul SETARE, opţiunea 1 (Modificare opţiuni sistem)

Autorizare:
*ALLOBJ şi *SECADM

Intrare jurnal:
SV

Notă: Înainte de a face modificări într-un sistem de producţie, citiţi secţiunea corespunzătoare despre migrarea de la un nivel la altul.

Sistemul oferă cinci niveluri de securitate:

10 **Nici o securitate impusă de sistem**

Notă: Nu puteţi seta valoarea de sistem QSECURITY la nivelul de securitate 10.

20 Securitatea semnării

30 Securitatea semnării şi resurselor

40 Securitatea semnării şi resurselor; protecţia integrităţii

50 Securitatea semnării şi resurselor; protecţie îmbunătăţită a integrităţii

Sistemul dumneavoastră este livrat la nivelul 40, care furnizează securitatea semnării şi resurselor şi asigură protecţia integrităţii. Pentru informaţii suplimentare, vedeţi “Nivelul de securitate 40” la pagina 11.

Dacă doriţi să modificaţi nivelul de securitate, folosiţi comanda WRKSYSVAL (Work with System Values - Gestionare valori de sistem). Nivelul minim de securitate pe care ar trebui să îl folosiţi este 30. Se recomandă însă nivelul 40 sau mai ridicat. Modificările au efect următoarea dată când realizaţi un IPL (Initial Program Load - Încărcare iniţială de program). Tabela 1 compară nivelurile de securitate din sistem:

Tabela 1. Niveluri de securitate: Comparaţie a funcţiilor

Funcţie	Nivel 20	Nivel 30	Nivel 40	Nivel 50
Este necesar numele de utilizator pentru semnare.	Da	Da	Da	Da
Este necesară parola pentru semnare.	Da	Da	Da	Da
Securitatea de parolă activă.	Da	Da	Da	Da
Securitatea de meniuri şi program iniţial activă.	Da[1]	Da[1]	Da[1]	Da[1]
Suportul pentru limitarea capabilităţilor activ.	Da	Da	Da	Da
Securitatea resurselor activă.	Nu	Da	Da	Da
Acces la toate obiectele.	Da	Nu	Nu	Nu
Profilul de utilizator este creat automat.	Nu	Nu	Nu	Nu
Capabilităţile de auditare securitate disponibile.	Da	Da	Da	Da

Tabela 1. Niveluri de securitate: Comparaţie a funcţiilor (continuare)

Funcţie	Nivel 20	Nivel 30	Nivel 40	Nivel 50
Programele care conţin instrucţiuni restricţionate nu pot fi create sau recompilate.	Da	Da	Da	Da
Programele care folosesc interfeţe nesuportate eşuează la rulare.	Nu	Nu	Da	Da
Este suportată protecţia hardware îmbunătăţită a spaţiului de stocare.	Nu	Nu	Da	Da
Biblioteca QTEMP este un obiect temporar.	Nu	Nu	Nu	Nu
Obiectele *USRSPC, *USRIDX şi *USRQ pot fi create doar în bibliotecile specificate în valoarea de sistem QALWUSRDMN.	Da	Da	Da	Da
Pointer-ii utilizaţi în parametri sunt validaţi pentru programele de domeniu utilizator care rulează în starea sistem.	Nu	Nu	Da	Da
Regulile de tratare a mesajelor sunt impuse între programele în starea sistem şi utilizator.	Nu	Nu	Nu	Da
Spaţiul asociat unui program nu poate fi modificat direct.	Nu	Nu	Da	Da
Blocurile de control intern sunt protejate.	Nu	Nu	Da	Da [2]

[1] Când este specificat LMTCPB(*YES) în profilul de utilizator.

[2] La nivelul 50 este impusă o protecţie mai înaltă a blocurilor de control intern decât la nivelul 40. Vedeţi “Împiedicarea modificării blocurilor de control interne” la pagina 17.

Nivelul de securitate al sistemului determină care sunt autorizările speciale implicite pentru fiecare clasă de utilizator. Când creaţi un profil de utilizator, puteţi selecta autorizări speciale pe baza clasei de utilizator. Autorizările speciale sunt de asemenea adăugate şi înlăturate din profilurile de utilizator când modificaţi nivelurile de securitate.

Pot fi specificate pentru un utilizator următoarele autorizări speciale:

***ALLOBJ**
Autorizarea specială toate obiectele acordă unui utilizator autorizarea de a realiza toate operaţiile pe obiecte.

***AUDIT**
Autorizarea specială de auditare permite unui utilizator să definească anumite caracteristici de auditare ale sistemului, obiectelor şi utilizatorilor de sistem.

***IOSYSCFG**
Autorizarea specială de configurare sistem permite unui utilizator să configureze dispozitivele de intrare şi de ieşire din sistem.

***JOBCTL**
Autorizarea specială de control al joburilor permite unui utilizator să controleze joburile şi tipărirea batch în sistem.

***SAVSYS**
Autorizarea specială de salvare sistem permite unui utilizator să salveze şi să restaureze obiecte.

***SECADM**
Autorizarea specială de administrator de securitate permite unui utilizator să gestioneze profilurile de utilizator din sistem.

***SERVICE**
Autorizarea specială de service permite unui utilizator să realizeze funcţii de service software în sistem.

***SPLCTL**
Autorizarea specială de control spool permite controlul nerestricţionat asupra joburilor batch şi asupra cozilor de ieşire din sistem.

Începând cu V5R2, puteţi de asemenea restricţiona utilizatorii cu autorizările *SECADM şi *ALLOBJ astfel încât să nu poată modifica aceste valori cu comanda CHGSYSVAL această valoare de sistem pentru securitate. Puteţi specifica această restricţie în SST (System Service Tools - Unelte de service sistem) cu opţiunea ″Work with system security - Gestionare securitate sistem″.

Notă: Această restricţie se aplică şi altor câteva valori de sistem.
Pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem referitoare la securitate şi pentru o listă completă a valorilor de sistem afectate, vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″.

Tabela 2 arată autorizările speciale implicite pentru fiecare clasă de utilizator. Intrările arată că autorizarea este dată doar la nivelurile de securitate 10 şi 20, la toate nivelurile de securitate sau deloc.

Tabela 2. Autorizările speciale implicite pentru clasele utilizator, după nivelul de securitate

Autorizare specială	Clase utilizator				
	***SECOFR**	***SECADM**	***PGMR**	***SYSOPR**	***USER**
*ALLOBJ	Toate	10 sau 20	10 sau 20	10 sau 20	10 sau 20
*AUDIT	Toate				
*IOSYSCFG	Toate				
*JOBCTL	Toate	10 sau 20	10 sau 20	Toate	
*SAVSYS	Toate	10 sau 20	10 sau 20	Toate	10 sau 20
*SECADM	Toate	Toate			
*SERVICE	Toate				
*SPLCTL	Toate				

Notă: Subiectele “Clasă utilizator” la pagina 61 şi “Autorizare specială” la pagina 66 furnizează informaţii suplimentare despre clasele de utilizator şi despre autorizările speciale.

Recomandări:

Este recomandat nivelul de securitate 30 sau mai mare, deoarece sistemul nu acordă automat acces utilizatorilor la toate resursele. La nivelurile de securitate mai mici, toţi utilizatorii primesc autorizarea specială *ALLOBJ.

De asemenea, la nivelul de securitate 30 (sau mai mic), utilizatorii pot apela interfeţe de sistem care fac schimb la profilul de utilizator QSECOFR sau permit utilizatorilor accesul la resurse pe care în mod normal nu ar fi lăsaţi să le acceseze. La nivelul de securitate 40, utilizatorii nu au permisiunea să apeleze direct aceste interfeţe; de aceea, este recomandat nivelul de securitate 40 sau mai mare.

Nivelul de securitate 40 furnizează protecţie suplimentară a integrităţii, fără a afecta performanţele sistemului. Aplicaţiile care nu rulează la nivelul de securitate 40 au un efect negativ asupra performanţei la nivelul de securitate 30. Ele determină sistemul să răspundă la violările de domeniu.

Nivelul de securitate 50 este conceput pentru sisteme cu cerinţe de securitate foarte ridicate. Dacă vă rulaţi sistemul la nivelul de securitate 50, puteţi observa un efect asupra performanţei, din cauza verificării suplimentare pe care o realizează sistemul.

Chiar dacă doriţi să acordaţi tuturor utilizatorilor acces la toate informaţiile, luaţi în considerare rularea sistemului la nivelul de securitate 30. Puteţi folosi capabilitatea de autorizare publică pentru a acorda utilizatorilor acces la informaţii. Utilizarea de la început a nivelului de securitate 30 vă oferă flexibilitatea de a securiza câteva resurse critice când este nevoie, fără a trebui să testaţi din nou toate aplicaţiile.

Nivelul de securitate 10

La nivelul de securitate 10 nu aveţi protecţie prin securitate; de aceea, nivelul de securitate 10 **nu este recomandat** de IBM. Începând cu Versiunea 4 Ediţia 3, nu vă puteţi seta nivelul de securitate la 10. Dacă sistemul dumneavoastră se află la nivelul 10, el va rămâne la acest nivel când instalaţi Versiunea 4 Ediţia 3. Dacă schimbaţi nivelul sistemului cu altă valoare, nu veţi putea să îl schimbaţi înapoi în nivelul 10.

Când un nou utilizator semnează, sistemul creează un profil de utilizator având ca nume de profil ID-ul de utilizator specificat în ecranul de semnare. Dacă acelaşi utilizator semnează mai târziu cu un alt ID de utilizator, atunci este creat un nou profil de utilizator. Anexa B arată valorile implicite care sunt folosite când sistemul creează automat un profil de utilizator.

Sistemul realizează verificarea autorizării la toate nivelurile de securitate. Deoarece toate profilurile de utilizator create la nivelul de securitate 10 primesc autorizare specială *ALLOBJ, utilizatorii trec cu succes de orice verificare de autorizare şi au acces la toate resursele. Dacă doriţi să testaţi efectul mutării la un nivel de securitate mai înalt, puteţi să înlăturaţi autorizarea specială *ALLOBJ din profilurile de utilizator şi să acordaţi autorizarea de a folosi anumite resurse. Totuşi, aceasta nu vă oferă nici o protecţie prin securitate. Oricine poate semna cu un nou ID de utilizator şi atunci este creat un nou profil, cu autorizarea specială *ALLOBJ. Nu puteţi împiedica aceasta la nivelul de securitate 10.

Nivelul de securitate 20

Nivelul 20 furnizează următoarele funcţii de securitate:

- Atât ID-ul utilizator, cât şi parola sunt necesare pentru semnare.
- Doar un responsabil cu securitatea sau cineva cu autorizare specială *SECADM poate crea profiluri de utilizator.
- Este impusă valoarea specificată în profilul de utilizator pentru limitarea capabilităţilor.

Implicit, la nivelul de securitate 20 toate profilurile sunt create cu autorizarea specială *ALLOBJ. De aceea, nivelul de securitate 20 **nu este recomandat** de IBM.

Trecerea la nivelul 20 de la nivelul 10

Când treceţi de la nivelul 10 la nivelul 20, este păstrat orice profil de utilizator care a fost creat automat în nivelul 10. Parola pentru fiecare profil utilizator care a fost creat la nivelul 10 este aceeaşi cu numele profilului de utilizator. Nu sunt făcute modificări asupra autorizărilor speciale din profilurile de utilizator.

Următoarea listă conţine activităţile recomandate dacă doriţi să treceţi de la nivelul 10 la nivelul 20 după ce sistemul dumneavoastră a fost pus în funcţiune:

- Listaţi toate profilurile de utilizator din sistem folosind comanda DSPAUTUSR (Display Authorized User - Afişare utilizator autorizat).
- Creaţi noi profiluri de utilizator, cu nume standardizate sau copiaţi profilurile existente şi daţi-le nume noi, standardizate.
- Setaţi parola să expire în fiecare profil existent, forţând fiecare utilizator să seteze o nouă parolă.
- Setaţi valorile de sistem pentru formatul parolei astfel încât să împiedicaţi utilizatorii să seteze parole triviale.
- Revedeţi valorile implicite în Tabela 143 din Anexa B pentru orice modificări pe care doriţi să le faceţi asupra profilurilor create automat la nivelul de securitate 10.

Trecerea la nivelul 20 de la un nivel mai înalt

Când treceţi de la un nivel de securitate mai înalt la nivelul 20, sunt adăugate autorizări speciale profilurilor de utilizator. Prin aceasta, utilizatorul are cel puţin autorizarea specială implicită pentru clasa de utilizator. Citiţi Tabela 2 la pagina 9 pentru a vedea cum diferă autorizările speciale între nivelul 20 şi nivelurile de securitate mai înalte.

Atenţie: Când treceţi la nivelul 20 de la un nivel de securitate mai înalt, sistemul adaugă autorizarea specială *ALLOBJ în toate profilurile utilizator. Aceasta permite utilizatorilor să vizualizeze, să modifice sau să şteargă orice obiect din sistem.

Nivelul de securitate 30

Nivelul 30 furnizează următoarele funcţii de securitate, în plus faţă de cele furnizate la nivelul 20:

- Utilizatorii trebuie să primească explicit autorizarea de a folosi resurse din sistem.
- Doar profilurile de utilizator create cu clasa de securitate *SECOFR primesc automat autorizarea specială *ALLOBJ.

Trecerea la nivelul 30 de la un nivel mai scăzut

Când treceţi la nivelul de securitate 30 de la un nivel de securitate mai scăzut, sistemul modifică toate profilurile de utilizator următoarea dată când realizaţi IPL. Sunt înlăturate autorizările speciale care au fost acordate utilizatorului la nivelul 10 sau 20, dar pe care utilizatorul nu trebuie să le aibă la nivelul 30 sau mai înalt. Autorizările speciale care au fost acordate utilizatorului şi care nu sunt asociate cu clasa lor de utilizator nu sunt modificate. De exemplu, autorizarea specială *ALLOBJ este înlăturată din toate profilurile de utilizator cu excepţia acelora cu clasa de utilizator *SECOFR. Vedeţi Tabela 2 la pagina 9 pentru o listă a autorizărilor speciale implicite şi a diferenţelor dintre nivelul 10 sau 20 şi nivelurile de securitate mai înalte.

Dacă sistemul dumneavoastră a rulat aplicaţii la un nivel de securitate scăzut, atunci ar trebui să setaţi şi să testaţi securitatea resurselor înainte de a trece la nivelul de securitate 30. Următoarea listă conţine activităţile recomandate:

- Pentru fiecare aplicaţie, setaţi autorizările corespunzătoare pentru obiectele de aplicaţie.
- Testaţi fiecare aplicaţie folosind fie profilurile de utilizator reale, fie profiluri de utilizator speciale, de testare:
  - Înlăturaţi autorizarea specială *ALLOBJ din profilurile de utilizator folosite pentru testare.
  - Acordaţi autorizări de aplicaţie corespunzătoare pentru profilurile de utilizator.
  - Rulaţi aplicaţia folosind profilurile de utilizator.
  - Verificaţi dacă există eşuări ale autorizării fie căutând mesaje de eroare, fie folosind jurnalul de auditare a securităţii.
- Când toate aplicaţiile rulează cu succes cu profilurile de testare, acordaţi autorizările corespunzătoare pentru obiectele de aplicaţie tuturor profilurilor de utilizator de producţie.
- Dacă valoarea de sistem QLMTSECOFR (limit security officer - limitare responsabil cu securitatea) este 1 (Da), utilizatorii cu autorizarea specială *ALLOBJ sau *SERVICE trebuie să fie anume autorizaţi asupra dispozitivelor la nivelul de securitate 30 sau mai înalt. Acordaţi acestor utilizatori autorizarea *CHANGE pentru dispozitivele selectate, acordaţi autorizarea QSECOFR *CHANGE dispozitivelor sau modificaţi valoarea de sistem QLMTSECOFR în 0.
- Modificaţi nivelul de securitate din sistemul dumneavoastră şi realizaţi IPL (initial program load - Încărcare iniţială de program).

Dacă doriţi să treceţi la nivelul 30 fără a defini autorizările fiecărui obiect, faceţi autorizarea publică pentru obiectele de aplicaţie destul de înaltă ca să ruleze aplicaţia. Faceţi testări ale aplicaţiilor pentru a vă asigura că nu au loc eşuări ale autorizărilor.

Notă: Vedeţi subiectul “Definirea modului în care pot fi accesate informaţiile” la pagina 110 pentru informaţii suplimentare despre autorizările de obiect.

Nivelul de securitate 40

Nivelul de securitate 40 previne riscurile potenţiale de integritate sau de securitate, cauzate de programe care pot trece peste măsurile de securitatea în anumite cazuri. Nivelul de securitate 50 furnizează protecţie îmbunătăţită a integrităţii pentru instalări cu cerinţe de securitate stricte. Tabela 3 la pagina 12 compară modul în care sunt suportate funcţiile de securitate la nivelurile 30, 40 şi 50. Aceste funcţii sunt explicate mai detaliat în secţiunile care urmează.

Tabela 3. Comparaţie a nivelurilor de securitate 30, 40 şi 50

Descriere scenariu	Nivel 30	Nivel 40	Nivel 50
Un program încearcă să acceseze obiecte folosind interfeţe care nu sunt suportate.	Intrare jurnal AF [1]	Intrare jurnal AF [1]; operaţia eşuează.	Intrare jurnal AF [1]; operaţia eşuează.
Un program încearcă să folosească o instrucţiune restricţionată.	Intrare jurnal AF [1]	Intrare jurnal AF [1]; operaţia eşuează.	Intrare jurnal AF [1]; operaţia eşuează.
Utilizatorul care a lansat un job nu are autorizare *USE asupra profilului de utilizator specificat în descrierea de job.	Intrare jurnal AF [1]	Intrare jurnal AF [1]; jobul nu rulează.	Intrare jurnal AF [1]; jobul nu rulează.
Un utilizator încearcă semnarea implicită fără ID utilizator şi parolă.	Intrare jurnal AF [1]	Intrare jurnal AF [1]; semnarea nu s-a făcut cu succes.	Intrare jurnal AF [1]; semnarea nu s-a făcut cu succes.
Un program în starea *USER încearcă să scrie în zona de sistem a discului, definită drept numai-citire sau fără acces.	Încercarea are succes.	Intrare jurnal AF; [1,2] operaţia eşuează. [2]	Intrare jurnal AF; [1,2] operaţia eşuează. [2]
Este făcută o încercare de a restaura un program care nu are o valoare de validare. [3]	Nu este făcută nici o validare. Programul trebuie să fie reinterpretat înainte de a putea fi folosit.	Nu este făcută nici o validare. Programul trebuie să fie reinterpretat înainte de a putea fi folosit.	Nu este făcută nici o validare. Programul trebuie să fie reinterpretat înainte de a putea fi folosit.
Este făcută o încercare de a restaura un program care are o valoare de validare.	Este făcută validarea programului.	Este făcută validarea programului.	Este făcută validarea programului.
Se încearcă modificarea spaţiului asociat unui program.	Încercarea are succes.	Intrare jurnal AF; [1,2] operaţia eşuează.[2]	Intrare jurnal AF; [1,2] operaţia eşuează.[2]
Se încearcă modificarea spaţiului de adresă al unui job.	Încercarea are succes.	Intrare jurnal AF; [1,2] operaţia eşuează.[2]	Intrare jurnal AF; [1,2] operaţia eşuează.[2]
Un program în stare utilizator încearcă să apeleze sau să transfere controlul unui program de domeniu sistem.	Încercarea are succes.	Intrare jurnal AF; [1,2] operaţia eşuează.[2]	Intrare jurnal AF; [1,2] operaţia eşuează.[2]
Este făcută o încercare de a crea un obiect de domeniu utilizator de tipul *USRSPC, *USRIDX sau *USRQ într-o bibliotecă ce nu este inclusă în valoarea de sistem QALWUSRDMN.	Operaţia eşuează.	Operaţia eşuează.	Operaţia eşuează.
Un program în starea utilizator trimite un mesaj de excepţie la un program în starea sistem care nu se află imediat deasupra lui în stiva de program.	Încercarea are succes.	Încercarea are succes.	Operaţia eşuează.
Un parametru este transmis unui program de domeniu utilizator care rulează în starea sistem.	Încercarea are succes.	Este făcută validarea parametrului.	Este făcută validarea parametrului.
O comandă livrată de IBM* este modificată să ruleze un alt program folosind comanda CHGCMD. Comanda este modificată din nou să ruleze programul original livrat de IBM, care este un program de domeniu sistem. Un utilizator încearcă să ruleze comanda.	Încercarea are succes.	Intrare jurnal AF; [1,2,4] operaţia eşuează.[2,4]	Intrare jurnal AF; [1,2,4] operaţia eşuează.[2,4]

1 Dacă funcţia de auditare este activă atunci este scrisă o intrare de tipul AF (authority failure - eşuare autorizare) în jurnalul de auditare (QAUDJRN). Vedeţi Capitolul 9 pentru informaţii suplimentare despre funcţiile de auditare.

2 Dacă procesorul suportă protecţie hardware îmbunătăţită a spaţiului de stocare.

3 Programele create înainte de Versiunea 1 Ediţia 3 nu au o valoare de validare.

4 Când modificaţi o comandă livrată de IBM, ea nu mai poate apela un program de domeniu sistem.

Dacă folosiţi funcţia de auditare la niveluri de securitate scăzute, sistemul înregistrează în istoric intrările de jurnal pentru majoritatea acţiunilor afişate în Tabela 3, cu excepţia acelora detectate de funcţia de protecţie îmbunătăţită hardware. Primiţi avertizări sub formă de intrări de jurnal în cazul potenţialelor violări ale integrităţii. La nivelul 40 sau mai înalt, violările de integritate determină sistemul să eşueze operaţia încercată.

Împiedicarea utilizării interfeţelor nesuportate

La nivelul de securitate 40 şi mai înalt, sistemul împiedică încercările de a apela direct programe de sistem care nu sunt înregistrate drept interfeţe de nivel de apelare. De exemplu, apelarea directă a programului de procesare a comenzii pentru comanda SIGNOFF eşuează.

Sistemul utilizează atributul de domeniu al unui obiect şi atributul de stare al unui program pentru a impune această protecţie:

- **Domeniu:**

  Fiecare obiect aparţine fie domeniului *SYSTEM, fie domeniului *USER. Obiectele de domeniu *SYSTEM pot fi accesate doar de programe în starea *SYSTEM sau de programe în starea *INHERIT care sunt apelate de programe în starea *SYSTEM.

  Puteţi afişa domeniul unui obiect folosind comanda DSPOBJD (Display Object Description - Afişare descriere obiect) şi specificând DETAIL(*FULL). Puteţi de asemenea utiliza următoarele comenzi:

  – DSPPGM (Display Program - Afişare program) pentru a afişa domeniul unui program
  – DSPSRVPGM (Display Service Program - Afişare program serviciu) pentru a afişa domeniul unui program serviciu

- **Stare:**

  Programele se află fie în starea *SYSTEM, fie în starea *INHERIT, fie în starea *USER. Programele în starea *USER pot accesa direct doar obiecte de domeniu *USER. Obiectele care sunt de domeniu *SYSTEM pot fi accesate folosind comanda corespunzătoaresau API-ul corespunzător (application programming interface - interfaţă de programare aplicaţie). Stările *SYSTEM şi *INHERIT sunt rezervate pentru programele livrate de IBM.

  Puteţi afişa starea unui program folosind comanda DSPPGM (Display Program - Afişare program). Puteţi afişa starea unui program serviciu folosind comanda DSPSRVPGM (Display Service Program - Afişare program serviciu).

Tabela 4 arată regulile de acces pentru domeniu şi stare:

Tabela 4. Accesul în funcţie de domeniu şi stare

	Domeniu obiect	
Starea program	***USER**	***SYSTEM**
*USER	YES	NO [1]
*SYSTEM	YES	YES

[1] O violare de domeniu sau de stare determină eşuarea operaţiei la nivelul de securitate 40 şi mai înalt. La toate nivelurile de securitate este scrisă o intrare de tipul AF în jurnalul de auditare dacă funcţia de auditare este activă.

Intrare jurnal:

Dacă funcţia de auditare este activă şi valoarea de sistem QAUDLVL include *PGMFAIL atunci o intrare AF (authority failure - eşuare autorizare), violare de tipul D, este scrisă în journalul QAUDJRN când este făcută o încercare de a folosi o interfaţă nesuportată.

Protecţia descrierilor de job

Dacă un nume de profil de utilizator este folosit drept valoare pentru câmpul *Utilizator* dintr-o descriere de job, atunci orice job lansat cu acea descriere de job poate fi rulat cu atribute luate din profilul de utilizator. Un utilizator neautorizat ar putea folosi o descriere de job pentru a viola securitatea prin lansarea unui job care să ruleze sub profilul de utilizator specificat în descrierea de job.

La nivelul de securitate 40 şi mai înalt, utilizatorul care lansează jobul trebuie să aibă autorizarea *USE atât pentru descrierea de job, cât şi pentru profilul de utilizator specificat în descrierea de job, altfel jobul eşuează. La nivelul de securitate 30, jobul rulează dacă cel care l-a lansat are autorizarea *USE pentru descrierea de job.

Intrare jurnal:

Dacă funcţia de auditare este activă şi valoarea de sistem QAUDLVL include *AUTFAIL, atunci în jurnalul QAUDJRN este scrisă o intrare AF, violare de tipul J, când un utilizator lansează un job şi nu este autorizat pentru profilul de utilizator dintr-o descriere de job.

Semnarea fără ID de utilizator şi parolă

La nivelul de securitate 30 şi mai scăzut, pentru anumite descrieri de subsistem este posibilă semnarea prin apăsarea tastei Enter fără un ID de utilizator şi parolă. La nivelul de securitate 40 şi mai înalt, sistemul opreşte orice încercare de semnarea fără ID de utilizator şi o parolă. Vedeţi subiectul “Descrierile de subsistem” la pagina 175 pentru informaţii suplimentare despre probleme privind securitatea asociate cu descrierile de subsistem.

Intrare jurnal:

În jurnalul QAUDJRN este scrisă o intrare AF, violare de tipul S, când un utilizator încearcă să semneze fără a introduce ID-ul de utilizator şi parola, iar descrierea de subsistem o permite. (Încercarea eşuează la nivelul de securitate 40 şi mai înalt.)

Protecţia hardware îmbunătăţită a spaţiului de stocare

Protecţia hardware îmbunătăţită a spaţiului de stocare permite ca blocurile de informaţii de sistem aflate pe disc să fie definite drept citire-scriere, numai-citire sau fără acces. La nivelul de securitate 40 şi mai înalt, sistemul controlează cum accesează programele în starea *USER aceste blocuri protejate. Acest suport nu este disponibil la nivelurile de securitate mai mici de 40.

Protecţia hardware îmbunătăţită a spaţiului de stocare este suportată pe toate modelele iSeries, *cu excepţia* următoarelor:

- Toate modelele B
- Toate modelele C
- Modelele D: 9402 D04, 9402 D06, 9404 D10 şi 9404 D20.

Intrare jurnal:

Dacă funcţia de auditare este activă şi valoarea de sistem QAUDLVL include *PGMFAIL, în journalul QAUDJRN este scrisă o intrare AF, violare de tipul R, atunci când un program încearcă să scrie într-o zonă a discului protejată de caracteristica de protecţie hardware îmbunătăţită a spaţiului de stocare. Acest suport este disponibil doar la nivelul de securitate 40 şi mai înalt.

Protecţia spaţiului asociat unui program

La nivelul de securitate 40 şi mai înalt, un program în starea utilizator nu poate modifica direct spaţiul asociat al unui obiect de program.

Protecţia spaţiului de adresă al unui job

La nivelul de securitate 50, un program în starea utilizator nu poate obţine adresa pentru un alt job din sistem. De aceea, un program în starea utilizator nu poate manevra direct obiecte asociate cu alt job.

Validarea parametrilor

Interfeţele pentru sistemul de operare sunt programe în starea sistem din domeniul utilizator. Cu alte cuvinte, ele sunt programe care pot fi apelate direct de un utilizator. Când parametrii sunt transmişi între programae în starea utilizator şi sistem, aceşti parametri trebuie să fie verificaţi pentru a împiedica orice valoare neaşteptată care ar periclita integritatea sistemului de operare.

Când vă rulaţi sistemul la nivelul de securitate 40 sau 50, sistemul verifică în mod specific toţi parametrii transmişi între un program în starea utilizator şi unul în starea sistem din domeniul utilizator. Această acţiune este necesară

pentru ca sistemul dumneavoastră să separe domeniul sistem de domeniul utilizator şi pentru a îndeplini cerinţele nivelului de securitate C2. Aţi putea observa un efect asupra performanţelor din cauza acestei verificări suplimentare.

Validarea programelor care sunt restaurate

Când este creat un program, sistemul iSeries calculează o valoare de validare care este memorată cu programul. Când un program este restaurat, valoarea de validare este calculată din nou şi comparată cu valoarea de validare care este memorată cu programul. Dacă valorile de validare nu sunt egale, acţiunile întreprinse de sistem sunt controlate de valorile de sistem QFRCCVNRST şi QALWOBJRST.

În plus faţă de valoarea de validare, un program ar putea avea opţional o semnătură digitală care poate fi verificată la restaurare. Orice acţiune a sistemului legată de semnăturile digitale este controlată de valorile de sistem QVFYOBJRST şi QFRCCVNRST. Cele trei valori de sistem, QVFYOBJRST (Verify Object on Restore - Verificare obiect la restaurare), QFRCCVNRST (Force Conversion on Restore - Forţare conversie la restaurare) şi QALWOBJRST (Allow Object Restore - Permitere restaurare obiect), acţionează ca o serie de filtre pentru a stabili dacă un program va fi restaurat fără modificări, dacă va fi creat din nou (convertit) la restaurare sau dacă nu va fi restaurat în sistem.

Primul filtru este valoarea de sistem QVFYOBJRST. Ea controlează operaţia de restaurare a unor obiecte care pot fi semnate digital. După ce un obiect este verificat cu succes şi este validat de această valoare de sistem, obiectul trece la al doilea filtru, valoarea de sistem QFRCCVNRST. Această valoare de sistem vă permite să specificaţi dacă să se convertească sau nu programe, programe serviciu sau obiecte modul în timpul unei operaţii de restaurare. Această valoare de sistem împiedică de asemenea anumite obiecte să fie restaurate. Doar când obiectele au trecut prin primele două filtre se trece la ultimul filtru, valoarea de sistem QALWOBJRST. Această valoare de sistem controlează dacă obiectele cu atribute sensibile la securitate pot fi sau nu restaurate.

Programele create pentru iSeries pot conţine informaţii care permit programului să fie creat din nou la restaurare, fără a fi necesară sursa programului. Programele create pentru iSeries Versiunea 5, Ediţia 1 şi mai recentă conţin informaţiile necesare pentru re-creare chiar şi când observabilitatea programului este înlăturată. Programele create pentru ediţii înainte de Versiunea 5, Ediţia 1 pot fi re-create la restaurare doar dacă informaţiile de observabilitate ale programului nu au fost şterse.

Fiecare dintre aceste valori de sistem este descrisă în Capitolul 3, ″ Valorile de sistem privind securitatea″, în secţiunea intitulată Valorile de sistem pentru restaurare referitoare la securitate.

Trecerea la nivelul de securitate 40

Asiguraţi-vă că toate aplicaţiile dumneavoastră rulează cu succes la nivelul de securitate 30 înainte de a migra la nivelul 40. Nivelul de securitate 30 vă oferă oportunitatea de a testa securitatea resurselor pentru toate aplicaţiile dumneavoastră. Folosiţi următoarea procedură pentru a migra la nivelul de securitate 40:

1. Activaţi funcţia de auditare a securităţii, dacă nu aţi făcut-o deja. Subiectul “Setarea auditării securităţii” la pagina 250 vă oferă instrucţiuni complete pentru setarea funcţiei de auditare.
2. Asiguraţi-vă că valoarea de sistem QAUDLVL include *AUTFAIL şi *PGMFAIL. *PGMFAIL înregistrează în istoric intrări jurnal pentru orice încercare de acces care violează protecţia integrităţii la nivelul de securitate 40.
3. Controlaţi jurnalul de auditare pentru intrări *AUTFAIL şi *PGMFAIL în timp ce rulaţi toate aplicaţiile dumneavoastră la nivelul de securitate 30. Fiţi în special atent la următoarele coduri motiv din intrările de tipul AF:

   B Violare de instrucţiune restricţionată (blocată)

   C Eşuare la validare obiect

   D Violare de interfaţă (domeniu) nesuportată

   J Eşuare autorizare descriere de job şi profil de utilizator

   R Încercare de accesare zonă protejată a discului (protecţie hardware îmbunătăţită a spaţiului de stocare)

   S Încercare de semnare implicită

   Aceste coduri indică prezenţa expunerilor integrităţii din aplicaţiile dumneavoastră. La nivelul de securitate 40, aceste programe eşuează.

4. Dacă aveţi programe care au fost create înainte de Versiunea 1 Ediţia 3, folosiţi comanda CHGPGM cu parametrul FRCCRT pentru a crea valori de validare pentru aceste programe. La nivelul de securitate 40, sistemul traduce orice program care este restaurat fără o valoare de validare. Aceasta poate creşte considerabil durata procesului de restaurare. Vedeţi subiectul “Validarea programelor care sunt restaurate” la pagina 15 pentru informaţii suplimentare despre validarea programelor.

   Notă: Restauraţi bibliotecile de program drept parte a testării dumneavoastră de aplicaţii. Controlaţi jurnalul de auditare pentru eşuări la validare.
5. Pe baza intrărilor din jurnalul de auditare, corectaţi-vă aplicaţiile şi împiedicaţi eşuările de program.
6. Modificaţi valoarea de sistem QSECURITY în 40 şi realizaţi un IPL.

Dezactivarea nivelului de securitate 40

După trecerea la nivelul de securitate 40, aţi putea descoperi că trebuie să vă întoarceţi temporar la nivelul 30. De exemplu, ar putea fi necesar să testaţi de eroari de integritate noile aplicaţii. Sau, aţi putea descoperi că nu aţi testat aplicaţiile destul de bine înainte de a trece la nivelul de securitate 40.

Puteţi trece de la nivelul de securitate 40 la nivelul 30 fără a vă periclita securitatea resurselor. Nu sunt făcute modificări asupra autorizărilor speciale din profilurile utilizator când treceţi de la nivelul 40 la nivelul 30. După ce v-aţi testat aplicaţiile şi aţi rezolvat orice eroare din jurnalul de auditare, vă puteţi întoarce la nivelul 40.

Atenţie: Dacă treceţi de la nivelul 40 la nivelul 20 atunci sunt adăugate unele autorizări speciale tuturor profilurilor utilizator. (Vedeţi Tabela 2 la pagina 9.) Aceasta înlătură protecţia de securitate a resurselor.

Nivelul de securitate 50

Nivelul de securitate 50 este proiectat pentru a asigura cerinţele definite de Departamentul Apărării al Statelor Unite pentru securitatea C2. El furnizează protecţie îmbunătăţită a integrităţii în plus faţă de cea furnizată de nivelul de securitate 40. Rularea sistemului dumneavoastră la nivelul de securitate 50 este necesară pentru securitatea C2. Alte cerinţe pentru securitatea C2 sunt descrise în cartea *Security - Enabling for C2*.

Aceste funcţii de securitate sunt incluse pentru nivelul de securitate 50. Ele sunt descrise în subiectele care urmează:

- Restricţionarea tipurilor de obiecte de domeniu utilizator (*USRSPC, *USRIDX şi *USRQ)
- Restricţionarea tratării mesajelor între programe în starea utilizator şi sistem
- Împiedicarea modificării tuturor blocurilor de control interne

Restricţionarea obiectelor de domeniu utilizator

Majoritatea obiectelor este creată în domeniul sistem. Când rulaţi sistemul dumneavoastră la nivelul de securitate 40 sau 50, obiectele de domeniu sistem pot fi accesate doar prin folosirea comenzilor şi API-urilor furnizate.

Aceste tipuri de obiecte pot fi fie domeniu sistem, fie domeniu utilizator:

- Spaţiu utilizator (*USRSPC)
- Index utilizator (*USRIDX)
- Coadă utilizator (*USRQ)

Obiectele de tipul *USRSPC, *USRIDX şi *USRQ din il utilizator pot fi manevrate direct fără folosirea API-urilor şi comenzilor furnizate de sistem. Aceasta permite unui utilizator să acceseze un obiect fără a crea o înregistrare de auditare.

Notă: Obiectele de tipul *PGM, *SRVPGM şi *SQLPKG se pot afla de asemenea în domeniul utilizator. Conţinutul lor nu poate fi manevrat direct şi ele nu sunt afectate de restricţii.

La nivelul de securitate 50, unui utilizator nu trebuie să i se permită să transmită informaţii relevante de securitate la un alt utilizator fără abilitatea de a trimite o înregistrare de auditare. Pentru a impune aceasta:

- La nivelul de securitate 50, nici un job nu poate poate obţine adresabilitate către biblioteca QTEMP pentru un alt job. De aceea, dacă în biblioteca QTEMP sunt memorate obiecte de domeniu utilizator, atunci ele nu pot fi folosite pentru a transmite informaţii către un alt utilizator.
- Pentru a furniza compatibilitate cu aplicaţiile existente care utilizează obiecte de domeniu utilizator, puteţi specifica biblioteci suplimentare în valoarea de sistem QALWUSRDMN. Valoarea de sistem QALWUSRDMN este impusă la toate nivelurile de securitate. Vedeţi “Permiterea obiectelor din domeniul de utilizator (QALWUSRDMN)” la pagina 21 pentru informaţii suplimentare.

Restricţionarea tratării mesajelor

Mesajele trimise între programe furnizează un potenţial de expunere a integrităţii. Următoarele se aplică tratării mesajelor la nivelul de securitate 50:

- Orice program în starea utilizator poate trimite un mesaj de orice tip către orice alt program în starea utilizator.
- Orice program în starea sistem poate trimite un mesaj de orice tip către orice program în starea utilizator sau sistem.
- Un program în starea utilizator poate trimite un mesaj non-excepţie către orice program în starea sistem.
- Un program în starea utilizator poate trimite un mesaj de tip excepţie (stare, notificare sau ieşire) către un program în starea sistem dacă una din următoarele afirmaţii este adevărată:
  - Programul în starea sistem este un procesor de cerere.
  - Programul în starea sistem a apelat un program în starea utilizator.

    Notă: Programul în starea utilizator care trimite mesajul de excepţie nu trebuie să fie programul apelat de programul în starea sistem. De exemplu, în această stivă de programe, un mesaj de excepţie poate fi trimis către programul A de către programul B, C sau D:

Programul A	Starea sistem
Programul B	Starea utilizator
Programul C	Starea utilizator
Programul D	Starea utilizator

- Când un program în starea utilizator primeşte un mesaj de la o sursă externă (*EXT) sunt înlăturaţi toţi pointer-ii din textul de înlocuire al mesajului.

Împiedicarea modificării blocurilor de control interne

La nivelul de securitate 40 şi mai înalt, unele blocuri de control interne, cum ar fi blocul de control funcţionare, pot fi modificate de un program în starea utilizator.

La nivelul de securitate 50, nu poate fi modificat nici un bloc de control intern. Aceasta include blocurile de control ODP (open data path - cale de date deschisă), de spaţii pentru comenzi şi programe CL şi de job de mediul S/36.

Trecerea la nivelul de securitate 50

Majoritatea măsurilor de securitate suplimentare care sunt impuse la nivelul de securitate 50 nu cauzează intrărilor jurnal de auditare de la nivelurile de securitate scăzute. De aceea, o aplicaţie nu poate fi testată pentru toate condiţiile posibile de eroare de integritate înainte de trecerea la nivelul de securitate 50.

Acţiunile care pot cauza erori la nivelul de securitate 50 sunt neobişnuite în software-ul de aplicaţii normal. Majoritatea software-ului care rulează cu succes la nivelul de securitate 40 rulează de asemenea şi la nivelul de securitate 50.

Dacă rulaţi sistemul dumneavoastră la nivelul de securitate 30, efectuaţi paşii descrişi în “Trecerea la nivelul de securitate 40” la pagina 15 pentru a pregăti sistemul pentru trecerea la nivelul de securitate 50.

Dacă rulaţi sistemul dumneavoastră la nivelul de securitate 30 sau 40, faceţi următoarele pentru a pregăti sistemul pentru nivelul de securitate 50:

- Evaluaţi setarea valorii sistem QALWUSRDMN. Controlarea obiectelor de domeniu utilizator este importantă pentru integritatea sistemului. Vedeţi “Restricţionarea obiectelor de domeniu utilizator” la pagina 16.

- Recompilaţi toate programele COBOL care alocă dispozitivul din clauza SELECT unei STAŢII DE LUCRU dacă programele COBOL au fost compilate folosind un compilator anterior versiunii V2R3.
- Recompilaţi toate programele COBOL de mediu S/36 care au fost compilate folosind un compilator anterior versiunii V2R3.
- Recompilaţi toate programele RPG* de mediu RPG/400* sau System/38 care folosesc fişiere de afişare dacă au fost compilate folosind un compilator anterior versiunii V2R3.

Puteţi trece direct de la nivelul de securitate 30 la nivelul de securitate 50. Rularea la nivelul de securitate 40 drept un pas intermediar nu furnizează avantaje semnificative pentru testare.

Dacă rulaţi la nivelul de securitate 40, puteţi trece la nivelul de securitate 50 fără testări suplimentare. Nivelul de securitate 50 nu poate fi testat în avans. Protecţia de integritate suplimentară care este impusă la nivelul de securitate 50 nu produce mesaje de eroare sau intrări jurnal la nivelurile scăzute de securitate.

Dezactivarea nivelului de securitate 50

După trecerea la nivelul de securitate 50, aţi putea descoperi că trebuie să vă întoarceţi temporar la nivelul de securitate 30 sau 40. De exemplu, ar putea fi necesar să testaţi de eroari de integritate noile aplicaţii. Sau, aţi putea descoperi probleme de integritate care nu au apărut la nivelurile scăzute de securitate.

Puteţi trece de la nivelul de securitate 50 la nivelul 30 sau 40 fără a vă periclita securitatea resurselor. Nu sunt făcute modificări asupra autorizărilor speciale din profilurile utilizator când treceţi de la nivelul 50 la nivelul 30 sau 40. După ce v-aţi testat aplicaţiile şi aţi rezolvat orice eroare din jurnalul de auditare, vă puteţi întoarce la nivelul 50.

Atenţie: Dacă treceţi de la nivelul 50 la nivelul 20 atunci sunt adăugate unele autorizări speciale tuturor profilurilor utilizator. Aceasta înlătură protecţia de securitate a resurselor. (Vedeţi Tabela 2 la pagina 9.)

Capitolul 3. Valorile de sistem privind securitatea

Acest capitol descrie valorile de sistem care controlează securitatea în sistemul. Valorile de sistem vă permit să personalizaţi multe dintre caracteristicile sistemului dumneavoastră. Pentru a defini setările de securitate ale întregului sistem, se utilizează un grup de valori de sistem.

Puteţi împiedica utilizatorii să modifice valorile de sistem referitoare la securitate. SST (system service tools - unelte de service sistem) şi DST (dedicated service tools - unelte de service dedicate) furnizează o opţiune de a bloca aceste valori de sistem. Prin blocarea valorilor de sistem puteţi împiedica chiar şi un utilizator cu autorizare *SECADM şi *ALLOBJ să modifice aceste valori de sistem cu comanda CHGSYSVAL. În plus faţă de restricţionarea modificărilor asupra acestor de valori de sistem, puteţi restricţiona adăugarea de certificate digitale în depozitul de certificate digitale cu API-ul Add Verifier şi puteţi restricţiona resetarea parolei pentru depozitul de certificate digitale.

Notă: Dacă blocaţi valorile de sistem referitoare la securitate şi este nevoie să executaţi o operaţie de restaurare ca parte a unei restaurări de sistem, fiţi atent că trebuie să deblocaţi valorile de sistem pentru a efectua operaţia de restaurare. Aceasta asigură faptul că valorile de sistem pot fi modificate în timpul IPL-ului.

Următoarele valori de sistem pot fi restricţionate prin utilizarea opţiunii de blocare:

Tabela 5. Valorile de sistem care pot fi blocate

QALWOBJRST	QAUTORMT	QINACTMSGQ	QPWDLMTREP	QRETSVRSEC
QALWUSRDMN	QAUTOVRT	QLMTDEVSSN	QPWDLVL	QRMTSIGN
QAUDCTL	QCRTAUT	QLMTSECOFR	QPWDMAXLEN	QRMTSRVATR
QAUDENACN	QCRTOBJAUD	QMAXSGNACN	QPWDMINLEN	QSECURITY
QAUDFRCLVL	QDEVRCYACN	QMAXSIGN	QPWDPOSDIF	QSHRMEMCTL
QAUDLVL	QDSPSGNINF	QPWDEXPITV	QPWDRQDDGT	QUSEADPAUT
QAUDLVL2	QDSCJOBITV	QPWDLMTAJC	QPWDRQDDIF	QVFYOBJRST
QAUTOCFG	QFRCCVNRST	QPWDLMTCHR	QPWDVLDPGM	QSCANFS
QSCANFSCTL				

Puteţi folosi SST (system service tools - unelte de service sistem) sau DST (dedicated service tools - unelte de service dedicate) pentru a bloca sau debloca valorile de sistem referitoare la securitate. Însă trebuie să folosiţi DST dacă vă aflaţi în modul de recuperare, deoarece SST este indisponibil în timpul acestui mod. Altfel, utilizaţi SST pentru a bloca sau de bloca valorile de sistem referitoare la securitate.

Pentru a bloca sau debloca valorile de sistem referitoare la securitate cu comanda STRSST (Start System Service Tools - Pornire unelte de service sistem), urmaţi aceşti paşi:

Notă: Trebuie să aveţi un profil utilizator de unelte de service şi o parolă pentru a bloca sau debloca valorile de sistem referitoare la securitate.

1. Deschideţi o interfaţă bazată pe caractere.
2. În linia de comandă, tastaţi STRSST.
3. Introduceţi numele de utilizator de unelte de service şi parola.
4. Selectaţi opţiunea 7 (Gestionare securitate sistem).
5. Tastaţi 1 pentru a debloca valorile de sistem referitoare la securitate sau 2 pentru a bloca valorile de sistem referitoare la securitate în parametrul *Permitere modificări de securitate asupra valorilor de sistem*.

Pentru a bloca sau debloca valorile de sistem referitoare la securitate folosind DST (dedicated service tools - unelte de service dedicate) în timpul unui IPL supravegheat al unei recuperări de sistem, urmaţi aceşti paşi:

1. În ecranul IPL sau instalare sistem, selectaţi opţiunea 3 (Utilizare unelte de service dedicate).

   Notă: Acest pas presupune că vă aflaţi în modul de recuperare şi efectuaţi un IPL supravegheat.
2. Semnaţi pentru DST utilizând numele dumneavoastră de utilizator de unelte de service şi parola.
3. Selectaţi opţiunea 13 (Gestionare securitate sistem).
4. Tastaţi 1 pentru a debloca valorile de sistem referitoare la securitate sau 2 pentru a bloca valorile de sistem referitoare la securitate în parametrul *Permitere modificări de securitate asupra valorilor de sistem*.

Secţiunile următoare discută anumite valori de sistem de securitate. Pentru informaţii despre valorile de sistem referitoare la securitate pe care le puteţi bloca, vedeţi secţiunea lor corespondentă:

- Valorile de sistem generale pentru securitate
- Valorile de sistem referitoare la securitate
- Valorile de sistem pentru restaurare referitoare la securitate
- Valorile de sistem pentru parole
- Valorile de sistem pentru controlul auditării

Valorile de sistem generale pentru securitate

Privire generală:

Scop: Specifică valorile de sistem care controlează securitatea din sistem.

Cum se face:
WRKSYSVAL *SEC (comanda Gestionare valori de sistem)

Autorizare:
*ALLOBJ şi *SECADM

Intrare jurnal:
SV

Notă: Modificările devin efective imediat. IPL-ul este necesar doar la schimbarea nivelului de securitate (valoarea de sistem QSECURITY) sau a nivelului de parolă (valoarea de sistem QPWDLVL).

Următoarele valori de sistem generale controlează securitatea în sistemul dumneavoastră:

QALWUSRDMN
Permitere obiecte de domeniu utilizator în biblioteci

QCRTAUT
Creare autorizare publică implicită

QDSPSGNINF
Afişare informaţii de semnare

QFRCCVNRST
Forţare conversie la restaurare

QINACTITV
Interval de timeout job inactiv

QINACTMSGQ
Coadă de mesaje job inactiv

QLMTDEVSSN
Limitare sesiuni dispozitiv

QLMTSECOFR
Limitare responsabil cu securitatea

QMAXSIGN
Număr maxim de încercări de semnare

QMAXSGNACN
Acţiune la depăşirea numărului maxim de încercări de semnare

QRETSVRSEC
Păstrare securitate server

QRMTSIGN
Cereri de semnare la distanţă

QSCANFS
Scanare sisteme de fişiere

QSCANFSCTL
Control scanare sisteme de fişiere

QSECURITY
Nivel de securitate

QSHRMEMCTL
Control memorie partajată

QUSEADPAUT
Utilizare autorizare adoptată

QVFYOBJRST
Verificare obiect la restaurare

În continuare sunt prezentate aceste valori de sistem. Sunt afişate opţiunile posibile. Opţiunile care sunt subliniate sunt valorile implicite ale sistemului. Pentru majoritatea valorilor de sistem este afişată o opţiune recomandată.

Permiterea obiectelor din domeniul de utilizator (QALWUSRDMN)

Valoarea de sistem QALWUSRDMN specifică căror biblioteci le este permis să conţină obiecte din domeniul de utilizator de tipul *USRSPC, *USRIDX şi *USRQ. Restricţia nu se aplică obiectelor din domeniul de utilizator de tipul *PGM, *SRVPGM şi *SQLPKG. Sistemele cu cerinţe de securitate mari necesită restricţionarea obiectelor de utilizator *USRSPC, *USRIDX şi *USRQ. Sistemul nu poate audita transferul de informaţii către şi de la obiectele din domeniul de utilizator.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 6. Valorile posibile pentru valoarea de sistem QALWUSRDMN:

***ALL**	Obiectele de domeniu utilizator sunt permise în toate bibliotecile şi directoarele din sistem.
***DIR**	Obiectele de domeniu utilizator sunt permise în toate directoarele din sistem.
nume-bibliotecă	Numele a până la 50 de biblioteci care pot conţine obiecte de domeniu utilizator de tipul *USRSPC, *USRIDX şi *USRQ. Dacă sunt afişate biblioteci individuale, atunci biblioteca QTEMP *trebuie* să fie inclusă în listă.

Valoare recomandată: Pentru majoritatea sistemelor, valoarea recomandată este *ALL. Dacă sistemul dumneavoastră are cerinţe de securitate mari, ar trebui să permiteţi obiecte de domeniu utilizator doar în biblioteca QTEMP. La nivelul de securitate 50, biblioteca QTEMP este un obiect temporar şi nu poate fi utilizat pentru a trasmite date confidenţiale între utilizatori.

Unele sisteme au software de aplicaţie care se bazează pe tipurile de obiecte *USRSPC, *USRIDX sau *USRQ. Pentru aceste sisteme, lista de biblioteci pentru valoarea de sistem QALWUSRDMN ar trebui să includă bibliotecile care sunt utilizate de software-ul de aplicaţie. Autorizarea publică a oricărei biblioteci din QALWUSRDMN, cu excepţia QTEMP, ar trebui setată la *EXCLUDE. În acest fel se limitează numărul utilizatorilor care pot folosi interfaţa MI (care nu poate fi auditată) pentru a citi sau modifica datele obiectelor din domeniul de utilizator aflate în aceste biblioteci.

Notă: Dacă rulaţi comanda RCLSTG (Reclaim Storage - pretindere spaţiu de stocare), obiectele de domeniu utilizator ar putea necesita să fie mutate în şi din biblioteca QRCL (reclaim storage - pretindere spaţiu de stocare). Pentru a rula cu succes comanda RCLSTG, ar trebui să adăugaţi biblioteca QRCL la valoarea de sistem QALWUSRDMN. Pentru a proteja securitatea de sistem, setaţi autorizarea publică pentru biblioteca QRCL la *EXCLUDE. Înlăturaţi biblioteca QRCL din valoarea de sistem QALWUSRDMN când aţi terminat de rulat comanda RCLSTG.

Autorizarea pentru noile obiecte (QCRTAUT)

Valoarea de sistem QCRTAUT este utilizată pentru a stabili autorizarea publică pentru un obiect nou creat dacă sunt îndeplinite următoarele condiţii:

- Valoarea Creare autorizare (CRTAUT) pentru biblioteca noului obiect este setată la *SYSVAL.
- Noul obiect este creat având autorizarea publică (AUT) setată la *LIBCRTAUT.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 7. Valorile posibile pentru valoarea de sistem QCRTAUT:

***CHANGE**	Utilizatorul public poate modifica obiectele nou create.
***USE**	Utilizatorul public poate vizualiza, dar nu poate modifica obiectele nou create.
***ALL**	Utilizatorul public poate executa orice funcţie cu obiectele noi.
***EXCLUDE**	Utilizatorul public nu are permisiunea de a utiliza obiecte noi.

Valoare recomandată:
*CHANGE

Valoarea de sistem QCRTAUT nu este folosită pentru obiecte create în directoare din sistemul de fişiere îmbunătăţit.

Atenţie: Mai multe biblioteci livrate de IBM, cum ar fi QSYS, au valoarea CRTAUT setată la *SYSVAL. Dacă modificaţi valoarea de sistem QCRTAUT în altceva decât *CHANGE, aţi putea avea probleme la semnarea la dispozitive noi sau create automat. Pentru a evita aceste probleme când modificaţi QCRTAUT în altceva decât *CHANGE, trebuie să vă asiguraţi că toate descrierile de dispozitiv şi cozile lor de mesaje asociate au autorizarea PUBLIC setată la *CHANGE. Un mod de a face aceasta este de a modifica valoarea CRTAUT pentru biblioteca QSYS în *CHANGE din *SYSVAL.

Afişarea informaţiilor de semnare (QDSPSGNINF)

Valoarea de sistem QDSPSGNINF stabileşte dacă după semnare este afişat ecranul Informaţii semnare. Ecranul Informaţii semnare afişează:

- Data ultimei semnări
- Orice încercare de semnare care nu a fost validă
- Numărul de zile până când mai expiră parola (dacă parola trebuie să expire în 7 zile sau mai puţin)

```
                          Sign-on Information
                                                                 System:
Previous sign-on . . . . . . . . . . . . . :   10/30/91  14:15:00

Sign-on attempts not valid . . . . . . . . :   3

Days until password expires  . . . . . . . :   5
```

| **Notă:** Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind
| securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de
| securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 8. Valorile posibile pentru valoarea de sistem QDSPSGNINF:

0	Ecranul nu este afişat.
1	Ecranul este afişat.

Valoare recomandată: Este recomandată opţiunea 1 (Ecranul este afişat), pentru ca utilizatorii să poată monitoriza încercările de utilizare a profilului lor şi să ştie când este necesară o nouă parolă.

Notă: Afişarea informaţiilor de semnare poate fi de asemenea specificată în profilurile de utilizator individuale.

Intervalul de timeout pentru job inactiv (QINACTITV)

Valoarea de sistem QINACTITV specifică în minute cât timp permite sistemul unui job să fie inactiv înainte de a executa o acţiune. O staţie de lucru este considerată inactivă dacă aşteaptă într-un meniu sau ecran sau dacă aşteaptă intrare de mesaj fără interacţiunea utilizatorului. Câteva exemple de interacţiune a utilizatorului sunt:

- Utilizarea tastei Enter
- Utilizarea funcţiei de derulare pagină
- Utilizarea tastelor funcţionale
- Utilizarea tastei Ajutor

Sunt incluse sesiunile de emulare prin iSeries Access. Joburile locale care sunt semnate pe un sistem la distanţă sunt excluse. Joburile care sunt conectate prin FTP (file transfer protocol - protocol de transfer de fişiere) sunt excluse. Înainte de Versiunea 4, Ediţia 2, erau excluse şi joburile Telnet. Pentru a controla timeout-ul conexiunilor FTP, modificaţi parametrul INACTTIMO din comanda CHGFTPA (Change FTP Attribute - Modificare atribut FTP). Pentru a controla timeout-ul sesiunilor Telnet mai vechi de V4R2, utilizaţi comanda CHGTELNA (Change Telnet Attribute - Modificare atribut Telnet).

Următoarele exemple arată cum stabileşte sistemul ce joburi sunt inactive:

- Un utilizator foloseşte funcţia de cerere sistem pentru a porni un al doilea job interactiv. O interacţiune cu sistemul, cum ar fi tasta Enter, în oricare dintre joburi, face ca ambele joburi să fie marcate drept active.
- Un job iSeries Access ar putea să apară ca inactiv pentru sistem dacă utilizatorul execută funcţii PC, cum ar fi editarea unui document fără a interacţiona cu sistemul iSeries.

Valoarea de sistem QINACTMSGQ determină ce acţiune execută sistemul când jobul inactiv depăşeşte intervalul specificat.

Când este pornit, sistemul verifică existenţa joburilor inactive în intervalul specificat de valoarea de sistem QINACTITV. De exemplu, dacă sistemul este pornit la 9:46 dimineaţa şi valoarea de sistem QINACTITV este de 30 de minute, el verifică existenţa joburilor inactive la 10:16, 10:46, 11:16 şi aşa mai departe. Dacă descoperă un job care a fost inactiv 30 de minute sau mai mult, sistemul execută acţiunea specificată de valoarea de sistem QINACTMSGQ. În acest exemplu, dacă un job devine inactiv la 10:17, el nu va fi accesat până la 11:16. La verificarea de la 10:46, a fost inactiv timp de 29 de minute.

Valorile de sistem QINACTITV şi QINACTMSGQ asigură securitatea împiedicând utilizatorii să lase semnate staţii de lucru inactive. O staţie de lucru inactivă ar putea permite unei persoane neautorizate să acceseze sistemul.

Tabela 9. Valorile posibile pentru valoarea de sistem QINACTITV:

***NONE:**	Sistemul nu verifică dacă există joburi inactive.
interval-în-minute	Specificaţi o valoare între 5 şi 300. Când un job a fost inactiv pentru acel număr de minute, sistemul execută acţiunea specificată în QINACTMSGQ.

Valoare recomandată: 60 de minute.

Coada de mesaje pentru timeout-ul de job inactiv (QINACTMSGQ)

Valoarea de sistem QINACTMSGQ specifică ce acţiune execută sistemul când intervalul de timeout al jobului inactiv a fost depăşit.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 10. Valorile posibile pentru valoarea de sistem QINACTMSGQ:

***ENDJOB**	Joburile inactive sunt oprite. Dacă jobul inactiv este un job de grup,[1] atunci toate joburile asociate cu grupul sunt de asemenea oprite. Dacă jobul este o parte a unui job secundar, [1] atunci ambele joburi sunt oprite. Acţiunea executată de *ENDJOB este echivalentă cu rularea comenzii ENDJOB JOB(nume) OPTION (*IMMED) ADLINTJOBS(*ALL) pentru jobul inactiv.
***DSCJOB**	Jobul inactiv este deconectat, la fel şi eventualele joburi secundare sau joburi de grup[1] asociate cu el. Valoarea de sistem QDSCJOBITV (disconnected job time-out interval - interval de timeout al jobului deconectat) controlează dacă sistemul, la sfârşit, termină joburile deconectate. Vedeţi “Intervalul de timeout pentru job deconectat (QDSCJOBITV)” la pagina 33 pentru informaţii suplimentare. **Atenţie:** Sistemul nu poate deconecta unele joburi, cum ar fi PC Organizer şi funcţia PCTA (PC text-assist - Asistent text PC). Dacă sistemul nu poate deconecta un job inactiv, el termină jobul respectiv.
nume-coadă-de-mesaje	Mesajul CPI1126 este trimis cozii de mesaje specificate când este atins intervalul de timeout pentru job inactiv. Aceste mesaj anunţă că: Jobul &3/&2/&1; nu a fost activ. Coada de mesaje trebuie să existe înainte să poată să fie specificată pentru valoarea de sistem QINACTMSGQ. Această coadă de mesaje este curăţată automat în timpul unui IPL. Dacă asignaţi QINACTMSGQ drept coada de mesaje a utilizatorului, toate mesajele din coada de mesaje sunt pierdute în timpul unui IPL.

[1] Cartea *Work Management* descrie joburile grup şi joburile secundare.

Valoare recomandată: *DSCJOB doar dacă utilizatorii dumneavoastră rulează joburile iSeries Access. Folosirea *DSCJOB atunci când unele joburi iSeries Access rulează, este echivalentă cu terminarea joburilor. Poate cauza pierderi semnificative de informaţii. Folosiţi opţiunea *coadă-mesaje* dacă aveţi programul licenţiat iSeries. Cartea *CL Programming* arată un exemplu de scriere a unui program pentru a trata mesajele.

Folosirea unei Cozi de mesaje: Un utilizator sau un program poate monitoriza coada de mesaje şi să acţioneze după cum este necesar, precum terminarea jobului sau trimiterea unui mesaj de avertisment utilizatorului. Folosirea unei cozi de mesaje vă permite să luaţi decizii în legătură cu anumite dispozitive şi profiluri de utilizator, în loc să trateze toate dispozitivele inactive în acelaşi fel. Această metodă este recomandată când folosiţi programul licenţiat iSeries Access.

Dacă o staţie de lucru cu 2 joburi secundare este activă, cele 2 mesaje sunt unul pentru fiecare job). Un utilizator sau program poate folosi comanda ENDJOB (End Job - Terminare job) pentru a termina unui sau ambele joburi secundare. Dacă un job inactiv are unul sau mai multe joburi grup, un singur mesaj este trimis spre coada de mesaje. Mesajele continuă să fie trimise spre coada de mesaje pentru fiecare interval în care jobul este inactiv.

Limitarea sesiunilor de dispozitiv (QLMTDEVSSN)

Valoarea de sistem QLMTDEVSSN specifică dacă un utilizator are permisiunea să semneze pe mai multe dispozitive în acelaşi timp. Această valoare nu restricţionează meniul Cerere sistem sau o a doua semnare de pe acelaşi dispozitiv. Dacă un utilizator are un job deconectat, utilizatorul are permisiunea să semneze pe sistem cu o nouă sesiune de dispozitiv.

| **Notă:** Această valoare de sistem este o valoarea restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind
| securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de
| securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 11. Valorile posibile pentru valoarea de sistem QLMTDEVSSN:

0	Sistemul permite un număr nelimitat de sesiuni de semnare.
1	Utilizatorii au limită de o singură sesiune dispozitiv.

Valoare recomandată: 1 (Da) pentru că limitarea utilizatorilor la un singur dispozitiv reduce asemănarea parolelor de partajare şi lăsarea dispozitivelor nesupravegheate.

Notă: Limitarea sesiunilor dispozitiv poate fi de asemenea specificată şi în profiluri utilizator individuale.

Limitarea responsabilului cu securitatea (QLMTSECOFR)

Valoarea de sistem QLMTSECOFR controlează dacă un utilizator cu autorizarea specială pentru toate obiectele (*ALLOBJ) sau service (*SERVICE) poate semna pe orice staţie de lucru. Limitarea profilurilor de utilizator puternic la anumite staţii de lucru bine controlate furnizează protecţie prin securitate.

Valorea sistem QLMTSECOFR este forţată doar de la nivelul de securitate 30 în sus. “Staţii de lucru” la pagina 171 furnizează mai multe informaţii despre autorizarea necesară pentru semnarea la o staţie de lucru.

Puteţi întotdeauna să semnaţi la consolă cu profilurile QSECOFR, QSRV şi QSRVBAS, indiferent de modul în care este setată valoarea QLMTSECOFR.

| **Notă:** Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind
| securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de
| securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 12. Valorile posibile pentru valoarea de sistem QLMTSECOFR:

1	Un utilizator cu autorizarea specială *ALLOBJ sau *SERVICE poate semna la o staţie de afişare doar dacă este autorizat în mod specific (dacă are autorizarea *CHANGE) la staţia de afişare sau dacă profilul de utilizator QSECOFR este autorizat (are autorizarea *CHANGE) la staţia de afişare. Această autorizare nu poate veni de la autorizarea publică.
0	Utilizatorii cu autorizarea specială *ALLOBJ sau *SERVICE pot semna pe orice staţie de afişare pentru care au autorizarea *CHANGE. Ei pot primi autorizarea *CHANGE prin autorizare privată sau publică sau pentru că au autorizarea specială *ALLOBJ.

Valoare recomandată: 1 (Da).

Numărul maxim de încercări de semnare (QMAXSIGN)

Valoarea de sistem QMAXSIGN controlează numărul de încercări consecutive de semnare care nu sunt corectate de utilizătorii locali şi de la distanţă. Încecările de semnare incorecte pot fi cauzate de un ID de utilizator care nu este corect, o parolă care nu este corectă sau de autorizare inadecvată pentru a folosi staţia de lucru.

Când este atins numărul maxim de încercări de semnare, valoarea de sistem QMAXSGNACN este folosită pentru a determina acţiunea ce trebuie făcută. Un mesaj este trimis la coada de mesaje QSYSOPR (şi coada de mesaje QSYSMSG dacă există în biblioteca QSYS) pentru a anunţa responsabilul cu securitatea de un posibil intrus.

Dacă creaţi coada de mesaje QSYSMSG în biblioteca QSYS, mesajele despre evenimentele de sistem critice sunt trimise la acea coadă de mesaje la fel ca şi QSYSOPR. Coada de mesaje QSYSMSG poate fi monitorizată separat de un program sau un operator de sistem. Aceasta furnizează protecţie suplimentară pentru resursele dumneavoastră sistem. Mesajele de sistem critice din QSYSOPR sunt câteodată omise din cauza volumului de mesaje trimise la acea coadă de mesaje.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 13. Valorile posibile pentru valoarea de sistem QMAXSIGN:

3	Un utilizator poate încerca să semneze de maxim 3 ori.
***NOMAX**	Sistemul permite un număr nelimitat de încercări de semnare incorecte. Aceasta permite unui potenţial intrus oportunităţi nelimitate de a ghici o combinaţie de ID al unui utilizator valid şi parola.
limită	Specificaţi o valoare între 1 şi 25. Numărul recomandat de încercări de semnare este de trei. De obicei, trei încercări sunt de ajuns pentru a corecta erorile de tastare, numărul fiind destul de mic pentru a ajuta la prevenirea accesului neautorizat.

Valoare recomandată: 3.

Acţiunea când este depăşit numărul maxim de încercări de semnare (QMAXSGNACN)

Valoarea de sistem QMAXSGNACN determină ce face sistemul când este atins numărul maxim de încercări de semnare la o staţie de lucru.

Notă: Valoarea de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 14. Valorile posibile pentru valoarea de sistem QMAXSGNACN:

3	Dezactivaţi profilul de utilizator şi dispozitivul.
1	Dezactivaţi doar dispozitivul.
2	Dezactivaţi doar profilul de utilizator.

Sistemul dezactivează un dispozitiv dezactivându-l. Dispozitivul este dezactivat dacă încercările de semnare care nu sunt valide sunt consecutive pe acelaşi dispozitiv. O semnare validă resetează numărarea de încercări de semnare incorecte pentru dispozitiv.

Sistemul dezactivează un profil de utilizator modificând parametrul *Status* pe *DISABLED. Profilul utilizatorului este dezactivat când numărul de încercări de semnare incorecte atinge valoarea din valoarea de sistem QMAXSIGN, indiferent dacă încercările de semnare incorecte au fost de la aceleaşi dispozitive sau de la dispozitive diferite. O semnare validă resetează numărul de încercări de semnare incorecte din profilul utilizatorului.

Dacă creaţi coada de mesaje QSYSMSG în QSYS, mesajul trimis (CPF1397) conţine numele utilizatorului şi dispozitivului. De aceea, este posibil să controlaţi dezactivarea dispozitivului bazându-vă pe dispozitivul ce este folosit.

“Numărul maxim de încercări de semnare (QMAXSIGN)” la pagina 25 furnizează informaţii suplimentare despre coada de mesaje QSYSMSG.

Dacă profilul QSECOFR este dezactivat, puteţi să semnaţi cu QSECOFR la consolă şi să activaţi profilul. Dacă este dezactivată consola şi nici un alt utilizator n-o poate activa, trebuie să executaţi un IPL de sistem pentru a face consola disponibilă.

Valoare recomandată: 3.

Reţinerea informaţiilor de securitate server (QRETSVRSEC)

Valoarea de sistem QRETSVRSEC determină dacă informaţiile de autentificare decriptabile asociate cu profilurile utilizatorilor sau cu intrările listei de validare (*VLDL) pot fi reţinere pe sistemul gazdă. Aceasta nu include parola profilului de utilizator iSeries.

Dacă modificaţi valoarea din 1 în 0, sistemul dezactivează accesul la informaţiile de autentificare. Dacă modificaţi valoarea înapoi la 1, sistemul reactivează accesul la informaţiile de autentificare.

Informaţiile de autentificare pot fi înlăturate din sistem setând valoarea de sistem QRETSVRSEC pe 0 şi rulând comanda CLRSVRSEC (Curăţare date de securitate server - Clear Server Security Data). Dacă aveţi un număr mare de profiluri de utilizator sau liste de validare pe sistemul dumneavoastră, rularea comenzii CLRSVRSEC poate necesita un interval mare de timp.

Câmpul cu date criptate al unei intrări de listă de validare este folosit în mod tipic pentru a memora informaţii de autentificare. Aplicaţiile specifică dacă să se memoreze datele criptate într-o formă decriptabilă sau nedecriptabilă. Dacă aplicaţiile aleg o formă decriptabilă şi valoarea QRETSVRSEC este modificată de pe 1 pe 0, informaţiile despre câmpul de date criptate nu sunt accesibile din intare. Dacă câmpul cu date criptate al unei intrări de listă de validare este memorat într-o formă nedecriptabilă, nu este afectat de valoarea de sistem QRETSVRSEC.

| **Notă:** Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind
| securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de
| securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 15. Valorile posibile pentru valoarea de sistem QRETSVRSEC:

0	Datele de securitate server nu sunt reţinute.
1	Datele de securitate server sunt reţinute.

Valoare recomandată: 0.

Controlul semnării de la distanţă (QRMTSIGN)

Valoarea de sistem QRMTSIGN specifică cum se tratează cererile de semnare la distanţă. Exemple de semnări la distanţă sunt staţia de afişare passthrough de la un alt sistem, funcţia staţiei de lucru a programului cu licenţă iSeries Access şi accesul TELNET.

| **Notă:** Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind
| securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de
| securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 16. Valorile posibile pentru valoarea de sistem QRMTSIGN:

***FRCSIGNON**	Cererile de semnare la distanţă trebuie să treacă prin procesul normal de semnare.
***SAMEPRF**	Când numele sursă şi destinaţie al profilului utilizatorului sunt aceleaşi, ecranul de semnare poate fi ocolit dacă este cerută semnarea automată. Verificarea parolei apare înainte să fie folosit programul destinaţie passthrough. Dacă o parolă care nu este validă este trimisă într-o încercare de semnare automată, sesiunea passthrough se termină întotdeauna şi un mesaj de eroare este trimis utilizatorului. Totuşi, dacă numele profilurilor sunt diferite, *SAMEPRF indică terminarea sesiunii cu o eşuare de securitate chiar dacă utilizatorul a introdus o parolă validă pentru profilul utilizatorului de la distanţă. Ecranul de semnare apare pentru încercări passthrough care nu cer semnarea automată.

Tabela 16. Valorile posibile pentru valoarea de sistem QRMTSIGN: (continuare)

***VERIFY**	Valoarea *VERIFY vă permite să ocoliţi ecranul de semnare al sistemului destinaţie dacă, împreună cu cererea automată de semnare, sunt trimise informaţii valide de securitate. Dacă parola nu este validă pentru profilul specificat al utilizatorului destinaţie, atunci sesiunea passthrough se termină cu o eşuare de sistem. Dacă sistemul destinaţie are valoarea QSECURITY de 10, orice cerere automată de semnare este permisă. Ecranul de semnare apare pentru încercări passthrough care nu cer semnarea automată.
***REJECT**	Nu este permisă nici o semnare de la distanţă. Pentru acces TELNET, nu există acţiune pentru *REJECT.
nume-program nume-bibliotecă	Programul specificat se rulează la pornirea şi oprirea fiecărei sesiuni passthrough.

Valoarea recomandată: *REJECT dacă nu doriţi să permiteţi vreun acces passthrough sau iSeries Access. Dacă permiteţi acces passthrough sau iSeries Access, folosiţi *FRCSIGNON sau *SAMEPRF.

Cartea *Remote Work Station Support* conţine informaţii detaliate despre valoarea de sistem QRMTSIGN. Conţine de asemenea necesităţi pentru un program de semnare de la distanţă şi un exemplu.

Scanarea sistemelor de fişiere (QSCANFS)

Valoarea de sistem QSCANFS (Scan File Systems - Scanare sisteme de fişiere) vă permite să specificaţi sistemul de fişiere integrat în care vor fi scanate obiecte. De exemplu, puteţi folosi această opţiune pentru a scana de viruşi. Scanarea sistemului integrat de fişiere este activată când sunt înregistrate programele de ieşire cu oricare dintre punctele de ieşire referitoare la scanarea sistemului integrat de fişiere.

Valoarea de sistem QSCANFS specifică sistemele integrate de fişiere în care obiectele vor fi scanate când sunt înregistrate programele de ieşire cu oricare dintre punctele de ieşire referitoare la scanarea sistemului integrat de fişiere.

Punctele de ieşire referitoare la scanarea sistemului integrat de fişiere sunt:

- QIBM_QP0L_SCAN_OPEN — Scanare sistem integrat de fişiere în ieşiere deschidere.
- QIBM_QP0L_SCAN_CLOSE — Scanare sistem integrat de fişiere în ieşiere închidere.

Pentru informaţii suplimentare despre sistemele integrate de fişiere, vedeţi subiectul sistemul integrat de fişiere.

Tabela 17. Valorile posibile pentru valoarea de sistem QSCANFS:.

*NONE	Nu va fi scanat nici un obiect sistem integrat de fişiere.
***ROOTOPNUD**	Obiectele de tip *STMF care sunt în directoare *TYPE2 din rădăcină(/), QOpenSy şi sistemele de fişiere definite de utilizator vor fi scanate.

Valoarea recomandată: Valoarea recomandată este *ROOTOPNUD, pentru ca rădăcina (/), QOpenSys şi sistemele de fişiere definite de utilizator să fie scanate când cineva înregistrează programe de ieşire cu puncte de ieşire referitoare la scanarea sistemului integrat de fişiere.

Pentru informaţii înrudite, vedeţi subiectul “Controlul scanării sistemelor de fişiere (QSCANFSCTL)”.

Controlul scanării sistemelor de fişiere (QSCANFSCTL)

Valoarea de sistem QSCANFSCTL (Control scanare sisteme de fişiere - Scan File Systems Control) controlează scanarea sistemului integrat de fişiere care este activat când programele de ieşire sunt înregistrate cu oricare dintre punctele de ieşire referitoare la scanarea sistemului integrat de fişiere.

Tabela 18. Valorile posibile pentru valoarea de sistem QSCANFSCTL:.

***NONE**	Nu este specificat nici un control pentru punctele de ieşire referitoare la scanarea sistemului integrat de fişiere.

| *Tabela 18. Valorile posibile pentru valoarea de sistem QSCANFSCTL: (continuare).*

*ERRFAIL	Dacă există erori la apelarea programului de ieşire (de exemplu, programul nu a fost găsit sau programul de ieşire semnalează o eroare), sistemul va eşua cererea care a declanşat apelul programului de ieşire. Dacă aceasta nu este specificată, sistemul va sări peste programul de ieşire şi îl va trata ca şi cum obiectul nu a fost scanat.
*FSVRONLY	Vor fi scanate doar accesările prin serverele de fişiere. De exemplu, accesările prin Sistemul de fişiere reţea va fi scanat la fel ca şi alte metode de servere de fişiere. Dacă nu este specificat, toate accesările vor fi scanate.
*NOFAILCLO	Sistemul nu vor eşua cererile de închidere cu o indicare de eşuare la scanare, chiar dacă obiectul a eşuat o scanare care a fost făcută ca parte a procesării de închidere. De asemenea, această valoare va înlocui specificaţia *ERRFAIL pentru procesarea de închidere, dar nu şi pentru celelalte puncte de ieşire referitoare la scanarea.
*NOPOSTRST	După ce obiectele sunt restaurate, nu vor fi scanate doar pentru că au fost restaurate. Dacă atributul obiectului este că ″obiectul nu va fi scanat″, obiectul nu va fi scnat niciodată. Dacă atributul obiectului este că ″obiectul va fi scanat doar dacă a fost modificat de la ultima scanare″, obiectul va fi scanat doar dacă este modificat după ce este restaurat. Dacă nu este specificat *NOPOSTRST, obiectele vor fi scanate cel puţin o dată după ce sunt restaurate. Dacă atributul obiectului este că ″obiectul nu va fi scanat″, obiectul va fi scanat o dată după ce va fi restaurat. Dacă atributul obiectului este că ″obiectul va fi scanat doar dacă a fost modificat de la ultima scanare″, obiectul va fi scanat după ce este restaurat pentru că restaurarea va fi tratată ca o modificare a obiectului. În general, poate fi periculos să restauraţi obiecte fără să le scanaţi măcar o dată. Este cel mai bine să folosiţi această opţiune doar când ştiţi că obiectele au fost scanate înainte să fie salvate sau că provin de la o sursă sigură.
*NOWRTUPG	Sistemul nu va încerca să actualizeze accesul pentru descriptorul de scanare transmis programului de ieşire pentru a include acces de scriere. Dacă nu este specificat, sistemul va încerca să actualizeze accesul de scriere.
*USEOCOATR	Sistemul va folosi specificaţiile atributului ″doar modificare obiect″ doar pentru a scana obiectul dacă a fost modificat (de asemenea şi pentru că software-ul de scanare a indicat o actualiyare). Dacă nu este specificat, acest atribut ″doar modificare obiect″ nu va fi folosit, iar obiectul va fi scanat după ce este modificat şi când software-ul de scanare indică o actualizare.

Valoarea recomandată: Dacă doriţi cele mai restricţionate valori specificate pentru scanarea sistemului integrat de fişiere, atunci setările recomandate sunt *ERRFAIL şi *NOWRTUPG. Aceasta asigură că orice eşec de la programele de ieşire de scanare vor preveni operaţiile asociate şi nu va da programului de ieşire niveluri de acces suplimentare. Totuşi, valoarea *NONE este o bună opţiune pentru majoritatea utilizatorilor. La instalarea codului care a fost livrat de o sursă de încredere, este recomandabil să fie specificat *NOPOSTRST în timpul acelei instaţări.

Pentru informaţii înrudite, vedeţi subiectul “Scanarea sistemelor de fişiere (QSCANFS)” la pagina 28.

Controlul memoriei de partajare (QSHRMEMCTL)

Valoarea de sistem QSHRMEMCTL defineşte care utilizatori au voie să folosească memorie partajată sau memorie mapată care are capabilitate de scriere. Pentru a modifica această valoare de sistem, utilizatorii trebuie să aibă autorizări speciale *ALLOBJ şi *SECADM. O modificare la această valoare de sistem se petrece imediat.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 19. Valori posibile pentru valoarea de sistem QSHRMEMCTL:.

0	Utilizatorii nu pot folosi memorie partajată sau folosiţi memorie mapată care are capabilitate de scriere. Această valoare înseamnă că utilizatorii nu pot folosi API-uri de memorie partajată (de exemplu, shmat() — API Ataşare memorie partajată) şi nu pot folosi obiecte de memorie mapată care au capabilitate de scriere (de exemplu, mmap() — API Memorie mapează un fişier furnizează această funcţie). Folosiţi această valoare în medii cu cereri mai mari de securitate.
1	Utilizatorii pot folosi memorie partajată sau mapată care are capabilitate de scriere. Această valoare înseamnă că utilizatorii pot folosi API-uri de memorie partajată (de exemplu, shmat() — API Ataşare memorie partajată) şi pot folosi obiecte de memorie mapată care au capabilitate de scriere (de exemplu, mmap() — API Memorie mapează un fişier furnizează această funcţie).

Valoare recomandată: 1.

Folosirea autorizării adoptate (QUSEADPAUT)

Valoarea de sistem QUSEADPAUT defineşte care utilizatori pot crea programe folosind atributul de autorizare adoptată (*USEADPAUT(*YES)). Toţi utilizatorii autorizaţi de către valoarea de sistem QUSEADPAUT pot crea sau modifica programe şi programe service pentru a folosi autorizare adoptată dacă utilizatorul are autorizarea necesară programului sau programului service.

Valoarea de sistem poate conţine numele unei liste de autorizări. Autorizarea utilizatorului este verificată în această listă. Dacă utilizatorul are cel puţin o autorizare *USE la lista de autorizaţii, el poate crea, modifica sau actualiza programe sau programe servicii cu atributul USEADPAUT(*YES). Autorizarea la lista de autorizaţii nu poate veni de la o autorizare adoptată.

Dacă o listă de autorizaţii este numită în valoarea de sistem şi lista de autorizaţii lipseşte, funcţia care este încercată nu se va termina. Este trimis un mesaj pentru a indica acest lucru.

Oricum, dacă programul este creat cu API-ul QPRCRTPG şi valoarea *NOADPAUT este specificată în şablonul opţiune, programul creează cu succes chiar dacă lista de autorizaţii nu există.

Dacă sunt cerute mai multe funcţii în comandă sau API şi lista de autorizaţii lipseşte, funcţia nu este executată. Dacă comanda care este încercată când nu poate fi găsită lista de autorizaţii este CRTPASPGM (Create Pascal Program - Creare program Pascal), rezultatul este o verificare de funcţie.

| **Notă:** Această valoarea de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 20. Valorile posibile pentru valoarea de sistem QUSEADPAUT:

nume listă de autorizaţii	Este semnalat un mesaj diagnostic pentru a indica faptul că programul este creat cu USEADPAUT(*NO) dacă toate următoarele sunt adevărate: • O listă de autorizaţii este specificată pentru valoarea de sistem QUSEADPAUT. • Utilizatorul nu are autorizare la lista de autorizaţii menţionată mai sus. • Nu mai există şi alte erori când programul sau programul serviciu este creat.
***NONE**	Toţi utilizatorii pot crea sau modifica programe şi programe service pentru a folosi autorizare adoptată dacă utilizatorul are autorizarea necesară programului sau programului service.

Valore recomandată: Pentru maşinile de producţie, creaţi o listă de autorizaţii cu autorizarea *PUBLIC(*EXCLUDE). Specificaţi această listă de autorizaţii pentru valoarea de sistem QUSEADPAUT. Aceasta previne crearea programelor de către cineva care foloseşte autorizare adoptată.

Ar trebui să luaţi în considerare proiectarea securităţii înainte de creare unei liste de autorizaţii pentru valoarea de sistem QUSEADPAUT. Acest lucru este important în special pentru mediile de dezvlotare de aplicaţii.

Valorile de sistem referitoare la securitate

Privire generală:

Scop: Specificaţi valorile de sistem care au legătură cu securitatea în sistem.

Cum se face:
WRKSYSVAL (comanda Work with System Values - Gestionare valori de sistem)

Autorizare:
*ALLOBJ şi *SECADM

Intrare jurnal:
SV

Notă: Modificările au efect imediat. IPL-ul nu este necesar.

În continuare sunt descrise celelalte valorile de sistem care au legătură cu securitatea din sistem. Aceste valori de sistem nu sunt incluse în grupul *SEC din ecranul Gestionare valori de sistem.

QAUTOCFG
Configurare automată dispozitiv

QAUTOVRT
Configurare automată dispozitive virtuale

QDEVRCYACN
Acţiune recuperare dispozitiv

QDSCJOBITV
Interval de timeout job deconectat

Notă: Această valoare de sistem este de asemenea discutată în Centrul de informaţii (vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii).

QRMTSRVATR
Atribut service la distanţă

Urmează descrierea acestor valori de sistem. Sunt afişate opţiunile posibile. Opţiunile care sunt subliniate sunt valorile implicite ale sistemului.

Configurarea automată a dispozitivelor (QAUTOCFG)

Valoarea de sistem QAUTOCFG configurează automat dispozitivele ataşate local. Valoarea specifică dacă dispozitivele care sunt adăugate în sistem sunt configurate automat.

| **Notă:** Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind
| securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de
| securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 21. Valorile posibile pentru valoarea de sistem QAUTOCFG:

0	Configurarea automată este dezactivată. Trebuie să configuraţi manual noile controlerele sau dispozitive locale pe care le adăugaţi sistemului dumneavoastră.
1	Configurarea automată este activată. Sistemul configurează automat noile controlere sau dispozitive locale pe care le adăugaţi sistemului dumneavoastră. Operatorul primeşte un mesaj care indică modificările din configuraţia sistemului.

Valoare recomandată: Când se iniţiază setarea sistemului sau când se adaugă multe dispozitive noi, valoarea de sistem trebuie să fie setată la 1. În orice alt moment, valoarea de sistem ar trebui să fie setată la 0.

Configurarea automată a dispozitivelor virtuale (QAUTOVRT)

Valoarea de sistem QAUTOVRT specifică dacă sunt configurate automat dispozitivele virtuale pass-through şi dispozitivele virtuale ecran întreg TELNET (diferite de dispozitivul virtual funcţie staţie de lucru).

Un **dispozitiv virtual** este o descriere de dispozitiv care nu are asociat hardware. Este folosit pentru a realiza o conexiune între un utilizator şi o staţie de lucru fizică ataşată la un sistem de la distanţă.

Dacă permiteţi sistemului să configureze automat dispozitive virtuale, utilizatorii vor putea pătrunde mai uşor în sistemul dumneavoastră folosind pass-through sau telnet. Fără configurare automată, un utilizator care încearcă să pătrundă are la dispoziţie un număr limitat de încercări pentru fiecare dispozitiv virtual. Limita este definită de responsabilul cu securitatea folosind valoarea de sistem QMAXSIGN. Când configurarea automată este activă, limita reală este mai mare. Limita de semnări pe sistem este multiplicată de numărul dispozitivelor virtuale care pot fi create prin suportul de configurare automată. Acest suport este definit de valoarea de sistem QAUTOVRT.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 22. Valorile posibile pentru valoarea de sistem QAUTOVRT:

0	Nici un dispozitiv virtual nu este creat automat.
Număr- dispozitive- virtuale	Specifică o valoare de la 1 la 9999. Dacă la controlerul virtual sunt ataşate mai puţine dispozitive decât numărul specificat şi nici un dispozitiv nu este disponibil când un utilizator încearcă pass-through sau TELNET ecran întreg, sistemul configurează un nou dispozitiv.

Valorea recomandată: 0

Cartea *Remote Work Station Support* conţine mai multe informaţii despre folosirea pass-through pentru staţia de afişare. Cartea *TCP/IP Configuration and Reference* conţine mai multe informaţii despre folosirea TELNET.

Acţiunea la recuperarea dispozitivelor (QDEVRCYACN)

QDEVRCYACN specifică ce acţiune se va executa când apare o eroare I/O pentru staţia de lucru a unui job interactiv.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 23. Valorile posibile pentru valoarea de sistem QDEVRCYACN:

***DSCMSG**	Deconectează jobul. Când semnează din nou, este trimis un mesaj de eroare programului aplicaţie al utilizatorului.
***MSG**	Semnalează mesajul de eroare I/O programului aplicaţie al utilizatorului. Programul aplicaţie execută recuperarea din eroare.
***DSCENDRQS**	Deconectează jobul. Când semnează din nou, este executată o funcţie de cerere anulare pentru a întoarce controlul jobului înapoi la nivelul ultim al cererii.
***ENDJOB**	Termină jobul. Pentru job este produs un istoric de job. În istoricul de job şi istoricul QHST este trimis un mn mesaj care indică faptul că jobul s-a terminat din cauza unei erori de dispozitiv. Pentru a minimiza impactul asupra performanţei al jobului care se termină, prioritatea jobului este scăzută cu 10, porţiunea de timp este setată la 100 milisecunde şi atributul de epurare este setat la da.
***ENDJOBNOLIST**	Termină jobul. Pentru job nu este produs un istoric de job. În istoricul QHST este trimis un mesaj indicând că jobul s-a terminat din cauza unei erori de dispozitiv.

Când este specificată valoarea *MSG sau *DSCMSG, acţiunea de recuperare a dispozitivului nu este executată decât după ce jobul execută următoarea operaţie I/O. Într-un mediu LAN/WAN, aceasta poate permite unui dispozitiv să se deconecteze şi altuia să se conecteze, folosind aceeaşi adresă, înainte să apară următoarea operaţie I/O pentru job. Jobul se poate recupera din mesajul de eroare I/O şi poate continua rularea la al doilea dispozitiv. Pentru a evita acest lucrul, trebuie să fie specificată o acţiune de recuperare dispozitiv *DSCENDRQS, *ENDJOB sau *ENDJOBNOLIST. Aceste acţiuni de recuperare dispozitiv sunt executate imediat când apare o eroare I/O, cum ar fi o operaţie de oprire a alimentării.

Valoare recomandată:
*DSCMSG

Notă: Autorizările speciale *ALLOBJ şi *SECADM nu sunt necesare pentru a modifica această valoare.

Înainte de Versiunea 3, Ediţia 6, valoarea implicită era *MSG. Păstrarea valorii *MSG prezintă o potenţială expunere de securitate.

Intervalul de timeout pentru job deconectat (QDSCJOBITV)

Valoarea de sistem QDSCJOBITV determină dacă sistemul termină un job deconectat. Intervalul este specificat în minute.

Dacă setaţi valoarea de sistem QINACTMSGQ penru a deconecta joburile inactive (*DSCJOB), trebuie setată QDSCJOBITV pentru a termina, la sfârşit, joburile deconectate. Un job deconectat consumă resurse de sistem şi păstrează blocări asupra obiectelor.

| **Notă:** Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 24. Valorile posibile pentru valoarea de sistem QDSCJOBITV:

240	Sistemul termină un job deconectat după 240 de minute.
***NONE**	Sistemul nu termină automat un job deconectat.
timp-în-minute	Specifcă o valoare între 5 şi 1440.

Valoare recomandată: 120

Atributul de service la distanţă (QRMTSRVATR)

QRMTSRVATR controlează abilitatea de a analiza o problemă de service pe un sistem la distanţă. Valoarea permite analizarea sistemului de la distanţă.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum să restricţionaţi modificările valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Valorile permise pentru valoarea de sistem QRMTSRVATR sunt:

Tabela 25. Valorile posibile pentru valoarea de sistem QRMTSRVATR:

0	Atributul service la distanţă este dezactivat.
1	Atributul service la distanţă este activat.

Valorea recomandată: 0

Pentru informaţii despre accesul la distanţă şi valoarea de sistem QRMTSRVATR, vedeţi “Securitatea privind cheia IPL” la pagina 2.

Valorile de sistem pentru restaurare referitoare la securitate

Privire generală:

Scop: Controlează modul în care obiectele în legătură cu securitatea sunt restaurate în sistem.

Cum se face:
WRKSYSVAL*SEC (comanda Gestionare valori de sistem)

Autorizare:
*ALLOBJ şi *SECADM

Intrare jurnal:
SV

Notă: Modificările au efect imediat. IPL-ul nu este necesar.

În continuare sunt descrise valorile de sistem care se referă la restaurarea obiectelor legate de securitatea sistemului, care ar trebui să fie de asemenea luate în considerare la restaurarea obiectelor. Vedeţi Tabela 18 la pagina 28pentru informaţii suplimentare despre valoarea de sistem QSCANFSCTL *NOPOSTRST.

QVFYOBJRST
Verificare obiect la restaurare

QFRCCVNRST
Forţare conversaţie la restaurare

QALWOBJRST
Permitere restaurare obiecte sensibile la securitate

Urmează o descriere a acestor valori de sistem. Sunt afişate opţiunile posibile. Opţiunile care sunt subliniate sunt valorile implicite ale sistemului.

Verificarea obiectului la restaurare (QVFYOBJRST)

Valoarea de sistem QVFYOBJRST determină dacă obiectele trebuie să aibă semnături digitale pentru a fi restaurate în sistemul dumneavoastră. Puteţi impune ca un obiect să nu fie restaurat decât dacă are o semnătură digitală corectă, de la un furnizor de software de încredere. Această valoare se aplică la obiecte de tip: *PGM, *SRVPGM, *SQLPKG, *CMD şi *MODULE. Se aplică de asemenea obiectelor *STMF care conţin programe Java.

Când se încearcă restaurarea unui obiect pe sistem, trei valori de sistem lucrează împreună ca filtre pentru a determina dacă este permisă restaurarea obiectului. Primul filtru este valoarea de sistem pentru verificarea obiectului la restaurare, QVFYOBJRST. Acesta este folosit pentru a controla restaurarea unor obiecte care pot fi semnate digital. Al doilea filtru este valoarea de sistem pentru forţarea conversiei la restaurare, QFRCCVNRST. Această valoare de sistem vă

permite să specificaţi dacă sunt convertite sau nu programele, programele serviciu, pachetele SQL şi obiectele modul în timpul unei operaţii de restaurare. De asemenea, poate împiedica restaurarea unor obiecte. Doar obiectele care pot trece de primele două filtre sunt procesate de al treilea filtru. Al treilea filtru este valoarea de sistem pentru permiterea restaurării obiectului (QALWOBJRST). Specifică dacă pot fi restaurate obiectele cu atribute sensibile la securitate.

Dacă Digital Certificate Manager (OS/400 opţiunea 34) nu este instalat pe sistem, toate obiectele cu excepţia celor semnate de o sursă sistem de încredere sunt tratate ca nesemnate când se determină efectele valorii de sistem QVFYOBJRST în timpul unei operaţii de restaurare.

Modificarea acestei valori de sistem devine imediat efectivă.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Atenţie

Când vă este livrat sistemul, valoarea de sistem QVFYOBJRST este setată pe 3. Dacă modificaţi valoarea QVFYOBJRST, este important să o setaţi la 3 sau mai puţin înainte de a instala o nouă ediţie de sistemului de operare OS/400.

Tabela 26. Valori posibile pentru valoarea de sistem QVFYOBJRST:

1	Nu verificaţi semnăturile la restaurare. Restauraţi toate obiectele indeferent de semnătura lor. Această valoare nu ar trebui să fie folosită decât dacă aveţi de restaurat obiecte semnate care vor eşua la verificarea semnăturii din unele motive acceptabile.
2	Verificaţi obiectele la restaurare. Restauraţi comenzile şi obiectele-stare utilizator nesemnate. Restauraţi comenzile şi obiectele stare utilizator semnate chiar dacă semnăturile nu sunt valide. Această valoare trebuie să fie folosită numai dacă există anumite obiecte cu semnături nevalide pe care doriţi să le restauraţi. În general, este periculos să restauraţi obiecte cu semnături care nu sunt valide pe sistemul dumneavoastră.
3	Verificaţi semnăturile la restaurare. Restauraţi comenzile şi obiectele stare utilizator nesemnate. Restauraţi comenzile şi obiectele stare utilizator semnate numai dacă semnăturile sunt valide. Această valoare poate fi folosită pentru operaţii normale, când vă aşteptaţi ca unele dintre obiectele pe care le restauraţi să nu fie semnate, dar doriţi să va asiguraţi că toate obiectele semnate au semnături valide. Comenzile şi programele pe care le-aţi creat sau cumpărat înainte ca semnăturile digitale să fie disponibile vor fi nesemnate. Această valoare permite acelor comenzi şi programe să fie restaurate. Aceasta este valoarea implicită.
4	Verificaţi semnăturile la restaurare. Nu restauraţi comenzile şi obiectele stare utilizator nesemnate. Restauraţi comenzile şi obiectele stare utilizator semnate chiar dacă semnăturile nu sunt valide. Această valoare trebuie să fie folosită numai dacă există anumite obiecte cu semnături nevalide pe care doriţi să le restauraţi, dar nu doriţi să existe posibilitatea de a fi restaurate obiectele nesemnate. În general, este periculos să restauraţi obiecte cu semnături care nu sunt valide pe sistemul dumneavoastră.

Tabela 26. Valori posibile pentru valoarea de sistem QVFYOBJRST: (continuare)

5	Verificaţi semnăturile la restaurare. Nu restauraţi comenzile şi obiectele stare utilizator nesemnate. Restauraţi comenzile şi obiectele stare utilizator semnate numai dacă semnăturile sunt valide. Această valoare este cea mai restrictivă valoare şi trebuie să fie folosită când singurele obiecte care doriţi să fie restaurate sun acelea care au fost semnate de surse de încredere.

Obiectele care au atributul stare sistem şi obiectele care au atributul stare moştenire trebuie să aibă semnături valide de la o sursă sistem de încredere. Singura valoare care va permite restaurarea unui obiect stare sistem sau stare moştenire fără o semnătură validă este 1. Permiterea unei astfel de comenzi sau program reprezintă un risc de integritate pentru sistemul dumneavoastră. Dacă modificaţi valoarea de sistem QVFYOBJRST pe 1 pentru a permite restaurarea unui astfel de obiect pe sistemul dumneavoastră, asiguraţi-vă că aţi modificat valoarea de sistem QVFYOBJRST înapoi la valoarea anterioară după ce obiectul a fost restaurat.

Unele comenzi folosesc o semnătură care nu acoperă toate părţile obiectului. Unele părţi de comandă nu sunt semnate, în timp ce alte părţi sunt semnate doar când conţin o valoare neimplicită. Acest tip de semnătură permite realizarea unor modificări în comandă fără ca semnătura sa să devină nevalidă. Exemple de modificări care nu vor invalida aceste tipuri de semnături includ:

- Modificarea valorilor implicite ale comenzii.
- Adăugarea unui program de verificare a validităţii unei comenzi care nu are unul.
- Modificarea parametrului 'unde este permisă rularea'.
- Modificarea parametrului 'permitere utilizator limitat'.

Dacă doriţi, puteţi să adăugaţi propria dumneavoastră semnătură comenzilor care includ aceste zone ale obiectului comandă.

Valoare recomandată: 3.

Forţarea conversiei la restaurare (QFRCCVNRST)

Această valoare de sistem vă permite să specificaţi dacă sunt convertite sau nu următoarele tipuri de obiecte în timpul unei restaurări:

- program (*PGM)
- program service (*SRVPGM)
- pachet SQL (*SQLPKG)
- modul (*MODULE)

De asemenea, poate împiedica restaurarea unor obiecte. Un obiect care este specificat să fie convertit de valoarea de sistem, dar nu poate fi convertit deoarece nu conţine suficiente date de creare, nu va fi restaurat.

Când se specifică *SYSVAL pentru parametrul FRCOBJCVN din comenzile de restaurare (RST, RSTLIB, RSTOBJ, RSTLICPGM), se foloseşte setarea acestei valori de sistem. De aceea, puteţi porni şi opri conversia pentru întreg sistemul modificând valoarea QFRCCVNRST. Totuşi, parametrul FRCOBJCVN înlocuieşte valoarea de sistem în unele cazuri. Dacă specificaţi *YES şi *ALL în FRCOBJCVN, vor fi înlocuite toate setările valorii de sistem. Dacă specificaţi *YES şi *RQD în parametrul FRCOBJCVN, este la fel ca şi cum aţi specifica '2' pentru această valoare de sistem şi poate fi înlocuită valoarea de sistem când este setată pe '0' sau '1'.

QFRCCVNRST este a doua dintre cele trei valori de sistem care lucrează consecutiv ca filtre pentru a determina dacă este permisă sau nu restaurarea unui obiect sau dacă este convertit în timpul restaurării. Primul filtru, valoarea de sistem pentru verificarea obiectului la restaurare (QVFYOBJRST), controlează restaurarea unor obiecte care pot fi semnate digital. Numai obiectele care pot trece de primele două filtre sunt procesate de al treilea filtru.

Valoarea livrată a QFRCCVNRST este 1. Pentru toate valorile QFRCCVNRST, un obiect care ar trebui convertit dar care nu poate fi convertit nu va fi restaurat. Obiectele semnate digital de o sursă de sistem de încredere sunt restaurate fără conversie pentru toate valorile acestei valori de sistem.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela de mai jos rezumă valorile permise pentru QFRCCVNRST:

Tabela 27. Valori QFRCCVNRST

0	Nu convertiţi nimic. Nu împiedicaţi restaurarea nici unui obiect.
1	Vor fi convertite obiectele cu erori de validare.
2	Vor fi convertite obiectele a căror conversie este necesară pentru sistemul de operare curent sau care au o eroare de validare.
3	Vor fi convertite obiectele care sunt suspectate de a fi fost modificate, obiectele care conţin erori de validare şi obiectele care necesită conversia la versiunea curentă a sistemului de operare.
4	Vor fi convertite obiectele care conţin suficiente date de creare pentru a fi convertite şi care nu au semnături digitale valide. Un obiect care nu conţine suficiente date de creare va fi restaurat fără conversie. Notă: Vor fi convertite obiectele (semnate şi nesemnate) care au erori de validare, care sunt suspectate de a fi fost modificate sau care necesită conversia la versiunea curentă a sistemului de operare, iar dacă nu se face conversia va eşua restaurarea lor.
5	Vor fi convertite obiectele care conţin suficiente date de creare. Un obiect care nu conţine suficiente date de creare pentru a fi convertit va fi restaurat. Notă: Obiectele care au erori de validare, care sunt suspectate de a fi fost modificate sau care necesită conversia la versiunea curentă a sistemului de operare şi care nu pot fi convertite nu vor fi restaurate.
6	Vor fi convertite toate obiectele care nu au o semnătură digitală validă. Notă: Un obiect cu o semnătură digitală validă care are de asemenea o eroare de validare sau este suspectat de a fi fost modificat va fi convertit, iar dacă nu poate fi convertit nu va fi restaurat.
7	Fiecare obiect va fi convertit.

Când un obiect este convertit, semnătura sa digitală este eliminată. Starea obiectului convertit este stare utilizator. Obiectele convertite vor avea o valoare bună de validare şi nu sunt suspectate de a fi fost modificate.

Valoare recomandată: 3 sau mai mare.

Permiterea restaurării obiectelor sensibile la securitate (QALWOBJRST)

Valoarea de sistem QALWOBJRST determină dacă obiectele care sunt sensibile la securitate pot fi restaurate pe sistemul dumneavoastră. O puteţi folosi pentru a împiedica pe oricine să restaureze un obiect stare sistem sau un obiect care adoptă autorizarea.

Când se încearcă restaurarea unui obiect pe sistem, trei valori de sistem lucrează împreună ca filtre pentru a determina dacă este permisă restaurarea obiectului. Primul filtru este valoarea de sistem pentru verificarea obiectului la restaurare, QVFYOBJRST. Acesta este folosit pentru a controla restaurarea unor obiecte care pot fi semnate digital. Al doilea filtru este valoarea de sistem pentru forţarea conversiei la restaurare, QFRCCVNRST. Această valoare de sistem vă permite să specificaţi dacă sunt convertite sau nu programele, programele serviciu, pachetele SQL şi obiectele modul în timpul unei operaţii de restaurare. De asemenea, poate împiedica restaurarea unor obiecte. Doar obiectele care pot trece de primele două filtre sunt procesate de al treilea filtru. Al treilea filtru este valoarea de sistem pentru permiterea restaurării obiectului (QALWOBJRST). Specifică dacă pot fi restaurate obiectele cu atribute sensibile la securitate.

Când sistemul dumneavoastră este livrat, valoarea de sistem QALWOBJRST este setată pe *ALL. Această valoare este necesară pentru a vă instala sistemul cu succes.

ATENŢIE: Este important să setaţi valoarea QALWOBJRST la *ALL înainte să realizaţi unele activităţi de sistem, precum:

- Instalarea unei noi ediţii a programului cu licenţă OS/400.
- Instalarea noilor programe cu licenţă.
- Recuperarea sistemului.

Aceste activităţi pot eşua dacă valoarea QALWOBJRST nu este *ALL. Pentru a asigura securitatea sistemului, readuceţi valoarea QALWOBJRST la setarea dumneavoastră normală după efectuarea activităţii de sistem.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Puteţi specifica valori multiple pentru valoarea de sistem QALWOBJRST, doar dacă nu specificaţi *ALL sau *NONE.

Tabela 28. Valori posibile pentru valoarea de sistem QALWOBJRST:.

***ALL**	Orice obiect poate fi restaurat pe sistemul dumneavoastră de un utilizator cu autorizarea corectă.
***NONE**	Obiectele sensibile la securitate, cum ar fi programele de stare sistem sau programele care adoptă autorizarea, nu pot fi restaurate pe sistem.
***ALWSYSSTT**	Sistemul şi obiectele de stare moştenire pot fi restaurate la sistem.
***ALWPGMADP**	Obiectele care adoptă autorizarea pot fi restaurate pe sistem.
***ALWPTF**	Sistemul şi obiectele de stare moştenire, obiectele care adoptă autorizarea, obiectele care au atributul ISUID (setare-ID-utilizator) activat şi obiectele care au atributul S_ISGID (setare-ID-grup) activat pot fi restaurate pe sistem în timpul instalării de PTF.
***ALWSETUID**	Permiteţi restaurarea fişierelor care au atributul S_ISUID (setare-ID-utilizator) activat.
***ALWSETGID**	Permiteţi restaurarea fişierelor care au atributul S_ISGID (setare-ID-grup) activat.
***ALWVLDERR**	Permiteţi restaurarea obiectelor care nu trec de testele de validare a obiectului. Dacă setarea valorii de sistem QFRCCVNRST cauzează convertirea obiectului, erorile sale de validare vor fi corectate.

Valoare recomandată: Valoarea de sistem QALWOBJRST furnizează o metodă de a proteja sistemul de programe care pot crea probleme serioase. Pentru operaţii normale, setaţi această valoare pe *NONE. Nu uitaţi s-o modificaţi pe *ALL înainte de a realiza activităţile menţionate anterior. Dacă restauraţi programe şi aplicaţii în mod regulat pe sistemul dumneavoastră, s-ar putea să fie necesară setarea valorii de sistem QALWOBJRST la *ALWPGMADP.

Valorile de sistem pentru parole

Privire generală:

Scop: Specificaţi valori de sistem pentru a seta cerinţele privind alocarea parolelor utilizatorilor.

Cum se face:
WRKSYSVAL *SEC (comanda Gestionare valori de sistem)

Autorizare:
*ALLOBJ şi *SECADM

Intrare jurnal:
SV

Notă: Modificările au efect imediat. IPL-ul nu este necesar.

Următoarele valori de sistem controlează parolele. Aceste valori de sistem obligă utilizatorii să modificae parolele regulat şi ajută la împiedicarea utilizatorilor de a aloca parole triviale sau uşor de ghicit. De asemenea, ele pot asigura faptul că parolele respectă cerinţele reţelei dumneavoastră de comunicaţii:

QPWDEXPITV [1]
Interval de expirare

QPWDLVL
Nivel parolă

QPWDMINLEN [1]
Lungime minimă

QPWDMAXLEN [1]
Lungime maximă

QPWDRQDDIF [1]
Diferenţă necesară

QPWDLMTCHR
Caractere restricţionate

QPWDLMTAJC
Caractere adiacente restricţionate

QPWDLMTREP
Caractere repetate restricţionate

QPWDPOSDIF
Diferenţă poziţie caracter

QPWDRQDDGT
Necesitate caracter numeric

QPWDVLDPGM
Program validare parolă

Valorile de sistem pentru compunerea parolelor sunt impuse doar când parola este modificată folosind comanda CHGPWD, opţiunea meniu ASSIST pentru a modifica o parolă sau interfaţa de programare aplicaţie (API) QSYCHGPW. Nu sunt impuse când parola este setată folosind comanda CRTUSRPRF sau CHGUSRPRF.

Dacă valoarea de sistem QPWDMINLEN (Password Minimum Length - Lungime minimă parolă) are o valoare diferită de 1 sau dacă valoarea de sistem QPWDMAXLEN (Password Maximum Length - Lungime maximă parolă) are o valoare diferită de 10 sau dacă modificaţi de pe implicit oricare dintre celelalte valori de sistem de control parolă, sistemul împiedică un utilizator să seteze parola egală cu numele de profil utilizator folosind comanda CHGPWD, meniul ASSIST sau API QSYCHGPW.

Dacă o parolă este uitată, responsabilul cu securitatea poate folosi comanda CHGUSRPRF (Change User Profile - Modificare profil utilizator) pentru a seta parola la fel cu numele profilului sau la oricare altă valoare. Câmpul *Setare parolă pe expirată* din profilul utilizatorului poate fi folosit pentru a cere modificarea unei parole la următoarea semnare a utilizatorului.

Intervalul de expirare a parolei (QPWDEXPITV)

Valoarea de sistem QPWDEXPITV controlează numărul de zile permise înainte a fi cerută schimbarea parolei. Dacă un utilizator încearcă să semneze după ce parola a expirat, sistemul arată un ecran care cere modificarea parolei înainte ca utilizatorul să aibă permisiunea de semnare.

1. Aceste valori de sistem sunt discutate de asemenea în Centrul de informare (vedeţi"Cerinţe preliminare şi informaţii înrudite" la pagina xvi pentru detalii).

```
                          Sign-on Information
                                                                 System:
Password has expired.  Password must be changed to continue sign-on
request.

Previous sign-on . . . . . . . . . . . . . :   10/30/91  14:15:00

Sign-on attempts not valid . . . . . . . . :   3
```

| **Notă:** Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind
| securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de
| securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 29. Valorile posibile pentru valoarea de sistem QPWDEXPITV:

***NOMAX**	Utilizatorii nu trebuie să-şi modifice parolele.
limită-în-zile	Specificaţi o valoare între 1 şi 366.

Valoare recomandată: de la 30 până la 90.

Notă: Un interval de expirare a parolei poate fi de asemenea specificat şi în profilurile de utilizator individuale.

Nivelul parolei (QPWDLVL)

Nivelul de parolă al sistemului poate fi setat pentru a permite profilurilor utilizatorilor parole de la 1 la 10 caractere sau pentru a permite pentru profilurile de utilizator parole de la 1 la 128 de caractere.

Nivelul de parolă poate fi setat să permită ’passphrase’ (frază-parolă) ca valoare a parolei. Termenul ’passphrase’ este uneori folosit în industria calculatoarelor pentru a descrie o valoare de parolă care poate fi foarte lungă şi are puţine restricţii (sau deloc) privind caracterele folosite în valoarea parolei. Într-o frază-parolă, pot fi folosite spaţii între litere, ceea ce vă permite să aveţi ca valoare de parolă o propoziţie sau un fragment de propoziţie. Singurele restricţii dintr-o frază-parolă sunt imposibilitatea de a începe cu un asterisc (’*’) şi înlăturarea spaţiilor din coadă. Înainte să modificaţi nivelul parolei pe sistemul dumneavoastră, revedeţi secţiunea “Planificarea modificărilor nivelului de parolă” la pagina 190.

| **Notă:** Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind
| securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de
| securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 30. Valori posibile pentru valoarea de sistem QPWDLVL:.

0	Sistemul suportă parole de profil de utilizator cu o lungime de 1-10 caractere. Caracterele permise sunt A-Z, 0-9 şi carecterele $, @, # şi liniuţa de subliniere. Setarea QPWDLVL 0 ar trebui folosită dacă sistemul dumneavoastră comunică cu alte sisteme iSeries într-o reţea, iar acele sisteme rulează cu o valoare QPWDLVL de 0 sau cu o ediţie de sistem de operare mai mică de V5R1M0. QPWDLVL 0 ar trebui folosită dacă sistemul dumneavoastră comunică cu orice alt sistem care limitează lungimea parolelor de 1-10 caractere. Trebuie să folosiţi QPWDLVL 0 dacă sistemul comunică cu produsul Windows 95/98/ME iSeries Client Support for Windows Network Neighborhood (NetServer) şi cu alte sisteme folosind parolde de 1-10 caractere. Când valoarea QPWDLVL a sistemului este setată pe 0, sistemul de operare va crea parola codată pentru folosirea la QPWDLVL 2 şi 3. Valoarea parolei care poate fi folosită la QPWDLVL 2 şi 3 va fi aceeaşi parolă ca şi cea folosită la QPWDLVL 0 sau 1.
1	QPWDLVL 1 este suportul echivalent al QPWDLVL 0 cu următoarea excepţie: parolele iSeries NetServer pentru clienţii Windows 95/98/ME vor fi înlăturate de pe sistem. Dacă folosiţi suportul client pentru produsul iSeries NetServer, nu puteţi folosi valoarea 1 a QPWDLVL. QPWDLVL 1 îmbunătăţeşte securitatea sistemului iSeries prin înlăturarea tuturor parolelor iSeries NetServer de pe sistem.

Tabela 30. Valori posibile pentru valoarea de sistem QPWDLVL: (continuare).

2	Sistemul suportă parole de profil utilizator de 1-128 caractere. Sunt permise caractere cu litere mici sau mari. Parolele pot conţine orice caracter iar parola va fi sensibilă la majuscule. Setarea QPWDLVL 2 este văzută ca un nivel de compatibilitate. Acest nivel permite mutarea înapoi la QPWDLVL 0 sau 1 atât timp cât parola creată la QPWDLVL 2 sau 3 îndeplineşte cerinţele de lungime şi sintaxă ale unei parole valide la QPWDLVL 0 sau 1. Se poate folosi QPWDLVL 2 dacă sistemul comunică cu produsul Windows 95/98/ME iSeries Client Support for Windows Network Neighborhood (NetServer), atât timp cât parola dumneavoastră este de 1-14 caractere lungime. Setarea QPWDLVL 2 nu poate fi folosită dacă sistemul dumneavoastră comunică cu alte sisteme iSeries într-o reţea, iar acele sisteme rulează cu o valoare QPWDLVL de 0 sau cu o ediţie de sistem de operare mai mică de V5R1M0. QPWDLVL 2 nu poate fi folosită dacă sistemul dumneavoastră comunică cu orice alt sistem care limitează lungimea parolelor de 1-10 caractere. Nu este înlăturată nici o parolă codată de pe sistem când se modifică QPWDLVL la 2.
3	Sistemul suportă parole de profil utilizator de 1-128 caractere. Sunt permise caractere cu litere mici sau mari. Parolele pot conţine orice caracter, iar parola va fi sensibilă la majuscule. Setarea QPWDLVL 3 nu poate fi folosită dacă sistemul dumneavoastră comunică cu alte sisteme iSeries într-o reţea, iar acele sisteme rulează cu o valoare QPWDLVL de 0 sau cu o ediţie de sistem de operare mai mică de V5R1M0. QPWDLVL 3 nu poate fi folosit dacă sistemul dumneavoastră comunică cu orice alt sistem care limitează lungimea parolelor de 1-10 caractere. Nu se poate folosi QPWDLVL 3 dacă sistemul comunică cu produsul Windows 95/98/ME iSeries Client Support for Windows Network Neighborhood (NetServer). Toate parolele de profil de utilizator care sunt folosite la QPWDLVL 0 şi 1 sunt înlăturate de pe sistem când QPWDLVL este 3. Modificarea de la QPWDLVL 3 înapoi la QPWDLVL 0 sau 1 necesită o modificare la QPWDLVL 2 înainte de trecerea la 0 sau 1. QPWDLVL 2 permite crearea parolelor de profil de utilizator care pot fi folosite la QPWDLVL 0 sau 1 atât timp cât cerinţele de lungime şi sintaxă pentru parolă îndeplinesc regulile pentru QPWDLVL 0 sau 1.

Modificarea nivelului parolei sistemului de la parole de 1-10 caractere la parole 1-128 caractere necesită o atenţie deosebită. Dacă sistemul dumneavoastră comunică cu alte sisteme dintr-o reţea, atunci toate sistemele trebuie să fie capabile să trateze parolele mai lungi.

Modificarea acestei valori de sistem are efect la următorul IPL. Pentru a vedea valoarea curentă şi în aşteptare ale nivelului de parolă, folosiţi comanda CL DSPSECA (Display Security Attributes - Afişare atribute securitate).

Lungimea minimă a parolelor (QPWDMINLEN)

Valoarea de sistem QPWDMINLEN controlează numărul minim de caractere dintr-o parolă.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 31. Valorile posibile pentru valoarea de sistem QPWDMINLEN:

6	Sunt necesare cel puţin şase caractere pentru parole.
număr-minim-de-caractere	Specificaţi o valoare de la 1 la 10 când valoarea de sistem a nivelului parolei (QPWDLVL) este 0 sau 1. Specificaţi o valoarea de la 1 la 128 când valoarea de sistem a nivelului parolei (QPWDLVL) este 2 sau 3.

Valoare recomandată: 6, pentru a împiedica utilizatorii să aloce parole care sunt uşor de ghicit, cum ar fi iniţiale sau un singur caracter.

Lungimea maximă a parolelor (QPWDMAXLEN)

Valoarea de sistem QPWDMAXLEN controlează numărul maxim de caractere dintr-o parolă. Aceasta furnizează o protecţie suplimentară, împiedicând utilizatorii să specifice parole prea lungi, care trebuie să fie notate undeva deoarece nu pot fi memorate uşor.

Unele reţele de comunicare necesită o parolă de 8 caractere sau mai puţin. Folosiţi această valoare de sistem pentru a vă asigura că parolele îndeplines cerinţele reţelei dumneavoastre.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 32. Valori posibile pentru valoarea de sistem QPWDMAXLEN:

8	Sunt permise maxim 8 caractere pentru o parolă.
număr-maxim-de-caractere	Specificaţi o valoare de la 1 la 10 când valoarea de sistem a nivelului parolei (QPWDLVL) este 0 sau 1. Specificaţi o valoarea de la 1 la 128 când valoarea de sistem a nivelului parolei (QPWDLVL) este 2 sau 3.

Valoare recomandată: 8.

Necesitatea diferenţei în parole (QPWDRQDDIF)

Valoarea de sistem QPWDRQDDIF controlează dacă parola trebuie să fie diferită de parolele anterioare. Această parolă furnizează securitate suplimentară împiedicând utilizatorii să specifice parole folosite anterior. Împiedică de asemenea un utilizator a cărui parolă a expirat să o modifice şi apoi să revină iar la parola veche.

Notă: Setarea valorii de sistem QPWDRQDDIF determină câte dintre aceste parole anterioare sunt verificate pentru duplicare.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 33. Valorile posibile pentru valoarea de sistem QPWDRQDDIF:

Valoare	*Număr de parole anterioare verificate pentru duplicări*
0	Sunt permise 0 parole duplicate.
1	32
2	24
3	18
4	12
5	10
6	8
7	6
8	4

Valoare recomandată: Selectaţi valoarea 5 sau mai mică, pentru a împiedica folosirea de parole repetate. Folosiţi o combinaţie a valorii de sistem QPWDRQDDIF şi a valorii de sistem QPWDEXPITV (interval expirare parolă) pentru a împiedica refolosirea unei parole pentru cel puţin 6 luni. De exemplu, setaţi valoarea de sistem QPWDEXPITV la 30 (zile) şi valoarea de sistem QPWDRQDDIF la 5 (10 parole unice). Aceasta înseamnă că un utilizator obişnuit, care modifică parola când este avertizat de sistem ,nu va repata o parolă pentru aproximativ 9 luni.

Restricţionarea caracterelor pentru parole (QPWDLMTCHR)

Valoarea de sistem QPWDLMTCHR limitează folosirea anumitor caractre într-o parolă. Această valoare furnizează securitate suplimentară împiedicând utilizatorii să folosească anumite caractere, precum vocale, într-o parolă. Restricţionarea vocalelor împiedică utilizatorii să folosească cuvinte normale pentru parolele lor.

Valoarea de sistem QPWDLMTCHR nu este impusă când valoarea de sistem pentru nivelul parolei (QPWDLVL) are valoarea 2 sau 3. Valoarea de sistem QPWDLMTCHR poate fi modificată la QPWDLVL 2 sau 3, dar nu va fi impusă decât după ce QPWDLVL este modificat la valoarea 0 sau 1.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 34. Valori posibile pentru valoarea de sistem QPWDLMTCHR:

***NONE**	Nu există caractere restricţionate pentru parole.
caractere-restricţionate	Specificaţi până la 10 caractere restricţionate. Caracterele valide sunt de la A la Z, 0 la 9 şi caracterele speciale liră sterlină (#), dolar ($), a rond (@) şi liniuţa de subliniere (_).

Valoare recomandată: A, E, I, O şi U. S-ar putea să doriţi de asemenea să împiedicaţi caractere speciale (#, $ şi @) pentru compatibilitatea cu alte sisteme.

Restricţionarea cifrelor consecutive pentru parole (QPWDLMTAJC)

Valoarea de sistem QPWDLMTAJC limitează folosirea caracterelor numerice unele lângă altele (adiacente) într-o parolă. Această valoare furnizează securitate suplimentară împiedicând utilizatorii să folosească zile de naştere, numere de telefon sau o secvenţă de numere ca parole.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 35. Valorile posibile pentru valoarea de sistem QPWDLMTAJC:

0	Caracterele numerice sunt permise unele lângă altele în parole.
1	Caracterele numerice nu sunt permise unele lângă altele în parole.

Restricţionarea caracterelor repetate pentru parole (QPWDLMTREP)

Valoarea de sistem QPWDLMTREP limitează folosirea caracterelor de repetare într-o parolă. Această valoare furnizează securitate suplimentară împiedicând utilizatorii să specifice parole care sunt uşor de ghicit, cum ar fi acelaşi caracter repetat de mai multe ori.

Când valoarea de sistem pentru nivelul parolei (QPWDLVL) este setată la 2 sau 3, testul pentru caractere repetate este sensibil la majuscule. Aceasta înseamnă că se face diferenţa între o literă mică ’a’ şi o literă mare ’A’.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 36. Valori posibile pentru valoarea de sistem QPWDLMTREP:

0	Aceleaşi caractere pot fi folosite de mai multe ori într-o parolă.
1	Un caracter nu poate fi folosit decât o dată într-o parolă.
2	Acelaşi caractre nu poate fi folosit consecutiv într-o parolă.

Tabela 37 arată exemple de parole permise în funcţie de valoarea de sistem QPWDLMTREP.

Tabela 37. Parole cu caractere ce se repetă cu QPWDLVL 0 sau 1

Exemplu parolă	QPWDLMTREP = 0	QPWDLMTREP = 1	QPWDLMTREP = 2
A11111	Permis	Nepermis	Nepermis
BOBBY	Permis	Nepermis	Nepermis
AIRPLANE	Permis	Nepermis	Permis
N707UK	Permis	Nepermis	Permis

Tabela 38. Parole cu caractere ce se repetă cu QPWDLVL 2 sau 3

Exemplu parolă	Valoare QPWDLMTREP de 0	Valoare QPWDLMTREP de 1	Valoare QPWDLMTREP de 2
j222222	Permis	Nepermis	Nepermis
ReallyFast	Permis	Nepermis	Nepermis
Mom'sApPlePie	Permis	Nepermis	Permis
AaBbCcDdEe	Permis	Permis	Permis

Diferenţa poziţiei caracterelor pentru parole (QPWDPOSDIF)

Valoarea de sistem QPWDPOSDIF controlează fiecare poziţie într-o nouă parolă. Aceasta furnizează securitate suplimentară împiedicând utilizatorii să folosească acelaşi caracter (alfabetic sau numeric) într-o poziţie corespunzătoare aceleaşi poziţii din parola anterioară.

Când valoarea de sistem pentru nivelul parolei (QPWDLVL) este setată la 2 sau 3, testul pentru aceleaşi caractere este sensibil la majuscule. Aceasta înseamnă că se face diferenţa între o literă mică 'a' şi o literă mare 'A'.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 39. Valorile posibile pentru valoarea de sistem QPWDPOSDIF:

0	Aceleaşi caractere pot fi folosite într-o poziţie corespunzătoare aceleaşi poziţii din parola anterioară.
1	Acelaşi caracter nu poate fi folosit într-o poziţie corespunzătoare aceleaşi poziţii din parola anterioară.

Necesitatea caracterelor numerice în parole (QPWDRQDDGT)

Valoarea de sistem QPWDRQDDGT controlează dacă un caracter numeric este necesar într-o nouă parolă. Această valoare furnizează securitate suplimentară împiedicând utilizatorii să folosească numai caractere alfabetice.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 40. Valori posibile pentru valoarea de sistem QPWDRQDDGT:

0	Caracterele numerice nu sunt necesare în parolele noi.
1	Unul sau mai multe caractere numerice sunt necesare în parole noi

Valoare recomandată: 1.

Programul de aprobare a parolei (QPWDVLDPGM)

Dacă s-a specificat *REGFAC sau un nume de program în valoarea de sistem QPWDVLDPGM, sistemul rulează unul sau mai multe programe după ce noua parolă a trecut de orice test de validare specificat de dumneavoastră în valorile de sistem pentru controlul parolei. Puteţi folosi programele pentru o verificare suplimentară a parolelor alocate de utilizator înainte de a fi acceptate de către sistem.

Subiectul "Folosirea unui program de aprobare a parolei" la pagina 45 discută cerinţele programului de aprobare a parolei şi arată un exemplu.

Un program de aprobare a parolei trebuie să se afle pe ASP-ul de sistem sau pe un ASP de utilizator de bază.

| **Notă:** Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind
| securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de
| securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 41. Valorile posibile pentru valoarea de sistem QPWDVLDPGM:

***NONE**	Nu este folosit nici un program scris de utilizator. Aceasta include orice program de aprobare a parolei înregistrat în facilitatea de semnare ieşire.
**REGFAC*	Programul de validare este extras din facilitatea de semnare, punctul de ieşire QIBM_QSY_VLD_PASSWRD. Pot fi specificate mai multe programe de validare în facilitatea de semnare. Fiecare program va fi apelat până când unul dintre ele indică respingerea parolei sau toate indică validitatea parolei.
nume-program	Specificaţi numele programului de validare scris de utilizator, de la 1 la 10 caractere. Un nume de program nu poate fi specificat când valoarea curentă sau în aşteptare a valorii de sistem pentru nivelul de parolă (QPWDLVL) este 2 sau 3.
nume-bibliotecă	Specificaţi numele bibliotecii unde este localizat programul scris de utilizator. Dacă numele bibliotecii nu este specificat, programul este căutat folosind lista de biblioteci (*LIBL) a utilizatorului care modifică valoarea de sistem. QSYS este biblioteca recomandată.

Folosirea unui program de aprobare a parolei

Dacă în valoarea de sistem QPWDVLDPGM s-a specificat *REGFAC sau un nume de program, unul sau mai multe programe sunt apelate de coamanda CHGPWD (Change Password - Modificare parolă) sau API-ul QSYCHGPW (Change Password - Modificare parolă). Programele sunt apelate doar dacă noua parolă introdusă de către utilizator a trecut de toate celelalte teste pe care le-aţi specificat în valorile de sistem pentru controlul parolei.

În cazul în care este necesar să vă recuperaţi sistemul dintr-o eşuare de disc, puneţi programul de aprobare a parolei în biblioteca QSYS. În acest fel, programul de aprobare a parolei este încărcat când restauraţi biblioteca QSYS.

Dacă este specificat un nume de program în valoarea de sistem QPWDVLDPGM, sistemul transmite următorii parametri programului de aprobare a parolei:

Tabela 42. Parametrii pentru programul de aprobare a parolei

Poziţie	Tip	Lungime	Descriere
1	*CHAR	10	Noua parolă introdusă de utilizator.
2	*CHAR	10	Parola veche a utilizatorului.
3	*CHAR	1	Cod retur: 0 pentru parolă validă; altceva pentru parolă incorectă.
4 [1]	*CHAR	10	Numele utilizatorului.

1 Poziţia 4 este opţională.

Dacă în valoarea de sistem QPWDVLDPGM s-a specificat *REGFAC, consultaţi informaţiile despre Programul de ieşire pentru securitate din manualul System API, pentru detalii despre parametrii transmişi programului de validare.

Dacă programul dumneavoastră determină că noua parolă nu este validă, puteţi fie să trimiteţi propriul dumneavoastră mesaj de excepţie (folosind comanda SNDPGMMSG), fie să setaţi codul retur la o valoare diferită de 0 şi să lăsaţi sistemul să afişeze un mesaj de eroare. Mesajele de excepţie care sunt semnalate de programul dumneavoastră trebuie să fie create cu opţiunea DMPLST(*NONE) a comenzii ADDMSGD (Add Message Description - Adăugare descriere mesaj).

Noua parolă este acceptată doar dacă programul scris de utilizator se termină fără nici un mesaj de ieşire şi un cod de retur 0. Deoarece iniţial codul de retur este setat pentru parole care nu sunt valide (este diferit de 0), programul de aprobare trebuie să seteze codul de retur la 0 pentru ca parola sa fie modificată.

Atenţie: Parola curentă şi noua parolă sunt trimise programului de validare fără criptare. Programul de validare poate stoca parolele într-un fişier de bază de date, compromiţând astfel securitatea sistemului. Asiguraţi-vă că funcţiile programului de validare sunt examinate de resposabilul cu securitatea şi că modificările aduse porgramului sunt controlate strict.

Următorul program CL este un exemplu de program de validare a parolei pentru cazul în care este specificat un nume de program pentru QPWDVLDLVL. Programul folosit ca exemplu verifică dacă parola este modificată de mai multe ori în aceeaşi zi. Pot fi adăugate calcule adiţionale pentru a verifica parolele cu alte criterii:

```
/*************************************************/
/* NAME:     PWDVALID - Password Validation      */
/*                                               */
/* FUNCTION: Limit password change to one per    */
/*           day unless the password is expired  */
/*************************************************/
   PGM (&NEW &OLD &RTNCD &USER)
   DCL VAR(&NEW)       TYPE(*CHAR) LEN(10)
   DCL VAR(&OLD)       TYPE(*CHAR) LEN(10)
   DCL VAR(&RTNCD)     TYPE(*CHAR) LEN(1)
   DCL VAR(&USER)      TYPE(*CHAR) LEN(10)
   DCL VAR(&JOBDATE)   TYPE(*CHAR) LEN(6)
   DCL VAR(&PWDCHGDAT) TYPE(*CHAR) LEN(6)
   DCL VAR(&PWDEXP)    TYPE(*CHAR) LEN(4)
/* Get the current date and convert to YMD format */
   RTVJOBA    DATE(&JOBDATE)
   CVTDAT     DATE(&JOBDATE) TOVAR(&JOBDATE) +
              TOFMT(*YMD)    TOSEP(*NONE)
/* Get date password last changed and whether    */
/* password is expired from user profile         */
   RTVUSRPRF  USRPRF(&USER)  PWDCHGDAT(&PWDCHGDAT)+
     PWDEXP(&PWDEXP)
/* Compare two dates                             */
/*    if equal and password not expired          */
/*    then send *ESCAPE message to prevent change */
/*    else set return code to allow change       */
   IF (&JOBDATE=&PWDCHGDAT *AND &PWDEXP='*NO ') +
       SNDPGMMSG  MSGID(CPF9898) MSGF(QCPFMSG) +
       MSGDTA('Password can be changed only +
               once per day') +
       MSGTYPE(*ESCAPE)
   ELSE  CHGVAR &RTNCD '0'
   ENDPGM
```

Următorul program CL este un exemplu de program de validare a parolei pentru cazul în care este specificat *REGFAC pentru QPWDVLDLVL.

Programul folosit ca exemplu verifică pentru a se asigura că noua parolă este în CCSID 37 (dacă este în CCSID 13488, converteşte noua parolă la CCSID 37), că parola nouă nu se termină într-un caracter numeric şi că noua parolă nu conţine numele profilului utilizatorului. Acest exemplu presupune că fost creat un fişier de mesaje (PWDERRORS) a şi au fost adăugate descrierile de mesaj (PWD0001 şi PWD0002) în fişierul de mesaje. Pot fi adăugate calcule adiţionale pentru a verifica parolele cu alte criterii:

```
| /*********************************************************/
| /*                                                       */
| /*  NAME:   PWDEXITPGM1 - Password validation exit 1     */
| /*                                                       */
| /*  Validates passwords when *REGFAC is specified for    */
| /*  QPWDVLDPGM. Program is registered using the ADDEXITPGM*/
| /*  CL command for the QIBM_QSY_VLD_PASSWRD exit point.  */
| /*                                                       */
| /*                                                       */
| /*  ASSUMPTIONS: If CHGPWD command was used, password    */
| /*  CCSID will be job default (assumed to be CCSID 37).  */
| /*  If QSYCHGPW API was used, password CCSID will be     */
| /*  UNICODE CCSID 13488.                                 */
```

```
| /*************************************************************/
|
| DCL &EXINPUT    *CHAR 1000
| DCL &RTN        *CHAR 1
|
| DCL &UNAME      *CHAR 10
| DCL &NEWPW      *CHAR 256
| DCL &NPOFF      *DEC 5 0
| DCL &NPLEN      *DEC 5 0
| DCL &INDX       *DEC 5 0
| DCL &INDX2      *DEC 5 0
| DCL &INDX3      *DEC 5 0
| DCL &UNLEN      *DEC 5 0
|
| DCL &XLTCHR2    *CHAR 2 VALUE(X'0000')
| DCL &XLTCHR     *DEC 5 0
| DCL &XLATEU     *CHAR 255 VALUE('............................... +
|                               !"#$%&''()*+,-./0123456789:;<=>?+
|                               @ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_+
|                               `ABCDEFGHIJKLMNOPQRSTUVWXYZ{|}~.+
|                               ................................+
|                               ................................+
|                               ................................+
|                               ................................')
|
| DCL &XLATEC     *CHAR 255 VALUE('................................+
|                               ................................+
|                               ................................+
|                               ................................+
|                               .ABCDEFGHI.......JKLMNOPQR......+
|                               ..STUVWXYZ......................+
|                               ................................+
|                               ................................')
|
| /*********************************************************************/
| /* FORMAT OF EXINPUT IS:                                             */
|
| /* POSITION   DESCRIPTION                                           */
| /* 001 - 020  EXIT POINT NAME                                       */
| /* 021 - 028  EXIT POINT FORMAT NAME                               */
| /* 029 - 032  PASSWORD LEVEL (binary)                              */
| /* 033 - 042  USER PROFILE NAME                                    */
| /* 043 - 044  RESERVED                                             */
| /* 045 - 048  OFFSET TO OLD PASSWORD (binary)                      */
| /* 049 - 052  LENGTH OF OLD PASSWORD (binary)                      */
| /* 053 - 056  CCSID OF OLD PASSWORD  (binary)                      */
| /* 057 - 060  OFFSET TO NEW PASSWORD (binary)                      */
| /* 061 - 064  LENGTH OF NEW PASSWORD (binary)                      */
| /* 065 - 068  CCSID OF NEW PASSWORD  (binary)                      */
| /* ??? - ???  OLD PASSWORD                                         */
| /* ??? - ???  NEW PASSWORD                                         */
| /*                                                                 */
| /*********************************************************************/
|
|
| /*********************************************************************/
| /*  Establish a generic monitor for the program.                     */
| /*********************************************************************/
|
| MONMSG     CPF0000
| /* Assume new password is valid */
| CHGVAR &RTN  VALUE('0') /* accept */
| /* Get new password length, offset and value. Also get user name */
| CHGVAR &NPLEN VALUE(%BIN(&EXINPUT 61 4))
| CHGVAR &NPOFF VALUE(%BIN(&EXINPUT 57 4) + 1)
| CHGVAR &UNAME VALUE(%SST(&EXINPUT 33 10))
| CHGVAR &NEWPW VALUE(%SST(&EXINPUT &NPOFF &NPLEN))
```

```
|  /* If CCSID is 13488, probably used the QSYCHGPW API which converts */
|  /* the passwords to UNICODE CCSID 13488. So convert to CCSID 37, if */
|  /* possible, else give an error */
|  IF COND(%BIN(&EXINPUT 65 4) = 13488) THEN(DO)
|      CHGVAR &INDX2 VALUE(1)
|      CHGVAR &INDX3 VALUE(1)
|     CVT1:
|      CHGVAR &XLTCHR VALUE(%BIN(&NEWPW &INDX2 2))
|      IF COND( (&XLTCHR *LT 1) *OR (&XLTCHR *GT 255) ) THEN(DO)
|         CHGVAR &RTN  VALUE('3') /* reject */
|         SNDPGMMSG MSG('INVALID CHARACTER IN NEW PASSWORD')
|         GOTO DONE
|      ENDDO
|      CHGVAR %SST(&NEWPW &INDX3 1) VALUE(%SST(&XLATEU &XLTCHR 1))
|      CHGVAR &INDX2  VALUE(&INDX2 + 2)
|      CHGVAR &INDX3  VALUE(&INDX3 + 1)
|      IF COND(&INDX2 > &NPLEN) THEN(GOTO ECVT1)
|      GOTO CVT1
|     ECVT1:
|      CHGVAR &NPLEN VALUE(&INDX3 - 1)
|      CHGVAR %SST(&EXINPUT 65 4) VALUE(X'00000025')
|   ENDDO
|
|   /* Check the CCSID of the new password value - must be 37     */
|   IF COND(%BIN(&EXINPUT 65 4) *NE 37) THEN(DO)
|     CHGVAR &RTN  VALUE('3') /* reject */
|     SNDPGMMSG MSG('CCSID OF NEW PASSWORD MUST BE 37')
|     GOTO DONE
|   ENDDO
|
|   /* UPPERCASE NEW PASSWORD VALUE                      */
|   CHGVAR &INDX2 VALUE(1)
|   CHGVAR &INDX3 VALUE(1)
|   CVT4:
|     CHGVAR %SST(&XLTCHR2 2 1) VALUE(%SST(&NEWPW &INDX2 1))
|     CHGVAR &XLTCHR VALUE(%BIN(&XLTCHR2 1 2))
|     IF COND( (&XLTCHR *LT 1) *OR (&XLTCHR *GT 255) ) THEN(DO)
|       CHGVAR &RTN  VALUE('3') /* reject */
|       SNDPGMMSG MSG('INVALID CHARACTER IN NEW PASSWORD')
|       GOTO DONE
|     ENDDO
|     IF COND(%SST(&XLATEC &XLTCHR 1) *NE '.') +
|     THEN(CHGVAR %SST(&NEWPW &INDX3 1) VALUE(%SST(&XLATEC &XLTCHR 1)))
|     CHGVAR &INDX2  VALUE(&INDX2 + 1)
|     CHGVAR &INDX3  VALUE(&INDX3 + 1)
|     IF COND(&INDX2 > &NPLEN) THEN(GOTO ECVT4)
|     GOTO CVT4
|   ECVT4:
|
|   /* CHECK IF LAST POSITION OF NEW PASSWORD IS NUMERIC */
|   IF COND(%SST(&NEWPW &NPLEN 1) = '0') THEN(GOTO ERROR1)
|   IF COND(%SST(&NEWPW &NPLEN 1) = '1') THEN(GOTO ERROR1)
|   IF COND(%SST(&NEWPW &NPLEN 1) = '2') THEN(GOTO ERROR1)
|   IF COND(%SST(&NEWPW &NPLEN 1) = '3') THEN(GOTO ERROR1)
|   IF COND(%SST(&NEWPW &NPLEN 1) = '4') THEN(GOTO ERROR1)
|   IF COND(%SST(&NEWPW &NPLEN 1) = '5') THEN(GOTO ERROR1)
|   IF COND(%SST(&NEWPW &NPLEN 1) = '6') THEN(GOTO ERROR1)
|   IF COND(%SST(&NEWPW &NPLEN 1) = '7') THEN(GOTO ERROR1)
|   IF COND(%SST(&NEWPW &NPLEN 1) = '8') THEN(GOTO ERROR1)
|   IF COND(%SST(&NEWPW &NPLEN 1) = '9') THEN(GOTO ERROR1)
|
|   /* CHECK IF PASSWORD CONTAINS USER PROFILE NAME        */
|   CHGVAR &UNLEN VALUE(1)
|   LOOP2:      /* FIND LENGTH OF USER NAME */
|    IF COND(%SST(&UNAME &UNLEN 1) *NE ' ') THEN(DO)
|      CHGVAR &UNLEN VALUE(&UNLEN + 1)
|      IF COND(&UNLEN = 11) THEN(GOTO ELOOP2)
```

```
      GOTO LOOP2
    ENDDO
   ELOOP2:
    CHGVAR &UNLEN VALUE(&UNLEN - 1)


   /* CHECK FOR USER NAME IN NEW PASSWORD             */
   IF COND(&UNLEN *GT &NPLEN) THEN(GOTO ELOOP3)
   CHGVAR &INDX VALUE(1)
   LOOP3:
     IF COND(%SST(&NEWPW &INDX &UNLEN) = %SST(&UNAME 1 &UNLEN))+
        THEN(GOTO ERROR2)
     IF COND((&INDX + &UNLEN + 1) *LT 128) THEN(DO)
        CHGVAR &INDX VALUE(&INDX + 1)
        GOTO LOOP3
     ENDDO
   ELOOP3:

   /* New Password is valid                        */
   GOTO DONE

   ERROR1:  /* NEW PASSWORD ENDS IN NUMERIC CHARACTER */
    CHGVAR &RTN  VALUE('3') /* reject */
    SNDPGMMSG TOPGMQ(*PRV) MSGTYPE(*ESCAPE) MSGID(PWD0001) MSGF(QSYS/PWDERRORS)
    GOTO DONE

   ERROR2:  /* NEW PASSWORD CONTAINS USER NAME */
    CHGVAR &RTN  VALUE('3') /* reject */
    SNDPGMMSG TOPGMQ(*PRV) MSGTYPE(*ESCAPE) MSGID(PWD0002) MSGF(QSYS/PWDERRORS)
    GOTO DONE

   DONE:
   ENDPGM
```

Valorile de sistem pentru controlul auditării

Privire generală:

Scop: Specificaţi valori de sistem pentru a controla auditarea securităţii pe sistem.

Cum se face:
WRKSYSVAL *SEC (comanda Gestionare valori de sistem)

Autorizare:
*AUDIT

Intrare jurnal:
SV

Notă: Modificările devin efective imediat. IPL-ul nu este necesar.

Aceste valori de sistem controlează auditarea pe sistem:

QAUDCTL
Control auditare

QAUDENDACN
Acţiune de terminare auditare

QAUDFRCLVL
Nivel forţare auditare

QAUDLVL
Nivel de auditare

| **QAUDLVL2**
| Extensie nivel de auditare

| **QCRTOBJAUD**
| Creare auditare implicită

În continuare sunt prezentate aceste valori de sistem. Sunt arătate alegerile posibile. Alegerile care sunt subliniate sunt valorile implicite furnizate de sistem. Pentru majoritatea valorilor de sistem, se menţionează o alegere recomandată.

Controlul auditării (QAUDCTL)

Valoarea de sistem QAUDCTL determină dacă se realizează auditarea. Funcţionează ca un comutator activat/dezactivat pentru următoarele:

| • Valorile de sistem QAUDLVL şi QAUDLVL2
- Auditarea definită pentru obiecte folosind comenzile CHGOBJAUD (Change Object Auditing - Modificare auditare obiect) şi CHGDLOAUD (Change DLO Auditing - Modificare auditare DLO)
- Auditarea definită pentru utilizatori folosind comanda CHGUSRAUD (Change User Audit - Modificare auditare utilizator)

| **Notă:** Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind
| securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de
| securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Puteţi specifica mai multe valori pentru valoarea de sistem QAUDCTL, în cazul în care nu specificaţi *NONE.

Tabela 43. Valorile posibile pentru valoarea de sistem QAUDCTL:

***NONE**	Nu este executată nici o auditare a acţiunilor utilizatorului şi a obiectelor.
***OBJAUD**	Auditarea este executată pentru obiectele care au fost selectate folosind comenzile CHGOBJAUD, CHGDLOAUD sau CHGAUD.
***AUDLVL**	Auditarea este executată pentru orice funcţii selectate în valorile de sistem QAUDLVL şi QAUDLVL2 şi în parametrul AUDLVL al profilurilor de utilizator individuale. Nivelul de auditare pentru un utilizator este specificat folosind comanda CHGUSRAUD (Change User Audit - Modificare auditare utilizator).
***NOQTEMP**	Pentru majoritatea acţiunilor auditarea nu este realizată dacă obiectul este în biblioteca QTEMP. Vedeţi Capitolul 9, “Auditarea securităţii pe sistemul iSeries”, la pagina 223 pentru detalii suplimentare. Trebuie să specificaţi această valoare cu *OBJAUD sau *AUDLVL. Vedeţi “Planificarea auditării securităţii” la pagina 228 pentru o descriere completă a procesului pentru controlarea auditării pe sistemul dumneavoastră.

Acţiunea pentru oprirea auditării (QAUDENDACN)

Valoarea de sistem QAUDENDACN determină ce acţiune execută sistemul dacă auditarea este activă şi sistemul nu este capabil să scrie intrări în jurnalul de auditare.

| **Notă:** Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind
| securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de
| securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 44. Valori posibile pentru valoarea de sistem QAUDENDACN:

***NOTIFY**	Mesajul CPI2283 este trimis în coada de mesaje QSYSOPR şi în coada de mesaje QSYSMSG (dacă există) din oră în oră, până când auditarea este repornită cu succes. Valoarea de sistem QAUDCTL este setată la *NONE pentru a împiedica sistemul să încerce să scrie intrări suplimentare în jurnalul de auditare. Continuă procesarea în sistem. Dacă este realizat un IPL înaintea repornirii auditării, este trimis mesajul CPI2284 în cozile de mesaje QSYSOPR şi QSYSMSG în timpul IPL-ului.
***PWRDWNSYS**	Dacă nu este capabil să scrie o intrare de jurnal de auditare, sistemul îşi opreşte alimentarea imediat. Unitatea de sistem afişează codul de referinţă sistem (SRC) B900 3D10. Când este pornit din nou, sistemul este într-o stare restricţionată. Această înseamnă că subsistemul de control este într-o stare restricţionată, nici un alt subsistem nu este activ şi semnarea este permisă doar de la consolă. Valoarea de sistem QAUDCTL este setată la *NONE. Utilizatorul care semnează la consolă pentru a completa IPL-ul trebuie să aibă autorizările speciale *ALLOBJ şi *AUDIT.

Valoare recomandată: Pentru majoritatea instalărilor, valoarea recomandată este *NOTIFY. Dacă politica dumneavoastră de securitatea necesită să nu fie executată nici o procesare pe sistem fără auditare, atunci trebuie să selectaţi *PWRDWNSYS.

Sunt foarte rare situaţiile în care sistemul să nu fie capabil să scrie intrări de jurnal de auditare. Totuşi, dacă aceasta se întâmplă şi valoarea de sistem QAUDENDACN este *PWRDWNSYS, sistemul dumneavoastră termină anormal. Aceasta poate cauza o încărcare iniţială de program (IPL) lungă când sistemul dumneavoastră este pornit din nou.

Nivelul de forţare a auditării (QAUDFRCLVL)

Valoarea de sistem QAUDFRCLVL determină cât de des se forţează noi intrări de jurnal de auditare din memorie spre spaţiul de stocare auxiliar. Această valoare de sistem controlează cantitatea de date de auditare care poate fi pierdută dacă sistemul termină anormal.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 45. Valorile posibile pentru valoarea de sistem QAUDFRCLVL:

***SYS**	Sistemul determină când sunt scrise intrările de jurnal în spaţiul de stocare auxiliar pe baza performanţei de sistem interne.
număr-de-înregistrări	Specificaţi un număr între 1 şi 100 pentru a determina câte intrări de auditare se pot acumula în memorie înainte de a fi scrise în spaţiul de stocare auxiliar. Cu cât este mai mic numărul, cu atât este mai mare impactul asupra performanţei sistemului.

Valoare recomandată: *SYS furnizează cea mai bună performanţă de auditare. Totuşi, dacă instalarea dumneavoastră necesită să nu fie pierdută nici o intrare de auditare când sistemul termină anormal, trebuie să specificaţi 1. Specificarea valorii 1 poate scădea nivelul performanţei.

Nivelul de auditare (QAUDLVL)

Valoarea de sistem QAUDLVL împreună cu valoarea de sistem QAUDLVL2 determină ce evenimente referitoare la securitatea sunt înregistrate în jurnalul de auditare a securităţii (QAUDJRN) pentru toţi utilizatorii sistemului. Puteţi specifica mai multe valori pentru valoarea de sistem QAUDLVL, în cazul în care nu specificaţi *NONE.

Pentru ca valoarea de sistem QAUDLVL să aibă efect, valoarea de sistem QAUDCTL trebuie să includă *AUDLVL.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum să restricţionaţi modificările valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 46. Valori posibile pentru valoarea de sistem QAUDLVL:

***NONE**	Nici un eveniment controlat de valorile de sistem QAUDLVL sau QAUDLVL2 nu este înregistrat. Evenimentele sunt înregistrate pentru utilizatori individuali pe baza valorilor AUDLVL din profilurile de utilizator.
***AUDLVL2**	Ambele valori de sistem, QAUDLVL şi QAUDLVL2, vor fi folosite pentru a determina acţiunile de securitate care vor fi auditate.
***AUTFAIL**	Sunt înregistrate evenimentele de eşuare a autorizării.
***CREATE**	Sunt înregistrate operaţiile de creare obiecte.
***DELETE**	Sunt înregistrate operaţiile de ştergere obiecte.
***JOBDTA**	Sunt înregistrate acţiunile care afectează un job.
***NETBAS**	Sunt auditate funcţiile de bază ale reţelei.
***NETCLU**	Sunt auditate operaţiile de cluster şi grup de resurse cluster.
***NETCMN**	Sunt auditate funcţiile de comunicaţie şi reţea. *NETCMN este compus din câteva valori pentru a vă permite să vă personalizaţi mai bine auditarea. Următoarele valori formează *NETCMN: *NETBAS *NETCLU *NETFAIL *NETSCK
***NETFAIL**	Sunt auditate eşuările de reţea.
***NETSCK**	Sunt auditate task-urile de socket.
***OBJMGT**	Sunt înregistrate operaţiile de redenumire şi mutare obiecte.
***OFCSRV**	Sunt înregistrate modificările aduse directorului de distribuţie sistem şi acţiunile de mail office.
***OPTICAL**	Este înregistrată folosirea volumelor optice.
***PGMADP**	Este înregistrată obţinerea autorizării de la un program care adoptă autorizare.
***PGMFAIL**	Sunt înregistrate violările de integritate a sistemului.
***PRTDTA**	Sunt înregistrate tipărirea unui fişier spool, trimiterea ieşirii direct la o imprimantă şi trimiterea ieşirii la o imprimantă la distanţă.
***SAVRST**	Sunt înregistrate operaţiile de restaurare.
***SECCFG**	Este auditată configuraţia de securitate.
***SECDIRSRV**	Sunt înregistrate modificările sau actualizările când se execută funcţii de serviciu de director.
***SECIPC**	Sunt auditate modificările aduse comunicaţiilor între procese.
***SECNAS**	Sunt auditate acţiunile serviciului de autentificare în reţea.
***SECRUN**	Sunt auditate funcţiile de timp de rulare securitate.
***SECSCKD**	Sunt auditaţi descriptorii de socket.
***SECURITY**	Sunt înregistrate funcţiile referitoare la securitate. *SECURITY este compus din câteva valori pentru a vă permite să personalizaţi mai bine auditarea dumneavoastră. Următoarele valori formează *SECURITY: *SECCFG *SECDIRSRV *SECIPC *SECNAS *SECRUN *SECSCKD *SECVFY *SECVLDL
***SECVFY**	Este auditată folosirea funcţiilor de verificare.
***SECVLDL**	Sunt auditate modificările aduse obiectelor din lista de validare.
***SERVICE**	Este înregistrată folosirea uneltelor de service.
***SPLFDTA**	Sunt înregistrate acţiunile executate asupra fişierelor spool.
***SYSMGT**	Folosirea funcţiilor de gestionare sisteme este înregistrată în istoric.

Vedeţi “Planificarea auditării acţiunilor” la pagina 228 pentru o descriere completă a tipurilor de intrare jurnal şi valorile posibile pentru QAUDLVL.

Extensia nivelului de auditare (QAUDLVL2)

Valoarea de sistem QAUDLVL2 este necesară atunci când este nevoie de mai mult de 16 valori de auditare. Dacă se specifică *AUDLVL2 pentru una dintre valorile din valoarea de sistem QAUDLVL, sistemul va căuta şi valorile de auditare din valoarea de sistem QAUDLVL2. Puteţi specifica mai multe valori pentru valoarea de sistem QAUDLVL2, în cazul în care nu specificaţi *NONE. Pentru ca valoarea de sistem QAUDLVL2 să aibă efect, valoarea de sistem QAUDCTL trebuie să includă *AUDLVL şi valoarea de sistem QAUDLVL trebuie să includă *AUDLVL2.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum să restricţionaţi modificările valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 47. Valorile posibile pentru valoarea de sistem QAUDLVL2:

***NONE**	În această valoare de sistem nu este conţinută nici o valoare de auditare.
***AUTFAIL**	Sunt înregistrate evenimentele de eşuare a autorizării.
***CREATE**	Sunt înregistrate operaţiile de creare obiecte.
***DELETE**	Sunt înregistrate operaţiile de ştergere obiecte.
***JOBDTA**	Sunt înregistrate acţiunile care afectează un job.
***NETBAS**	Sunt auditate funcţiile de bază ale reţelei.
***NETCLU**	Sunt auditate operaţiile de cluster şi grup de resurse cluster.
***NETCMN**	Sunt auditate funcţiile de comunicaţie şi reţea. *NETCMN este compus din câteva valori pentru a vă permite să vă personalizaţi mai bine auditarea. Următoarele valori formează *NETCMN: *NETBAS *NETCLU *NETFAIL *NETSCK
***NETFAIL**	Sunt auditate eşuările de reţea.
***NETSCK**	Sunt auditate task-urile de socket.
***OBJMGT**	Sunt înregistrate operaţiile de redenumire şi mutare obiecte.
***OFCSRV**	Sunt înregistrate modificările aduse directorului de distribuţie sistem şi acţiunile de mail office.
***OPTICAL**	Este înregistrată folosirea volumelor optice.
***PGMADP**	Este înregistrată obţinerea autorizării de la un program care adoptă autorizare.
***PGMFAIL**	Sunt înregistrate violările de integritate a sistemului.
***PRTDTA**	Sunt înregistrate tipărirea unui fişier spool, trimiterea ieşirii direct la o imprimantă şi trimiterea ieşirii la o imprimantă la distanţă.
***SAVRST**	Sunt înregistrate operaţiile de restaurare.
***SECCFG**	Este auditată configuraţia de securitate.
***SECDIRSRV**	Sunt înregistrate modificările sau actualizările când se execută funcţii de serviciu de director.
***SECIPC**	Sunt auditate modificările aduse comunicaţiilor între procese.
***SECNAS**	Sunt auditate acţiunile serviciului de autentificare în reţea.
***SECRUN**	Sunt auditate funcţiile de timp de rulare securitate.
***SECSCKD**	Sunt auditaţi descriptorii de socket.

| *Tabela 47. Valorile posibile pentru valoarea de sistem QAUDLVL2: (continuare)*

***SECURITY**	Sunt înregistrate funcţiile referitoare la securitate. *SECURITY este compus din câteva valori pentru a vă permite să vă personalizaţi mai bine auditarea. Următoarele valori formează *SECURITY: *SECCFG *SECDIRSRV *SECIPC *SECNAS *SECRUN *SECSCKD *SECVFY *SECVLDL
***SECVFY**	Este auditată folosirea funcţiilor de verificare.
***SECVLDL**	Sunt auditate modificările aduse obiectelor din lista de validare.
***SERVICE**	Este înregistrată folosirea uneltelor de service.
***SPLFDTA**	Sunt înregistrate acţiunile executate asupra fişierelor spool.
***SYSMGT**	Folosirea funcţiilor de gestionare sisteme este înregistrată în istoric.

Vedeţi “Planificarea auditării acţiunilor” la pagina 228 pentru o descriere completă a tipurilor de intrare jurnal şi valorile posibile pentru QAUDLVL2.

Auditarea noilor obiecte (QCRTOBJAUD)

Valoarea de sistem QCRTOBJAUD este folosită pentru a determina valoarea de auditare pentru un obiect nou dacă auditarea implicită pentru biblioteca obiectului nou este setată la *SYSVAL. Valoarea de sistem QCRTOBJAUD este de asemenea valoarea de auditare a obiectului implicit pentru noile documente fără folder.

De exemplu, valoarea CRTOBJAUD pentru biblioteca CUSTLIB este *SYSVAL. Valoarea QCRTOBJAUD este *CHANGE. Dacă veţi crea un obiect nou în biblioteca CUSTLIB, valoarea sa de auditare obiect este automat setată la *CHANGE. Puteţi modifica valoarea de auditare folosind comanda CHGOBJAUD.

Notă: Această valoare de sistem este o valoare restricţionată. Vedeţi Capitolul 3: ″Valorile de sistem privind securitatea″ pentru detalii despre cum se face restricţionarea modificărilor asupra valorilor de sistem de securitate şi pentru o listă completă a valorilor de sistem restricţionate.

Tabela 48. Valori posibile pentru valoarea de sistem QCRTOBJAUD:

***NONE**	Nu este realizată nici o auditare pentru obiect.
***USRPRF**	Auditarea obiectului este bazată pe valoarea din profilul utilizatorului care accesează obiectul.
***CHANGE**	Este scrisă o înregistrare de auditare atunci când obiectul este modificat.
***ALL**	Este scrisă o înregistrare de auditare pentru orice acţiune care afectează conţinutul obiectului. De asemenea, este scrisă o înregistrare de auditare dacă se modifică conţinutul obiectului.

Valoare recomandată: Valoarea pe care o selectaţi depinde de cerinţele de auditare ale instalării dumneavoastră. Secţiunea “Planificarea auditării accesului la obiect” la pagina 246 furnizează mai multe informaţii despre metodele de setare a auditării de obiecte pe sistemul dumneavoastră. Puteţi de asemenea controla valoarea de auditare la nivelul bibliotecii cu parametrul CRTOBJAUD cu comanda CRTLIB şi comanda CHGLIB.

Capitolul 4. Profilurile de utilizator

Acest capitol descrie profilurile de utilizator: scopul, caracteristicile şi proiectarea lor. Profilurile de utilizator sunt o unealtă puternică şi flexibilă. Dacă sunt proiectate corespunzător vă pot ajuta să vă protejaţi sistemul şi să îl personalizaţi pentru utilizatori.

Privire generală:

Scop: Crearea şi întreţinerea profilurilor de utilizator şi a profilurilor de grup în sistem.

Cum se face:

Comanda WRKUSRPRF (Work with User Profiles - Gestionare profiluri utilizator)

Comanda CHGUSRAUD (Change User Audit - Modificare auditare utilizator)

Autorizare:

Autorizarea specială *SECADM

Autorizarea specială *AUDIT pentru modificarea auditării de utilizator

Intrare jurnal:

CP pentru modificări asupra profilurilor de utilizator

AD pentru modificări asupra auditării de utilizator

ZC pentru modificări asupra unui profil de utilizator care nu se referă la securitate

Rolurile profilului de utilizator

Profilul utilizator are mai multe roluri în sistem:

- El conţine informaţii referitoare la securitate care controlează cum se face semnarea utilizatorului pe sistem, ce îi este permis utilizatorului să facă după ce semnează şi cum se face auditarea acţiunilor utilizatorului.
- El conţine informaţii care sunt proiectate să personalizeze sistemul şi să îl adapteze la utilizator.
- El este o unealtă de administrare şi de recuperare pentru sistemul de operare. Profilul de utilizator conţine informaţii despre obiectele deţinute de utilizator şi toate autorizările private pentru obiecte.
- Numele profilului de utilizator identifică joburile utilizatorului şi ieşirile de imprimantă.

Dacă valoarea de sistem pentru nivelul de securitate (QSECURITY) din sistemul dumneavoastră este 10, sistemul creează automat un profil de utilizator când cineva semnează cu un ID de utilizator care nu există deja în sistem. Tabela 143 din Anexa B arată valorile alocate când sistemul creează un profil de utilizator.

Dacă valoarea de sistem QSECURITY din sistemul dumneavoastră este 20 sau mai mare, trebuie să existe un profil de utilizator pentru ca un utilizator să poată semna.

Profilurile de grup

Un profil de grup este un tip special de profil de utilizator. El are două scopuri în sistem:

Unealtă de securitate

Un profil de grup furnizează o metodă de organizare a autorizărilor în sistemul dumneavoastră şi de partajare a lor între utilizatori. Puteţi defini autorizări de obiect sau autorizări speciale pentru profiluri de grup în loc să le definiţi pentru fiecare profil de utilizator în parte. Un utilizator poate fi membrul a cel mult 16 profiluri de grup.

Unealtă de personalizare

Un profil de grup poate fi folosit drept un model pentru crearea de profiluri de utilizator individuale.

Majoritatea persoanelor care fac parte din acelaşi grup au aceleaşi necesităţi de personalizare, cum ar fi meniul iniţial şi imprimanta implicită. Puteţi defini aceste lucruri în profilul de grup şi puteţi apoi copia profilul de grup pentru a crea profiluri de utilizator individuale.

Puteţi crea profiluri de grup în acelaşi mod în care creaţi profiluri individuale. Sistemul recunoaşte un profil de grup când adăugaţi primul membru la grup. În acel moment, sistemul setează informaţiile din profil indicând astfel că acela este un profil de grup. Sistemul generează de asemenea un număr GID (group identification number - număr de identificare grup) pentru profil. Puteţi de asemenea să desemnaţi un profil drept un profil de grup în momentul în care îl creaţi specificând o valoare în parametrul GID. “Planificarea profilurilor de grup” la pagina 207 arată un exemplu de setare a unui profil de grup.

Câmpuri parametru profil utilizator

Profilurile de utilizator pot fi create în următoarele moduri:

- Navigator iSeries
- Administrare centrală
- Interfaţa bazată pe caractere

Când creaţi un profil de utilizator, profilului îi sunt date următoarele autorizări pentru el însuşi: *OBJMGT, *CHANGE. Aceste autorizări sunt necesare pentru funcţiile sistemului şi nu trebuie înlăturate.

În continuare sunt explicate câmpurile din profilul de utilizator. Câmpurile sunt descrise în ordineaîn care apar în promptul de comenzi Creare profil utilizator.

Multe ecrane de sistem au diferite versiuni, numite **niveluri de ajutorare**, pentru a îndeplini nevoile diferiţilor utilizatori:

- Nivelul de ajutorare elementar, care conţine informaţii mai puţine şi nu foloseşte terminologie tehnică.
- Nivelul de ajutorare intermediar, care arată mai multe informaţii şi foloseşte termeni tehnici.
- Nivelul de ajutorare avansat, care foloseşte termeni tehnici şi arată cantitatea maximă de date, neafişând întotdeauna tasta funcţională şi informaţiile de opţiune.

Secţiunile care urmează arată cum sunt numite câmpurile din profilul de utilizator atât în ecranele la nivel de ajutorare elementar, cât şi în cele la nivel de ajutorare intermediar. Formatul utilizat este:

Titlu câmp
Titlul secţiunii arată cum apare numele de câmp în promptul de comandă Creare profil utilizator, care apare când creaţi un profil de utilizator cu Nivelul de asistenţă intermediar pentru comanda Creare profil utilizator (CRTUSRPRF).

Promptul Adăugare utilizator:
Acesta arată cum apare numele de câmp în ecranul Adăugare utilizator şi alte ecrane de profil utilizator care folosesc nivelul de ajutorare elementar. Ecranele la nivel de ajutorare elementar afişează un subset al câmpurilor din profilul de utilizator. *Neafişat* înseamnă că acel câmp nu apare în ecranul la nivel de ajutorare elementar. Când folosiţi ecranul Adăugare utilizator pentru a crea un profil utilizator, sunt folosite valorile implicite pentru toate câmpurile care nu sunt afişate.

Parametru CL:
Folosiţi numele de parametru CL pentru un câmp dintr-un program CL sau când introduceţi o comandă de profil de utilizator fără promptare.

Lungime:
Dacă folosiţi comanda Extragere profil utilizator (RTVUSRPRF) într-un program CL, aceasta este lungimea pe care trebuie să o folosiţi pentru a defini parametrul asociat cu câmpul.

Autorizare:
Dacă un câmp se referă la un obiect separat, precum o bibliotecă sau un program, vi se spun necesităţile de autorizare pentru acel obiect. Pentru a specifica obiectul când creaţi sau modificaţi un profil de utilizator,

trebuie să listaţi autorizările. Pentru a semna folosind profilul, utilizatorul trebuie să menţioneze autorizarea. De exemplu, dacă creaţi profilul de utilizator USERA cu descrierea de job JOBD1, trebuie să aveţi autorizarea *USE pentru JOBD1. USERA trebuie să aibă autorizarea *USE la JOBD1 pentru a semna cu succes cu profilul.

În plus, fiecare secţiune descrie valorile posibile pentru câmp şi o valoare recomandată.

Nume profil utilizator

Promptul Adăugare utilizator:
Utilizator

Parametru CL:
USRPRF

Lungime:
10

Numele profilului de utilizator indentifică utilizatorul pentru sistem. Acest nume de profil de utilizator mai este numit şi ID de utilizator. Este numele pe care utilizatorul îl tastează la promptul *Utilizator* în ecranul Semnare.

Numele profilului de utilizator poate fi de maxim 10 caractere. Caracterele pot fi:

- Orice literă (A până la Z)
- Orice cifră (0 până la 9)
- Aceste caractere speciale: diez (#), dolar ($), liniuţă de subliniere (_), a rond (@).

Notă: Ecranul Adăugare utilizator permite numai un nume de utilizator de opt caractere.

Numele profilului de utilizator nu poate începe cu o cifră.

Notă: Este posibilă crearea unui profil de utilizator astfel încât atunci când un utilizator semnează, ID-ul de utilizator să conţină numai cifre. Pentru a crea un astfel de profil, specificaţi Q ca prim caracter, de exemplu Q12345. Apoi un utilizator poate semna tastând 12345 sau Q12345 la promptul *Utilizator* în ecranul Semnare.

Pentru informaţii suplimentare despre specificarea numelor în sistem, consultaţi cartea *CL Programming* .

Recomandări pentru deumirea profilurilor de utilizator: Ţineţi cont de următoarele când alegeţi numele profilurilor de utilizator:

- Un nume de profil de utilizator poate avea până la 10 caractere lungime. Unele metode de comunicare limitează ID-ul de utilizator la 8 caractere. Ecranul Adăugare utilizator limitează şi numele de profil de utilizator la 8 caractere.
- Folosiţi o schemă de numire care face ID-urile de utilizator uşor de ţinut minte.
- Sistemul nu face distincţie între literele mari şi cele mici într-un nume de profil de utilizator. Dacă introduceţi caractere alfabetice mici la staţia dumneavoastră de lucru, sistemul le traduce în majuscule.
- Ecranele şi listele folosite pentru gestionarea profilurilor de utilizator le arată în ordine alfabetică, după numele de profil de utilizator.
- Evitaţi folosirea caracterelor speciale în numele de profiluri de utilizator. Caracterele speciale pot cauza probleme legate de maparea tastaturii pentru anumite staţii de lucru sau de versiunile de limbă naţională ale programului licenţiat OS/400.

O tehnică de alocare a numelor de profil de utilizator este folosirea primelor 7 caractere ale numelui urmate de primul caracter al prenumelui. De exemplu:

Nume utilizator	Nume profil utilizator
Anderson, George	ANDERSOG
Anderson, Roger	ANDERSOR
Harrisburg, Keith	HARRISBK
Jones, Sharon	JONESS
Jones, Keith	JONESK

Recomandări pentru denumirea profilurilor de grup: Dacă doriţi să identificaţi uşor profilurile de grup în liste şi ecrane, folosiţi o convenţie de numire. Începeţi toate numele de profiluri de grup cu aceleaşi caractere, precum GRP (pentru grup) sau DPT (pentru departament).

Parolă

Promptul Adăugare utilizator:
Parolă

Parametru CL:
PAROLĂ

Lungime:
128

Parola este folosită pentru a verifica autorizarea unui utilizator pentru semnarea pe sistem. Pentru semnare trebuie să fie specificate un ID de utilizator şi o parolă când securitatea de parolă este activă (valoarea de sistem QSECURITY este 20 sau mai mare).

Parolele pot avea maxim 10 caractere când valoarea de sistem QPWDLVL este setată la 0 sau 1. Parolele pot avea maxim 128 caractere când valoarea de sistem este setată la 2 sau 3.

Când valoarea de sistem pentru nivelul de parolă (QPWDLVL) este 0 sau 1, regulile pentru specificarea parolelor sunt cele folosite pentru numele de profiluri de utilizator. Când primul caracter al parolei este un Q şi al doilea caracter este un caracter numeric, Q poate fi omis în ecranul de semnare. Dacă un utilizator specifică parola Q12345 în ecranul Modificare parolă, el poate specifica fie 12345, fie Q12345 ca parolă în ecranul Semnare. Când QPWDLVL este 2 sau 3, utilizatorul trebuie să specifice parola Q12345 în ecranul de semnare dacă profilul de utilizator a fost creat cu parola Q12345. Când QPWDLVL este 2 sau 3 este permisă o parolă care conţine numai cifre, dar parola profilului de utilizator trebuie să fie creată doar din cifre.

Când valoarea de sistem pentru nivelul de parolă (QPWDLVL) este 2 sau 3, parola este sensibilă la majuscule şi poate conţine orice caracter, inclusiv caractere spaţiu. Totuşi, parola nu poate începe cu un caracter asterix (’*’) şi caracterele spaţiu de la sfârşit sunt înlăturate.

Notă: Parolele pot fi create folosind caractere pe doi octeţi. Însă o parolă care conţine caractere pe doi octeţi nu poate fi folosită pentru semnare printr-un ecran de semnare sistem. Parolele care conţin caractere pe doi octeţi pot fi create prin comenzile CRTUSRPRF şi CHGUSRPRF şi pot fi trecute API-urilor sistemului care suportă parametrul parolă.

Pentru a memora parola în sistem este folosită criptarea într-un sens. Dacă o parolă este uitată, responsabilul cu securitatea poate folosi comanda Modificare profil utilizator (CHGUSRPRF) pentru a aloca o parolă temporară şi a seta acea parolă să expire, cerând utilizatorului să aloce o nouă parolă la următoarea semnare.

Puteţi seta valori de sistem pentru a controla parolele pe care le alocă utilizatorii. Valorile de sistem pentru compoziţia parolei se aplică doar când un utilizator modifică o parolă folosind comanda Modificare parolă (CHGPWD), opţiunea Modificare parolă din meniul ASSIST sau API-ul QSYCHGPW. Dacă valoarea de sistem QPWDMINLEN (lungime minimă parolă) nu este 1 sau valoarea de sistem lungime maximă parolă (QPWDMAXLEN) nu este 10 sau oricare

dintre celelalte valori de sistem pentru compoziţie parolă a fost modificată faţă de valoarea iplicită, un utilizator nu poate seta parola egală cu numele profilului de utilizator folosind comanda CHGPWD, meniul ASSIST sau API-ul QSYCHGPW.

Consultaţi subiectul “Valorile de sistem pentru parole” la pagina 38 pentru informaţii despre setarea valorilor de sistem compoziţie parolă.

Tabela 49. Valori posibile pentru PASSWORD:

***USRPRF**	Parola pentru acest utilizator este numele profilului de utilizator. Când valoarea de sistem pentru nivelul de parolă (QPWDLVL) este 2 sau 3, parola este numele profilului de utilizator scris cu majuscule. Pentru profilul JOHNDOE, parola va fi JOHNDOE, nu johndoe.
***NONE**	Nici o parolă nu este alocată acestui profil de utilizator. Semnarea nu este permisă cu acest profil de utilizator. Puteţi să lansaţi un job batch folosind un profil de utilizator cu parola *NONE dacă aveţi autorizarea corespunzătoare pentru profilul de utilizator.
parolă-utilizator	Un şir de caractere (128 caractere sau mai puţin).

Recomandări pentru parole:

- Setaţi parola pentru un profil de grup la *NONE. Acest lucru împiedică pe oricine să semneze cu profilul de grup.
- Când creaţi un profil de utilizator individual, setaţi parola la o valoare iniţială şi cereţi să fie alocată o parolă nouă când utilizatorul semnează (setaţi expirarea parolei la *YES). Parola implicită la crearea unui profil de utilizator este numele profilului de utilizator.
- Dacă folosiţi o parolă trivială sau implicită la crearea unui nou profil de utilizator, asiguraţi-vă că utilizatorul intenţionează să semneze imediat. Dacă vă aşteptaţi ca utilizatorul să semneze mai târziu, setaţi starea profilului de utilizator la *DISABLED. Modificaţi starea în *ENABLED când utilizatorul este gata să semneze. Asta protejează noul profil de utilizator faţă de folosirea sa de către cineva neautorizat.
- Folosiţi valorile de sistem pentru compoziţia parolei pentru a împiedica alocarea de către utilizatori de parole triviale.
- Unele metode de comunicaţii trimit parole între sisteme şi limitează lungimea parolei şi caracterele pe care le pot conţine parolele. Dacă sistemul dumneavoastră comunică cu alte sisteme, folosiţi valoarea de sistem QPWDMAXLEN pentru a limita lungimea parolelor. La nivelurile de parolă 0 şi 1, valoarea de sistem QPWDLMTCHR poate fi folosită pentru a specifica anumite caractere care nu pot fi folosite în parole.

Setare parolă la Expirată

Prompt adăugare utilizator:
Neafişat

Parametru CL:
PWDEXP

Lungime:
4

Câmpul *Setare parolă la expirată* permite unui administrator de securitate să indice în profilul de utilizator că parola utilizatorului este expirată şi că trebuie modificată la următoarea semnare a utilizatorului. Această valoare este resetată la *NO când parola este modificată. Puteţi modifica parola folosind fie comanda CHGPWD sau CHGUSRPRF, fie API-ul QSYCHGPW, fie ca parte a procesului următor de semnare.

Acest câmp poate fi folosit când un utilizator nu îşi aminteşte parola şi un administrator de securitate trebuie să aloce una nouă. Dacă se cere utilizatorului să modifice parola alocată de administratorul de securitate, se împiedică cunoaşterea de către administratorul de securitate a noii parole şi semnarea acestuia în locul utilizatorului.

Când parola unui utilizator a expirat, utilizatorul primeşte un mesaj la semnare (vedeţi Figura 1). Utilizatorul poate apăsa tasta Enter pentru a aloca o nouă parolă sau poate apăsa F3 (Ieşire) pentru a anula încercarea de semnare fără

alocarea unei noi parole. Dacă utilizatorul alege să modifice parola, este arătat ecranul Modificare parolă şi este rulată validarea parolei pentru noua parolă.

```
                          Sign-on Information
                                                                System:
Password has expired.  Password must be changed to continue sign-on
request.

Previous sign-on . . . . . . . . . . . . . :   10/30/91  14:15:00
```

Figura 1. Mesaj de expirare parolă

Tabela 50. Valori posibile pentru PWDEXP:

***NO:**	Parola nu este setată la expirată.
***YES:**	Parola este setată la expirată.

Recomandări: Setaţi parola la expirată când creaţi un profil nou de utilizator sau alocaţi o parolă temporară utilizatorului.

Stare

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
STATUS

Lungime:
10

Valoarea câmpului *Stare* indică dacă profilul este valid pentru semnare. Dacă starea profilului este activă, profilul este valid pentru semnare. Dacă starea profilului este dezactivată, un utilizator autorizat trebuie să activeze din nou profilul pentru a-l face valid pentru semnare.

Puteţi folosi comanda CHGUSRPRF pentru a activa un profil care a fost dezactivat. Trebuie să aveţi autorizarea specială *SECADM şi autorizările *OBJMGT şi *USE la profil pentru a-i schimba starea. Subiectul “Activarea unui profil de utilizator” la pagina 101 prezintă un exemplu de program cu autorizare adoptată pentru a permite unui operator de sistem să activeze un profil.

Sistemul poate dezactiva un profil după un anumit număr de încercări de semnare incorecte cu acel profil, în funcţie de setările valorilor de sistem QMAXSIGN şi QMAXSGNACN.

Puteţi întotdeauna să semnaţi cu profilul QSECOFR (responsabil cu securitatea) la consolă, chiar şi când starea QSECOFR este *DISABLED. Dacă profilul de utilizator QSECOFR devine dezactivat, semnaţi cu QSECOFR la consolă şi tastaţi CHGUSRPRF QSECOFR STATUS(*ENABLED).

Tabela 51. Valori posibile pentru STATUS:

***ENABLED**	Profilul este valid pentru semnare.
***DISABLED**	Profilul nu este valid pentru semnare până când un utilizator autorizat nu îl activează din nou.

Recomandări: Setaţi starea la *DISABLED dacă doriţi să împiedicaţi semnarea cu un profil de utilizator. De exemplu, puteţi dezactiva profilul unui utilizator care nu va lucra o perioadă mai lungă.

Clasă utilizator

Promptul Adăugare utilizator:
Tip de utilizator

Parametru CL:
USRCLS

Lungime:
10

Clasa de utilizator este folosită pentru controlul opţiunilor de meniu care sunt afişate utilizatorului în meniurile OS/400. Aceasta nu limitează în mod necesar folosirea comenzilor. Câmpul *Limitare capabilităţi* controlează dacă utilizatorul poate introduce comenzi. Clasa de utilizator nu poate afecta opţiunile care sunt arătate în meniurille furnizate de alte programe licenţiate.

Dacă nu este specificată nici o autorizare specială când este creat un profil de utilizator, autorizărilor speciale pentru utilizator sunt determinate folosind clasa de utilizator şi valoarea de sistem pentru nivelul de securitate (QSECURITY).

Valorile posibile pentru USRCLS: Tabela 52 arată clasele de utilizator posibile şi autorizările speciale implicite pentru fiecare clasă de utilizator. Intrările arată că autorizarea este dată doar la nivelurile de securitate 10 şi 20, la toate nivelurile de securitate sau deloc.

Valoarea implicită pentru clasa de utilizator este ***USER**.

Tabela 52. Autorizările speciale implicite după clasa de utilizator

	Clase utilizator				
Autorizare specială	***SECOFR**	***SECADM**	***PGMR**	***SYSOPR**	***USER**
*ALLOBJ	Toate	10 sau 20	10 sau 20	10 sau 20	10 sau 20
*SECADM	Toate	Toate			
*JOBCTL	Toate	10 sau 20	10 sau 20	Toate	
*SPLCTL	Toate				
*SAVSYS	Toate	10 sau 20	10 sau 20	Toate	10 sau 20
*SERVICE	Toate				
*AUDIT	Toate				
*IOSYSCFG	Toate				

Recomandări: Cei mai mulţi utilizatori nu au nevoie să execute funcţii de sistem. Setaţi clasa de utilizator la *USER, exceptând cazul în care pentru un utilizator există necesităţi specifice de folosire a funcţiilor de sistem.

Nivel de ajutorare

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
ASTLVL

Lungime:
10

Pentru fiecare utilizator, sistemul ţine evidenţa ultimului nivel de ajutorare folosit pentru fiecare ecran de sistem care are mai mult de un nivel de ajutorare. Acel nivel este folosit următoarea dată când utilizatorul cere ecranul respectiv. În timpul unui job activ, un utilizator poate modifica nivelul de ajutorare pentru un ecran sau un grup de ecrane înrudite prin apăsarea tastei F12 (Selectare nivel de ajutorare). Noul nivel de ajutorare pentru acel ecran este memorat cu informaţiile de utilizator.

Specificarea parametrului pentru nivelul de ajutorare (ASTLVL) într-o comandă nu modifică nivelul de ajutorare care este memorat pentru utilizatorul ecranului asociat.

Câmpul *Nivel de ajutorare* din profilul de utilizator este folosit pentru specificarea nivelului de ajutorare implicit pentru utilizator atunci când este creat profilul. Dacă nivelul de ajutorare din profilul de utilizator este modificat folosind comanda CHGUSRPRF sau comanda Modificare profil (CHGPRF), nivelurile de ajutorare memorate pentru toate ecranele acelui utilizator sunt resetate la noua valoare.

De exemplu, să presupunem că profilul de utilizator pentru USERA este creat cu nivelul de ajutorare implicit (de bază). Tabela 53 ne arată dacă USERA vede ecranul Gestionare profiluri utilizator sau ecranul Gestionare înrolare utilizator când foloseşte opţiuni diferite. Tabela de asemenea arată dacă sistemul modifică versiunea pentru ecranul care este memorat cu profilul USERA.

Tabela 53. Cum sunt memorate şi modificate nivelurile de ajutorare

Acţiune executată	Versiunea ecranului arătat	Versiunea ecranului memorat
Folosire comandă WRKUSRPRF	Ecranul Gestionare înrolare utilizator	Nici o modificare (nivelul de asistenţă de bază)
Din ecranul Gestionare înrolare utilizator, apăsaţi F12 şi selectaţi Nivelul de asistenţă intermediar.	Ecranul Gestionare profiluri utilizator	Modificat la Nivelul de asistenţă intermediar
Folosire comandă WRKUSRPRF	Ecranul Gestionare profiluri utilizator	Nici o modificare (intermediară)
Selectaţi opţiunea gestionare înrolare utilizator de la meniul SETUP.	Ecranul Gestionare profiluri utilizator	Nici o modificare (intermediară)
Tastaţi CHGUSRPRF USERA ASTLVL(*BASIC)		Modificat la nivelul de asistenţă de bază
Folosire comandă WRKUSRPRF	Ecranul Gestionare înrolare utilizator	Nici o modificare (elementară)
Tastare WRKUSRPRF ASTLVL(*INTERMED)	Ecranul Gestionare profiluri utilizator	Nici o modificare (elementară)

Notă: Câmpul *Opţiune utilizator* din profilul utilizator de asemenea afectează afişarea ecranelor de sistem. Acest câmp este descris la pagina 87.

Tabela 54. Valori posibile pentru ASTLVL:

***SYSVAL**	Este folosit nivelul de ajutorare specificat în valoarea de sistem QASTLVL.
***BASIC**	Este folosită interfaţa de utilizator Asistent operaţional.
***INTERMED**	Este folosită interfaţa de sistem.
***ADVANCED**	Este folosită interfaţa de sistem expert. Pentru a permite mai multe intrări de listă, numerele de opţiune şi tastele funcţionale nu sunt întotdeauna afişate. Dacă o comandă nu are un nivel avansat (*ADVANCED), este folosit nivelul intermediar (*INTERMED).

Bibliotecă curentă

Promptul Adăugare utilizator:
Bibliotecă implicită

Parametru CL:
CURLIB

Lungime:
10

Autorizare
*USE

Eete căutată biblioteca curentă înaintea bibliotecilor din porţiunea de utilizator a listei de biblioteci, pentru orice obiect specificat ca *LIBL. Dacă utilizatorul creează obiecte şi specifică *CURLIB, obiectele sunt puse în biblioteca curentă.

Biblioteca curentă este adăugată în mod automat la lista de biblioteci a utilizatorului când utilizatorul semnează. Nu este necesar să fie inclusă în lista de biblioteci iniţială din descrierea de job a utilizatorului.

Utilizatorul nu poate modifica biblioteca curentă dacă opţiunea din câmpul *Limitare capabilităţi* din profilul de utilizator este *YES sau *PARTIAL.

Subiectul “Lista de biblioteci” la pagina 177 furnizează informaţii suplimentare despre folosirea listelor de biblioteci şi a bibliotecii curente.

Tabela 55. Valori posibile pentru CURLIB:

***CRTDFT**	Acest utilizator nu are o bibliotecă curentă. Dacă obiectele sunt create folosind *CURLIB într-o comandă de creare, este folosită biblioteca QGPL ca bibliotecă curentă implicită.
nume-bibliotecă-curentă	Numele unei biblioteci.

Recomandări: Folosiţi câmpul *Bibliotecă curentă* pentru a controla unde li se permite utilizatorilor să introducă obiecte noi, cum ar fi programe de interogare. Folosiţi câmpul *Limitare capabilităţi* pentru a împiedica utilizatorii să modifice biblioteca curentă.

Program iniţial

Promptul Adăugare utilizator:
Program de semnare

Parametru CL:
INLPGM

Lungime:
10 (nume program) 10 (nume bibliotecă)

Autorizare:
*USE pentru program *EXECUTE pentru bibliotecă

Puteţi specifica numele unui program pentru a fi apelat când semnează un utilizator. Acest program rulează înainte de a fi afişat meniul iniţial, dacă există. Dacă opţiunea din câmpul *Limitare capabilităţi* din profilul utilizatorului este *YES, utilizatorul nu poate specifica un program iniţial pe ecranul Semnare.

Programul iniţial este apelat numai dacă programul de rutare al utilizatorului este QCMD sau QCL. Consultaţi “Pornirea unui job interactiv” la pagina 169 pentru informaţii suplimentare despre scvenţa de procesare când semnează un utilizator.

Programele iniţiale sunt folosite pentru două scopuri principale:

- Ca să restricţionaţi un utilizator la un set specific de funcţii.
- Ca să realizaţi unele procesări iniţiale, cum ar fi deschiderea fişierelor sau stabilirea listei de biblioteci, când utilizatorul semnează prima dată.

Parametrii nu se pot transmite la un program iniţial. Dacă programul iniţial eşuează, utilizatorul nu este capabil să semneze.

Tabela 56. Valori posibile pentru INLPGM:

***NONE**	Nici un program nu este apelat când utilizatorul semnează. Dacă este specificat un nume de meniu în parametrul de meniu iniţial (INLMNU), este afişat acel meniu.
nume-program	Numele programului care este apelat când utilizatorul semnează.

Tabela 57. Valori posibile pentru Biblioteca INLPGM:

***LIBL**	Este folosită lista de biblioteci pentru localizarea programului. Dacă descrierea de job pentru profilul de utilizator are o listă de biblioteci iniţială, este folosită acea listă. Dacă descrierea de job specifică *SYSVAL pentru lista de biblioteci iniţială, este folosită valoarea de sistem QUSRLIBL.
***CURLIB**	Pentru localizarea programului este folosită biblioteca curentă specificată în profilul de utilizator. Dacă nu este specificată nici o bibliotecă curentă, se foloseşte QGPL.
nume-bibliotecă	Biblioteca unde se află programul.

Meniu iniţial

Promptul Adăugare utilizator:
Primul meniu

Parametru CL:
INLMNU

Lungime:
10 (nume meniu) 10 (nume bibliotecă)

Autorizare
*USE pentru meniu *EXECUTE pentru bibliotecă

Puteţi specifica numele unui meniu pentru a fi afişat când utilizatorul semnează. Meniul iniţial este afişat după rularea programului iniţial al utilizatorului. Meniul iniţial este apelat numai dacă programul de rutare al utilizatorului este QCMD sau QCL.

Dacă doriţi ca utilizatorul să ruleze numai programul iniţial, puteţi specifica *SIGNOFF pentru meniul iniţial.

Dacă opţiunea din câmpul *Limitare capabilităţi* din profilul utilizatorului este *YES, utilizatorul nu poate specifica un meniu iniţial diferit în ecranul Semnare. Dacă unui utilizator îi este permis să specifice un meniu iniţial în ecranul Semnare, meniul specificat înlocuieşte meniul din profilul utilizator.

Tabela 58. Valori posibile pentru MENU:

MAIN	Este arătat Meniul principal de sistem iSeries .
***SIGNOFF**	Sistemul anulează semnarea utilizatorului când programul iniţial se termină. Folosiţi aceasta ca să limitaţi utilizatorii la rularea unui singur program.
nume-meniu	Numele meniului care este apelat când utilizatorul semnează.

Tabela 59. Valori posibile pentru Biblioteca MENU:

***LIBL**	Este folosită lista de biblioteci pentru localizarea meniului. Dacă programul iniţial adaugă intrări în lista de biblioteci, aceste intrări sunt incluse în căutare, deoarece meniul este apelat după ce programul iniţial s-a terminat.
***CURLIB**	Este folosită biblioteca curentă a jobului pentru localizarea meniului. Dacă nu există nici o intrare de bibliotecă curentă în lista de biblioteci, se foloseşte QGPL.
nume bibliotecă	Biblioteca în care este localizat meniul.

Limitare capabilităţi

Promptul Adăugare utilizator:
Restricţionare folosire linie de comandă

Parametru CL:
LMTCPB

Lungime:
10

Puteţi folosi câmpul *Limitare capabilităţi* pentru a limita abilitatea utilizatorului de a introduce comenzi şi de a înlocui programul iniţial, meniul iniţial, biblioteca curentă şi programul de tratare a tastei de atenţionare, specificate în profilul de utilizator. Acest câmp este o unealtă pentru împiedicarea utilizatorilor de a experimenta pe sistem.

Un utilizator cu LMTCPB(*YES) poate rula numai comenzile care sunt definite cu permitere utilizator limitat, (ALWLMTUSR) *YES. Următoarele comenzi sunt livrate de IBM cu ALWLMTUSR(*YES):

Anulare semnare (SIGNOFF)

Trimitere mesaj (SNDMSG)

Afişare mesaje (DSPMSG)

Afişare job (DSPJOB)

Afişare istoric de job (DSPJOBLOG)

Pornire Organizator PC (STRPCO)

Gestionare mesaje (WRKMSG)

Câmpul *Limitare capabilităţi* din profilul de utilizator şi parametrul ALWLMTUSR din comenzi se aplică doar comenzilor care sunt rulate din linia de comandă, ecranul Intrare comandă sau o opţiune dintr-un meniu de grupare comandă. Utilizatorii nu au restricţii în folosirea următoarelor:

- Rularea comenzilor în programe CL care rulează o comandă ca rezultat al alegerii unei opţiuni dintr-un meniu
- Rularea comenzilor la distanţă prin aplicaţii.

Puteţi permite utilizatorului cu capabilitate limitată să ruleze comenzi suplimentare sau să înlăturaţi câteva comenzi din listă, modificând parametrul ALWLMTUSR într-o comandă. Folosiţi comanda Modificare comandă (CHGCMD). Dacă vă creaţi prpriile comenzi, puteţi specifica parametrul ALWLMTUSR din comanda Creare comandă (CRTCMD).

Valori posibile: Tabela 60 arată valorile posibile pentru *Limitare capabilităţi* şi ce funcţii sunt permise pentru fiecare valoare.

Tabela 60. Funcţii permise pentru valorile de limitare capabilităţi

Funcţie	*YES	*PARTIAL	*NO
Modificare program iniţial	Nu	Nu	Da
Modificare meniu iniţial	Nu	Da	Da
Modificare bibliotecă curentă	Nu	Nu	Da
Modificare program Attn	Nu	Nu	Da
Introducere comenzi	Câteva[1]	Da	Da

[1] Sunt permise următoarele comenzi: SIGNOFF, SNDMSG, DSPMSG, DSPJOB, DSPJOBLOG, STRPCO, WRKMSG. Utilizatorul nu poate folosi F9 pentru afişarea unei linii de comandă de la orice meniu sau ecran.

Recomandări: Folosirea un meniu iniţial, restricţionarea utilizării liniei de comandă şi furnizarea de acces la meniu vă permit să setaţi un mediu pentru un utilizator care nu are nevoie sau nu doreşte să acceseze funcţii de sistem. Consultaţi subiectul “Planificarea meniurilor” la pagina 197 pentru informaţii suplimentare despre acest tip de mediu.

Text

Promptul Adăugare utilizator:
Descriere utilizator

Parametru CL:
TEXT

Lungime:
50

Textul din profilul de utilizator este folosit ca să descrie profilul de utilizator sau la ce este folosit. Pentru profiluri de utilizator, textul trebuie să conţină informaţii de identificare, cum ar fi numele utilizatorului şi departamentul. Pentru profiluri de grup, textul ar trebui să identifice grupul, cum ar fi care departament include grupul.

Tabela 61. Valori posibile pentru text:

***BLANK:**	Nu este specificat nici un text.
descriere	Specificaţi cel mult 50 de caractere.

Recomandări: Câmpul *Text* este trunchiat pe multe ecrane de sistem. Puneţi cele mai importante informaţii de identificare la începutul câmpului.

Autorizare specială

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
SPCAUT

Lungime:
100 (10 caractere pentru autorizare specială)

Autorizare:
Pentru a da o autorizare specială la un profil utilizator, trebuie să aveţi acea autorizare specială.

Autorizarea specială este folosită pentru specificarea tipurilor de acţiuni pe care un utilizator le poate realiza asupra resurselor de sistem. Unui utilizator îi pot fi date una sau mai multe autorizări speciale.

Tabela 62. Valori posibile pentru SPCAUT:

***USRCLS**	Autorizările speciale sunt acordate acestui utilizator pe baza câmpului de clasă utilizator (USRCLS) din profilul de utilizator şi a valorii de sistem pentru nivelul de securitate (QSECURITY). Dacă se specifică *USRCLS, nici o autorizare specială adiţională nu poate fi specificată pentru acest utilizator. Dacă specificaţi *USRCLS când creaţi sau modificaţi un profil de utilizator, sistemul pune autorizările speciale corecte în profilul de utilizator, ca şi cum le-aţi fi introdus dumneavoastră. Când afişaţi profilurile, nu puteţi preciza dacă autorizările speciale au fost introduse individual sau au fost introduse de sistem pe baza clasei de utilizator. Tabela 52 la pagina 61 arată autorizările speciale implicite pentru fiecare clasă de utilizator.
***NONE**	Nu este acordată nici o autorizare specială pentru acest utilizator.
nume-autorizare-specială	Specificaţi una sau mai multe autorizări speciale pentru utilizator. Autorizările speciale sunt descrise în secţiunile care urmează.

Autorizarea specială *ALLOBJ

Autorizarea specială toate obiectele (*ALLOBJ) permite utilizatorului să acceseze orice resursă din sistem, indiferent dacă există sau nu autorizare privată pentru utilizator. Chiar dacă utilizatorul are autorizarea *EXCLUDE pentru un obiect, autorizarea specială *ALLOBJ permită utilizatorului să acceseze obiectul.

Riscuri: autorizarea specială *ALLOBJ dă utilizatorului autorizare extinsă pentru toate resursele din sistem. Utilizatorul poate vizualiza, modifica sau şterge orice obiect. Utilizatorul poate de asemenea acorda altor utilizatori autorizarea de a folosi obiecte.

Un utilizator cu autorizarea *ALLOBJ nu poate realiza direct operaţii care necesită autorizare specială. De exemplu, autorizarea specială *ALLOBJ nu permite unui utilizator să creeze alt profil de utilizator, deoarece crearea profilurilor de utilizator necesită autorizarea specială *SECADM. Totuşi, un utilizator cu autorizarea specială *ALLOBJ poate lansa un job batch folosind un profil care are autorizarea specială necesară. În esenţă, acordarea autorizării speciale *ALLOBJ dă utilizatorului acces la toate funcţiile din sistem.

Autorizarea specială *SECADM

Autorizarea specială administrator de securitate (*SECADM) permite unui utilizator să creeze, să modifice şi să şteargă profiluri de utilizator. Un utilizator cu autorizarea specială *SECADM poate:

- Să adauge utilizatori la directorul de distribuire sistem.
- Să afişeze autorizarea pentru documente sau foldere.
- Să adauge şi să înlăture coduri de acces la sistem.
- Să dea şi să înlăture autorizarea unui utilizator pentru cod de acces
- Să dea şi să înlăture permisiunea pentru utilizatori ca să lucreze în numele altor utilizatori
- Să şteargă documente şi foldere.
- Să şteargă liste de documente.
- Să modifice liste de distribuţie create de alţi utilizatori.

Numai un utilizator cu autorizarea specială *SECADM şi *ALLOBJ poate da autorizare specială *SECADM altui utilizator.

Autorizarea specială *JOBCTL

Autorizarea specială de control job (*JOBCTL) permite utilizatorului să:

- Modifice, şteargă, reţină şi elibereze toate fişierele din orice coadă de ieşire specificată ca OPRCTL(*YES).
- Afişeze, trimită şi copieze toate fişierele din orice coadă de ieşire specificată ca DSPDTA(*YES sau *NO) şi OPRCTL(*YES).
- Reţină, elibereze şi şteargă cozi de joburi specificate ca OPRCTL(*YES).
- Reţină, elibereze şi şteargă cozi de ieşire specificate ca OPRCTL(*YES).
- Reţină, elibereze, modifice şi anuleze joburile altor utilizatori.
- Pornească, modifice, oprească, reţine şi elibereze scriitori, dacă coada de ieşire este specificată ca OPRCTL(*YES).
- Modifice atributele de rulare ale unui job, cum ar fi imprimanta pentru un job.
- Oprească subsisteme.
- Realizeze o încărcare de program iniţial (IPL).

Securizarea ieşirii de imprimantă şi a cozilor de ieşire este discutată în “Tipărire” la pagina 180.

Puteţi modifica prioritatea de job (JOBPTY) şi prioritatea de ieşire (OUTPTY) a jobului dumneavoastră fără autorizarea specială control de job. Trebuie să aveţi autorizarea specială *JOBCTL pentru a modifica prioritatea de rulare (RUNPTY) a jobului dumneavoastră.

Modificările priorităţii de ieşire şi a priorităţii de job a unui job sunt limitate de limita de prioritate (PTYLMT) din profilul utilizatorului care face modificările.

Riscuri: Un utilizator cu autorizarea specială *JOBCTL poate modifica prioritatea joburilor şi a tipăririi, poate opri un job înainte de a se termina sau poate şterge ieşirea înainte de a fi tipărită. Autorizarea specială *JOBCTL poate de asemenea acorda acces unui utilizator la ieşiri spool confidenţiale, dacă cozile de ieşire sunt specificate OPRCTL(*YES). Un utilizator care abuzează de autorizarea specială *JOBCTL poate cauza un impact negativ asupra joburilor individuale şi asupra performanţei generale a sistemului.

Autorizarea specială *SPLCTL

Autorizarea specială control spool (*SPLCTL) permite utilizatorului să realizeze toate funcţiile de control spool, precum modificarea, ştergerea, afişarea, reţinearea şi eliberarea de fişiere spool. Utilizatorul poate realiza aceste funcţii în toate cozile de ieşire, indiferent de autorizările pentru coada de ieşire sau parametrul OPRCTL al cozii de ieşire.

De asemenea, autorizarea specială *SPLCTL permite utilizatorului să gestioneze cozi de joburi, inclusiv să reţină, să elibereze şi să şteargă coada de joburi. Utilizatorul poate realiza aceste funcţii în toate cozile de joburi, indiferent de autorizările pentru coada de joburi sau parametrul OPRCTL al cozii de joburi.

Riscuri: Utilizatorul cu autorizarea specială *SPLCTL poate realiza orice operaţii pe orice fişier spool din sistem. Fişierele spool confidenţiale nu pot fi protejate de un utilizator cu autorizarea specială *SPLCTL.

Autorizarea specială *SAVSYS

Autorizarea specială de salvare sistem (*SAVSYS) acordă utilizatorului autorizarea de salvare, restaurare şi eliberare de spaţiu pentru toate obiectele din sistem, indiferent dacă utilizatorul are sau nu autorizare de existenţă obiect asupra obiectelor.

Riscuri: Un utilizator cu autorizare specială *SAVSYS poate:

- Să salveze un obiect şi să-l ducă pe un alt sistem iSeries pentru a fi restaurat.
- Să salveze un obiect şi să afişeze banda pentru a vedea datele.
- Să salveze un obiect şi să elibereze spaţiu, astfel ştergând porţiuni din datele obiectului.
- Să salveze un document şi să-l şteargă.

Autorizarea specială *SERVICE

Autorizarea specială service (*SERVICE) permite utilizatorului să pornească unelte de service sistem folosind comanda STRSST. Permite utilizatorului şi depanarea unui program doar cu autorizarea *USE şi realizarea funcţiilor de afişare şi modificare serviciu. Funcţia dump poate fi realizată fără autorizare *SERVICE. Permite utilizatorului şi realizarea de diferite funcţii de urmărire.

Riscuri: Un utilizator cu autorizarea specială *SERVICE poate afişa şi modifica informaţii confidenţiale folosind funcţiile de service. Utilizatorul trebuie să aibă autorizarea specială *ALLOBJ pentru a modifica informaţiile folosind funcţii de service.

Pentru a minimiza riscul comenzilor de urmărire, utilizatorilor lui se poate acorda autorizare de realizare urmărire service fără a fi nevoie să se acorde utilizatorului autorizarea specială *SERVICE. În acest fel, numai utilizatorii specificaţi vor avea abilitatea de a efectua o comandă de urmărire, cărora li se vor acorda acces la datele sensibile. Utilizatorul trebuie să fie autorizat pentru comandă şi să aibă autorizare specială *SERVICE, sau să fie autorizat de funcţia Urmărire serviciu a sistemului de operare prin suportul Administrare aplicaţie al NavigatoruluiiSeries . Comanda Modificare folosire funcţie (CHGFCNUSG), cu ID-ul de funcţie al QIBM_SERVICE_TRACE, poate fi şi folosită la modificarea listei de utilizatori cărora le sunt permise efectuarea de operaţii de urmărire.

Comenzile la care poate fi acordat accesul în acest fel includ:

Tabela 63.

STRCMNTRC	Pornire urmărire comunicaţii
ENDCMNTRC	Oprire urmărire comunicaţii
PRTCMNTRC	Tipărire urmărire comunicaţii
DLTCMNTRC	Ştergere urmărire comunicaţii
CHKCMNTRC	Verificare urmărire comunicaţii
TRCCNN	Conexiune de urmărire (consultaţi“Acordarea accesului la urmăriri” la pagina 69)
TRCINT	Urmărire internă
STRTRC	Pornire job de urmărire
ENDTRC	Oprire job de urmărire
PRTTRC	Tipărire job de urmărire
DLTTRC	Ştergere job de urmărire

Acordarea accesului la urmăriri: Comenzile de urmărire, cum ar fi TRCCNN (Conexiune de urmărire) sunt comenzi puternice care nu ar trebui acordate tuturor utilizatorilor care au nevoie de acces la alte servicii şi unelte de depanare. Următorii paşi de mai jos vă permit să limitaţi accesul la aceste comenzi de urmărire fără să aveţi autorizare *SERVICE:

1. În Navigator iSeries, deschideţi Utilizatori şi grupuri.
2. Selectaţi Toţi utilizatorii pentru a vedea o listă a profilurilor de utilizator.
3. Faceţi clic dreapta pe profilul de utilizator de transformat.
4. Selectaţi Proprietăţi.
5. Faceţi clic pe Capabilităţi.
6. Deschideţi fişa Aplicaţii.
7. Selectaţi Acces pentru.
8. Selectaţi Aplicaţii gazdă.
9. Selectaţi Sistem de operare.
10. Selectaţi Service.
11. Folosiţi caseta de bifare ca să acordaţi sau să înlăturaţi accesul la comanda de urmărire.

Autorizarea specială *AUDIT

Autorizarea specială de auditare (*AUDIT) permite utilizatorului abilitatea de a modifica caracteristicile de auditare. Utilizatorul poate:

- Modifica valorile de sistem care controlează auditarea.
- Folosi comenzile CHGOBJAUT, CHGDLOAUD şi CHGAUD ca să modifice auditarea pentru obiecte.
- Folosi comanda CHGUSRAUD ca să modifice auditarea pentru un utilizator.

Riscuri: Un utilizator cu utilizare specială *AUDIT poate opri şi porni auditarea pe sistem sau poate împiedica auditarea acţiunilor particulare. Dacă aveţi o înregistrare de auditare a evenimentelor relevante de securitate este important pentru sistemul dumneavoastră să controlaţi cu atenţie şi să monitorizaţi folosirea autorizării speciale *AUDIT.

Notă: Numai un utilizator cu autorizările speciale *ALLOBJ, *SECADM şi *AUDIT poate da altui utilizator autorizare specială *AUDIT.

Autorizarea specială *IOSYSCFG

Autorizarea specială configurare de sistem (*IOSYSCFG) permite utilizatorului abilitatea de a modifica felul în care sistemul este configurat. De exemplu, adăugarea şi înlăturarea informaţiilor de configurare comunicaţii, gestionarea serverelor TCP/IP şi configurarea serverului de conectare la internet (ICS). Majoritatea comenzilor pentru configurarea comunicaţiilor necesită autorizare specială *IOSYSCFG. Anexa D arată ce autorizări speciale sunt necesare pentru comenzi specifice.

Notă: Aveţi nevoie de *ALLOBJ pentru a fi capabil de modificare a datelor folosind funcţii de service.

Recomandări pentru Autorizări speciale: Acordarea autorizărilor speciale pentru utilizatori reprezintă o expunere de securitate. Pentru fiecare utilizator, evaluaţi cu atenţie nevoile pentru orice autorizare specială. Urmăriţi îndeaproape care utilizatori au autorizări speciale şi revedeţi în mod periodic cerinţele lor pentru autorizări.

În plus, ar trebui să controlaţi următoarele situaţii pentru profilurile utilizator şi programe:

- Dacă profilurile utilizator cu autorizări speciale pot fi folosite să introducă joburi
- Dacă programele create de aceşti utilizatori pot rula folosind autorizarea deţinătorului de program.

Programele adoptă autorizarea specială *ALLOBJ a deţinătorului dacă:

- Dacă programele sunt create de utilizatori care au autorizare specială *ALLOBJ
- Utilizatorul specifică parametrul USRPRF(*OWNER) într-o comandă care creează programul.

Cum foloseşte Server LAN autorizările speciale

Programul cu licenţă Server LAN foloseşte autorizările speciale din profilul unui utilizator ca să determine ce capabilităţi de operare ar trebui să aibă utilizatorul într-un mediu server LAN. Următoarele sunt capabilităţile de operare pe care sistemul le acordă utilizatorilor de server LAN:

***ALLOBJ**
Administrator de sistem

***IOSYSCFG**
Privilegiu de operare resursă server

***JOBCTL**
Privilegiu de operare dispozitiv de comunicare

***SECADM**
Privilegiu de operare conturi

***SPLCTL**
Privilegiu de operare tipărire

- Autorizarea specială *SAVSYS se aplică atunci când salvaţi informaţiile folosind directorul /QFPNWSSTG. Autorizarea specială *SAVSYS se aplică atunci când se salvează obiectele folosind directorul /QLANSrv, trebuie să aveţi permisiunea (autorizarea) necesară pentru obiect sau autorizarea administratorului LAN.
- Autorizarea specială *ALLOBJ permite suficientă autorizare pentru salvarea obiectelor /QLANSrv şi informaţiilor lor de autorizare dacă amândouă propoziţiile următoare sunt adevărate:
  - Sunteţi un utilizator definit într-un domeniu LAN.
  - Controlerul de domeniu este un Procesor I/O server de fişiere pe sistemul local iSeries.

Mediu special

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
SPCENV

Lungime:
10

Mediul special determină mediul operării utilizatorului după semnare. Utilizatorul poate opera în mediul iSeries, System/36 sau System/38. Când utilizatorul semnează, sistemul foloseşte programul de rutare şi mediul special din profilul utilizatorului pentru a determina mediul utilizatorului. Consultaţi Figura 2 la pagina 71.

Tabela 64. Valori posibile pentru SPCENV:

***SYSVAL**	Valoarea de sistem QSPCENV este folosită pentru determinarea mediului când utilizatorul semnează, dacă programul de rutare al utilizatorului este QCMD.
***NONE**	Utilizatorul operează în mediul iSeries .
***S36**	Utilizatorul operează în mediul System/36 dacă programul de rutare al utilizatorului este QCMD.

Recomandări: Dacă utilizatorul rulează o combinaţie de aplicaţii iSeries şi System/36, folosiţi comanda Pornire System/36 (STRS36) înaintea rulării aplicaţiilor System/36 mai repede decât specificarea mediului System/36 în profilul utilizator. Aceasta furnizează performanţă mai bună pentru aplicaţii iSeries .

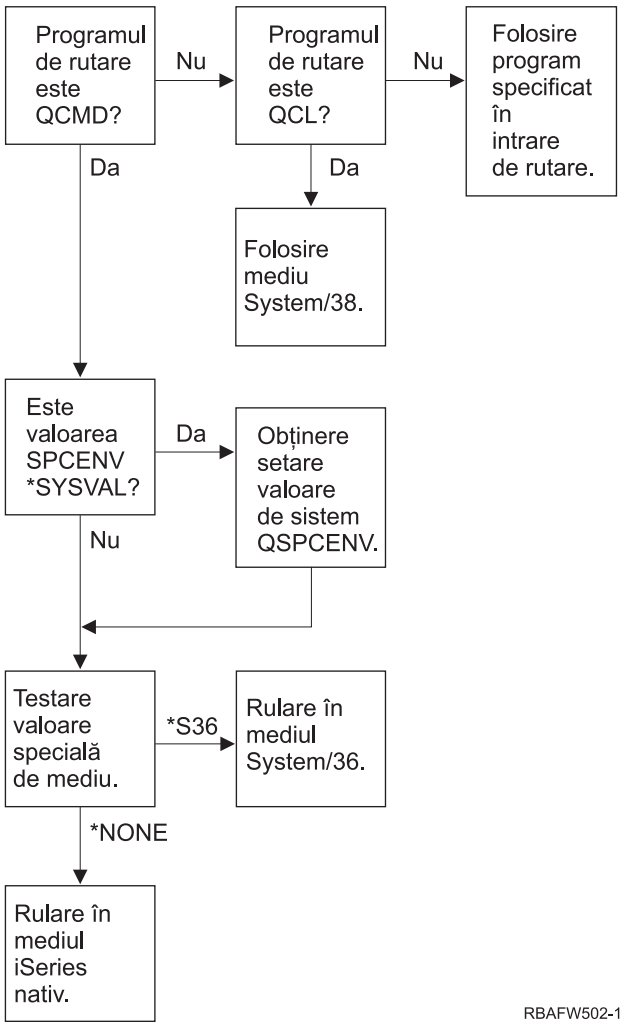

Figura 2. Descriere mediu special

Descriere mediu special

Mediul special determină mediul operării utilizatorului după semnare. Utilizatorul poate opera în mediul iSeries, System/36 sau System/38. Când utilizatorul semnează, sistemul foloseşte programul de rutare şi mediul special din profilul utilizatorului pentru a determina mediul utilizatorului. În continuare este explicată Figura 2.

Sistemul determină dacă programul de rutare este QCMD. Dacă nu este, atunci sistemul verifică dacă programul de rutare este QCL. Dacă programul de rutare este QCL, atunci sistemul va folosi mediul special System/38. Dacă programul de rutare nu este QCL, atunci sistemul foloseşte programul specificat în intrarea de rutare.

Dacă programul de rutare este QCMD, atunci sistemul determină dacă valoarea de sistem SPCENV este setată. Dacă este setată atunci sistemul extrage estimarea pentru valoarea de sistem QSPCENV şi testează valoarea de mediu special. Dacă valoarea de sistem SPCENV nu este setată, atunci sistemul testează valoarea de mediu special.

Dacă valoarea de mediu special este setată la *S36, sistemul rulează mediul special System/36. Dacă valoarea de mediu special este setată la *NONE, atunci sistemul rulează mediul nativ iSeries.

Ecranul Informaţii semnare

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
DSPSGNINF

Lungime:
7

Câmpul *Afişare informaţii semnare* specifică dacă ecranul Informaţii semnare este arătat când utilizatorul semnează. Figura 3 arată ecranul. Informaţiile de expirare parolă sunt afişate numai dacă parola expiră în şapte zile.

```
                          Sign-on Information
                                                                System:
Previous sign-on . . . . . . . . . . . . . . :   10/30/91  14:15:00

Sign-on attempts not valid . . . . . . . . . :   3

Days until password expires  . . . . . . . . :   5
```

Figura 3. Ecranul Informaţii semnare

Tabela 65. Valori posibile pentru DSPSGNINF:

***SYSVAL**	Este folosită valoarea de sistem QDSPSGNINF.
***NO**	Ecranul Informaţii semnare nu este arătat când utilizatorul semnează.
***YES**	Ecranul Informaţii semnare este arătat când utilizatorul semnează.

Recomandări: Ecranul Informaţii semnare este o unealtă pentru utilizatori pentru monitorizarea profilurilor lor şi pentru detectarea încercărilor greşite. Se recomandă ca toţii utilizatorii să vadă acest ecran. Utilizatorii cu autorizare specială sau autorizare la obiectele critice ar trebui încurajaţi să folosească ecranul pentru a se asigura că nimeni nu încearcă să folosească profilurile lor.

Interval de expirare parolă

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
PWDEXPITV

Lungime:
5,0

Necesitatea utilizatorilor pentru modificarea parolelor lor după o perioadă de timp specificată reduce riscul de accesare la sistem a unei persoane neautorizate. Întervalul de expirare parolă controlează numărul de zile în care o parolă validă poate fi folosită înainte de a fi schimbată.

Când parola unui utilizator a expirat, utilizatorul primeşte un mesaj la semnare. Utilizatorul poate apăsa tasta Enter pentru a aloca o nouă parolă sau poate apăsa F3 (Ieşire) pentru a anula încercarea de semnare fără alocarea unei noi parole. Dacă utilizatorul alege să modifice parola, este arătat ecranul Modificare parolă şi este rulată validarea parolei pline pentru noua parolă. Figura 1 la pagina 60 arată un exemplu de mesj de expirare parolă.

Recomandări: Folosiţi intervalul parolă profil utilizator ca să necesite profiluri cu autorizări speciale *SERVICE, *SAVSYS sau *ALLOBJ pentru modificarea parolelor mai frecvent decât alţi utilizatori.

Tabela 66. Valori posibile pentru PWDEXPITV:

***SYSVAL**	Este folosită valoarea de sistem QPWDEXPITV.
***NOMAX**	Sistemul nu cere utilizatorului să modifice parola.
interval de expirare parolă	Specificaţi un număr de la 1 până la 366.

Recomandări: Setaţi valoarea de sistem QPWDEXPITV pentru un interval corespunzător, cum ar fi 60 până la 90 de zile. Folosiţi câmpul *Interval de expirare parolă* din profilul utilizator pentru utilizatorii individuali care ar trebui să-şi modifice parolele mai frecvent, cum ar fi adminstratorii de securitate.

Gestiune parolă locală

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
LCLPWDMGT

Lungime:
4

Specifică dacă parola profilului utilizator ar trebui să fie gestionată local. Dacă parola este gestionată local, atunci parola este memorată local cu profilul utilizator. Aceasta este metoda tradiţională de memorare a parolei.

Dacă parola nu este gestionată local, atunci parola locală OS/400 este setată la *NONE. Valoarea specificată în parametrul de parolă va fi trimisă la alte produse IBM care fac sincronizare de parolă, cum ar fi serverul IBM iSeries Integration for Windows. Utilizatorul nu-şi va putea modifica parola folosind comanda Modificare parolă (CHGPWD). În plus, el nu va putea semna direct pe sistem. Specificarea acestei valori va afecta alte produse IBM care fac sincronizare de parolă, cum ar fi serverul IBM Integration for Windows. Consultaţi-vă documentaţia de produs pentru detalii.

Acest parametru nu ar trebui setat la *NO decât dacă utilizatorul are nevoie numai să acceseze sistemul prin alte platforme, cum ar fi Windows.

Tabela 67. Valori posibile pentru LCLPWDMGT:

***YES**	Parola este gestionată local.
***NO**	Parola nu este gestionată local.

Limitare sesiuni dispozitiv

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
LMTDEVSSN

Lungime:
7

Câmpul *Limitare sesiuni dispozitiv* controlează dacă un utilizator poate fi semnat la mai mult de o staţie de lucru în acelaşi timp. Valoarea nu restricţionează folosirea meniului Cerere sistem sau a unei a doua semnări de la acelaşi dispozitiv.

Tabela 68. Valori posibile pentru LMTDEVSSN:

***SYSVAL**	Este folosită valoarea de sistem QLMTDEVSSN.
***NO**	Utilizatorul poate fi semnat la mai multe dispozitive în acelaşi timp.
***YES**	Utilizatorul nu poate fi semnat la mai multe dispozitive în acelaşi timp.

Recomandări: Limitarea utilizatorilor la o singură staţie de lucru în acelaşi timp este o cale de descurajare a partajării profilurilor de utilizator. Setaţi valoarea de sistem QLMTDEVSSN la 1 (YES). Dacă unii utilizatori trebuie să semneze pe mai multe staţii de lucru, folosiţi câmpul *Limitare sesiuni de dispozitiv* din profilul de utilizator pentru acei utilizatori.

Punere în buffer tastatură

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
KBDBUF

Lungime:
10

Acest parametru specifică valoarea de punere în buffer tastatură folosită când un job este iniţializat pentru acest profil utilizator. Noua valoare îşi va face efectul următoarea dată când utilizatorul semnează.

Câmpul de punere în buffer tastatură controlează două funcţii:

Tastare înainte:
Lasă utilizatorul să tasteze datele mai repede decât pot fi trimise la sistem.

Punere în buffer tastă Attn:
Dacă punerea în buffer tastă Attn este pornită, tasta Attn este tratată la fel ca orice altă tastă. Dacă punerea în buffer tastă Attn nu este pornită, apăsarea tastei Attn determină trimiterea informaţiilor la sistem chiar dacă altă intrare de la staţia de lucru este inhibată.

Tabela 69. Valori posibile pentru KBDBUF:

***SYSVAL**	Este folosită valoarea de sistem QKBDBUF.
***NO**	Caracteristica tastare înainte şi opţiunea de punere în buffer tastă Attn nu sunt active pentru acest profil utilizator.
***TYPEAHEAD**	Caracteristica tastare înainte este activă pentru acest profil utilizator.
***YES**	Caracteristica tastare înainte şi opţiunea de punere în buffer tastă Attn sunt active pentru acest profil utilizator.

Spaţiu de stocare maxim

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
MAXSTG

Lungime:
11,0

Puteţi specifica dimensiunea maximă a spaţiului de stocare auxiliar care este utilizat la stocarea obiectelor permanente care sunt deţinute de un profil utilizator, inclusiv obiecte plasate în biblioteca temporară (QTEMP) în timpul unui job. Spaţiul maxim este specificat în kiloocteţi (1024 octeţi).

Dacă spaţiul necesar este mai mare decât dimensiunea maximă specificată când utilizatorul încearcă să creeze un obiect, obiectul nu este creat.

Valoarea maximă de spaţiu este aplicată independent pentru fiecare pool de memorie auxiliară (ASP) independent din sistem. De aceea, specificarea valorii 5000 înseamnă că profilul de utilizator poate folosi următoarele:

- 5000 KB de memorie auxiliară în ASP-ul de sistem şi ASP-urile de utilizator de bază.

- 5000 KB de memorie auxiliară în ASP-ul independent 00033 (dacă există).
- 5000 KB de memorie auxiliară în ASP-ul independent 00034 (dacă există).

Aceasta oferă un total de 15000 KB de memorie auxiliară din întregul sistem.

Când planificaţi memoria maximă pentru profilurile de utilizator, luaţi în onsiderare următoarele funcţii de sistem, care pot afecta memoria maximă cerută de un utilizator:

- O operaţie de restaurare întâi alocă memoria utilizatorului care efectuează operaţia de restaurare şi apoi transferă obiectele la OWNER. Utilizatorii care efectuează operaţii de restaurare mari ar trebui să aibă MAXSTG(*NOMAX) în profilurile lor de utilizatori.
- Profilul utilizator care deţine un receptor jurnal este alocat memoriei pe măsură ce dimensiunea receptorului creşte. Dacă sunt create noi receptoare, spaţiul continuă să fie alocat profilului utilizator care deţine receptorul de jurnal activ. Utilizatorii care deţin receptoare de jurnal active ar trebui să aibă MAXSTG(*NOMAX) în profilurile lor de utilizatori.
- Dacă un profil utilizator specifică OWNER(*GRPPRF), dreptul de proprietate al oricărui obiect creat de utilizator este transferat la profilul de grup după crearea obiectului. Totuşi, utilizatorul care creează obiectul trebuie să aibă spaţiu de stocare adecvat pentru a conţine orice obiecte create anterior transferării dreptului de proprietate asupra obiectului la profilul de grup.
- Proprietarul unei biblioteci este alocat spaţiului de stocare pentru descrierile obiectelor plasate în bibliotecă, chiar dacă obiectele sunt deţinute de alt profil utilizator. Exemple ale unor asemenea descrieri sunt referinţele text şi de program.
- Spaţiu de stocare este alocat profilului utilizator pentru obiecte temporare care sunt folosite în timpul procesării unui job. Exemple ale unor asemenea obiecte sunt blocurile de control comitere, spaţiile de editare fişier şi documentele.

Tabela 70. Valori posibile pentru MAXSTG:

***NOMAX**	Poate fi alocat atâta spaţiu cât este necesar acestui profil.
maxim KB	Specificaţi dimensiunea maximă de spaţiu în kiloocteţi (1 kilooctet are 1024 octeţi) care poate fi alocată acestui profil utilizator.

Limită de prioritate

Prompt adăugare utilizator:
Neafişat

Parametru CL:
PTYLMT

Lungime:
1

Un job batch are trei valori de prioritate diferite:

Rulare prioritate:
Determină cum concurează jobul pentru resursele maşinii când rulează. Prioritatea de rulare este determinată de clasa jobului.

Prioritate job:
Determină prioritatea de planificare pentru un job batch când jobul este în coada de joburi. Prioritatea de job poate fi setată de descrierea de job sau în comanda de lansare.

Prioritate ieşire:
Determină prioritatea de planificare pentru o ieşire creată de job în coada de ieşire. Prioritatea de ieşire poate fi setată de descrierea de job sau în comanda de lansare.

Limita de prioritate din profilul de utilizator determină priorităţile de planificare maxime (prioritate de job şi prioritate de ieşire) permise pentru joburile pe care le lansează utilizatorul. Controlează prioritatea când jobul este lansat, precum şi orice modificări făcute în timp ce jobul rulează sau aşteaptă în coadă.

Limita de prioritate limitează şi modificările pe care un utilizator cu autorizarea specială *JOBCTL le poate face pentru jobul altui utilizator. Nu puteţi da jobului altcuiva o prioritate mai mare decât limita specificată în propriul dumneavoastră profil de utilizator.

Dacă un job batch rulează sub un profil utilizator diferit de utilizatorul care lansează jobul, limitele de prioritate pentru jobul batch sunt determinate de profilul sub care rulează jobul. Dacă o prioritate de planificare cerută pe un job lansat este mai mare decât limita de prioritate din profilul utilizator, prioritatea jobului este redusă la nivelul permis de profilul de utilizator.

Tabela 71. Valori posibile pentru PTYLMT:

3	Limita de prioritate implicită pentru profiluri utilizator este 3. Prioritatea implicită pentru prioritatea de job şi cea de ieşire pe descrieri de job este 5. Setarea limitei de prioritate pentru profilul utilizator la 3 dă utilizatorului abilitatea de a muta unele joburi înaintea altora în cozi.
limită de prioritate	Specificaţi o valoare, de la 1 la 9. Cea mai mare prioritate este 1; cea mai mică prioritate este 9.

Recomandări: Folosirea valorilor de prioritate din descrierile de job şi din comenzile de lansare job este de obicei un mod mai bun de a gestiona utilizarea resurselor de sistem decât modificarea limitei de prioritate în profilurile de utilizator.

Folosiţi limita de prioritate din profilul de utilizator pentru a controla modificările pe care utilizatorii le pot face la joburile lansate. De exemplu, operatorii de sistem pot necesita o limită de prioritate mai mare pentru a putea muta joburile în cozi.

Descriere de job

Prompt adăugare utilizator:
Neafişat

Parametru CL:
JOBD

Lungime
10 (nume descriere de job) 10 (nume bibliotecă)

Autorizare:
*USE pentru descriere de job, *READ şi *EXECUTE pentru bibliotecă

Când un utilizator semnează, sistemul caută intrarea staţiei de lucru în descrierea de subsistem pentru a determina care descriere de job să o folosească pentru un job interactiv. Dacă intrarea staţie de lucru specifică *USRPRF pentru descrierea de job, este folosită descrierea de job din profilul de utilizator.

Descrierea de job pentru un job batch este specificată când jobul este pornit. Poate fi specificată prin nume sau poate fi descrierea de job din profilul de utilizator sub care rulează jobul.

O descriere de job conţine un set specific de atribute legate de job, precum cozile de joburi pe care să le folosească, prioritaea de planificare, datele de rutare, gravitatea cozii de mesaje, lista de biblioteci şi informaţiile de ieşire. Atributele determină cum este rulat fiecare job în sistem.

Vedeţi cartea *Work Management* pentru informaţii suplimentare despre descrierile de job şi utilizările lor.

Tabela 72. Valori posibile pentru JOBD:

QDFTJOBD	Este folosită descrierea de job furnizată de sistem, găsită în biblioteca QGPL. Puteţi folosi comanda Afişare descriere job (DSPJOBD) pentru a vedea atributele conţinute în această descriere de job.
nume descriere de job	Specificaţi numele descrierii de job, 10 caractere sau mai puţin.

Tabela 73. Valori posibile pentru Biblioteca JOBD:

***LIBL**	Este folosită lista de biblioteci pentru localizarea descrierii de job.
***CURLIB**	Pentru localizarea descrierii de job este folosită biblioteca curentă pentru job. Dacă nu există nici o intrare de bibliotecă curentă în lista de biblioteci, se foloseşte QGPL.
nume-bibliotecă	Specificaţi biblioteca unde este localizată descrierea de job, 10 caractere sau mai puţin.

Recomandări: Pentru joburi interactive, descrierea de job este o metodă bună de controlare a accesului la bibliotecă. Puteţi folosi o descriere de job pentru un individ pentru a specifica o listă unică de biblioteci, în loc să folosiţi valoarea de sistem QUSRLIBL.

Profil de grup

Prompt adăugare utilizator:
Profil grup

Parametru CL:
GRPPRF

Lungime:
10

Autorizare:
Pentru specificarea unui grup când creaţi sau modificaţi un profil de utilizator, trebuie să aveţi autorizarea *OBJMGT, *OBJOPR, *READ, *ADD, *UPD şi *DLT la profilul de grup.

Notă: Autorizarea adoptată nu este folosită pentru verificarea autorizării *OBJMGT la profilul de grup. Pentru detalii suplimentare despre autorizarea adoptată, consultaţi “Obiecte care adoptă autorizarea proprietarului” la pagina 123.

Specificarea unui nume de profil de grup face ca utilizatorul să devină membru al acelui profil de grup. Profilul de grup poate furniza utilizatorului autorizarea de folosire a obiectelor pentru care utilizatorul nu are autorizare specifică. Puteţi specifica până la 15 grupuri adiţionale pentru utilizator în parametrul *Profil de grup suplimentar* (SUPGRPPRF).

Când este specificat un profil de grup într-un profil de utilizator, utilizatorului îi sunt acordate în mod automat autorizările *OBJMGT, *OBJOPR, *READ, *ADD, *UPD şi *DLT la profilul de grup, dacă profilul de grup nu este deja unul dintre profilurile de grup ale utilizatorului. Aceste autorizări sunt necesare pentru funcţiile sistemului şi nu trebuie înlăturate.

Dacă un profil specificat în parametrul GRPPRF nu este deja un profil de grup, sistemul setează informaţiile din profil marcându-l ca profil de grup. De asemenea, sistemul generează un gid pentru profilul de grup, dacă deja nu are unul.

Consultaţi “Planificarea profilurilor de grup” la pagina 207 pentru informaţii suplimentare despre folosirea profilurilor de grup.

Tabela 74. Valori posibile pentru GRPPRF:

***NONE**	Nici un profil de grup nu este folosit cu acest profil de utilizator.
nume profil utilizator	Specificaţi numele unui profil de grup în care acest profil de utilizator este membru.

Proprietar

Prompt adăugare utilizator:
Neafişat

Parametru CL:
OWNER

Lungime:
10

Dacă un utilizator este membrul unui grup, folosiţi parametrul *propietar* din profilul de utilizator ca să specificaţi cine deţine obictele nou create de utilizator. Obiectele pot fi deţinute fie de utilizator, fie de primul grup al utilizatorului (valoarea parametrului GRPPRF). Puteţi specifica câmpul *OWNER* numai dacă aţi specificat câmpul *Profil de grup*.

Tabela 75. Valori posibile pentru OWNER:

***USRPRF**	Acest profil de utilizator este OWNER pentru orice obiect nou pe care îl creează.
***GRPPRF**	Profilul de grup este făcut OWNER pentru toate obiectele create de utilizator şi îi este dată autorizarea *ALL pentru obiecte. Profilului de utilizator nu îi este dată nici o autorizare specifică pentru noile obiecte create. Dacă este specificat *GRPPRF, trebuie să specificaţi un nume de profil de grup în parametrul GRPPRF şi parametrul GRPAUT trebuie să fie *NONE. **Note:** 1. Dacă daţi drept de propietate grupului, toţi membrii acelui grup pot modifica, înlocui şi şterge obiectul. 2. Parametrul *GRPPRF este ignorat pentru toate sistemele de fişiere cu excepţia QSYS.LIB. În cazurile în care parametrul este ignorat, utilizatorul păstrează dreptul de proprietate asupra obiectului.

Autorizare de grup

Prompt adăugare utilizator:
Neafişat

Parametru CL:
GRPAUT

Lungime:
10

Dacă profilul de utilizator este membrul unui grup şi este specificat OWNER(*USRPRF), câmpul *Autorizare de grup* controlează ce autorizare este dată profilului de grup pentru orice obiect creat de acest utilizator.

Autorizarea de grup poate fi specificată numai când GRPPRF nu este *NONE şi OWNER este *USRPRF. Autorizarea de grup se aplică profilului specificat în parametrul GRPPRF. Nu se aplică profilurilor de grup suplimentare specificate în parametrul SUPGRPPRF.

Tabela 76. Valori posibile pentru GRPAUT:

***NONE**	Nici o autorizare specifică nu este dată profilului de grup când utilizatorul creează obiecte.
***ALL**	Profilului de grup îi sunt date toate autorizările de gestionare şi de date pentru orice obiect create de utilizator.
***CHANGE**	Profilului de grup îi este dată autorizarea de modificare a oricărui obiect creat de utilizator.
***USE**	Profilului de grup îi este dată autorizarea de vizualizare a oricărui obiect creat de utilizator.
***EXCLUDE**	Profilului de grup îi este refuzat specific accesul la orice obiect creat de utilizator.

Consultaţi “Definirea modului în care pot fi accesate informaţiile” la pagina 110 pentru o explicaţie completă a autorizărilor care pot fi acordate.

Tip autorizare de grup

Prompt adăugare utilizator:
Neafişat

Parametru CL:
GRPAUTTYP

Lungime:
10

Când un utilizator creează un obiect nou, parametrul *Tip autorizare de grup* din profilul utilizatorului determină ce tip de autorizare primeşte grupul utilizatorului pentru noul obiect. Parametrul GRPAUTTYP lucrează împreună cu parametrii OWNER, GRPPRF şi GRPAUT la determinarea autorizării grupului pentru un obiect nou.

Tabela 77. Valori posibile pentru GRPAUTTYP: [1]

***PRIVATE**	Autorizarea definită în parametrul GRPAUT este alocată la profilul de grup ca şi o autorizare privată.
***PGP**	Profilul de grup definit în parametrul GRPPRF este grupul primar pentru obiectul nou creat. Autorizarea de grup primar pentru obiect este autorizarea specificată în parametrul GRPAUT.

[1] Autorizarea privată şi autorizarea de grup primar furnizează acelaşi acces la obiect, dar ele au caracteristici de performanţă diferite. “Grupul primar pentru un obiect” la pagina 119 explică cum lucrează autorizarea de grup primar.

Recomandări: Specificarea *PGP este o metodă pentru începerea folosirii autorizăriii de grup primar. Luaţi în considerare folosirea GRPAUTTYP(*PGP) pentru utilizatorii care creează frecvent obiecte noi.

Grupuri suplimentare

Prompt adăugare utilizator:
Neafişat

Parametru CL:
SUPGRPPRF

Lungime:
150

Autorizare:
Pentru specificarea grupurilor suplimentare atunci când creaţi sau modificaţi un profil de utilizator, trebuie să aveţi autorizarea *OBJMGT, *OBJOPR, *READ, *ADD, *UPD şi *DLT la fiecare profil.

Notă: Autorizarea *OBJMGT nu poate veni de la autorizarea adoptată. Pentru detalii suplimentare, consultaţi “Obiecte care adoptă autorizarea proprietarului” la pagina 123.

Puteţi specifica numele de până la 15 profiluri pentru care acest utilizator primeşte autorizare. Utilizatorul devine un membru al fiecărui profil de grup suplimentar. Utilizatorul nu poate avea profiluri de grup suplimentare dacă parametrul GRPPRF este *NONE.

Când profilurile de grup suplimentare sunt specificate într-un profil utilizator, utilizatorului îi sunt acordate în mod automat autorizările *OBJMGT, *OBJOPR, *READ, *ADD, *UPD şi *DLT la fiecare profil de grup, dacă profilul de grup nu este deja unul dintre profilurile de grup ale utilizatorului. Aceste autorizări sunt necesare pentru funcţiile sistemului şi nu trebuie înlăturate. Dacă un profil specificat în parametrul SUPGRPPRF nu este deja un profil de grup, sistemul setează informaţii în semnarea profilului ca şi un profil de grup. De asemenea sistemul generează un gid pentru profilul de grup, dacă deja nu are unul.

Consultaţi “Planificarea profilurilor de grup” la pagina 207 pentru informaţii suplimentare despre folosirea profilurilor de grup.

Tabela 78. Valori posibile pentru SUPGRPPRF

***NONE**	Nici un grup suplimentar nu este folosit cu acest profil utilizator.
nume profil de grup	Specificaţi până la 15 nume de profiluri de grup pentru a fi folosite cu acest profil de utilizator. Aceste profiluri, în plus faţă de profilul specificat în parametrul GRPPRF, sunt utilizate pentru a da acces utilizatorului la obiecte.

Cod de contabilizare

Prompt adăugare utilizator:
Neafişat

Parametru CL:
ACGCDE

Lungime:
15

Contabilizarea jobului este o funcţie opţională folosită la adunarea de informaţii despre utilizarea resurselor de sistem. Valoarea de sistem pentru nivelul de contabilizare (QACGLVL) determină dacă este activă contabilizarea de job. Codul de contabilizare pentru un job vine fie din descrierea de job, fie din profilul de utilizator. Codul de contabilizare poate fi specificat şi când un job rulează, folosind comanda Modificare cod de contabilizare (CHGACGCDE).

Vedeţi cartea *Work Management* pentru informaţii suplimentare despre contabilizarea de job.

Tabela 79. Valori posibile pentru ACGCDE:

***BLANK**	Un cod de contabilizare de 15 spaţii este alocat acestui profil utilizator.
cod de contabilizare	Specificaţi un cod de contabilizare de 15 caractere. Dacă sunt specificate mai puţin de 15 caractere, şirul este completat cu spaţii în partea dreaptă.

Parolă document

Prompt adăugare utilizator:
Neafişat

Parametru CL:
DOCPWD

Lungime:
8

Puteţi specifica o parolă de document pentru utilizator pentru a proteja distribuirea de poştă personală de vizionarea de către persoane care lucrează în numele utilizatorului. Parola de document este suportată de unele produse DIA (Document Interchange Architecture), cum ar fi Scriitorul de ecran.

Tabela 80. Valori posibile pentru DOCPWD:

***NONE**	Nici o parolă de document nu este folosită de acest utilizator.
parolă document	Specificaţi o parolă document pentru acest utilizator. Parola trebuie să conste din 1 până la 8 caractere (litere de la A la Z şi numere de la 0 la 9). Primul caracter al parolei de document trebuie să fie alfabetic; restul caracterelor pot fi alfanumerice. Nu sunt permise spaţii incluse, spaţii la început şi caractere speciale.

Coadă de mesaje

Prompt adăugare utilizator:
Neafişat

Parametru CL:
MSGQ

Lungime:
10 (nume coadă de mesaje) 10 (nume bibliotecă)

Autorizare:
*USE pentru coada de mesaje, dacă există. *EXECUTE pentru biblioteca coadă de mesaje.

Puteţi specifica numele unei cozi de mesaje pentru un utilizator. O **coadă de mesaje** este un obiect în care mesajele sunt plasate când sunt trimise la o persoană sau un program. O coadă de mesaje este folosită când un utilizator trimite sau primeşte mesaje. Dacă coada de mesaje nu există, ea este creată când este creat sau modificat profilul. Coada de mesaje este deţinută de profilul creat sau modificat. Utilizatorului care creează profilul îi este dată autorizarea *ALL la coada de mesaje.

Dacă coada de mesaje pentru un profil utilizator este modificată folosind comanda Modificare profil utilizator (CHGUSRPRF), coada de mesaje anterioară nu este ştearsă automat de către sistem.

Tabela 81. Valori posibile pentru MSGQ:

***USRPRF**	O coadă de mesaje cu acelaşi nume cu numele de profil utilizator este folosită ca şi coadă de mesaje pentru acest utilizator. Dacă coada de mesaje nu există, ea este creată în biblioteca QUSRSYS.
nume coadă de mesaje	Specificaţi numele cozii de mesaje care este folosit pentru acest utilizator. Dacă specificaţi un nume de coadă de mesaje, trebuie să specificaţi şi parametrul de bibliotecă.

Tabela 82. Valori posibile pentru Biblioteca MSGQ:

***LIBL**	Lista de biblioteci este folosită pentru localizarea cozii de mesaje. Dacă coada de mesaje nu există, nu puteţi specifica *LIBL.
***CURLIB**	Pentru localizarea cozii de mesaje este folosită biblioteca curentă pentru job. Dacă nu există nici o intrare de bibliotecă curentă în lista de biblioteci, se foloseşte QGPL. Dacă nu există coada de mesaje, este creată în biblioteca curentă sau în QGPL.
nume-bibliotecă	Specificaţi biblioteca în care este localizată coada de mesaje. Dacă nu există coada de mesaje, este creată în această bibliotecă.

Recomandări: Când un utilizator semnează, coada de mesaje din profilul de utilizator este alocată acelui job utilizator. În cazul în care coada de mesaje este deja alocată altui job, utilizatorul primeşte un mesaj de evertizare în timpul semnării. Pentru a evita aceasta, daţi fiecărui utilizator o coadă de mesaje unică, de preferat cu acelaşi nume ca profilul de utilizator.

Livrare

Prompt adăugare utilizator:
Neafişat

Parametru CL:
DLVRY

Lungime:
10

Modul de livrare al unei cozi de mesaje determină dacă utilizatorul este întrerupt când ajunge un nou mesaj în coadă. Modul de livrare specificat în profilul de utilizator se aplică cozii de mesaje personale a utilizatorului. Dacă modificaţi livrarea cozii de mesaje în profilul de utilizator şi utilizatorul este semnat, modificarea are efect la următoarea semnare a utilizatorului. Puteţi modifica şi livrarea cozii de mesaje cu comanda Modificare coadă de mesaje (CHGMSGQ).

Tabela 83. Valori posibile pentru DLVRY:

***NOTIFY**	Jobul la care este alocată coada de mesaje este anunţat când ajunge un mesaj la coada de mesaje. Pentru joburi interactive la o staţie de lucru, alarma sonoră este pornită şi este aprinsă lumina de aşteptare mesaj. Tipul de livrare nu poate fi modificat în *NOTIFY dacă coada de mesaje este folosită şi de un alt utilizator.
***BREAK**	Jobul la care este alocată coada de mesaje este întrerupt când ajunge un mesaj la coada de mesaje. Dacă jobul este interactiv, este sunată alarma sonoră (dacă alarma este instalată). Tipul de livrare nu poate fi modificat în *BREAK dacă coada de mesaje este folosită şi de un alt utilizator.
***HOLD**	Mesajele sunt ţinute în coada de mesaje până când sunt cerute de utilizator sau de program.
***DFT**	Mesajelor care necesită răspunsuri li se răspunde cu răspunsul implicit; mesajele care au doar caracter informativ sunt ignorate.

Gravitate

Prompt adăugare utilizator:
Neafişat

Parametru CL:
SEV

Lungime:
2,0

Dacă o coadă de mesaje este în mod *BREAK sau *NOTIFY, codul de gravitate determină mesajele de cel mai jos nivel care sunt livrate utilizatorului. Mesajele a căror gravitate este mai mică decât codul de gravitate specificat sunt ţinute în coada de mesaje fără ca utilizatorul să fie anunţat.

Dacă modificaţi gravitatea cozii de mesaje în profilul de utilizator şi utilizatorul este semnat, modificarea are efect la următoarea semnare a utilizatorului. Puteţi modifica şi gravitatea cozii de mesaje cu comanda Modificare coadă de mesaje (CHGMSGQ).

Tabela 84. Valori posibile pentru SEV:

00:	Dacă nu este specificat un cod de gravitate, este folosit 00. Utilizatorul este anunţat de toate mesajele, dacă coada de mesaje este în mod *NOTIFY sau *BREAK.
gravitate cod	Specificaţi o valoare, între 00 şi 99, pentru cel mai mic cod de gravitate care cauzează anunţarea utilizatorului. Orice valoare de 2 cifre poate fi specificată, chiar dacă nici un cod de gravitate nu a fost definit pentru el (definit de sistem sau de utilizator).

Dispozitiv de tipărire

Prompt adăugare utilizator:
Imprimantă implicită

Parametru CL:
PRTDEV

Lungime:
10

Puteţi specifica imprimanta folosită la tipărirea ieşirii pentru acest utilizator. Fişierele spool sunt plasate într-o coadă de ieşire cu acelaşi nume ca şi imprimanta când coada de ieşire (OUTQ) este specificată ca dispozitiv de tipărire (*DEV).

Informaţii dispozitiv de tipărire şi coadă de ieşire din profilul utilizator sunt folosite doar dacă fişierul imprimantă specifică *JOB şi descrierea de job specifică *USRPRF. Pentru informaţii suplimentare despre directarea ieşirii imprimantă, vedeţi cartea *Printer Device Programming*.

Tabela 85. Valori posibile pentru PRTDEV:

***WRKSTN**	Este folosită imprimanta alocată staţiei de lucru a utilizatorului (în descrierea dispozitiv).
***SYSVAL**	Este folosită imprimanta de sistem implicită în valoarea de sistem QPRTDEV.
nume dispozitiv de tipărire	Specificaţi numele imprimantei folosite la tipărirea ieşirii pentru acest utilizator.

Coadă de ieşire

Prompt adăugare utilizator:
Neafişat

Parametru CL:
OUTQ

Lungime:
10 (nume coadă de ieşire) 10 (nume bibliotecă)

Autorizare:
*USE pentru coadă de ieşire *EXECUTE pentru bibliotecă

Atât procesările interactive, cât şi cele batch pot avea ca rezultat fişiere spool care sunt trimise la imprimantă. Fişierele spool sunt plasate într-o coadă de ieşire. Sistemul poate avea mai multe cozi de ieşire diferite. O coadă de ieşire nu trebuie neaparat să fie ataşată la o imprimantă pentru a primi fişiere spool noi.

Sunt folosite informaţiile din profilul de utilizator pentru dispozitivul de tipărire şi coada de ieşire numai dacă fişierul de imprimantă specifică *JOB şi descrierea de job specifică *USRPRF. Pentru informaţii suplimentare despre directarea ieşirii imprimantă, vedeţi cartea *Printer Device Programming*.

Tabela 86. Valori posibile pentru OUTQ:

***WRKSTN**	Este folosită coada de ieşire alocată staţiei de lucru a utilizatorului (în descrierea dispozitiv).
***DEV**	Este folosită o coadă de ieşire cu acelaşi nume ca şi dispozitivul de tipărire specificat în parametrul PRTDEV.
nume coadă de ieşire	Specificaţi numele cozii de ieşire care va fi folosită. Coada de ieşire trebuie să existe deja. Dacă este specificată o coadă de ieşire, trebuie să fie specificată şi biblioteca.

Tabela 87. Valori posibile pentru biblioteca OUTQ:

***LIBL**	Este folosită lista de biblioteci pentru localizarea cozii de ieşire.
***CURLIB**	Pentru localizarea cozii de ieşire este folosită biblioteca curentă pentru job. Dacă nu există nici o intrare de bibliotecă curentă în lista de biblioteci, se foloseşte QGPL.
nume-bibliotecă	Specificaţi biblioteca în care se află coada de ieşire.

Program de tratare tastă Attn

Prompt adăugare utilizator:
Neafişat

Parametru CL:
ATNPGM

Lungime:
10 (nume program) 10 (nume bibliotecă)

Autorizare:
*USE pentru program

*EXECUTE pentru bibliotecă

Programul de tratare a tastei Attention (ATNPGM) este programul apelat când utilizatorul apasă tasta Attention (ATTN) în timpul unui job interactiv.

ATNPGM este activat numai dacă programul de rutare al utilizatorului este QCMD. ATNPGM este activat înainte de apelarea programului iniţial. Dacă programul iniţial modifică ATNPGM, noul ATNPGM rămâne activ doar până când programul iniţial se termină. Dacă comanda Setare program tratare tastă Attention (SETATNPGM)e ste rulat dintr-o linie de comandă sau aplicaţie, noul ATNPGM specificat înlocuieşte ATNPGM din profilul de utilizator.

Notă: Consultaţi “Pornirea unui job interactiv” la pagina 169 pentru informaţii suplimentare despre scvenţa de procesare când semnează un utilizator.

Câmpul *Limitare capabilităţi* determină dacă un program de tratare tastă Attn diferit poate fi specificat de utilizator cu comanda Modificare profil (CHGPRF).

Tabela 88. Valori posibile pentru ATNPGM:

***SYSVAL**	Este folosită valoarea de sistem QATNPGM.
***NONE**	Nici un program de tratare tastă Attn nu este folosit de acest utilizator.
***ASSIST**	Este folosit Programul Attn din Asistent operaţional (QEZMAIN).
nume program	Specificaţi numele programului de tratare tastă Attn. Dacă este specificat un nume de program, trebuie să fie specificată o bibliotecă.

Tabela 89. Valori posibile pentru Biblioteca ATNPGM:

***LIBL**	Este folosită lista de biblioteci pentru localizarea programului de tratare tastă Attn.
***CURLIB**	Pentru localizarea programului de tratare a tastei Attn este folosită biblioteca curentă pentru job. Dacă nu există nici o intrare de bibliotecă curentă în lista de biblioteci, se foloseşte QGPL.
nume-bibliotecă:	Specificaţi biblioteca în care se află programul de tratare a tastei Attn.

Secvenţă de sortare

Prompt adăugare utilizator:
Neafişat

Parametru CL:
SRTSEQ

Lungime:
10 (valoare sau nume tabel) 10 (nume bibliotecă)

Autorizare:
*USE pentru tabelă *EXECUTE pentru bibliotecă

Puteţi specifica secvenţa de sortare folosită pentru ieşirea utilizatorului. Puteţi să folosiţi tabela de sortare furnizată de sistem sau să vă creaţi una proprie. O tabelă de sortare poate fi asociată cu un identificator de limbă particular de pe sistem.

Tabela 90. Valori posibile pentru SRTSEQ:

***SYSVAL**	Este folosită valoarea de sistem QSRTSEQ.
***HEX**	Pentru utilizator este folosită secvenţa de sortare hexazecimală standard.
***LANGIDSHR**	Este folosită tabela secvenţă de sortare asociată cu identificatorul de limbă al utilizatorului. Tabela poate conţine aceeaşi pondere pentru mai multe caractere.
***LANGIDUNQ**	Este folosită tabela secvenţă de sortare asociată cu identificatorul de limbă al utilizatorului. Tabela trebuie să conţină o pondere unică pentru fiecare caracter din pagina de cod.
nume tabel	Specificaţi numele tabelei secvenţă de sortare pentru acest utilizator.

Tabela 91. Valori posibile pentru Biblioteca SRTSEQ:

***LIBL**	Este folosită lista de biblioteci pentru localizarea tabelei specificate pentru valoarea SRTSEQ.
***CURLIB**	Pentru localizarea tabelei specificate pentru valoarea SRTSEQ este folosită biblioteca curentă pentru job. Dacă nu există nici o intrare de bibliotecă curentă în lista de biblioteci, se foloseşte QGPL.
nume-bibliotecă	Specificaţi biblioteca în care se află tabela secvenţă de sortare.

Identificator de limbă

Prompt adăugare utilizator:
Neafişat

Parametru CL:
LANGID

Lungime:
10

Puteţi specifica identificatorul de limbă pentru a fi folosit de sistem pentru utilizator. Pentru a consulta o listă de identificatori de limbă, apăsaţi F4 (prompt) pentru parametrul de identificator de limbă din ecranul Creare profil utilizator sau din ecranul Modificare profil utilizator.

Tabela 92. Valori posibile pentru LANGID:

***SYSVAL:**	Este folosită valoarea de sistem QLANGID pentru determinarea identificatorului de limbă.
identificator de limbă	Specificaţi un identificator de limbă pentru acest utilizator.

Identificator de regiune sau ţară

Prompt adăugare utilizator:
Neafişat

Parametru CL:
CNTRYID

Lungime:
10

Puteţi specifica identificatorul de regiune sau ţară pentru a fi folosit de sistem pentru utilizator. Pentru a consulta o listă de identificatori de regiune sau ţară, apăsaţi F4 (prompt) pentru parametrul identificator de regiune sau ţară din ecranul Creare profil utilizator sau din ecranul Modificare profil utilizator.

Tabela 93. Valori posibile pentru CNTRYID:

***SYSVAL**	Este folosită valoarea de sistem QCNTRYID pentru determinarea identificatorului de regiune sau ţară.
identificator de regiune sau ţară	Specificaţi identificatorul de regiune sau ţară pentru acest utilizator.

Identificator set de caractere codate

Prompt adăugare utilizator:
Neafişat

Parametru CL:
CCSID

Lungime:
5,0

Puteţi specifica identificatorul setului de caractere codate care va fi folosit de sistem pentru utilizator. Pentru a consulta o listă de identificatori de seturi de caractere codate, apăsaţi F4 (prompt) pentru parametrul de identificator de set de caractere codate în ecranul Creare profil utilizator sau în ecranul Modificare profil utilizator.

Tabela 94. Valori posibile pentru CCSID:

***SYSVAL**	Este folosită valoarea de sistem QCCSID pentru determinarea identificatorului de set de caractere codate.
identificator-set-caractere-codate	Specificaţi identificatorul de set de caractere codate pentru acest utilizator.

Control identificator de caracter

Prompt adăugare utilizator:
Neafişat

Parametru CL:
CHRIDCTL

Lungime:
10

Atributele *CHRIDCTL* controlează tipul de conversie a setului de caractere codate care apare pentru fişierele de afişare, fişierele de imprimantă şi grupurile de panouri. Informaţiile de control al identificatorului de caractere din profilul de utilizator sunt folosite numai dacă este specificată valoarea specială *CHRIDCTL în parametrul CHRID din comenzile de creare, modificare sau înlocuire pentru fişierele de afişare, fişierele de imprimantă şi grupurile de panouri.

Tabela 95. Valori posibile pentru CHRIDCTL:

***SYSVAL**	Este folosită valoarea de sistem QCHRIDCTL pentru determinarea controlului de identificator de caractere.
***DEVD**	Este folosită setarea CHRID a dispozitivului pentru CCSID-ul datelor. Nu survine nici o conversie, deoarece CCSID-ul datelor este întotdeauna identic cu setarea CHRID a dispozitivului.
***JOBCCSID**	Conversia de caractere apare atunci când există o diferenţă între valorile CHRID pentru dispozitiv, CCSID pentru job sau CCSID date. La intrare, datele caracter sunt convertite de la CHRID dispozitiv la CCSID job atunci când este necesar. La ieşire, datele caracter sunt convertite de la CCSID-ul jobului la CHRID-ul dispozitivului atunci când este necesar. La ieşire, datele caracter sunt convertite de la CCSID-ul fişierului sau grupului de panouri la CHRID-ul dispozitivului atunci când este necesar.

Atribute de job

Prompt adăugare utilizator:
Neafişat

Parametru CL:
SETJOBATR

Lungime:
160

Câmpul *SETJOBATR* specifică ce fel de atribute de job urmează să fie luate la iniţierea jobului din Locale-ul specificat în parametrul LOCALE.

Tabela 96. Valori posibile pentru SETJOBATR:

***SYSVAL**	Este folosită valoarea de sistem QSETJOBATR ca să se determine ce atribute de job urmează să fie luate din Locale.
***NONE**	Nici un atribut de job nu va fi luat din Locale.
	Orice combinaţie a următoarelor valori poate fi specificată:
***CCSID**	Este folosit identificatorul de set de caractere codate din Locale. Valoarea CCSID din Locale va înlocui CCSID-ul din profilul de utilizator.
***DATFMT**	Este folosit formatul de dată din Locale.
***DATSEP**	Este folosit separatorul de dată din Locale.
***DECFMT**	Este folosit formatul zecimal din Locale.
***SRTSEQ**	Este folosită secvenţa de sortare din Locale. Secvenţa de sortare din Locale va înlocui secvenţa de sortare din profilul de utilizator.
***TIMSEP**	Este folosit separatorul de timp din Locale.

Locale

Prompt adăugare utilizator:
Neafişat

Parametru CL:
LOCALE

Lungime:
2048

Câmpul *LOCALE* specifică numele de cale pentru Locale-ul care este alocat variabilei de mediu LANG pentru acest utilizator.

Tabela 97. Valori posibile pentru LOCALE:

***SYSVAL**	Este folosită valoarea de sistem QLOCALE este folosită pentru determinarea numelui de cale Locale spre a fi alocat pentru acest utilizator.
***NONE**	Nici un Locale nu este alocat pentru acest utilizator.
***C**	Utilizatorului îi este alocat Locale C.
***POSIX**	Utilizatorului îi este alocat Locale POSIX.
nume cale locale	Utilizatorului îi este alocat numele de cale Locale specificat.

Opţiuni utilizator

Prompt adăugare utilizator:
Neafişat

Parametru CL:
USROPT

Lungime:
240 (10 caractere fiecare)

Câmpul *Opţiuni utilizator* vă permite să personalizaţi anumite ecrane de sistem şi funcţii pentru utilizator. Puteţi specifica mai multe valori pentru parametrul opţiune utilizator.

Tabela 98. Valori posibile pentru USROPT:

***NONE**	Nu este folosită nici o opţiune specială pentru acest utilizator. Este folosită interfaţa de sistem standard.
***CLKWD**	Sunt afişate cuvinte cheie în loc de posibile valori de parametri când este promptată o comandă CL. Aceasta este echivalentul apăsării tastei F11 din ecranul de prompt normal pentru o comandă CL.
***EXPERT**	Când utilizatorul vizualizează ecrane care arată autorizări de obiect, precum ecranul Editare autorizare obiect sau ecranul Editare listă autorizări, informaţiile de autorizare detaliate sunt afişate fără ca utilizatorul să apese F11 (Afişare detalii). “Ecrane pentru autorizare” la pagina 128 prezintă un exemplu al versiunii experte a ecranului.
***HLPFULL**	Utilizatorul vede informaţiile de ajutor în ecran complet, nu într-o fereastră.
***PRTMSG**	Un mesaj este trimis la coada de mesaje a utilizatorului când un fişier spool este tipărit pentru acest utilizator.
***ROLLKEY**	Acţiunile tastelor Page Up şi Page Down sunt inversate.
***NOSTSMSG**	Mesajele de stare afişate de obicei în partea de jos a ecranului nu sunt arătate utilizatorului.
***STSMSG**	Mesajele de stare sunt afişate când sunt trimise la utilizator.

Numărul de identificare utilizator

Prompt adăugare utilizator:
Neafişat

Parametru CL:
UID

Lungime:
10,0

Sistemul de fişiere integrat foloseşte numărul de identificare utilizator (uid) pentru a identifica un utilizator şi verifică autorizarea utilizatorului. Fiecare utilizator din sistem trebuie să aibă un uid unic.

Tabela 99. Valori posibile pentru UID:

***GEN**	Sistemul generează un unic uid pentru acest utilizator. Va fi generat un uid mai mare de 100.
uid	O valoare de la 1 la 4294967294 care va fi alocată ca uid pentru acest utilizator. Trebuie ca uid să nu fi fost deja alocat altui utilizator.

Recomandare: Pentru majoritatea instalărilor, lăsaţi sistemul să genereze un uid pentru utilizatorii noi specificând UID(*GEN). Totuşi, dacă sistemul dumneavoastră este parte a unei reţele, ar putea fi necesar să alocaţi uid-uri care să se potrivească cu cele alocate altor sisteme din reţea. Consultaţi administratorul de reţea.

Număr identificare grup

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
GID

Lungime:
10,0

Sistemul de fişiere integrat foloseşte numărul de identificare grup (gid) pentru a identifica acest profil ca profil de grup. Un profil care este folosit ca profil de grup de către Sistemul de fişiere integrat trebuie să aibă un gid.

Tabela 100. Valori posibile pentru GID:

***NONE**	Acest profil nu are un gid.
***GEN**	Sistemul generează un unic gid pentru acest profil. Va fi generat un gid mai mare de 100.
gid	O valoare de la 1 la 4294967294 care va fi alocată ca gid pentru acest profil. Trebuie ca gid să nu fi fost deja alocat altui profil.

Recomandare: Pentru majoritatea instalărilor, lăsaţi sistemul să genereze un gid pentru noi profiluri de grup specificând GID(*GEN). Totuşi, dacă sistemul dumneavoastră este parte a unei reţele, ar putea fi necesar să alocaţi gid-uri care să se potrivească cu cele alocate altor sisteme din reţea. Consultaţi administratorul de reţea.

Nu alocaţi un gid unui profil de utilizator pe care nu intenţionaţi să îl folosiţi ca profil de grup. În unele medii, un utilizator care este semnat şi are un gid are restricţii asupra executării anumitor funcţii.

Directorul de bază

Prompt adăugare utilizator:
Neafişat

Parametru CL:
HOMEDIR

Lungime:
2048

Directorul de bază este diretorul de lucru iniţial al utilizatorului pentru Sistemul de fişiere integrat. Directorul de bază este directorul curent al utilizatorului dacă un alt director curent nu a fost specificat. Dacă directorul de bază specificat în profil nu există când utilizatorul semnează, directorul de bază al utilizatorului este directorul rădăcină (/).

Tabela 101. Valori posibile pentru HOMEDIR:

***USRPRF**	Directorul rădăcină alocat utilizatorului este /home/xxxxx, unde xxxxx este numele profilului utilizatorului.
director de bază	Numele directorului de bază de alocat acestui utilizator.

Asociere EIM

Prompt adăugare utilizator:
Neafişat

Parametru CL:
EIMASSOC

Lungime:
128

Specifică dacă trebuie să fie adăugată o asociere EIM (Mapare identitate întreprindere) unui identificator EIM pentru acest utilizator. Opţional, identificatorul EIM poate fi creat dacă nu există deja.

Notă:

1. Aceste informaţii nu sunt stocate în profilul de utilizator. Aceste informaţii nu sunt salvate sau restaurate cu profilul de utilizator.
2. Dacă acest sistem nu este configurat pentru EIM, nu este făcută nici o procesare. Neputinţa de a realiza operaţii EIM nu cauzează eşuarea comenzii.

Tabela 102. Valori posibile pentru EIMASSOC, valori singulare:

Valori singulare	
***NOCHG**	Asocierea EIM nu va fi adăugată.

Tabela 103. Valori posibile pentru EIMASSOC, Elementul 1:

Elementul 1: identificatorul EIM

Specificaţi identificatorul EIM pentru această asociere.

***USRPRF**	Numele identificatorului EIM este acelaşi cu numele profilului utilizator.
valoare caracter	Specificaţi numele indentificatorului EIM.

Tabela 104. Valori posibile pentru EIMASSOC, Elementul 2:

Elementul 2: Tip de asociere

Specifică tipul de asociere. Este recomandat ca o asociere destinaţie să fie adăugată pentru un utilizator OS/400.

Asocierile destinaţie sunt în principal folosite pentru a securiza datele existente. Ele sunt găsite ca rezultat al mapării operaţiei de căutare (de exemplu, eimGetTargetFromSource()), dar nu pot fi folosite ca identitatea sursă pentru o operaţie de căutare mapare.

Asocierile sursă sunt în principal folosite pentru scopuri de autentificare. Ele pot fi folosite ca identitate sursă a mapării operaţiei de căutare, dar nu vor fi găsite ca destinaţie a operaţiei de căutare mapare.

Asocierile administrative sunt folosite pentru a arăta că o identitate este asociată cu un identificator EIM, dar nu pot fi folosite ca sursă pentru, şi nu vor fi găsite ca destinaţie a unei operaţii de căutare mapare.

***TARGET**	Procesaţi o asociere destinaţie.
***SOURCE**	Procesaţi o asociere sursă.
***TGTSRC**	Procesaţi o asociere sursă şi una destinaţie.
***ADMIN**	Procesaţi o asociere administrativă.
***ALL**	Procesaţi toate tipurile de asocieri.

Tabela 105. Valori posibile pentru EIMASSOC, Elementul 3:

Elementul 3: Acţiune de asociere

***REPLACE**	Asocierile de tipul specificat vor fi înlăturate din identificatoarele EIM care au o asociere pentru acest profil utilizator şi registru EIM local. O nouă asociere va fi adăugată la identificatorul EIM specificat.
***ADD**	Adăugaţi o asociere.
***REMOVE**	Înlăturaţi o asociere.

Tabela 106. Valori posibile pentru EIMASSOC, Elementul 4:

Elementul 4: Creare identificator EIM

Specifică dacă identificatorul EIM ar trebui să fie creat dacă nu există deja.

***NOCRTEIMID**	Identificatorul EIM nu este creat.
***CRTEIMID**	Identificatorul EIM este creat dacă nu există.

Autorizare

Prompt adăugare utilizator:
Neafişat

Parametru CL:
AUT

Lungime:
10

Câmpul *Autorizare* specifică autorizarea publică pentru profilul de utilizator. Autorizarea pentru un profil controlează multe funcţii asociate cu profilul, precum:

Modificarea lui

Afişarea lui

Ştergerea lui

Lansarea unui job folosindu-l

Specificarea lui într-o descriere de job

Transferarea dreptului de proprietate a obiectului la el

Adăugarea de membri, dacă este un profil de grup

Tabela 107. Valori posibile pentru AUT:

***EXCLUDE**	Publicului îi este în mod explicit refuzat accesul la profilul de utilizator.
***ALL**	Publicului îi sunt date toate autorizările de date şi de gestionare pentru profilul de utilizator.
***CHANGE**	Publicului îi este dată autorizarea de modificare a profilului de utilizator.
***USE**	Publicului îi este dată autorizarea de vizualizare a profilului de utilizator.

Consultaţi “Definirea modului în care pot fi accesate informaţiile” la pagina 110 pentru o explicaţie completă a autorizărilor care pot fi acordate.

Recomandare: Pentru a preveni folosirea greşită a profilurilor de utilizator care au autorizare pentru obiecte critice, asiguraţi-vă că autorizarea publicului pentru profiluri este *EXCLUDE. Printre posibilele folosiri greşite ale unui profil se numără lansarea unui job care rulează sub acel profil de utilizator sau modificarea unui program astfel încât să adopte autorizarea acelui profil de utilizator.

Auditare obiect

Prompt adăugare utilizator:
Neafişat

Parametru CL:
OBJAUD

Lungime:
10

Valoarea de auditare obiect pentru un profil de utilizator lucrează împreună cu valoarea de auditare obiect pentru un obiect pentru a detrmina dacă accesul utilizatorului la un obiect este auditat. Auditarea de obiect pentru un profil de utilizator nu poate fi specificată în nici un ecran pentru profilul de utilizator. Folosiţi comanda CHGUSRAUD pentru a specifica auditarea de obiect pentru un utilizator. Doar un utilizator cu autorizarea specială *AUDIT poat folosi comanda CHGUSRAUD.

Tabela 108. Valori posibile pentru OBJAUD:

***NONE**	Valoarea OBJAUD pentru obiecte determină dacă auditarea de obiect este efectuată pentru acest utilizator.
***CHANGE**	Dacă valoarea OBJAUD pentru un obiect specifică *USRPRF, este scrisă o înregistrare de auditare când acest utilizator modifică obiectul.
***ALL**	Dacă valoarea OBJAUD pentru un obiect specifică *USRPRF, este scrisă o înregistrare de auditare când acest utilizator modifică sau citeşte obiectul.

Tabela 109 arată cum lucrează împreună valorile OBJAUD pentru utilizator şi obiecte:

Tabela 109. Auditarea realizată pentru accesul la obiect

Valoare OBJAUD pentru obiect	**Valoare OBJAUD pentru utilizator**		
	***NONE**	***CHANGE**	***ALL**
*NONE	Nimic	Nimic	Nimic
*USRPRF	Nimic	Modificare	Modificare şi folosire
*CHANGE	Modificare	Modificare	Modificare

Tabela 109. Auditarea realizată pentru accesul la obiect (continuare)

Valoare OBJAUD pentru obiect	Valoare OBJAUD pentru utilizator		
	***NONE**	***CHANGE**	***ALL**
*ALL	Modificare şi folosire	Modificare şi folosire	Modificare şi folosire

"Planificarea auditării accesului la obiect" la pagina 246 furnizează informaţii despre cum se folosesc valorile de sistem şi valorile de auditare obiect pentru a vă indeplini nevoile de auditare securitate.

Acţiune de auditare

Prompt adăugare utilizator:
Neafişat

Parametru CL:
AUDLVL

Lungime:
640

Pentru un utilizator individual, puteţi specifica care acţiune relevantă de securitate ar trebui înregistrată în jurnalul de auditare. Acţiunile specificate pentru un utilizator individual se aplică în plus faţă de acţiunile specificate pentru toţi utilizatorii de valorile de sistem QAUDLVL şi QAUDLVL2. Acţiunea de auditare pentru un profil de utilizator nu poate fi specificată în nici un ecran de profil de utilizator. Este definită folosind comanda CHGUSRAUD. Doar un utilizator cu autorizarea specială *AUDIT poat folosi comanda CHGUSRAUD.

Tabela 110. Valori posibile pentru AUDLVL:

***NONE**	Valoarea de sistem QAUDLVL controlează acţiunea de auditare pentru acest utilizator. Nu este terminată nici o auditare suplimentară.
***CMD**	Şirurile de comenzi sunt înregistrate în istoric. *CMD poate fi specificat numai pentru utilizatori individuali. Auditarea şirurilor de comenzi nu este disponibilă ca opţiune de sistem folosind valoarea de sistem QAUDLVL.
***CREATE**	Operaţiile de creare obiect sunt înregistrate în istoric.
***DELETE**	Operaţiile de ştergere obiect sunt înregistrate în istoric.
***JOBDTA**	Modificările de job sunt înregistrate în istoric.
***OBJMGT**	Operaţiile de redenumire şi mutare obiect sunt înregistrate în istoric.
***OFCSRV**	Modificările la directorul de distribuţie sistem şi acţiunile de poştă birou sunt înregistrate în istoric.
***PGMADP**	Obţinerea autorizării la un obiect printr-un program care adoptă autorizare este înregistrată în istoric.
***SAVRST**	Operaţiile de restaurare şi salvare sunt înregistrate în istoric.
***SECURITY**	Sunt înregistrate funcţiile referitoare la securitate.
***SERVICE**	Folosirea uneltelor de service este înregistrată în istoric.
***SPLFDTA**	Acţiunile efectuate pe fişierele spool sunt înregistrate în istoric.
***SYSMGT**	Folosirea funcţiilor de gestionare sisteme este înregistrată în istoric.

"Planificarea auditării acţiunilor" la pagina 228 furnizează informaţii despre cum se folosesc valorile de sistem şi acţiunile de auditare pentru utilizatori ca să vă indepliniţi nevoile de auditare securitate.

Informaţiile suplimentare asociate cu un profil de utilizator

Secţiunile anterioare descriu câmpurile pe care le specificaţi atunci când creaţi sau modificaţi profiluri de utilizator. Şi alte informaţii sunt asociate cu un profil de utilizator din sistem şi sunt salvate cu el:

- Autorizări private
- Informaţii obiect deţinut
- Informaţii obiect grup primar

Cantitatea acestor informaţii afectează timpul necesar pentru slavarea şi restaurarea profilurilor şi pentru construirea ecranelor de autorizare. “Modul în care sunt stocate informaţiile de securitate” la pagina 214 furnizează detalii suplimentare despre cum profilurile de utilizator sunt memorate şi salvate.

Autorizările private

Toate autorizările private ale unui utilizator pentru obiecte sunt memorate cu profilul de utilizator. Când un utilizator are nevoie de autorizare pentru un obiect, pot fi căutate autorizările private ale utilizatorului. “Organigrama 3: Cum este verificată autorizarea utilizatorului asupra unui obiect” la pagina 146 furnizează detalii suplimentare despre verificarea autorizării.

Puteţi afişa o autorizare privată a utilizatorului folosind comanda Afişare profil utilizator: DSPUSRPRF *nume profil utilizator* TYPE(*OBJAUT). Pentru modificarea autorizărilor private ale unui utilizator, puteţi folosi comenzile care lucrează cu autorizări de obiecte, cum ar fi Editare autorizare obiect (EDTOBJAUT).

Puteţi copia toate autorizările private de la un profil de utilizator la altul folosind comanda Acordare autorizare utilizator (GRTUSRAUT). Consultaţi “Copierea autorizării de la un utilizator” la pagina 139 pentru informaţii suplimentare.

Autorizările de grup primar

Numele tuturor obiectelor pentru care profilul este grup primar sunt memorate cu profilul de utilizator. Puteţi afişa obiectele pentru care profilul este grup primar folosind comanda DSPUSRPRF: DSPUSRPRF *nume profil grup* TYPE(*OBJPGP). De asemenea puteţi folosi şi comanda Gestionare obiecte după grup primar (WRKOBJPGP).

Informaţiile privind obiectul deţinut

Informaţiile de autorizare privată pentru un obiect sunt memorate cu profilul utilizator care deţine acel obiect. Aceste informaţii sunt folosite la construcţia ecranelor de sistem care gestionează autorizările pentru obiecte. Dacă un profil deţine un număr mare de obiecte care au multe autorizări private, performanţa construirii ecranelor de autorizare pentru obiecte pentru aceste obiecte poate fi afectată. Mărimea unui profil proprietar afectează performanţa când se afişează şi se lucrează cu autorizări la obiectele deţinute şi când se salvează sau se restaurează profiluri. De asemenea, pot fi afectate operaţiile de sistem. Pentru a preveni afectarea fie a performanţei, fie a operaţiilor de sistem, distribuiţi dreptul de proprietate a obiectelor la mai multe profiluri. Deoarece mărimea unui profil de utilizator vă poate influenţa performanţa, se recomandă să nu alocaţi toate obiectele (sau aproape toate) unui singur profil proprietar.

Autentificarea prin ID digital

Infrastructura de securitate iSeries vă permite folosirea pentru identificare a certificatelor digitale x.509. Certificatele digitale permit utilizatorilor să securizeze comunicaţiile şi să menţină integritatea mesajelor.

API-urile pentru ID digital creează, distribuie şi gestionează certificate digitale asociate cu profiluri utilizator. Consultaţi subiectul API din Centrul de informare (consultaţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi) pentru informaţii despre următoarele API-uri:

- Adăugare certificat utilizator (QSYADDUC)
- Înlăturare certificat utilizator (QSYRMVUC)
- Listare certificat utilizator (QSYLSTUC)
- Găsire certificat utilizator (QSYFNDUC)

- Adăugare listă de validare certificat (QSYADDVC)
- Înlăturare listă de validare certificat (QSYRMVVC)
- Listare listă de validare certificat (QSYLSTVC)
- Verificare listă de validare certificat (QSYCHKVC)
- Analizare certificat (QSYPARSC)

Gestionarea profilurilor de utilizator

Această parte a capitolului descrie comenzile şi ecranele pe care le folosiţi ca să creaţi, modificaţi şi ştergeţi profiluri de utilizator. Nu sunt descrise toate câmpurile, opţiunile şi tastele funcţionale. Folosiţi informaţiile online pentru detalii.

Trebuie să aveţi autorizarea specială *SECADM ca să creaţi, modificaţi sau ştergeţi profiluri de utilizator.

Crearea profilurilor de utilizator

Puteţi crea profiluri utilizator în mai multe căi:

- Folosind ecranul Gestionare profiluri utilizator (WRKUSRPRF).
- Folosind comanda Creare profil utilitator (CRTUSRPRF).
- Folosind opţiunea Gestionare înrolare utilizator din meniul Setare.
- Folosind ecranul Navigator iSeries de la folderul iSeries Access.

Utilizatorul care creează profilul utilizator îl deţine şi primeşte pentru el autorizarea *ALL. Profilului de utilizator îi este dată autorizarea *OBJMGT şi *CHANGE pentru el însuşi. Aceste autorizări sunt necesare pentru operaţii normale şi nu trebuie înlăturate.

Un profil de utilizator nu poate fi creat cu mai multe autorizări sau capabilităţi decât acelea ale utilizatorului care creează profilul.

Notă: Când executaţi o comandă CRTUSRPRF, nu puteţi crea un profil de utilizator (*USRPRF) într-un pool de discuri independent. Însă când un utilizator este autorizat în particular asupra unui obiect din pool-ul de discuri independent, când este proprietarul unui obiect dintr-un pool de discuri independent sau când este grupul primar al unui obiect dintr-un pool de discuri independent, numele profilului este memorat în pool-ul de discuri independent. Dacă pool-ul de discuri independent este mutat în alt sistem, autorizarea particulară, dreptul de proprietate asupra obiectului şi intrările de grup primar vor fi ataşate la profilul cu acelaşi nume din sistemul destinaţie. Dacă nu există un profil în sistemul destinaţie, este creat. Utilizatorul nu va avea nici o autorizare specială şi parola va fi setată la *NONE.

Folosirea comenzii Gestionare profiluri utilizator

În comanda WRKUSRPRF puteţi introduce un nume de profil specific, un set de profiluri generice sau *ALL. Nivelul de ajutorare determină ce listă de afişare vedeţi. Când folosiţi comanda WRKUSRPRF cu nivelul de ajutorare *BASIC, veţi accesa ecranul Gestionare înrolare utilizator. Dacă este specificat nivelul de ajutorare *INTERMED, veţi accesa ecranul Gestionare profiluri utilizator.

Puteţi specifica parametrul ASTLVL (nivel de ajutorare) în comandă. Dacă nu specificaţi ASTLVL, sistemul va folosi nivelul de ajutorare memorat cu profilul dumneavoastră de utilizator.

În ecranul Gestionare profiluri utilizator, tastaţi 1 şi numele profilului pe care doriţi să-l creaţi:

```
                          Work with User Profiles

Type options, press Enter.
  1=Create   2=Change   3=Copy   4=Delete   5=Display
  12=Work with objects by owner

     User
Opt  Profile     Text
1   NEWUSER
__   DPTSM       Sales and Marketing Departme
__   DPTWH       Warehouse Department
```

Puteţi vizualiza ecranul Creare profil utilizator:

```
                       Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . . .   NEWUSER
User password  . . . . . .   NEWUSER1
Set password to expired  . . . .   *YES
Status . . . . . .   *ENABLED
User class . . . . . .   *USER
Assistance level . . . . . .   *SYSVAL
Current library  . . . . . .   *CRTDFT
Initial program to call  . . . .   *NONE
Library  . . . . . .
Initial menu . . . . . .   MAIN
Library  . . . . . .     QSYS
Limit capabilities . . . . . .   *NO
Text 'description' . . . . . .
```

Ecranul Creare profil utilizator afişează toate câmpurile din profilul utilizator. Folosiţi tastele F10 (Parametri suplimentari) şi Page Down ca să introduceţi informaţii suplimentare. Folosiţi F11 (Afişare cuvinte cheie) ca să vizualizaţi numele parametrilor.

Ecranul Creare profil utilizator nu adaugă utilizatorul la directorul de sistem.

Folosirea comenzii Creare profil utilizator

Puteţi folosi comanda CRTUSRPRF ca să creaţi un profil de utilizator. Puteţi introduce parametrii prin comandă sau puteţi cere promptarea (F4) şi consulta ecranul Creare profil utilizator.

Folosirea opţiunii Gestionare înrolare utilizator

Selectaţi opţiunea Gestionare înrolare utilizator din meniul SETUP. Nivelul de ajutorare memorat cu profilul dumneavoastră determină dacă veţi vedea ecranul Gestionare profiluri utilizator sau ecranul Gestionare înrolare utilizator. Puteţi folosi F21 (Selectare nivel de ajutorare) ca să modificaţi nivelurile.

În ecranul Gestionare înrolare utilizator, folosiţi opţiunea 1 (Adăugare) ca să adăugaţi un utilizator nou pe sistem.

```
                        Work with User Enrollment

Type options below, then press Enter.
1=Add   2=Change   3=Copy   4=Remove   5=Display

Opt     User           Description
1       NEWUSER
_       DPTSM          Sales and Marketing Departme
_       DPTWH          Warehouse Department
```

Apare ecranul Adăugare utilizator:

```
                                Add User

Type choices below, then press Enter.

User  . . . . . .   NEWUSER
User description  . . . .
Password  . . . . . .   NEWUSER
Type of user  . . . . . .   *USER
User group  . . . . . .   *NONE

Restrict command line use   N
Uses OfficeVision/400 . .   Y

Default library . . . . .
Default printer . . . . .   *WRKSTN
Sign on program . . . . .   *NONE
Library . . . . . .

First menu  . . . . . .
Library . . . . . .

F1=Help   F3=Exit   F5=Refresh   F12=Cancel
```

Ecranul Adăugare utilizator este proiectat pentru un administrator de securitate fără experienţă tehnică. Nu afişează toate câmpurile din profilul de utilizator. Sunt folosite valorile implicite pentru toate câmpurile care nu sunt afişate.

Notă: Dacă folosiţi ecranul Adăugare utilizator, aveţi limitat numele de profil utilizator la 8 caractere.

Apăsaţi Page down ca să vedeţi al doilea ecran:

```
                                Add User

Type choices below, then press Enter.

Attention key program . .   *SYSVAL
Library . . . . . .

Option 50 on OfficeVision/400 menu:
Text for menu option      Operational Assistant Menu
User program  . . . . .   QEZAST
Library . . . . . .         QSYS
```

Ecranul Adăugare utilizator adaugă în mod automat o intrare în directorul de sistem cu acelaşi ID utilizator ca şi numele de profil utilizator (primele opt caractere) şi o adresă a numelui sistem.

Meniul principal include şi Opţiunile de utilizator 51—59. Aceste opţiuni adiţionale (Opţiunile 51--59) sunt procesate similar la Opţiunea 50, exceptând valorile implicite pentru următoarele câmpuri necompletate:

- Text pentru opţiuni de meniu
- Program utilizator
- Bibliotecă

Copierea profilurilor de utilizator

Pteţi crea un profil de utilizator copiind alt profil de utilizator sau profil de grup. Aţi putea dori să setaţi un profil dintr-un grup ca model. Copiaţi primul profil din grup pentru a crea profiluri adiţionale.

Puteţi copia un profil în mod interactiv din ecranul Gestionare înrolare utilizator sau Gestionare profiluri utilizator. Nici o comandă nu există pentru a copia un profil de utilizator.

Copierea dintr-un ecran Gestionare profiluri utilizator

În ecranul Gestionare profiluri utilizator, tastaţi 3 în faţa profilului pe care doriţi să îl copiaţi. Apare ecranul Creare profil utilizator:

```
                      Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . . .                Name
User password  . . . . . > *USRPRF      Name
Set password to expired  . . . . > *NO  *NO, *YES
Status . . . . . > *ENABLED     *ENABLED,
User class . . . . . > *USER    *USER,
Assistance level . . . . . > *SYSVAL    *SYSVAL,
Current library  . . . . . > DPTWH      Name,
Initial program to call  . . . . > *NONE    Name,
Library    . . . . . .                  Name,
Initial menu . . . . . > ICMAIN     Name,
Library    . . . . . > ICPGMLIB     Name,
Limit capabilities . . . . . > *NO      *NO,
Text 'description' . . . . . > 'Warehouse Department'
```

Toate valorile din profilul de utilizator de copiere sunt arătate în ecranul Creare profil utilizator, cu excepţia acestor câmpuri:

Director de bază
*USRPRF

Atribute de job locale
Atribute de job locale

Locale Locale

Profil utilizator
Spaţiu liber. Trebuie completat.

Parolă *USRPRF

Coadă de mesaje
*USRPRF

Parolă document
*NONE

Număr identificare utilizator
*GEN

Număr identificare grup
*NONE

Asociere EIM
*NOCHG

Autorizare
*EXCLUDE

6Puteţi modifica orice câmpuri în ecranul Creare profil utilizator. Autorizările private ale profilului de copiere nu sunt copiate. În plus, obiectele interne care conţin preferinţe de utilizator şi alte informaţii despre utilizator nu vor fi copiate.

Copierea dintr-un ecran Gestionare înrolare utilizator

În ecranul Gestionare înrolare utilizator, tastaţi 3 în faţa profilului pe care doriţi să îl copiaţi. Apare ecranul Copiere utilizator:

```
                                Copy User

Copy from user  . . . . :   DPTWH

Type choices below, then press Enter.

User  . . . . . . . . . .
User description  . . . .   Warehouse Department
Password  . . . . . . . .
Type of user  . . . . . .   USER
User group  . . . . . . .

Restrict command line use   N
Uses OfficeVision/400 . .   Y

Default library . . . . .   DPTWH
Default printer . . . . .   PRT04
Sign on program . . . . .   *NONE
  Library . . . . . . . .
```

Toate valorile din profilul de copiere apar în ecranul Adăugare utilizator, cu excepţia următoarelor:

Utilizator
Spaţiu liber. Trebuie completat. Limitat la 8 caractere.

Parolă Spaţiu liber. Dacă nu introduceţi o valoare, profilul este creat cu parola egală cu valoarea implicită specificată pentru parametrul PASSWORD al comenzii CRTUSRPRF.

Puteţi modifica orice câmpuri din ecranul Copiere utilizator. Câmpurile profil utilizator care nu apar în versiunea nivelul de asistenţă de bază sunt copiate din profilul de copiere, cu următoarele excepţii:

Coadă de mesaje
*USRPRF

Parolă document
*NONE

Număr identificare utilizator
*GEN

Număr identificare grup
*NONE

Asociere EIM
*NOCHG

Autorizare
*EXCLUDE

Autorizările private ale profilului de copiere nu sunt copiate.

Copierea autorizărilor private

Puteţi copia autorizările private de la un profil utilizator la altul folosind comanda Acordare autorizare utilizator (GRTUSRAUT). Această posibilitate poate fi de folos în unele situaţii, dar nu ar trebui folosită în locul profilurilor de grup sau a listelor de autorizare. Copierea autorizărilor nu ajută la gestionarea autorizărilor similare în viitor şi poate cauza probleme de performanţă în sistem.

Subiectul “Copierea autorizării de la un utilizator” la pagina 139 are informaţii suplimentare despre folosirea acestei comenzi.

Modificarea profilurilor de utilizator

Puteţi modifica un profil utilizator folosind opţiunea 2 (Modificare) din ecranul Gestionare înrolare utilizator sau Gestionare profiluri utilizator. Puteţi folosi şi comanda Modificare profil utilizator (CHGUSRPRF).

Utilizatorilor cărora li se permite să introducă comenzi pot modifica unii parametri al propriului profil folosind comanda Modificare profil (CHGPRF).

Un utilizator nu poate modifica un profil de utilizator pentru a avea mai multe autorizări speciale sau capabilităţi decât utilizatorul care modifică profilurile.

Ştergerea profilurilor de utilizator

Nu puteţi şterge un profil de utilizator care deţine obiecte. Trebuie să ştergeţi orice obiecte deţinute de profil sau să transferaţi dreptul de proprietate asupra acelor obiecte la alt profil. Nivelul de asistenţă de bază şi Nivelul de asistenţă intermediar vă permit să manipulaţi obiectele deţinute când ştergeţi un profil.

Nu puteţi şterge un profil de utilizator dacă este grupul primar pentru vreun obiect. Când folosiţi Nivelul de asistenţă intermediar pentru a şterge un profil utilizator, puteţi modifica sau înlătura grupul primar pentru obiecte. Puteţi folosi comanda DSPUSRPRF cu opţiunea *OBJPGP (grup primar obiect) pentru a lista orice obiecte pentru care un profil este grupul primar.

Când ştergeţi un profil utilizator, utilizatorul este înlăturat din toate listele de distribuire şi din directorul sistem.

Trebuie să modificaţi dreptul de proprietate sau să ştergeţi coada de mesaje a utilizatorului. Sistemul şterge automat coada de mesaje când profilul este şters.

Nu puteţi şterge un profil grup care are membri. Pentru a lista membrii unui profil de grup, tastaţi DSPUSRPRF *nume-profil-grup* *GRPMBR . Modificaţi câmpul GRPPRF în fiecare profil membru înainte de a şterge profilul de grup.

Folosirea comenzii Ştergere profil utilizator

Puteţi introduce direct comanda Ştergere profil utilizator (DLTUSRPRF) sau puteţi folosi opţiunea 4 (Ştergere) din ecranul Gestionare profiluri utilizator. Comanda DLTUSRPRF are parametri care vă permit să trataţi:

- Toate obiectele deţinute de profil
- Toate obiectele pentru care profilul este grupul primar
- Asocieri EIM

```
                      Delete User Profile (DLTUSRPRF)

Type choices, press Enter.

User profile . . . . . > HOGANR        Name
Owned object option:
  Owned object value . . . . . .   *CHGOWN       *NODLT, *DLT, *CHGOWN
  User profile name if *CHGOWN     WILLISR       Name
Primary group option:
  Primary group value  . . . . .   *NOCHG        *NOCHG, *PGP
  New primary group  . . . . . .
  New primary group authority  .
```

Puteţi şterge toate obiectele deţinute sau le puteţi transfera unui nou utilizator. Dacă doriţi să manipulaţi individual obiectele deţinute, puteţi folosi comanda Gestionare obiecte după proprietar (WRKOBJOWN). Puteţi modifica grupul primar pentru toate obiectele pentru care profilul este grupul primar. Dacă doriţi să manipulaţi individual obiectele, puteţi folosi comanda Gestionare obiecte după proprietar (WRKOBJOWN). Ecranele pentru ambele comenzi sunt similare:

```
                        Work with Objects by Owner

User profile . . . . . :   HOGANR

Type options, press Enter.
  2=Edit authority        4=Delete   5=Display author
  8=Display description   9=Change owner
                                                          ASP
Opt  Object        Library       Type      Attribute      Device
 4   HOGANR        QUSRSYS       *MSGQ                    *SYSBAS
 9   QUERY1        DPTWH         *PGM                     *SYSBAS
 9   QUERY2        DPTWH         *PGM                     *SYSBAS
```

Folosirea opţiunii Înlăturare utilizator

Din ecranul Gestionare înrolare utilizator, tastaţi 4 (Înlăturare) în faţa profilului pe care doriţi să îl ştergeţi. Vedeţi ecranul Înlăturare utilizator:

```
                              Remove User

User . . . . . :   HOGANR
User description . . . . . :   Sales and Marketing Department


To remove this user type a choice below, then press Enter.

     1. Give all objects owned by this user to a new owner
     2. Delete or change owner of specific objects owned by this user.
```

Pentru a modifica dreptul de proprietate al tuturor obiectelor înainte de a şterge profilul, selectaţi opţiunea 1. Apare un ecran care vă cere noul utilizator.

Pentru a manipula obiecte individuale, selectaţi opţiunea 2. Vedeţi un ecran detaliat Înlăturare utilizator:

```
                              Remove User

User . . . . . :   HOGANR
User description . . . . . :   Hogan, Richard - Warehouse DPT

New owner  . . . . . .                    Name, F4 for list

To remove this user, delete or change owner of all objects.
Type options below and press Enter.
  2=Change to new owner   4=Delete   5=Display details


Opt  Object        Library       Description
 4   HOGANR        QUSRSYS       HOGANR message queue
 2   QUERY1        DPTWH         Inventory Query, on-hand report
 2   QUERY2        DPTWH         Inventory Query, on-order report
```

Folosiţi opţiunile din ecran pentru a şterge obiectele sau a le transfera la un nou proprietar. Când toate obiectele au fost înlăturate din ecran, puteţi şterge profilul.

Note:

1. Puteţi folosi F13 pentru a şterge toate obiectele deţinute de profilul utilizator.
2. Fişierele spool nu apar în ecranul Gestionare obiecte după proprietar. Puteţi şterge un profil utilizator chiar dacă acel profil încă deţine fişiere spool. După ce aţi şters un profil de utilizator, folosiţi comanda Gestionare fişiere spool (WRKSPLF) pentru a localiza şi şterge orice fişier spool deţinut de profilul de utilizator, dacă nu mai este necesar.
3. Obiectele pentru care profilul de utilizator şters a fost grupul primar vor avea un grup primar *NONE.

Gestionarea obiectelor după grup primar

Puteţi folosi comanda Gestionare obiecte după grup primar (WRKOBJPGP) pentru a lista şi gestiona orice obiecte pentru care un profil este grupul primar. Puteţi folosi acest ecran pentru a înlocui grupul primar al unui obiect cu alt profil sau pentru a-i seta grupul primar la *NONE.

```
                    Work with Objects by Primary Group

Primary group  . . . . . :   DPTAR

Type options, press Enter.
  2=Edit authority        4=Delete   5=Display authority
  8=Display description   9=Change primary group
                                                 ASP
Opt    Object     Library    Type   Attribute    Device
       CUSTMAST   CUSTLIB    *FILE              *SYSBAS
       CUSTWRK    CUSTLIB    *FILE              *SYSBAS
       CUSTLIB    QSYS       *LIB               *SYSBAS
```

Activarea unui profil de utilizator

Dacă valorile de sistem QMAXSIGN şi QMAXSGNACN sunt setate să dezactiveze un profil de utilizator după prea multe încercări de semnare, aţi putea dori ca o persoană, cum ar fi operatorul de sistem, să activeze profilul modificând starea în *ENABLE. Totuşi, pentru a activa un profil utilizator, trebuie să aveţi autorizare specială *SECADM şi autorizare *OBJMGT şi *USE la profil pentru profilul utilizator. În mod normal, un operator de sistem nu are autorizare specială *SECADM.

O soluţie este de a folosi un program simplu care adoptă autorizare:

1. Creaţi un program CL deţinut de un utilizator care are autorizare specială *SECADM şi autorizare *OBJMGT şi *USE la profilurile utilizator din sistem. Adoptaţi autorizarea proprietarului când programul este creat specificând USRPRF(*OWNER).
2. Folosiţi comanda EDTOBJAUT pentru a face autorizare publică la programul *EXCLUDE şi daţi operatorilor de sistem autorizarea *USE.
3. Operatorul activează profilul introducând:

   ```
   CALL ENABLEPGM nume-profil
   ```

4. Partea principală a programului ENABLEPGM arată astfel:

   ```
   PGM &PROFILE
   DCL VAR(&PROFILE) TYPE(*CHAR) LEN(10)
   CHGUSRPRF USRPRF(&PROFILE) STATUS(*ENABLED)
   ENDPGM
   ```

Listarea profilurilor de utilizator

Puteţi afişa şi tipări informaţii despre profiluri utilizator într-o varietate de formate.

Afişarea unui profil individual

Pentru a afişa valori pentru un profil utilizator individual, folosiţi opţiunea 5 (Afişare) din ecranul Gestionare înrolare utilizator sau Gestionare profiluri utilizator. Sau, puteţi folosi comanda Afişare profil utilizator (DSPUSRPRF).

Listarea tuturor profilurilor

Folosiţi comanda Afişare utilizatori autorizaţi (DSPAUTUSR) pentru a tipări sau a afişa toate profilurile utilizator din sistem. Parametrul de secvenţă (SEQ) din comandă vă permite să sortaţi lista după numele de profil sau după profilul de grup.

```
                          Display Authorized Users

                      Password
Group       User      Last         No
Profile     Profile   Changed   Password  Text
DPTSM
            ANDERSR   08/04/0x            Anders, Roger
            VINCENT   09/15/0x            Vincent, Mark
DPTWH
            ANDERSR   08/04/0x            Anders, Roger
            HOGANR    09/06/0x            Hogan, Richard
            QUINN     09/06/0x            Quinn, Rose
QSECOFR
            JONESS    09/20/0x            Jones, Sharon
            HARRISON  08/29/0x            Harrison, Ken
*NO GROUP
            DPTSM     09/05/0x     X      Sales and Marketing
            DPTWH     09/18/0x     X      Warehouse
```

Apăsând F11, puteţi vedea care profiluri utilizator au parole definite pentru folosire la diferite niveluri de parolă.

```
                    Display Authorized Users

                  Password  Password   Password   Password
User      Group     Last      for level  for level     for
Profile   Profile   Changed    0 or 1     2 or 3    NetServer
ANGELA              04/21/0x    *YES       *NO        *YES
ARTHUR              07/07/0x    *YES       *YES       *YES
CAROL1              05/15/0x    *YES       *YES       *YES
CAROL2              05/15/0x    *NO        *NO        *NO
CHUCKE              05/18/0x    *YES       *NO        *YES
DENNISS             04/20/0x    *YES       *NO        *YES
DPORTER             03/30/0x    *YES       *NO        *YES
GARRY               08/04/0x    *YES       *YES       *YES
JANNY               03/16/0x    *YES       *NO        *YES
```

Tipuri de ecrane pentru profil de utilizator

Comanda Afişare profil utilizator (DSPUSRPRF) oferă câteva tipuri de listări şi ecrane:

- Unele ecrane şi listări sunt disponibile doar pentru profiluri individuale. Altele pot fi tipărite pentru toate profilurile sau un set generic de profiluri. Consultaţi informaţii online pentru detalii despre tipurile disponibile.
- Puteţi crea un fişier de ieşire din câteva ecrane specificând ieşire(*OUTFILE). Folosiţi o unealtă de interogare sau un program pentru a produce rapoarte personalizate din fişierul de ieşire. Subiectul “Analizarea profilurilor de utilizator” la pagina 258 dă sugestii pentru rapoarte.

Tipuri de rapoarte pentru profil de utilizator

Următoarele comenzi furnizează rapoarte profil utilizator.

- Tipărire profil utilizator (PRTUSRPRF)

  Această comandă vă permite să tipăriţi un raport care conţine informaţii pentru profilurile utilizator din sistem. Pot fi tipărite patru rapoarte diferite. Unul conţine informaţii de tip autorizare, unul conţine informaţii de tip mediu, unul informaţii de tip parolă şi unul informaţii de tip nivel parolă.
- Analizare parolă implicită (ANZDFTPWD)

  Această comandă vă permite să tipăriţi un raport al tuturor profilurilor utilizator din sistem care au o parolă implicită şi să efectuaţi o acţiune împotriva profilurilor. Un profil are o parolă implicită când numele profil utilizator se potriveşte parolei profilului.

  Profilurile utilizator din sistem care au parolă implicită pot fi dezactivate şi parolele lor pot fi setate să expire.

Redenumirea unui profil de utilizator

Sistemul nu oferă o metodă directă pentru redenumirea unui profil utilizator.

Un profil nou poate fi creat cu aceleaşi autorizări pentru un utilizator cu nume nou. Unele informaţii, totuşi, nu pot fi transferate la noul profil. Următoarele sunt exemple de informaţii care nu pot fi transferate:

- Fişiere spool.
- obiecte interne care conţin preferinţe utilizator şi alte informaţii despre utilizator vor fi pierdute.
- Certicatele digitale care conţin numele utilizator nu vor fi validate.
- Informaţiile uid şi gid reţinute de sistemul de fişiere integrat nu pot fi modificate.
- Nu veţi putea să modificaţi informaţiile care sunt memorate de aplicaţii şi care conţin numele utilizator.

Aplicaţiile care sunt rulate de utilizator pot avea ″profiluri de aplicaţie″. Crearea unui profil utilizator iSeries nou pentru redenumirea unui utilizator nu duce la redenumirea oricărui profil de aplicaţie pe care utilizatorul il poate avea. Un profil Lotus Notes este un exemplu de profil de aplicaţie.

Următorul exemplu arată cum se creează un profil nou pentru un utilizator cu un nume nou şi aceleaşi autorizări. Vechiul nume de profil este SMITHM. Noul nume de profil este JONESM:

1. Copiaţi vechiul profil (SMITHM) la un nou profil (JONESM) folosind opţiunea de copiere de la ecranul Gestionare înrolare utilizator.
2. Acordaţi lui JONESM toate autorizările private ale lui SMITHM folosind comanda Acordare autorizare utilizator (GRTUSRAUT):

   ```
   GRTUSRAUT JONESM REFUSER(SMITHM)
   ```

3. Modificaţi grupul primar a tuturor obiectelor la care SMITHM este grup primar prin folosirea comenzii Gestionare obiecte după grup primar (WRKOBJPGP):

   ```
   WRKOBJPGP PGP(SMITHM)
   ```

   Introduceţi opţiunea 9 pe toate obiectele care au nevoie de modificarea grupului primar şi introdceţi din linia de comandă NEWPGP (JONESM).

   Notă: JONESM trebuie să aibă un gid alocat folosind parametrul GID din comanda Creare sau modificare profil utilizator (CRTUSRPRF sau CHGUSRPRF).
4. Afişaţi profilul utilizator SMITHM folosind comanda Afişare profil utilizator (DSPUSRPRF):

   ```
   DSPUSRPRF USRPRF(SMITHM)
   ```

   Scrieţi uid şi gid pentru SMITHM.
5. Transferaţi dreptul de proprietate all altor obiecte deţinute la JONESM şi înlăturaţi profilul utilizator SMITHM, folosind opţiunea 4 (Înlăturare) de la ecranul Gestionare înrolare utilizator.
6. Modificaţi uid şi gid al JONESM la uid şi gid care aparţine lui SMITHM prin folosirea comenzii Modificare profil utilizator (CHGUSRPRF):

   ```
   CHGUSRPRF USRPRF(JONESM) UID(uid de la SMITHM)
             GID(gid de la SMITHM)
   ```

   Dacă JONESM deţine obiecte într-un director, comanda CHGUSRPRF nu poate fi folosită la modificarea uid şi gid. Folosiţi API QSYCHGID pentru modificarea uid şi gid a prfilului utilizator JONESM.

Gestionarea auditării utilizatorilor

Folosiţi comanda Modificare auditare utilizator (CHGUSRAUD) ca să setaţi caracteristicile de auditare pentru utilizatori. Ca să folosiţi această comandă, trebuie să aveţi autorizare *AUDIT.

```
          Change User Audit (CHGUSRAUD)

Type choices, press Enter.

User profile . . . . . .   HOGANR
                           JONESS
Object auditing value  . . . . .   *SAME
User action auditing . . . . . .   *CMD
                           *SERVICE
```

Puteţi specifica simultan caracteristicile de auditare pentru mai mulţi utilizatori prin listarea numelor de profil de utilizator.

Parametrul AUDLVL (acţiune de auditare utilizator) poate avea mai multe valori. Valoarea pe care o specificaţi în această comandă înlocuieşte valoarea curentă AUDLVL pentru utilizatori. Valorile pe care le specificaţi nu sunt adăugate la valorile curente AUDLVL pentru utilizatori.

Puteţi folosi comanda Afişare profil utilizator (DSPUSRPRF) ca să vedeţi caracteristicile de auditare pentru un utilizator.

Gestionarea profilurilor în programele CL

Veţi dori să extrageţi informaţii despre profilul utilizator de la un program CL. Puteţi folosi comanda Extragere profil utilizator (RTVUSRPRF) în programul dumneavoastră CL. Comanda întoarce atributele cerute ale profilului la variabilele pe care le-aţi asociat cu numele de câmp profil utilizator. Descrierea câmpurilor profil utilizator din acest capitol arată lungimea câmpurilor aşteptată de comanda RTVUSRPRF. În unele cazuri, un câmp zecimal poate să aibă o valoare care nu este numerică. De exemplu, câmpul spaţiu de stocare maxim (MAXSTG) este definit ca şi un câmp zecimal, dar poate avea o valoare de *NOMAX. Informaţiile online pentru comanda RVTUSRPRF descriu valorile care sunt întoarse într-un câmp zecimal pentru valorile care nu sunt numerice.

Programul eşantion din “Folosirea unui program de aprobare a parolei” la pagina 45 arată un exemplu de utilizare a comenzii RTVUSRPRF.

Puteţi de asemenea folosi comanda CRTUSRPRF sau CHGUSRPRF într-un program CL. Dacă folosiţi variabile pentru parametrii acestor comenzi, definiţi variabilele ca şi câmpuri de caracter ca să le potriviţi cu ecranul prompt Creare profil utilizator. Mărimea variabilei nu trebuie să se potrivească cu mărimea câmpului.

Nu puteţi extrage o parolă de utilizator, deoarece parola este memorată cu criptare într-un singur sens. Dacă doriţi ca utilizatorul să introducă parola din nou înainte să acceseze informaţii critice, puteţi folosi comanda Verificare parolă Check Password (CHKPWD) din programul dumneavoastră. Sistemul compară parola introdusă cu parola utilizatorului şi trimite un mesaj de scăpare la programul dumneavoastră dacă parola nu este corectă.

Punctele de ieşire pentru profil de utilizator

Punctele de ieşire sunt furnizate pentru crearea, modificarea, ştergerea sau restaurarea profilurilor de utilizator. Puteţi să vă scrieţi propriile programe de ieşire ca să realizeze funcţii specifice pentru profilul de utilizator. Când vă înregistraţi programele de ieşire cu puncte de ieşire pentru profil de utilizator, sunteţi anunţat când un utilizator este creat, modificat, şters sau restaurat. În timpul notificării, programul dumneavoastră de ieşire poate realiza oricare dintre următoarele:

- Extragerea informaţiilor despre profilul de utilizator
- Înscrierea profilului de utilizator creat în directorul de sistem.
- Crearea obiectelor necesare pentru profilul de utilizator.

Notă: Toate autorizările adoptate vor fi suprimate înaintea programelor de ieşire care sunt apelate. Aceasta înseamnă că programul de ieşire nu are autorizare de accesare obiect profil utilizator.

Pentru informaţii despre securitatea programelor de ieşire, consultaţi subiectul API din Centrul de informare (consultaţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii).

Profiluri utilizator livrate de IBM

Un număr de profiluri utilizator este livrat cu software-ul dumneavoastră de sistem. Aceste profiluri utilizator furnizate de IBM sunt folosite ca şi obiecte deţinute pentru funcţii de sistem variate. Unele funcţii de sistem rulează şi sub profiluri utilizator livrate de IBM specifice.

Profilurile de utilizator livrate de IBM, cu excepţia QSECOFR, sunt furnizate cu parola *NONE şi nu sunt destinate semnării. Pentru a vă permite să instalaţi sistemul pentru prima dată, parola pentru profilul responsabil cu securitatea (QSECOFR) este aceeaşi pentru fiecare sistem livrat. Însă parola pentru QSECOFR este livrată ca expirată. În cazul sistemelor sistemele noi, vi se va cere să modificaţi parola prima dată când semnaţi cu QSECOFR.

Când instalaţi o nouă ediţie de sistem de operare, parolele pentru profilurile livrate de IBM nu sunt modificate. Dacă profiluri cum ar fi QPGMR şi QSYSOPR au parole, aceste parole nu se vor seta în mod automat la *NONE.

Anexa B, “Profilurile de utilizator furnizate de IBM”, la pagina 271 conţine o listă completă a tuturor profilurilor utilizator livrate de IBM şi valorile de câmp pentru fiecare profil.

Notă: Profilurile livrate de IBM sunt furnizate, dar sunt folosite de IBM i5/OS. Pri urmare, semnarea cu aceste profiluri sau folosirea profilurilor care deţin obiecte utilizator (nelivrate de IBM) **nu** este recomandată.

Modificarea parolelor pentru profilurile de utilizator livrate de IBM

Dacă doriţi să semnaţi cu unul dintre profilurile furnizate de IBM, puteţi modifica parola folosind comanda CHGUSRPRF. Puteţi modifica aceste parole şi folosind o opţiune de la meniul SETUP. Pentru a vă proteja sistemul, ar trebui să lăsaţi parola setată la *NONE pentru toate profilurile livrate de IBM cu excepţia QSECOFR. Nu lăsaţi parole triviale pentru profilul QSECOFR.

```
                  Change Passwords for IBM-Supplied

Type new password below for IBM-supplied user,
type password again to verify  change, then
press Enter.

New security officer (QSECOFR) password  . . . . . .
  New password (to verify) . . . . . .

New system operator (QSYSOPR) password . . . . . .
  New password (to verify) . . . . . .

New programmer (QPGMR) password  . . . . . .
  New password (to verify) . . . . . .

New user (QUSER) password  . . . . . .
  New password (to verify) . . . . . .

New service (QSRV) password  . . . . . .
  New password (to verify) . . . . . .
```

Apăsaţi Page down ca să modificaţi parole adiţionale:

```
                  Change Passwords for IBM-Supplied

Type new password below for IBM-supplied user, type
change, then press Enter.

New basic service (QSRVBAS) password . . . . . .
  New password (to verify) . . . . . .
```

Gestionarea ID-urilor de utilizator unelte de service

Sunt mai multe îmbunătăţiri adăugate la uneltele de service pentru această ediţie care le face mai uşor de folosit şi de înţeles.

- **Unelte de service sistem (SST)**

  Acum puteţi gestiona şi crea ID-uri utilizator unelte de service de la unelte de service sistem (SST) prin selectarea opţiunii 8 (Gestionare ID-uri utilizator unelte de service) de la ecranul SST prncipal. Nu mai aveţi nevoie să mergeţi în unelte de service dedicate (DST) ca să resetaţi parole, acordaţi sau revocaţi privilegii, sau creaţi ID-uri utilizator unelte de service. **Notă**: Informaţiile privind Uneltele de service au fost mutate la Centrul de informare.

- **Îmbunătăţiri de gestionare parolă**

  Serverul este livrat cu abilitatea limitată de modificare implicită şi parole expirate. Aceasta înseamnă faptul că nu puteţi modifica ID-urile utilizator unelte de service care au implicite şi parole expirate prin API-ul Modificare ID uilizator unelte de service (QSYCHGDS), nu puteţi modifica parolele lor prin SST. Puteţi modifica numai un ID utilizator unelte de service cu o implicită şi parolă expirată prin DST. Şi puteţi modifica setările de permisiune

implicită şi parole expirate ca să fie modificate. De asemenea, puteţi folosi noul privilegiu Pornire unelte de service (STRSST) ca să creaţi un ID utilizator unelte de service care poate accesa DST, dar poate fi restricţionat de la accesarea SST.

- **Modificări de terminologie**

  Datele textuale alte documentaţii au fost modificate ca să reflecte noua terminologie unelte de service. Specific, termenul ID-uri utilizator unelte de service înlocuieşte termenii anteriori, cum ar fi profiluri utilizator DST, ID-uri utilizator, profiluri utilizator unelte de service, sau variaţii ale acestor nume.

Pentru informaţii despre cum se gestionează uneltele de service, consultaţi subiectul Centrului de informare, Unelte de service (**Securitate—>Unelte de service**). Vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru informaţii suplimentare asupra accesării, Centrul de informare.

Parola de sistem

Parola de sistem este folosită ca să autorizeze modificările modelului de sistem, anumite condiţii de service şi modificări ale dreptului de proprietate. Dacă aceste modificări au survenit pe sistemul dumneavoastră, veţi fi promptat pentru parola de sistem când veţi realiza un IPL.

Capitolul 5. Securitatea resurselor

Securitate resursă defineşte căror utilizatori le este permis să utilizeze obiecte din sistem şi care operaţie le este permis să realizeze pe aceste obiecte.

Acest capitol descrie fiecare din componentele de securitate resursă şi cum lucrează ele împreună pentru a proteja informaţiile din sistemul dvs. Explică de asemenea cum să se utilizeze comanda CL şi afişază organizarea de securitate resursă pe sistemul dvs.

Capitolul 7 discuţii tehnice pentru a proiecta securitatea resursă, inclusiv cum afectează aceasta şi design aplicaţiile şi performanţa sistemului.

Capitolul “Cum verifică sistemul autorizarea” la pagina 142 furnizează diagrame de flux detaliate şi descrie cum sistemul verifică autorizarea. Puteţi găsi util să consultaţi aceste informaţii cum citiţi explicaţiile următoare.

Definirea celor care pot accesa informaţii

Puteţi autoriza utilizatori individuali, grupuri de utilizatori şi publicul.

Notă: În unele medii, o autorizare a nui utilizator se referă la un asemenea **privilegiu**.

Definiţi cum puteţi utiliza un obiect în mai multe modalităţi:

Autorizare publică:

Publicul este format din toţi cei care sunt autorizaţi să semneze pe sistemul dumneavoastră. Autorizarea publică este definită pentru fiecare obiect din sistem, deşi autorizarea publică pentru un obiect poate fi *EXCLUDE. Autorizarea publică la un obiect este utilizată dacă nici o altă autorizare specifică nu este găsită pentru obiect.

Autorizare publică:

Puteţi defini autorizare specifică pentru a utiliza un (sau pentru a nu utiliza) obiect. Puteţi acorda autorizare unui profil utilizator individual sau unui profil de grup. Un obiect are **autorizare privată** dacă orice autorizare, alta decât autorizarea publică, drept de proprietate obiect sau autorizare de grup primar este definită pentru obiect.

Autorizare utilizator:

Unor profiluri utilizator individuale le poate fi acordată autorizare să utilizeze obiece în sistem. Acesta este un tip de autorizare privată.

Autorizare de group:

Unor profiluri de grup le poate fi acordată autorizarea de a utiliza obiecte în sistem. Un membru al grupului primeşte autorizarea de grup doar dacă o autorizare este definită specific pentru acel utilizator. Autorizarea de grup este de asemenea considerată autorizare privată.

Drept de proprietate obiect:

Fiecare obiect din sistem are un proprietar. Proprietarul are autorizare implicită *ALL la toate obiectele. Totuşi, autorizarea proprietarului la obiect poate fi schimbată sau înlăturată. Autorizarea proprietarului la obiect nu este considerată autorizare privată.

Autorizare grup primar:

Puteţi specifica un grup primar pentru un obiect şi autorizarea pe care o are grupul primar la obiect. Autorizarea de grup primar este memorată cu obiectul şi poate furniza performanţe mai bune decât autorizarea privată acordată unui profil de grup. Numai un profil utilizator cu un număr de identificare grup (gid) poate fi grupul primar pentru un obiect. Autorizarea de grup primar nu este considerată autorizare privată.

Definirea modului în care pot fi accesate informaţiile

Autorizare înseamnă tipul de acces permis unui obiect. Operaţii diferite necesită diferite tipuri de autorizare.

Notă: În unele medii, autorizarea asociată cu un obiect este numită **mod de acces** al obiectului.

Autorizarea la un obiect este divizată în trei categorii: 1) **Autorizare obiect** defineşte că operaţiile pot fi realizate la obiect ca un întreg. 2) **Autorizare pentru date** defineşte că operaţiile pot fi realizate în conţinutul obiectului.**Autorizare câmp** defineşte care operaţii pot fi realizate în câmpurile de date.

Tabela 111descrie tipurile de autorizare disponibile şi listează unele exemple despre cum sunt utilizate autorizările. În cele mai multe cazuri, accesarea unui obiect necesită o combinaţie de obiect, date,autorizări câmp. Anexa D furnizează informaţii despre autorizarea necesară pentru a realiza o funcţie specifică.

Tabela 111. Descrier tipuri de autorizare

Autorizare	Nume	Funcţii permise
Autorizări obiect:		
*OBJOPR	Obiect Operaţional	Vedeţi descrierea unui obiect. Folosiţi obiectul aşa cum este determinat de către autorizările de date ale utilizatorului.
*OBJMGT	Management Obiect	Specificaţi securitatea pentru obiect. Mutaţi sau redenumiţi obiectul. Toate funcţiile definite pentru *OBJALTER şi *OBJREF.
*OBJEXIST	Object Existence - Existenţă obiect	Şterge obiect. Eliberează spaţiul ocupat de obiect. Efectuaţi operaţii de salvare şi de restaurare a obiectului [1]. Transfer proprietate asupra obiectului.
*OBJALTER	Object Alter - Modificare obiect	Adăugare, ştergere, iniţializare şi reorganizare membri ai fişierelor bază de date. Modificare şi adăugare atribute ale fişierelor bază de date: adăugare şi ştergere declanşatori. Modificare atribute ale pachetelor SQL.
*OBJREF	Object Reference - Referinţă la obiect	Specificaţi un fişier bază de date ca părinte într-o restricţie referenţiale. De exemplu, vreţi să definiţi o regulă conform căreia trebuie să existe o înregistrare despre client în fişierul CUSMAS înainte să poată fi adăugată o comandă pentru ale client în fişierul CUSORD. Vă trebuie autorizarea *OBJREF pentru fişierul CUSMAS pentru a defini această regulă.
*AUTLMGT	Authorization List Management - Gestiune listă de autorizare	Adăugaţi şi eliminaţi utilizatori şi autorizările lor din lista de autorizare [2].
Autorizări asupra datelor:		
*READ	Read - Citire	Afişarea conţinutului obiectului, precum vizualizarea înregistrărilor dintr-un fişier.
*ADD	Add - Adăugare	Adăugare intrări la un obiect, precum este adăugarea de mesaje la o coadă de mesaje sau adăugarea de înregistrări la un fişier.
*UPD	Update - Actualizare	Modificarea intrărilor dintr-un obiect, precum este modificarea înregistrărilor dintr-un fişier.
*DLT	Delete - Ştergere	Ştergerea intrărilor dintr-un obiect, precum este ştergerea mesajelor dintr-o coadă de mesaje sau ştergerea înregistrărilor dintr-un fişier.
*EXECUTE	Execute - Execuţie	Rularea unui program, unui program de serviciu sau a unui pachet SQL. Localizarea unui obiect într-o bibliotecă sau într-un director.
Autorizări asupra unui câmp:		

Tabela 111. Descrier tipuri de autorizare (continuare)

Autorizare	Nume	Funcţii permise
*Mgt	Management - Gestiune	Specificarea securităţii câmpului.
*Alter	Alter - Modificare	Modificarea atributelor câmpului.
*Ref	Reference - Referinţă	Specificarea câmpului ca parte a cheii părinte într-o restricţie referenţială.
*Read	Read - Citire	Accesarea conţinutului unui câmp. De exemplu, afişarea conţinutului câmpului.
*Add	Add - Adăugare	Adăugarea de intrări la date, precum adăugarea de informaţii la un anumit câmp.
*Update	Update - Actualizare	Modificarea conţinutului unor intrări existente într-un câmp.

1 Dacă un utilizator are autorizarea specială *SAVSYS (save system - salvare sistem), atunci nu este necesară autorizarea de existenţă obiect pentru a efectua operaţii de salvare şi restaurare asupra obiectului.

2 Vedeţi capitolul “Gestionarea listei de autorizare” la pagina 116 pentru mai multe informaţii.

Autorizările folosite în mod obişnuit

Anumite seturi de autorizări asupra datelor şi obiectelor sunt necesare în mod normal pentru a efectua operaţii asupra obiectelor. Puteţi specifica aceste seturi de autorizări definite de sistem (*ALL, *CHANGE, *USE) în loc de a defini în mod individual autorizările necesare pentru un obiect. Autorizarea *EXCLUDE este diferită de lipsa unei autorizări. Autorizarea *EXCLUDE refuză în mod special accesul la obiect. A nu avea nici o autorizare înseamnă că folosiţi autorizarea publică definită pentru obiect. Tabela 112 arată autorizările definite de sistem disponibile la folosirea comenzilor şi ecranelor de autorizare obiect.

Tabela 112. Autorizare definită de sistem

Autorizare	*ALL	*CHANGE	*USE	*EXCLUDE
Autorizări obiect				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
Autorizări de date				
*READ	X	X	X	
*ADD	X	X		
*UPD	X	X		
*DLT	X	X		
*EXECUTE	X	X	X	

Tabela 113 arată autorizări suplimentare definite de sistem care sunt disponibile la folosirea comenzilor WRKAUT şi CHGAUT:

Tabela 113. Autorizare definită de sistem

Autorizare	*RWX	*RW	*RX	*R	*WX	*W	*X
Autorizări obiect							
*OBJOPR	X	X	X	X	X	X	X
*OBJMGT							
*OBJEXIST							
*OBJALTER							
*OBJREF							
Autorizări de date							

Tabela 113. Autorizare definită de sistem (continuare)

Autorizare	*RWX	*RW	*RX	*R	*WX	*W	*X
*READ	X	X	X	X			
*ADD	X	X			X	X	
*UPD	X	X			X	X	
*DLT	X	X			X	X	
*EXECUTE	X		X		X		X

Programul cu licenţă LAN Server foloseşte liste de control al accesului pentru a gestiona autorizările. Autorizările unui utilizator sunt numite **permisii**. Tabela 114 arată cum sunt mapate permisiunile LAN Server către autorizările de obiect şi de date:

Tabela 114. Permisiunile LAN Server

Autorizare	Permisiunile LAN Server
*EXCLUDE	nici una
Autorizări de obiect	
*OBJOPR	Vedeţi nota 1
*OBJMGT	Permisiunea
*OBJEXIST	Creare, Ştergere
*OBJALTER	Atribut
*OBJREF	Fără echivalent
Autorizări de date	
*READ	Read - Citire
*ADD	Create - Creare
*UPD	Write - Scriere
*DLT	Delete - Ştergere
*EXECUTE	Execute - Execuţie

1 Numai dacă nu este specificat NONE pentru un utilizator în lista de control al accesului, utilizatorul primeşte în mod implicit autorizarea *OBJOPR.

Definirea informaţiilor care pot fi accesate

Puteţi defini securitatea de resursă pentru obiecte individuale din sistem. De asemenea puteţi defini securitatea pentru grupuri de obiecte folosind ori securitatea de bibliotecă, ori o listă de autorizare:

Securitatea bibliotecii

Majoritatea obiectelor din sistem se află în biblioteci. Pentru a accesa un obiect, vă trebuie autorizarea atât pentru obiectul însuşi, cât şi pentru biblioteca în care se află obiectul. Pentru majoritatea operaţiilor, inclusiv ştergerea unui obiect, autorizarea *USE pentru biblioteca obiectului este suficientă (în plus faţă de autorizarea necesară pentru obiect). Crearea unui nou obiect necesită autorizarea *ADD pentru biblioteca obiectului. Anexa D arată ce autorizare este necesară pentru comenzile CL pentru obiecte şi pentru bibliotecile de obiecte.

Folosirea securităţii de bibliotecă este o tehnică pentru protejarea informaţiilor păstrând în acelaşi timp o schemă de securitate simplă. De exemplu, pentru a securiza informaţiile confidenţiale pentru un set de aplicaţii, puteţi face următoarele:

- Să folosiţi o bibliotecă pentru a stoca toate fişierele confidenţiale pentru un anumit grup de aplicaţii.
- Să asiguraţi că autorizarea publică este suficientă pentru toate obiectele (din bibliotecă) care sunt folosite de către aplicaţii (*USE sau *CHANGE).
- Să restricţionaţi autorizarea publică doar la biblioteca însăşi (*EXCLUDE).

- Să daţi grupurilor selectate sau indivizilor selectaţi autorizarea pentru bibliotecă (*USE, sau *ADD dacă aplicaţiile o cer).

Deşi securitatea de bibliotecă este o metodă simplă şi eficientă pentru protejarea informaţiilor, ea poate să nu fie adecvată pentru date cu cerinţe de securitate mare. Obiectele foarte sensibile ar trebui să fie securizate individual sau cu o listă de autorizare, în loc de a vă baza pe securitatea bibliotecii.

Securitatea bibliotecii şi listele de biblioteci

Când o bibliotecă este adăugată la lista de biblioteci a utilizatorului, autorizarea pe care o are utilizatorul asupra bibliotecii este stocată împreună cu informaţiile de listă biblioteci. Autorizarea utilizatorului asupra bibliotecii rămâne pentru întregul job, chiar dacă autorizarea utilizatorului pentru bibliotecă este revocată în timp ce jobul este activ.

Când este cerut accesul la un obiect şi este specificat *LIBL pentru obiect, informaţiile din lista de biblioteci sunt folosite pentru a verifica autorizarea pentru bibliotecă. Dacă este specificat un nume calificat, autorizarea pentru bibliotecă este verificată în mod special, chiar dacă biblioteca este inclusă în lista de biblioteci a utilizatorului.

Atenţie: Dacă un utilizator rulează sub autorizarea adoptată când este adăugată o bibliotecă la lista de biblioteci, utilizatorul rămâne autorizat pentru bibliotecă chiar dacă el nu mai rulează sub autorizarea adoptată. Aceasta reprezintă un potenţial risc pentru securitate. Orice intrări adăugate la lista de biblioteci utilizatorului de către un program care rulează sub autorizarea adoptată ar trebui eliminate înainte ca programul cu autorizarea adoptată să se termine.

În plus, aplicaţiile care folosesc liste de biblioteci în locul numelor calificate de biblioteci au un potenţial risc de securitate. Un utilizator care este autorizat pentru comenzile de lucru cu liste de biblioteci poate rula o versiune diferită a unui program. Vedeţi “Lista de biblioteci” la pagina 177 pentru mai multe informaţii.

Autorizările de câmp

Autorizările de câmp sunt acum suportate pentru fişierele bază de date. Autorizările suportate sunt Reference şi Update. Puteţi administra aceste autorizări doar prin instrucţiunile SQL GRANT şi REVOKE. Puteţi afişa aceste autorizări prin comenzile DSPOBJAUT (Display Object Authority - Afişare autorizare obiect) şi EDTOBJAUT (Edit Object Authority - Editare autorizare obiect). Puteţi afişa numai autorizările de câmp cu comanda EDTOBJAUT; nu le puteţi edita.

```
                        Display Object Authority

Object . . . . . :   PLMITXT     Owner  . . . . . . . :   PGMR1
  Library. . . . :   RLN         Primary group  . . . :   DPTAR
Object type. . . :   *FILE       ASP Device   . . . . :   *SYSBAS

Object secured by authorization list  . . . . . . . . :   *NONE
                      Object    ---------------Data---------------
User        Group     Authority  Read  Add  Update  Delete  Execute
*PUBLIC               *CHANGE     X     X     X       X       X
PGMR1                 *ALL        X     X     X       X       X
USER1                 *USE        X                           X
USER2                 USER DEF    X           X               X
USER3      USER DEF               X    X



Press Enter to continue


F3=Exit  F11=Nondisplay detail F12=Cancel F16=Display field authorities
```

Figura 4. Ecranul Display Object Authority care arată F16=Display field authorities. Această tastă funcţională va fi afişată când un fişier bază de date are autorizări de câmp.

```
                          Display Field Authority

Object . . . . . :   PLMITXT         Owner  . . . . . . . :   PGMR1
  Library  . . . . :     RLN           Primary group  . . . :   *NONE
Object type  . . . . :   *FILE

                          Object    -----Field Authorities-----------
Field       User       Authority  Mgt  Alter Ref  Read  Add  Update
Field3      PGMR1      *ALL        X      X   X    X     X      X
            USER1      *Use                        X
            USER2      USER DEF                    X            X
            USER3      USER DEF                X   X
            *PUBLIC    *CHANGE                     X     X      X
Field4      PGMR1      *ALL        X      X        X     X      X
            USER1      *Use                        X
            USER2      USER DEF                    X
            USER3      USER DEF                    X
            *PUBLIC    *CHANGE                     X     X      X
                                                                More
Press Enter to continue.

F3=Exit F5=Refresh F12=Cancel F16=Repeat position to F17=Position to
```

Figura 5. Ecranul Display Field Authority. Când este apăsat F17=Position to, este afişat promptul Position the List. Dacă este apăsat F16, va fi repetată operaţia anterioară de poziţionare

Schimbările pentru autorizările de câmp includ următoarele:

- Comanda PRTPVTAUT (Print Private Authority - Tipărire autorizare privată) are un nou câmp care indică atunci când un fişier are autorizări de câmp.

- Comanda DSPOBJAUT (Display Object Authority - Afişare autorizare obiect) are acum un nou parametru Authority Type pentru a permite afişarea autorizărilor de obiect, autorizărilor de câmp, sau a tuturor autorizărilor. Dacă tipul de obiect nu este *FILE, puteţi afişa doar autorizările de obiect.
- Informaţiile oferite de API-ul QSYLUSRA (List Users Authorized to Object - Listare utilizatori autorizaţi pentru obiect) indică acum dacă un fişier are autorizări de câmp.
- Comanda GRTUSRAUT (Grant User Authority - Acordare autorizare utilizator) nu va acorda autorizări de câmp unui utilizator.
- Când o permisiune cu un obiect referinţă este realizat utilizând comanda GRTOBJAUT şi ambele obiecte (cel cu permisiune şi cel la care ne referim) sunt fişiere baze de date, toate câmpurile autorizate vor fi acordate unde numele câmpului se potriveşte.
- Dacă o autorizare de utilizator la un fişier de bază de date este înlăturată, orice autorizare de câmp pentru acel utilizator este înlăturată.

Securitatea şi mediul System/38

System/38 mediu şi program CL al tipului CLP38 reprezintă o potenţială expunere securitate. Când o comandă calificată non-bibliotecă este introdusă din ecranul Introducere Comenzi System/38, sau când este invocată de programul CL CLP38, biblioteca QUSER38 (dacă există) este prima bibliotecă în care este căutată acea comandă. Biblioteca QSYS38 este a doua bibliotecă în care se caută. Un programator sau un alt utilizator cunoscător poate pune altă comandă CL ori în aceste biblioteci şi în acest fel această comandă va fi utilizată în locul uneia dintr-o bibliotecă în lista de biblioteci.

Biblioteca QUSER38 nu este livrată cu sistemul de operare. Totuşi, el poate fi creat de oricine cu suficientă autorizare pentru a crea o bibliotecă.

Vedeţi manualul *System/38 Environment Programming* pentru informaţii suplimentare despre Mediu System/38.

Recomandare pentru mediul System/38

Utilizaţi aceste măsuri pentru a vă proteja sistemul pentru Mediu System/38 şi programe CL ale tipului CLP38:

- Verificaţi autorizării publice a bibliotecii QSYS38 şi dacă este *ALL sau *CHANGE, atunci schimbaţi-o în *USE.
- Verificaţi autorizarea publică a bibliotecii QUSER38 şi dacă este *ALL sau *CHANGE, atunci schimbaţi-o în *USE.
- Dacă nu există QUSER38 şi QSYS38 atunci creaţi-le şi setaţi-le cu autorizare *USE publică. Aceasta va împiedica alte persoane să o creeze la un moment ulterior şi să îşi dea lor sau publicului o autorizare prea mare la ea.

Securitatea directorului

La accesarea unui obiect dintr-un director, trebuie să aveţi autorizare la toate directoarele din calea care conţine obiectul. Trebuie de asemenea să aveţi autorizarea necesară la obiect pentru a realiza operaţia pe care aţi cerut-o.

Aţi putea dori să folosiţi securitatea director în acelaşi mod în care folosiţi securitatea bibliotecă. Limitaţi accesul la directoare şi folosiţi autorizare publică la obiectele din cadrul directorului. Limitarea numărului de autorizări private definite pentru obiecte îmbunătăţeşte performana procesului de verificare autorizare.

Securitatea listei de autorizare

Puteţi grupa obiecte cu cerinţe de securitate similare folosind o listă de autorizare. O listă de autorizare, conceptual, conţine o listă de utilizatori şi autorizarea pe care o au utilizatorii pentru obiectele asigurate de listă. Fiecare utilizator poate avea o autorizare diferită la setul de obiecte pe care le asigură lista. Când daţi unui utilizator autorizare la lista de autorizare, sistemul de operare efectiv permite o **autorizare privată pentru acel utilizator** la lista de autorizare.

Puteţi de asemenea să folosiţi o listă de autorizare pentru a defini o autorizare publică pentru obiectele din listă. Dacă autorizarea publică pentru un obiect este setată pe *AUTL, obiectul îşi obţine autorizarea publică din lista sa de autorizare.

Obiectul din lista de autorizare este folosit ca o unealtă de gestionare de către sistem. Ea conţine în realitate o listă a tuturor obiectelor care sunt asigurate de lista de autorizare. Această informaţie este folosită pentru a construi ecrane pentru vizualizarea sau editarea obiectelor din lista de autorizare.

Nu puteţi folosi o listă de autorizare pentru a asigura un profil utilizator sau altă listă de autorizare. Poate fi specificată o singură listă de autorizare pentru un obiect.

Doar proprietarul obiectului, un utilizator cu autorizare specială toate obiectele (*ALLOBJ) sau un utilizator cu autorizare tot (*ALL) la obiect, poate adăuga sau şterge lista de autorizare pentru un obiect.

Obiectele din biblioteca sistem (QSYS) pot fi asigurate cu o listă de autorizare. Totuşi, numele listei de autorizare care asigură un obiect este stocat cu obiectul. În unele cazuri, când instalaţi o nouă ediţie a sistemului de operare, toate obiectele din biblioteca QSYS sunt înlocuite. Asocierea dintre obiecte şi lista de autorizare se pierde.

Vedeţi subiectul “Planificarea listelor de autorizări” la pagina 206 pentru exemple de moduri de utilizare a listelor de autorizare.

Gestionarea listei de autorizare

Puteţi acorda o autorizare operaţională specială numită Gestionare listă autorizare (*AUTLMGT) pentru liste de autorizare. Utilizatorii cu autorizare *AUTLMGT au permisiunea de a adăuga şi şterge autorizarea utilizatorilor la lista de autorizare şi de a schimba autorizările pentru acei utilizatori. Autorizarea *AUTLMGT, de una singură, nu oferă autorizare pentru a asigura noi obiecte cu lista sau de a şterge obiecte din listă.

Un utilizator cu autorizarea *AUTLMGT poate oferi doar aceeaşi autorizare sau mai mică altor utilizatori. De exemplu, presupuneţi că USERA are autorizare *CHANGE şi *AUTLMGT la lista de autorizare CPLIST1. USERA poate adăuga USERB la CPLIST1 şi să îi dea lui USERB autorizare *CHANGE sau mai mică. USERA nu poate să îi dea lui USERB autorizare *ALL la CPLIST1, deoarece USERA nu are autorizare *ALL.

Un utilizator cu autorizare *AUTLMGT poate şterge autorizarea pentru un utilizator dacă utilizatorul *AUTLMGT are autorizare egală sau mai mare la listă decât numele profilului de utilizator care este şters. Dacă USERC are autorizare *ALL la CPLIST1, atunci USERA nu îl poate şterge pe USERC din listă, deoarece USERA are doar *CHANGE şi *AUTLMGT.

Folosirea listelor de autorizare pentru a asigura obiectele furnizate de IBM

Puteţi alege să folosiţi o listă de autorizare pentru a asigura obiecte furnizate de IBM. De exemplu, poate doriţi să restricţionaţi folosirea unui grup de comenzi câtorva utilizatori.

Obiectele din bibliotecile furnizate de IBM, altele decât bibliotecile QUSRSYS şi QGPL, sunt înlocuite de fiecare dată când instalaţi o nouă ediţie a sistemului de operare. Aşadar, legătura dintre obiectele din bibliotecile furnizate de IBM şi listele de autorizare este pierdută. De asemenea, dacă o listă de autorizare asigură un obiect din QSYS şi este necesară o refacere sistem completă, legătura dintre obiectele din QSYS şi lista de autorizare este pierdută. După ce instalaţi o nouă ediţie sau restaurare a sistemului dvs., folosiţi comanda EDTOBJAUT sau GRTOBJAUT pentru a restabili legătura dintre obiectul furnizat de IBM şi lista de autorizare.

Cartea roşie *Implementation Guide for AS/400 Security and Auditing* conţine programe eşantion, cum sunt ALLAUTL şi FIXAUTL, care pot fi folosite pentru a ataşa liste de autorizare la obiecte după ce listele de autorizare sunt restaurate.

Autorizarea pentru obiectele noi dintr-o bibliotecă

Fiecare bibliotecă are un parametru numit CRTAUT (creare autorizare). Acest parametru determină autorizarea publică implicită pentru orice nou obiect care este creat în acea biblitoecă. Când creaţi un obiect, parametrul AUT din comanda de creare determină autorizarea publică pentru obiect. Dacă valoarea lui AUT din comanda de creare este *LIBCRTAUT, care este implicită, autorizarea publică pentru obiect este setată la valoarea CRTAUT pentru bibliotecă.

De exemplu, presupuneţi că biblioteca CUSTLIB are o valoare CRTAUT de *USE. Ambele din comenzile de mai jos creează o zonă de date denumită DTA1 cu autorizarea publică *USE:

- Specificarea parametrului AUT:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1) +
   TYPE(*CHAR) AUT(*LIBCRTAUT)
```

- Permiterea parametrului AUT să ia valoarea implicită. *LIBCRTAUT este implicit:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1) +
   TYPE(*CHAR)
```

Valoarea implicită CRTAUT pentru o bibliotecă este *SYSVAL. Orice obiecte noi create în bibliotecă folosind AUT(*LIBCRTAUT) au autorizarea publică setată la valoarea valorii sistem QCRTAUT. Valoarea de sistem QCRTAUT este livrată ca *CHANGE. De exemplu, presuăuneţi că biblioteca ITEMLIB are o valoare CRTAUT de *SYSVAL. Această comandă creează zona de date DTA2 cu autorizarea publică de modificare:

```
CRTDTAARA DTAARA(ITEMLIB/DTA2) +
   TYPE(*CHAR) AUT(*LIBCRTAUT)
```

“Asignarea autorizării şi dreptului de proprietate pentru noile obiecte” la pagina 119 arată mai multe exemple de moduri în care sistemul asignează drept de proprietate şi autorizare noilor obiecte.

Atenţie: Anumite biblioteci furnizate de IBM, inclusiv QSYS, au o valoare CRTAUT de *SYSVAL. Dacă modificaţi QCRTAUT în altceva decât *CHANGE, s-ar putea să întâlniţi probleme. De exemplu, dispozitivele sunt create în biblioteca QSYS. Valoarea implicită la crearea dispozitivelor este AUT(*LIBCRTAUT). Valoarea CRTAUT pentru biblioteca QSYS este *SYSVAL. Dacă QCRTAUT este setat pe *USE sau *EXCLUDE, autorizarea publică nu este suficientă pentru a permite semnarea la dispozitive noi.

Valoarea CRTAUT pentru o bibliotecă poate fi setată de asemenea la un nume de listă de autorizare. Orice nou obiect creat în bibliotecă cu AUT(*LIBCRTAUT) este asigurat de lista de autorizare. Autorizarea publică pentru obiect este setată la *AUTL.

Valoarea CRTAUT a bibliotecii nu este folosită în timpul unei mutări (MOVOBJ), creări duplicat (CRTDUPOBJ) sau restaurări a unui obiect în bibliotecă. Autorizarea publică a obiectului existent este folosită.

Dacă parametrul REPLACE (*YES) este folosit în comanda de creare, atunci autorizarea obiectului existent este folosită în loc de valoarea CRTAUT a bibliotecii.

Riscurile legate de crearea autorizării (CRTAUT)

Dacă aplicaţiile dvs. folosesc autorizarea implicită pentru obiectele noi create în timpul procesării aplicaţiei, ar trebui să controlaţicine are autorizarea să schimbe descrierile bibliotecii. Schimbarea autorizării CRTAUT pentru o bibliotecă de aplicaţie poate permite accesul neautorizat la obiectele noi create în bibliotecă.

Autorizare petru obiectele noi dintr-un director

Când creaţi un nou obiect într-un director folosind comenzile CRTDIR, MD sau MKDIR, specificaţi autorizarea datelor şi a obiectelor pe care le primeşte publicul pentru obiect. Dacă folosiţi opţiunea *INDIR, autorizarea pentru directorul creat este determinată de directorul în care este creat. Altfel, puteţi specifica autorizarea dorită.

Dreptul de proprietate asupra obiectului

Fiecărui obiect îi este asignat un proprietar când este creat. Proprietarul este fie utilizatorul care creează obiectul, fie profilul de grup dacă profilul utilizator membru a specificat că profilul de grup ar trebui să fie proprietarul obiectului. Când este creat obiectul, proprietarului îi sunt date toate autorizările de date şi de obiect la obiect. “Asignarea autorizării şi dreptului de proprietate pentru noile obiecte” la pagina 119 arată exemple de moduri în care sistemul asignează drept de proprietate noilor obiecte.

Proprietarul unui obiect are întotdeauna toate autorizările pentru obiect, doar dacă nu este ştearsă una sau toate autorizările. Ca un proprietar de obiect, puteţi alege să ştergeţi unele autorizări ca o măsură de precauţie. De exemplu,

dacă un fişier există care conţine informaţii critice, puteţi şterge autorizarea de existenţă a obiectului dvs. pentru a împiedica ştergerea accidentală a fişierului de către dvs. Totuşi, ca proprietar de fişier, vă puteţi oferi orice autorizare obiect în orice moment.

Dreptul de proprietate al unui obiect poate fi transferat de la un utilizator la altul. Dreptul de proprietate poate fi transferat unui profil de utilizator individual sau un profil de grup. Un profil de grup poate deţine obiecte dacă grupul are membrii.

Când schimbaţi proprietarul unui obiect, aveţi opţiunea să păstraţi sau să revocaţi autorizarea proprietarului anterior. Un utilizator cu autorizare *ALLOBJ poate transfera dreptul de proprietate, aşa cum poate orice utilizator care are următoarele:

- Autorizare de existenţă obiect pentru obiect (cu excepţia unei liste de autorizare)
- Dreptul de proprietate al obiectului, dacă obiectul este o listă de autorizare
- Autorizarea de Adăugare pentru profilul de utilizator al noului proprietar
- Autorizarea de Ştergere pentru profilul de utilizator al proprietarului actual

Nu puteţi şterge un profil care deţine obiecte. Dreptul de proprietate al obiectelor trebuie să fie transferat către un nou proprietar sau obiectele trebuie şterse înainte ca profilul să poată fi şters. Comanda Ştergere profil utilizator (DLTUSRPRF) vă permite să manipulaţi obiecte deţinute când ştergeţi profilul.

Dreptul de proprietate al obiectului este folosit ca o unealtă de gestionare de către sistem. Profilul de proprietar pentru un obiect conţine o listă a tuturor utilizatorilor care au autorizare privată la obiect. Aceste informaţii sunt folosite pentru a construi ecrane pentru editarea sau vizualizarea autorizării obiectelor.

Profilurile care deţin multe obiecte cu multe autorizări private pot deveni foarte mari. Dimensiunea unui profil care deţine multe obiecte afectează performanţa la afişarea şi la lucrul cu autorizarea la obiectele pe care le deţine şi la salvarea sau restaurarea profilurilor. Operaţiile sistem pot fi afectate de asemenea. Pentru a împiedica impacturi asupra performanţei sau operaţiilor sistem, nu asignaţi obiecte unui singur profil proprietar pentru întregul dvs. sistem iSeries Fiecare aplicaţie şi obiectele aplicaţiei ar trebui deţinute de un profil separat. De asemenea, profilurile utilizator furnizate de IBM nu ar trebui să deţină date utilizator sau obiecte.

Proprietarul unui obiect necesită de asemenea spaţiu de stocare suficient pentru obiect. Vedeţi “Spaţiu de stocare maxim” la pagina 74 pentru mai multe informaţii.

Dreptul de proprietate al grupului asupra obiectelor

Când este creat un obiect, sistemul verifică profilul utilizatorului care a creat obiectul pentru a determina dreptul de proprietate al obiectului. Dacă utilizatorul este un membru al unui profil de grup, câmpul OWNER din profilul utilizator specifică dacă utilizatorul sau grupul ar trebui să deţină noul obiect.

Dacă grupul deţine obiectul (OWNER este *GRPPRF), utilizatorului care creează obiectul nu îi este dat automat nici o autorizare specifică la obiect. Utilizatorul primeşte autorizare la obiect prin grup. Dacă utilizatorul deţine obiectul (OWNER este *USRPRF), autorizarea grupului la obiect este determinată de câmpul GRPAUT din profilul utilizator.

Câmpul *tip autorizare grup* (GRPAUTTYP) din profilul utilizator determină dacă grupul 1) devine grupul primar pentru obiect sau 2) îi este dată autorizare privată la obiect. “Asignarea autorizării şi dreptului de proprietate pentru noile obiecte” la pagina 119arată câteva exemple.

Dacă utilizatorul care deţine obiectul se schimbă la un alt grup utilizator, profilul de grup original încă reţine autorizarea la orice obiect creat.

Chiar dacă câmpul *Proprietar* dintr-un profil utilizator este *GRPPRF, utilizatorul trebuie să aibă încă suficient spaţiu de stocare pentru a reţine un obiect nou cât timp este creat. După ce este creat, dreptul de proprietate este transferat profilului de grup. Parametrul MAXSTG din profilul utilizator determină cât spaţiu de stocare auxiliar îi este permis unui utilizator.

Evaluaţi obiectele pe care le poate crea un utilizator, cum sunt programele interogare, când alegeţi între drept de proprietate utilizator individual sau grup:

- Dacă utilizatorul se mută în alt department şi alt grup utilizator, ar trebui ca utilizatorul să mai deţină încă obiectul?
- Este important de ştiut cine creează obiecte? Ecranele de autorizare obiect arată proprietarul obiectului, nu utilizatorul care a creat obiectul.

  Notă: Ecranul Afişare descriere obiect arată creatorul obiectului.

  Dacă funcţia de jurnal auditare este activă, este scrisă o intrare Creare obiect (CO) în jurnalul de auditare QAUDJRN în momentul creării unui obiect. Această intrare identifică profilul utilizator creator. Intrarea este scrisă doar dacă valoarea de sistem QAUDLVL specifică *CREATE şi valoarea de sistem QAUDCTL include *AUDLVL.

Grupul primar pentru un obiect

Puteţi specifica un grup primar pentru un obiect. Numele profilului de grup primar şi autorizarea grupului primar la obiect sunt stocate cu obiectul. Folosirea autorizării de grup primar poate furniza o performanţă mai bună decât autorizarea de grup privat la verificarea autorizării la un obiect.

Un profil trebuie să fie un profil grup (să aibă un gid) pentru a fi asignat ca grup primar pentru un obiect. Acelaşi profil nu poate fi proprietarul obiectului şi grupul său primar.

Când un utilizator creează un obiect nou, parametrii din profilul utilizator controlează dacă grupul utilizatorului are autorizare la obiect şi tipul autorizării este dat. Parametrul *Tip autorizare grup* (GRPAUTTYP) dintr-un profil utilizator poate fi folosit pentru a face grupul utilizatorului grupul primar pentru obiect. “Asignarea autorizării şi dreptului de proprietate pentru noile obiecte” arată exemple de cum este asignată autorizarea când sunt create noi obiecte.

Folosiţi comanda Schimbare grup primar obiect (CHGOBJPGP) sau Gestionare obiecte după grup primar (WRKOBJPGP) pentru a specifica grupul primar pentru un obiect. Puteţi schimba autorizarea pe care o are grupul primar folosind ecranul Editare autorizare obiect sau comenzile acordare sau revocare autorizare.

Profilul de utilizator proprietar implicit (QDFTOWN)

Profilul utilizator Proprietar implicit (QDFTOWN) este un profil utilizator livrat de IBM care este folosit când un obiect nu are proprietar sau când dreptul de proprietate al unui obiect poate ridica o expunere de securitate. Urmează situaţiile care fac ca dreptul de proprietate al unui obiect să fie asignat profilului QDFTOWN:

- Dacă un profil deţinător devine deteriorat şi este şters, obiectele sale nu mai au proprietar. Folosirea comenzii Pretindere spaţiu de stocare (RCLSTG) asignează dreptul de proprietate al acestor obiecte profilului utilizator proprietar implicit (QDFTOWN).
- Dacă un obiect este restaurat şi profilul proprietarului nu există.
- Dacă un program care are nevoie să fie creat din nou este restaurat, dar crearea programului nu se realizează cu succes. Vedeţi subiectul “Validarea programelor care sunt restaurate” la pagina 15 pentru mai multe informaţii despre ce condiţii fac ca dreptul de proprietate să fie asignat lui QDFTOWN.
- Dacă limita de stocare maximă este depăşită pentru profilul utilizator care deţine un deţinător de autorizare care are acelaşi nume ca fişierul care este mutat, redenumit sau a cărui bibliotecă este redenumită.

Sistemul furnizează profilul utilizator QDFTOWN deoarece toate obiectele trebuie să aibă un proprietar. Când sistemul este livrat, doar un utilizator cu autorizare specială *ALLOBJ poate afişa şi accesa acest profil utilizator şi transfera dreptul de proprietate al obiectelor asociate cu profilul utilizator QDFTOWN. Puteţi acorda alte autorizări utilizator profilului QDFTOWN. Profilul utilizator QDFTOWN este destinat folosirii doar de către sistem. Nu ar trebui să proiectaţi securitatea dvs. astfel încât QDFTOWN să deţină normal obiectul.

Asignarea autorizării şi dreptului de proprietate pentru noile obiecte

Sistemul foloseşte câteva valori pentru a asigna autorizare şi drept de proprietate când un obiect nou este creat pe sistem:

Parametrii din comanda CRTxxx

Valoarea de sistem QCRTAUT

Valoarea CRTAUT a bibliotecii

Valorile din profilul utilizator al creatorului

Figura 6 până la Figura 9 arată câteva exemple de cum sunt folosite aceste valori:

Valoarea de sistem QCRTAUT:
*CHANGE

Parametrul bibliotecii CRTAUT:
*USE

Valorile din profilul USERA (Creator):

GRPPRF:
DPT806

OWNER:
*USRPRF

GRPAUT:
*CHANGE

GRPAUTTYP:
*PRIVATE

Comanda folosită pentru a crea obiectul:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
        TYPE(*CHAR) AUT(*LIBCRTAUT)
```

sau

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
        TYPE(*CHAR)
```

Valorile pentru noul obiect:

Autorizare publică:
*USE

Autorizare proprietar:
USERA *ALL

autorizare grup primar:
nici una

autorizare privată:
DPT806 *CHANGE

Notă:

*LIBCRTAUT este valoarea implicită pentru parametrul AUT în majoritatea comenzilor CRTxxx.

Figura 6. Exemplu obiect nou: Autorizare publică din bibliotecă, Grup cu autorizare privată dată

Valoarea de sistem QCRTAUT:
*CHANGE

Parametrul bibliotecii CRTAUT:
*SYSVAL

Valorile din profilul USERA (Creator):

GRPPRF:
DPT806

OWNER:
*USRPRF

GRPAUT:
*CHANGE

GRPAUTTYP:
*PRIVATE

Comanda folosită pentru a crea obiectul:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
        TYPE(*CHAR) AUT(*LIBCRTAUT)
```

Valorile pentru noul obiect:

Autorizare publică:
*CHANGE

Autorizare proprietar:
USERA *ALL

autorizare grup primar:
nici una

autorizare privată:
DPT806 *CHANGE

Figura 7. Exemplu obiect nou: Autorizare publică din valoare de sistem, Grup cu autorizare privată dată

Valoarea de sistem QCRTAUT:
*CHANGE

Parametrul bibliotecii CRTAUT:
*USE

Valorile din profilul USERA (Creator):

GRPPRF:
DPT806

OWNER:
*USRPRF

GRPAUT:
*CHANGE

GRPAUTTYP:
*PGP

Comanda folosită pentru a crea obiectul:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
        TYPE(*CHAR) AUT(*LIBCRTAUT)
```

Valorile pentru noul obiect:

Autorizare publică:
*USE

Autorizare proprietar:
USERA *ALL

autorizare grup primar:
DPT806 *CHANGE

autorizare privată:
nici una

Figura 8. Exemplu obiect nou: Autorizare publică din bibliotecă, Grup cu autorizare de grup primar dată

Valoarea de sistem QCRTAUT:
*CHANGE

Parametrul bibliotecii CRTAUT:
*USE

Valorile din profilul USERA (Creator):

GRPPRF:
DPT806

OWNER:
*GRPPRF

GRPAUT:

GRPAUTTYP:

Comanda folosită pentru a crea obiectul:

```
CRTDTAARA DTAARA(CUSTLIB/DTA1)
        TYPE(*CHAR) AUT(*CHANGE)
```

Valorile pentru noul obiect:

Autorizare publică:
*CHANGE

Autorizare proprietar:
DPT806 *ALL

autorizare grup primar:
nici una

autorizare privată:
nici una

Figura 9. Exemplu obiect nou: Autorizare publică specificată, Grupul deţine obiectul

Obiecte care adoptă autorizarea proprietarului

Uneori un utilizator are nevoie de diferite autorizări la un obiect sau o aplicaţie, în funcţie de situaţie. De exemplu, un utilizator poate avea voie să schimbe informaţia dintr-un fişier client când foloseşte programul aplicaţie care furnizează acea funcţie. Totuşi, acelaşi utilizator ar trebui să aibă permisiunea să vizualizeze, dar să nu modifice, informaţiile client când foloseşte o unealtă de suport decizie, cum este SQL.

O soluţie la această situaţie este 1) să dea utilizatorului autorizare *USE la informaţiile client pentru a permite interogarea fişierelor şi 2) să folosească autorizare adoptată în programele de mentenanţă clienţi pentru a permite utilizatorului să modifice fişierele.

Când un obiect foloseşte autorizarea proprietarului, aceasta este numită **autorizare adoptată**. Obiectele de tipul *PGM, *SRVPGM, *SQLPKG şi programele Java pot adopta autorizare.

Când creaţi un program, specificaţi un parametru profil utilizator (USRPRF) în comanda CRTxxxPGM. Acest parametru determină dacă programul foloseşte autorizarea proprietarului programului în plus faţă de autorizarea utilizatorului care rulează programul.

Consultaţi Centrul de informare cu privire la considerente de securitate şi autorizare adoptată când folosiţi pachete SQL (vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii).

Următoarele se aplică la autorizarea adoptată:

- Autorizarea adoptată este adăugată oricărei alte autorizări găsite pentru utilizator.
- Autorizarea adoptată este verificată doar dacă autorizarea pe care utilizatorul, grupul utilizatorului sau publicul o are la un obiect nu este adecvată pentru operaţia cerută.
- Autorizările speciale (cum sunt *ALLOBJ) din profilul proprietarului sunt folosite.
- Dacă profilul proprietar este un membru al unui profil grup, autorizarea grupului *nu* este folosită pentru autorizarea adoptată.
- Autorizarea publică *nu* este folosită pentru autorizarea adoptată. De exemplu, USER1 rulează programul LSTCUST, care necesită autorizarea *USE la fişiereul CUSTMST:
  - Autorizarea publică la fişierul CUSTMST este *USE.
  - Autorizarea lui USER1 este *EXCLUDE.
  - USER2 deţine programul LSTCUST, care adoptă autorizarea proprietarului.
  - USER2 nu deţine fişierul CUSTMST şi nu are autorizare privată la el.
  - Deşi autorizarea publică este suficientă pentru a îi da lui USER2 acces la fişierul CUSTMST, USER1 nu obţine accesul. Autorizarea utilizator, autorizarea grup primar şi autorizarea privată sunt folosite pentru autorizare adoptată.
  - Doar autorizarea este adoptată. Nici un alt atribut de profil utilizator nu este adoptat. De exemplu, atributele cu capabilităţi limitate nu sunt adoptate.
- Autorizarea adoptată este activă atât timp cât programul care foloseşte autorizarea adoptată rămâne în stiva de programe. De exemplu, presupuneţi că PGMA foloseşte autorizare adoptată:
  - Dacă PGMA porneşte PGMB folosind comanda CALL, acestea sunt stivele cu programe înainte şi după comanda CALL:

Stiva de programe înainte de comanda CALL:	**Stiva de programe după comanda CALL:**
QCMD : : PGMA	QCMD : : PGMA PGMB

Figura 10. Autorizare adoptată şi comanda CALL

    Deoarece PGMA rămâne în stiva de programe după ce este apelat PGMB, PGMB foloseşte autorizarea adoptată a PGMA. (Parametrul Folosire autorizare adoptată (USEADPAUT) poate înlocui aceasta. Vedeţi “Programe care ignoră autorizarea adoptată” la pagina 126 pentru mai multe informaţii despre parametrul USEADPAUT.)
  - Dacă PGMA porneşte PGMB folosind comanda Transferare control (TFRCTL), stivele programului arată astfel:

Stiva de programe înainte de comanda TFRCTL:	**Stiva de programe după comanda TFRCTL:**
QCMD : : PGMA	QCMD : : PGMB

Figura 11. Comanda TFRCTL şi Autorizare adoptată

    PGMB nu foloseşte autorizarea adoptată a lui PGMA, deoarece PGMA nu mai este în stiva de programe.
- Dacă programul care rulează sub autorizare adoptată este întrerupt, folosirea autorizării adoptate este suspendată. Următoarele nu folosesc autorizarea adoptată:
  - Cerere sistem
  - Tasta Atenţie (dacă o comandă Transfer la job grup (TFRGRPJOB) rulează, autorizarea adoptată nu este pasată la jobul de grup.)
  - Program de tratare a mesajului de întrerupere

– Funcţii de depanare

Notă: Autorizarea adoptată este imediat întreruptă de tasta Atenţie sau de o cerere job grup. Utilizatorul trebuie să aibă autorizare pentru programul de tratare a tastei atenţie sau programul iniţial de job grup, altfel încercarea eşuează.

De exemplu, USERA rulează programul PGM1, care adoptă autorizarea USERB. PGM1 foloseşte comanda SETATNPGM şi specifică PGM2. USERB are autorizare *USE la PGM2. USERA are autorizare *EXCLUDE la PGM2. Funcţia SETATNPGM are succes deoarece este rulată folosind autorizare adoptată. USERA primeşte o eroare de autorizare când încearcă să folosească tasta de atenţie deoarece autorizarea lui USERB nu mai este activă.

- Dacă un program care foloseşte autorizare adoptată lansează un job, acel job lansat nu are autorizarea adoptată a programului lansator.
- Când un program declanşator sau un program punct de ieşire este apelat, autorizarea adoptată de la programele anterioare din stiva de apel nu va fi folosită ca o sursă de autorizare pentru programul declanşator sau programul punct de ieşire.
- Funcţie de adoptare program nu este folosită când folosiţi comanda Schimbare job (CHGJOB) pentru a schimba coada de ieşire pentru un job. Profilul utilizator care face modificarea trebuie să aibă autorizare la noua coadă de ieşire.
- Orice obiect creat, inclusiv fişierele spool care pot conţine date confidenţiale, sunt deţinute de utilizatorul programului sau de profilul de grup al utilizatorului, nu de proprietarul programului.
- Autorizarea adoptată poate fi specificată fie în comanda care creează programul (CRTxxxPGM) fie în comanda Schimbare program (CHGPGM).
- Dacă un program este creat folosind REPLACE(*YES) în comanda CRTxxxPGM, noua copie a programului are aceleaşi valori USRPRF, USEADPAUT şi AUT ca programul înlocuit. Parametrii USRPRF şi AUT specificaţi în parametrul CRTxxxPGM sunt ignoraţi.
- Doar proprietarul programului poate specifica REPLACE(*YES) în comanda CRTxxxPGM când este specificat USRPRF(*OWNER) în programul original.
- Doar un utilizator care deţine programul sau are autorizări speciale *ALLOBJ şi *SECADM poate schimba valoarea parametrului USRPRF.
- Trebuie să fiţi semnat ca utilizator cu autorizările speciale *ALLOBJ şi *SECADM pentru a transfera dreptul de proprietate al unui obiect care adoptă autorizare.
- Dacă cineva diferit de proprietarul programului sau un utilizator cu autorizările speciale *ALLOBJ şi *SECADM restaurează un program care adoptă autorizare, toate autorizările publice şi provate la program sunt revocate pentru a împiedica o posibilă expunere de securitate.

Comenzile Afişare program (DSPPGM) şi Afişare program service (DSPSRVPGM) arată dacă un program adoptă autorizare (prompt *profil utilizator*) şi dacă foloseşte autorizare adoptată de la programele anterioare din stiva de programe (prompt *Folosire autorizare adoptată*). Comanda Afişare adoptare program (DSPPGMADP) arată toate obiectele care adoptă autorizarea unui profil de utilizator specific. Comanda Tipărire obiecte care adoptă (PRTADPOBJ) furnizează un raport cu mai multe informaţii despre obiectele care adoptă autorizare. Această comandă furnizează de asemenea o opţiune de a tipări un raport pentru obiectele care s-au modificat de ultima dată de când a fost rulată comanda.

“Organigrama 8: Cum este verificată autorizarea adoptată” la pagina 154 furnizează mai multe informaţii despre autorizarea adoptată. Subiectul “Folosirea autorizării adoptate în proiectarea meniului” la pagina 197 arată un exemplu de cum să folosiţi autorizarea adoptată într-o aplicaţie.

Autorizare adoptată şi Programe legate:

Un program ILE* (*PGM) este un obiect care conţine unul sau mai multe module. Este creat de un compilator ILE*. Un program ILE poate fi legat de unul sau mai multe programe service (*SRVPGM).

Pentru a activa un program ILE cu succes, utilizatorul trebuie să aibă autorizare *EXECUTE la programul ILE şi la toate programele service la care este legat. Dacă un program ILE foloseşte autorizare adoptată de la un program de mai

sus în stiva de apel programe, care adoptă autorizarea **este** folosit pentru a verifica autorizarea la toate programele service la care programul ILE este legat. Dacă programul ILE adoptă autorizare, autorizarea adoptată nu va fi verificată când sistemul verifică autorizarea utilizatorului la programele service la momentul activării programului.

Riscurile şi recomandările privind autorizarea adoptată

Permiterea unui program să ruleze folosind autorizare adoptată este o eliberare intenţională de control. Permiteţi utilizatorului să aibă autorizări la obiecte, şi posibil autorizări speciale, pe care în mod normal utilizatorul nu le-ar fi avut. Autorizarea adoptată furnizează o unealtă importantă pentru întrunirea diverselor cerinţe de autorizare, dar ar trebui să fie folosită cu grijă:

- Adoptaţi autorizarea minimă necesară pentru a întruni cerinţele aplicaţiei. Adoptarea autorizării unui proprietar de aplicaţie este de preferat faţă de adoptarea autorizării QSECOFR sau a unui utilizator cu autorizare specială *ALLOBJ.
- Monitorizaţi cu grijă funcţia oferită de programele care adoptă autorizarea. Asiguraţi-vă că aceste programe nu oferă un mijloc prin care utilizatorul să acceseze obiecte dinafara controlului programului, precum capabilităţi de introducere comenzi.
- Programele care adoptă autorizarea şi apelează alte programe trebuie să efectueze un apel de bibliotecă calificat. Nu folosiţi lista de biblioteci (library list - *LIBL) în apel.
- Controlaţi ce utilizatori au voie să apeleze programe care adoptă autorizarea. Folosiţi interfeţe de tip meniu şi securitate de bibliotecă pentru a împiedica aceste programe de a fi apelate fără suficient control.

Programe care ignoră autorizarea adoptată

Aţi putea dori ca unele programe să nu folosească autorizarea adoptată a programelor anterioare din stiva program. De exemplu, dacă folosiţi un program iniţial de tip meniu care adoptă autorizarea proprietarului, aţi putea dori ca unele dintre programele apelate din programul meniu să folosească acea autorizare.

Parametrul use adopted authority (USEADPAUT) al programului determină dacă sistemul foloseşte autorizarea adoptată a programelor anterioare din stivă la verificarea autorizării pentru obiecte.

Când creaţi un program, valoarea implicită este de a adopta autorizarea de la programele anterioare din stivă. Dacă nu vreţi ca programul să folosească autorizarea adoptată, puteţi modifica programul cu comanda Change Program (CHGPGM) sau cu comanda Change Service Program (CHGSRVPGM) pentru a seta parametrul USEADPAUT pe *NO. Dacă un program este creat folosind REPLACE(*YES) în comanda CRTxxxPGM, noua copie a programului are aceleaşi valori USRPRF, USEADPAUT AUT ca şi programul înlocuit.

Subiectul “Ignorarea autorizării adoptate” la pagina 200 arată un exemplu a modului de folosire a acestui parametru în proiectarea meniului. Vedeţi “Folosirea autorizării adoptate (QUSEADPAUT)” la pagina 30 pentru informaţii despre valoarea de sistem QUSEADPAUT.

Atenţie: În unele situaţii, puteţi folosi instrucţiunea MI MODINVAU pentru a împiedica pasarea autorizării adoptate către funcţiile apelate. Instrucţiunea MODINVAU poate fi folosită pentru a împiedica transmiterea oricărei autorizări adoptate din programele C şi C++ către funcţiile apelate din alt program sau program de serviciu. Acest lucru poate fi folositor când nu cunoaşteţi setarea USEADPAUT a funcţiei care este apelată.

Deţinătorii de autorizare

Un deţinător de autorizare este o unealtă pentru păstrarea autorizărilor pentru un fişier bază de date descris prin program care nu există în sistem. Utilizarea lui principală este pentru aplicaţiile din mediul System/36, care adese şterg fişiere descrise prin program şi le creează din nou.

Un deţinător de autorizare poate fi creat pentru un fişier care există deja sau pentru un fişier care nu există, folosind comanda Create Authority Holder (CRTAUTHLR). Următoarele se aplică la deţinătorii de autorizare:

- Deţinătorii de autorizare pot securiza doar fişiere din spaţiul de stocare auxiliar al sistemului (auxiliary storage pool - ASP) sau un ASP utilizator de bază. Ei nu pot securiza fişiere dintr-un ASP independent.

- Deţinătorul de autorizare este asociat cu un anumit fişier şi bibliteca. El are acelaşi nume ca şi fişierul.
- Deţinătorii de autorizare pot fi folosiţi doar pentru fişiere bază de date descrise prin program şi fişiere logice create în mediul S/36.
- O dată ce deţinătorul de autorizare este creat, puteţi adăuga autorizări private pentru el la fel ca la un fişier. Folosiţi comenzile pentru a acorda, revoca şi afişa autorizările de obiect şi pentru a specifica tipul de obiect *FILE. În ecranele de autorizare obiect, un deţinător de autorizare nu poate fi deosebit de fişierul propiu-zis. Ecranele nu indică dacă fişierul există şi nici nu arată dacă fişierul are un deţinător de autorizare.
- Dacă un fişier este asociat cu un deţinător de autorizare, autorizările definite pentru deţinătorul de autorizare sunt folosite în timpul verificării autorizării. Orice autorizări private definite pentru fişier sunt ignorate.
- Folosiţi comanda Display Authority Holder (DSPAUTHLR) pentru a afişa sau tipări toţi deţinătorii de autorizare din sistem. O puteţi de asemenea folosi pentru a crea un fişier de ieşire (output file - Outfile) pentru procesare.
- Dacă creaţi un deţinător de autorizare pentru un fişier care există:
  - Utilizatorul care creează deţinătorul de autorizare trebuie să aibă autorizarea *ALL pentru fişier.
  - Proprietarul fişierului devine proprietarul deţinătorului de autorizare indiferent de utilizatorul care creează deţinătorul de autorizare.
  - Autorizarea publică pentru deţinătorul de autorizare provine de la fişier. Parametrul public authority (AUT) din comanda CRTAUTHLR este ignorat.
  - Autorizarea fişierului existent este copiată la deţinătorul de autorizare.
- Dacă creaţi un fişier şi există deja un deţinător de autorizare pentru acel fişier:
  - Utilizatorul care creează fişierul trebuie să aibă autorizarea *ALL pentru deţinătorul de autorizare.
  - Proprietarul deţinătorului de autorizare devine proprietarul fişierului indiferent de utilizatorul care creează fişierului.
  - Autorizarea publică pentru fişier provine de la deţinătorul de autorizare. Parametrul public authority (AUT) din comanda CRTPF sau CRTLF este ignorat.
  - Deţinătorul de autorizare este legat de fişier. Autorizarea specificată pentru deţinătorul de autorizare este folosită pentru a securiza fişierul.
- Dacă un deţinător de autorizare este şters, informaţiile de autorizare sunt transferate către fişierul însuşi.
- Dacă un fişier este redenumit şi noul nume de fişier corespunde cu un deţinător de autorizare existent, autorizarea şi dreptul de proprietate asupra fişierului sunt schimbate pentru a corespunde cu deţinătorul de autorizare. Utilizatorul care redenumeşte fişierul trebuie să aibă autorizarea *ALL pentru deţinătorul de autorizare.
- Dacă un fişier este mutat în altă bibliotecă şi un deţinător de autorizare există pentru acel nume de fişier şi bibliotecă destinaţie, atunci autorizarea şi dreptul de proprietate asupra fişierului sunt schimbate pentru a corespunde cu deţinătorul de autorizare. Utilizatorul care mută fişierul trebuie să aibă autorizarea *ALL pentru deţinătorul de autorizare.
- Dreptul de proprietate asupra deţinătorului de autorizare şi asupra fişierului corespund întotdeauna. Dacă schimbaţi dreptul de proprietate asupra fişierului, atunci se schimbă şi dreptul de proprietate asupra deţinătorului de autorizare.
- Când un fişier este restaurat, dacă există un deţinător de autorizare pentru acel nume de fişier şi biblioteca în care este restaurat, el este legat de deţinătorul de autorizare.
- Deţinătorii de autorizare nu pot fi creaţi pentru fişierele din bibliotecile: QSYS, QRCL, QRECOVERY, QSPL, QTEMP şi QSPL0002 – QSPL0032.

Deţinătorii de autorizare şi migrarea la System/36

Ajutorul de migrare la System/36 creează un autorizare deţinător de autorizare pentru fiecare fişier care este migrat. El creează de asemenea un deţinător de autorizare pentru intrările din fişierul de securitate resurse System/36 dacă nu există un fişier corespunzător în System/36.

Vă trebuie deţinători de autorizare doar pentru fişierele care sunt şterse şi re-create de aplicaţiile dvs. Folosiţi comanda Delete Authority Holder (DLTAUTHLR) pentru a şterge orice deţinători de autorizare de care nu aveţi nevoie.

Riscurile privind deţinătorii de autorizare

Un deţinător de autorizare oferă capabilitatea de a defini autorizarea pentru un fişier înainte ca acel fişier să existe. În unele circumstanţe, aceasta poate permite unui utilizator neautorizat să obţină acces la informaţii. Dacă un utilizator ar şti că o aplicaţie ar crea, muta, sau redenumi un fişier, utilizatorul ar putea crea un deţinător de autorizare pentru noul fişier. Utilizatorul ar obţine astfel accesul la fişier.

Pentru a limita acest risc, comanda CRTAUTHLR este livrată cu autorizarea publică *EXCLUDE. Doar utilizatorii cu autorizarea *ALLOBJ pot folosi comanda, doar dacă nu acordaţi autorizarea şi altora.

Gestionarea autorizărilor

Aceasră parte a capitolului descrie metode folosite în mod obişnuit pentru setarea, întreţinerea şi afişarea informaţiilor de autorizare de pe sistemul dumneavoatră. Anexa A, “Comenzile de securitate”, la pagina 263 oferă o listă completă de comenzi disponibile pentru lucrul cu autorizări. Descrierile care urmează nu discută toţi parametrii comenzilor sau toate câmpurile din ecrane. Consultaţi informaţiile online pentru detalii complete.

Ecrane pentru autorizare

Patru ecrane arată autorizările de obiect:

- Ecranul Afişare autorizare obiect
- Ecranul Editare autorizare obiect
- Ecranul Afişare autorizare
- Ecranul Gestionare autorizări

Această secţiune descrie unele caracteristici ale acestor ecrane. Figura 12 arată versiunea de bază a ecranului Afişare autorizare obiect:

```
                          Display Object Authority

Object . . . . . :   CUSTNO    Owner  . . . . . :   PGMR1
  Library. . . . . :   CUSTLIB   Primary group  . . . :   DPTAR
Object type  . . . :   *DTAARA   ASP device   . . . . :   *SYSBAS

Object secured by authorization list  . . . . . :   *NONE

                        Object
User        Group       Authority
*PUBLIC                 *EXCLUDE
PGMR1                   *ALL
DPTAR                   *CHANGE
DPTSM                   *USE
F3=Exit F11=Display detail object authorities F12=Cancel  F17=Top
```

Figura 12. Ecranul Afişare autorizare obiect

Numele definite de sistem ale autorizărilor sunt arătate în acest ecran. F11 acţionează ca un comutator între aceasta şi alte două versiuni ale ecranului. Una arată autorizările detaliate pentru obiect:

```
                          Display Object Authority

Object . . . . . :   CUSTNO          Owner . . . . . :   PGMR1
  Library. . . . . :   CUSTLIB       Primary group . . . :   DPTAR
Object type. . . . :   *DTAARA         ASP device  . . . :   *SYSBAS

Object secured by authorization list   . . . . . :   *NONE

                       Object    ----------Object-----------
User        Group      Authority  Opr  Mgt  Exist  Alter  Ref
*PUBLIC                *EXCLUDE    X
PGMR1                  *ALL        X    X     X      X     X
DPTAR                  *CHANGE     X
DPTSM                  *USE        X
   :
F3=Exit F11=Display data authorities F12=Cancel F17=Top F18=Bottom
```

Cealaltă arată autorizările de date:

```
                          Display Object Authority

Object . . . . . :   CUSTNO      Owner  . . . . . :   PGMR1
  Library. . . . . :   CUSTLIB     Primary group  . . . :   DPTAR
Object type. . . . :   *DTAARA     ASP device   . . . . :   *SYSBAS

Object secured by authorization list. . . . . :   *NONE

                       Object     ---------------Data---------------
User        Group      Authority  Read  Add  Update  Delete  Execute
*PUBLIC                *EXCLUDE
PGMR1                  *ALL        X     X     X       X       X
DPTAR                  *CHANGE     X     X     X       X       X
DPTSM                  *USE        X                           X
```

Dacă aveţi autorizarea *OBJMGT asupra unui obiect, vedeţi toate autorizările private pentru acel obiect. Dacă nu aveţi autorizarea *OBJMGT, vedeţi doar propriile dvs. surse de autorizare pentru acel obiect.

De exemplu, dacă USERA afişează autorizarea pentru zona de date CUSTNO, este arătată doar autorizarea publică.

Dacă USERB, care este un membru al profilului de grup DPTAR, afişează autorizările pentru zona de date CUSTNO, acestea vor arăta astfel:

```
                          Display Object Authority

Object . . . . . :   CUSTNO      Owner  . . . . . :   PGMR1
  Library. . . . . :   CUSTLIB     Primary group  . . . :   DPTAR
Object type. . . . :   *DTAARA     ASP device   . . . . :   *SYSBAS

Object secured by authorization list. . . . . :   *NONE

                       Object
User        Group      Authority
*GROUP      DPTAR      *CHANGE
```

Dacă USERB rulează un program care adoptă autorizarea lui PGMR1 şi afişează autorizările pentru zona de date CUSTNO, acestea vor arăta astfel:

```
                          Display Object Authority

Object .. . . . . :   CUSTNO      Owner  . . . . . . . :   PGMR1
  Library   . . . . :   CUSTLIB     Primary group  . . . :   DPTAR
Object type. . . . :   *DTAARA      ASP device   . . . . :   *SYSBAS

Object secured by authorization list . . . . . . . . . . :   *NONE

                        Object
User        Group       Authority
*ADOPTED                USER DEF
*PUBLIC                 *EXCLUDE
PGMR1                   *ALL
*GROUP      DPTAR       *CHANGE
DPTSM                   *USE
```

Autorizarea *ADOPTED indică doar autorizarea suplimentară primită de la proprietarul programului. USERB primeşte de la PGMR1 toate autorizările care nu sunt incluse în *CHANGE. Ecranul arată toate autorizările private, deoarece USERB a adoptat *OBJMGT. Ecranul detaliat arată astfel:

```
                          Display Object Authority

Object . . . . . :   CUSTNO       Owner  . . . . . . . :   PGMR1
  Library. . . . . :   CUSTLIB      Primary group  . . . :   DPTAR
Object type. . . . :   *DTAARA      ASP device   . . . . :   *SYSBAS

Object secured by authorization list . . . . . . . . . . :   *NONE

                         Object     -----------Object-----------
User       Group       Authority  Opr  Mgt  Exist  Alter  Ref
*ADOPTED                USER DEF         X     X      X     X
*PUBLIC                 *EXCLUDEPGMR1
                        *ALL        X    X     X      X     X
*GROUP     DPTAR        *CHANGE     X
DPTSM                   *USE        X
F3=Exit F11=Display data authorities F12=Cancel F17=Top F18=Bottom
```

Dacă valoarea câmpului USROPT (user option - opţiune utilizator) din profilul utilizatorului USERB include *EXPERT, atunci ecranul va arăta astfel:

```
                          Display Object Authority

Object . . . . . :   CUSTNO     Owner  . . . . . :   PGMR1
  Library. . . . . :   CUSTLIB    Primary group  . . . :   DPTAR
Object type. . . . :   *DTAARA    ASP device  . . . . .:   *SYSBAS

Object secured by authorization list . . . . . :   *NONE

                 OBJECT     -----Object------   ------Data--------
User    Group    Authority   O   M   E   A   R   R   A   U   D   E
*ADOPTED         USER DEF        X   X   X   X
*PUBLIC          *EXCLUDE
PGMR1            *ALL        X   X   X   X   X   X   X   X   X   X
*GROUP  DPTAR    *CHANGE     X                   X   X   X   X   X
DPTSM            *USE        X                   X               X
```

Rapoarte pentru autorizare

Sunt disponibile mai multe rapoarte pentru a vă ajuta să monitorizaţi implementarea dvs. de securitate. De exemplu, puteţi monitoriza obiectele cu autorizarea *PUBLIC diferită de *EXCLUDE şi obiectele cu autorizările private cu următoarele comenzi:

- PRTPUBAUT (Print Public Authority - Tipărire autorizare publică)
- PRTPVTAUT (Print Private Authority - Tipărire autorizare privată)

Pentru mai multe informaţii despre unelte de securitate, vedeţi *Tips and Tools for Securing Your iSeries*.

Gestionarea bibliotecilor

Doi parametri ai comenzii CRTLIB (Create Library) afectează autorizarea:

Authority (AUT): Parametrul AUT poate fi folosit pentru a specifica oricare dintre următoarele:

- Autorizarea publică pentru bibliotecă
- Lista de autorizare care securizează biblioteca.

Parametrul AUT se aplică la biblioteca însăşi, nu la obiectele din bibliotecă. Dacă specificaţi un nume de listă de autorizare, autorizarea publică pentru bibliotecă este setată la *AUTL.

Dacă nu specificaţi AUT când creaţi o bibliotecă, *LIBCRTAUT este valoarea implicită. Sistemul foloseşte valoarea CRTAUT din biblioteca QSYS, care este livrată ca *SYSVAL.

Create Authority (CRTAUT): Parametrul CRTAUT determină autorizarea implicită pentru orice obiecte noi care sunt create în bibliotecă. CRTAUT poate fi setat la una dintre următoarele autorizări definite de sistem (*ALL, *CHANGE, *USE sau *EXCLUDE), la *SYSVAL (valoarea de sistem QCRTAUT), sau poate avea ca valoarea numele unei liste de autorizare.

Notă: Puteţi schimba valoarea CRTAUT pentru o bibliotecă folosind comanda CHGLIB (Change Library - Modificare bibliotecă).

Dacă utilizatorul PGMR1 introduce această comandă:

```
CRTLIB TESTLIB AUT(LIBLST) CRTAUT(OBJLST)
```

atunci autorizarea pentru bibliotecă arată astfel:

```
                          Display Object Authority

Object . . . . . :   TESTLIB       Owner  . . . . . :   PGMR1
  Library. . . . . :     QSYS        Primary group  . . . :   *NONE
Object type. . . . :   *LIB          ASP device   . . . . :   *SYSBAS

Object secured by authorization list. . . . . . . . . . . :   LIBLST

                         Object
User        Group        Authority
*PUBLIC                  *AUTL
PGMR1                    *ALL
```

- Deoarece a fost specificată o listă de autorizare în parametrul AUT, autorizarea publică este setată la *AUTL.
- Utilizatorul care a introdus comanda CRTLIB este proprietarul bibliotecii, doar dacă profilul utilizatorului nu specifică OWNER(GRPPRF). Proprietarul primeşte în mod automat autorizarea *ALL.
- Valoarea CRTAUT nu este arătată în ecranele autorizării obiect. Folosiţi comanda DSPLIBD (Display Library Description - Afişare descriere bibliotecă) pentru a vedea valoarea CRTAUT pentru o bibliotecă.

```
                       Display Library Description

Library  . . . . . . . . . . . . . . . . . :   CUSTLIB

Type . . . . . . . . . . . . . . . . . . . :   PROD
ASP number . . . . . . . . . . . . . . . . :   1
ASP device . . . . . . . . . . . . . . . . :   *SYSBAS
Create authority . . . . . . . . . . . . . :   *OBJLST
Create object auditing . . . . . . . . . . :   *SYSVAL
Text description . . . . . . . . . . . . . :   Customer Rec
```

Crearea obiectelor

Când creaţi un nou obiect, puteţi ori să specificaţi autorizarea (AUT), ori să folosiţi valoarea implicită *LIBCRTAUT. Dacă PGMR1 introduce această comandă:

```
CRTDTAARA (TESTLIB/DTA1) +
   TYPE(*CHAR)
```

atunci autorizarea pentru zona de date arată astfel:

```
                          Display Object Authority

Object . . . . . :   DTA1        Owner  . . . . . :   PGRM1
  Library. . . . . :   TESTLIB     Primary group  . . . :   *NONE
Object type. . . . :   *DTAARA     ASP device . . . . . :   *SYSBAS

Object secured by authorization list. . . . . . . . . . . :   OBJLST

                        Object
User        Group       Authority
*PUBLIC                 *AUTL
PGMR1                   *ALL
```

Lista de autorizare (OBJLST) vine de la parametrul CRTAUT care a fost specificat când a fost creată TESTLIB.

Dacă PGMR1 introduce această comandă:

```
CRTDTAARA (TESTLIB/DTA2) AUT(*CHANGE) +
   TYPE(*CHAR)
```

atunci autorizarea pentru zona de date arată astfel:

```
                          Display Object Authority

Object . . . . . :   DTA2       Owner  . . . . . . . :   PGRM1
  Library  . . . . :   TESTLIB    Primary group  . . . :   *NONE
Object type. . . . :   *DTAARA    ASP device . . . . . :   *SYSBAS

Object secured by authorization list . . . . . . . . . :   *NONE

                        Object
User        Group       Authority
*PUBLIC                 *CHANGE
PGMR1                   *ALL
```

Gestionarea autorizării de obiect individuale

Pentru a schimba autorizarea pentru un obiect trebuie să aveţi una dintre următoarele:

- Autorizarea *ALLOBJ sau apartenenţa la un profil de grup care are autorizarea specială *ALLOBJ.

  Notă: Autorizarea grupului nu este folosită dacă aveţi autorizare privată pentru obiect.
- Proprietatea asupra obiectului. Dacă un profil de grup deţine obiectul, atunci orice membru al grupului poate acţiona ca proprietar al obiectului, doar dacă membrul nu a primit o autorizare specifică şi care nu îndeplineşte cerinţele pentru schimbarea autorizării obiectului.
- Autorizarea *OBJMGT pentru obiect şi orice autorizări care sunt acordate sau revocate (cu excepţia *EXCLUDE). Orice utilizator căruia îi este permis să lucreze cu autorizarea obiectului poate acorda sau revoca autorizarea *EXCLUDE.

Cea mai uşoară cale de a schimba autorizarea pentru un obiect individual este cu ecranul Editare autorizare obiect. Acest ecran poate fi apelat direct prin folosirea comenzii Edit Object Authority (EDTOBJAUT) sau poate fi selectat ca o opţiune din ecranul WRKOBJOWN (Work with Objects by Owner - Gestionare obiecte după proprietar) sau WRKOBJ (Work with Objects - Gestionare obiecte).

```
                          Edit Object Authority

Object. . . . . :   DTA1       Owner  . . . . . . . :   PGMR1
  Library . . . . :   TESTLIB    Primary group  . . . :   *NONE
Object type.. . . :   *DTAARA    ASP device . . . . . :   *SYSBAS

Type changes to current authorities, press Enter.

  Object secured by authorization list  . . . . . . . :   OBJLST

                        Object
User        Group       Authority
*PUBLIC                 *AUTL
PGMR1                   *ALL
```

De asemenea puteţi folosi aceste comenzi pentru a schimba autorizarea unui obiect:

Change Authority (CHGAUT)

Work with Authority (WRKAUT)

Grant Object Authority (GRTOBJAUT)

Revoke Object Authority (RVKOBJAUT)

Pentru a specifica subseturile de autorizare generică, precum Read/Write (*RX) sau Write/Execute (*WX), trebuie să folosiţi comenzile CHGAUT sau WRKAUT.

Specificarea unei autorizări definite de utilizator

Coloana Autorizare obiect din ecranul Editare autorizare obiect vă permite să specificaţi oricare dintre seturile de autorizări definite de sistem (*ALL, *CHANGE, *USE, *EXCLUDE). Dacă vreţi să specificaţi o autorizare care nu este dintr-un set definit de sistem, folosiţi F11 (Display detail - Afişare detalii).

Notă: Dacă valoarea câmpului *Opţiuni utilizator* (USROPT) din profilul dvs. de utilizator este setată pe *EXPERT, atunci veţi vedea întotdeauna această versiune detaliată a ecranului fără a trebui să apăsaţi F11.

De exemplu, PGMR1 şterge autorizarea *OBJEXIST pentru fişierul CONTRACTS, pentru a împiedica ştergerea accidentală a fişierului. Deoarece PGMR1 are o combinaţie de autorizări care nu este dintre seturile definite de sistem, sistemul pune *USER DEF* (user-defined) în coloana Autorizare obiect:

```
                          Edit Object Authority

Object . . . . . :   CONTRACTS   Owner  . . . . . :   PGMR1
  Library. . . . . :   TESTLIB     Primary group  . . . :   *NONE
Object type. . . . :   *FILE       ASP device . . . . . :   *SYSBAS

Type changes to current authorities, press Enter.

  Object secured by authorization list. . . . . :   LIST2

                       OBJECT          ----------Object-----------
User        Group      Authority  Opr  Mgt  Exist  Alter  Ref
*PUBLIC                *AUTL
PGMR1                  USER DEF    X    X            X     X
```

Puteţi apăsa F11 (Display data authorities - Afişare autorizări de date) pentru a vedea sau modifica autorizările de date:

```
                          Edit Object Authority

 Object . . . . . :   CONTRACTS   Owner  . . . . . :   PGMR1
  Library . . . . . :   TESTLIB     Primary group  . . . :   *NONE
 Object type. . . . :   *FIL        ASP device . . . . . :   *SYSBAS

Type changes to current authorities, press Enter.

 Object secured by authorization list. . . . . :   LIST2

                       OBJECT    ---------------Data---------------
User        Group      Authority  Read  Add  Update  Delete  Execute
*PUBLIC                *AUTL
PGMR1                  USER DEF    X     X     X       X        X
```

Acordarea de autorizări noilor utilizatori

Pentru a acorda autorizare utilizatorilor suplimentari, apăsaţi F6 (Add new users - Adăugare noi utilizatori) din ecranul Editare autorizare obiect. Veţi vedea fereastra de dialog Adăugare utilizatori noi, care vă permite să definiţi autorizarea pentru mai mulţi utilizatori:

```
                            Add New Users

Object . . . . . :   DTA1
  Library  . . . . . :     TESTLIB

Type new users, press Enter.

            Object
User        Authority
USER1       *USE
USER2       *CHANGE
PGMR2       *ALL
```

Ştergerea autorizării pentru un utilizator

Ştergerea autorizării unui utilizator pentru un obiect este diferită de acordarea către utilizator a autorizării *EXCLUDE. Autorizarea *EXCLUDE înseamnă că utilizatorului îi este interzis în mod special să folosească obiectul. Doar autorizarea specială *ALLOBJ şi autorizarea adoptată suprascriu autorizarea *EXCLUDE. Ştergerea autorizării unui utilizator înseamnă că utilizatorul nu are nici o autorizare specifică asupra obiectului. Utilizatorul poate obţine accesul la obiect prin intermediul unui profil de grup, al unei liste de autorizare, al autorizării publice, autorizării speciale *ALLOBJ sau prin intermediul autorizării adoptate.

Puteţi şterge autorizarea unui utilizator prin folosirea ecranului Editare autorizare obiect. Tastaţi nişte spaţii albe (blancuri) în câmpul Autorizare obiect pentru acel utilizator şi apăsaţi tasta Enter. Utilizatorul este eliminat din ecran. De asemenea puteţi folosi comanda Revoke Object Authority (RVKOBJAUT). Ori revocaţi autorizare specifică pe care o are utilizatorul, ori revocaţi autorizarea *ALL pentru acel utilizator.

Notă: Comanda RVKOBJAUT revocă doar autorizarea pe care o specificaţi. De exemplu, USERB are autorizarea *ALL pentru FILEB din biblioteca LIBB. Dvs. revocaţi autorizarea *CHANGE:

```
RVKOBJAUT OBJ(LIBB/FILEB) OBJTYPE(*FILE) +
USER(*USERB) AUT(*CHANGE)
```

După comandă, autorizarea lui USERB asupra FILEB arată astfel:

```
                       Display Object Authority

Object . . . . . :   FILEB     Owner  . . . . . :   PGMR1
  Library. . . . . :   LIBB      Primary group  . . . :   *NONE
Object type. . . . :   *FILE     ASP device   . . . . :   *SYSBAS

  Object secured by authorization list. . . . . :   *NONE

                     Object     --------Object------------
User     Group   Authority  Read  Add  Update  Delete  Execute
USERB            USER DEF         X    X       X       X
```

```
                      Display Object Authority

Object . . . . . :   FILEB     Owner  . . . . . :   PGMR1
  Library. . . . . :   LIBB      Primary group  . . . :   *NONE
Object type  . . . :   *FILE     ASP device . . . . . :   *SYSBAS

tion list  . . . . . .   *NONE

                       Object    ---------------Data---------------
User       Group       Authority  Read  Add  Update  Delete  Execute
PGMR1                  USER DEF
```

Gestionarea autorizării pentru mai multe obiecte

Ecranul Editare autorizare obiect vă permite să lucraţi în mod interactiv cu autorizarea pentru un obiect la un moment dat. Comanda GRTOBJAUT (Grant Object Authority - Acordare autorizare obiect) vă permite să faceţi schimbări de autorizare asupra mai multor obiecte la un moment dat. Puteţi folosi comanda de autorizare GRTOBJAUT în mod interactiv sau în batch. De asemenea o puteţi apela dintr-un program.

În continuare sunt date exemple de folosire a comenzii GRTOBJAUT, care arată ecranul prompt. Când este rulată comanda, dumneavoastră primiţi un mesaj pentru fiecare obiect care indică dacă schimbarea a fost efectuată. Schimbările de autorizare necesită un lacăt exclusiv asupra obiectului şi nu pot fi făcute atunci când obiectul este folosit deja. Tipăriţi istoricul dvs. de job pentru evidenţa schimbărilor încercate şi efectuate.

- Pentru a acorda tuturor obiectelor din biblioteca TESTLIB o autorizare publică *USE:

```
                    Grant Object Authority (GRTOBJAUT)

Type choices, press Enter.
Object . . . . . .   *ALL
Library . . . . . .  TESTLIB
Object type  . . . . . .  *ALL
ASP device  . . . . . .  *
Users  . . . . . .   *PUBLIC
+ for more values
Authority  . . . . . .  *USE
```

Acest exemplu pentru comanda GRTOBJAUT acordă autorizarea pe care o specificaţi, dar nu şterge nici o autorizare care este mai mare decât cea specificată de dvs. Dacă unele obiecte din biblioteca TESTLIB au autorizarea publică *CHANGE, atunci comanda tocmai arătată nu reduce autorizarea lor publică la *USE. Pentru a vă asigura că toate obiectele din TESTLIB au autorizarea publică *USE, folosiţi comanda GRTOBJAUT cu parametrul REPLACE.

```
GRTOBJAUT OBJ(TESTLIB/*ALL) OBJTYPE(*ALL) +
          USER(*PUBLIC) REPLACE(*YES)
```

Parametrul REPLACE indică dacă autorizările pe care le specificaţi înlocuiesc autorizarea existentă pentru acel utilizator. Valoarea implicită REPLACE(*NO) acordă autorizarea pe care o specificaţi, dar nu şterge nici o autorizare care este mai mare decât autorizarea specificată de dvs., decât dacă acordaţi autorizarea *EXCLUDE.

Aceste comenzi setează autorizarea publică doar pentru obiectele care există deja în bibliotecă. Pentru a seta autorizarea publică pentru orice noi obiecte care sunt create ulterior, folosiţi parametrul CRTAUT în descrierea bibliotecii.

- Pentru a da autorizarea *ALL fişierelor de lucru din biblioteca TESTLIB pentru utilizatorii AMES şi SMITHR. În acest exemplu, numele fişierelor de lucru încep toate cu caracterele WRK:

```
                    Grant Object Authority (GRTOBJAUT)

Type choices, press Enter.

Object . . . . . .   WRK*
  Library  . . . . . .   TESTLIB
Object type  . . . . . .   *FILE
ASP device  . . . . . .  *
Users  . . . . . .   AMES
              + for more values   SMITHR
Authority  . . . . . .   *ALL
```

  Această comandă foloseşte un nume generic pentru a specifica fişierele. Puteţi specifica un nume generic prin tastarea unui şir de caractere urmat de un asterisc (*). Informaţiile de ajutor online vă spun ce parametrii ai unei comenzi acceptă ca valoare un nume generic.
- Pentru a securiza toate fişierele care încep caracterele AR* folosind o listă de autorizare numită ARLST1 şi să faceţi ca fişierele să îşi obţină autorizarea publică din acea listă, folosiţi următoarele două comenzi:
  1. Securizarea fişierelor cu lista de autorizare folosind comanda GRTOBJAUT:

```
                    Grant Object Authority

Type choices, press Enter.

Object . . . . . .   AR*
  Library  . . . . . .   TESTLIB
Object type  . . . . . .   *FILE
ASP device  . . . . . .  *

   ⋮
Authorization list . . . . . .   ARLST1
```

  2. Setarea autorizării publice pentru fişierele cu *AUTL, folosind comanda GRTOBJAUT:

```
                    Grant Object Authority

Type choices, press Enter.

Object . . . . . .   AR*
  Library  . . . . . .   TESTLIB
Object type  . . . . . .   *FILE
ASP device  . . . . . .  *
Users  . . . . . .   *PUBLIC
              + for more values
Authority  . . . . . .   *AUTL
```

Gestionarea proprietăţii asupra obiectelor

Pentru a schimba dreptul de proprietate asupra unui obiect, folosiţi una dintre următoarele:

Comanda Change Object Owner (CHGOBJOWN)

Comanda Work with Objects by Owner (WRKOBJOWN)

Comanda Change Owner (CHGOWN)

Ecranul Gestionare obiecte după proprietar vă arată toate obiectele deţinute de un profil de utilizator. Puteţi asigna obiecte individuale unui nou proprietar. De asemenea puteţi schimba dreptul de proprietate pentru mai multe obiecte în acelaşi timp prin folosirea parametrului NEWOWN (new owner - nou proprietar) de la baza ecranului:

```
                         Work with Objects by Owner

User profile . . . . . :   OLDOWNER

Type options, press Enter.
  2=Edit authority        4=Delete   5=Display author
  8=Display description   9=Change owner
                                                              ASP
Opt  Object        Library       Type      Attribute          Device
     COPGMMSG      COPGMLIB      *MSGQ                        *SYSBAS
9    CUSTMAS       CUSTLIB       *FILE                        *SYSBAS
9    CUSTMSGQ      CUSTLIB       *MSGQ                        *SYSBAS
     ITEMMSGQ      ITEMLIB       *MSGQ                        *SYSBAS

Parameters or command
===> NEWOWN(OWNIC)
F3=Exit   F4=Prompt   F5=Refresh   F9=Retrieve
F18=Bottom
```

Când schimbaţi proprietatea folosind oricare dintre metode, puteţi alege să ştergeţi autorizarea proprietarului anterior asupra obiectului. Valoarea implicită pentru parametrul CUROWNAUT (current owner authority - autorizare proprietar curent) este *REVOKE.

Pentru a transfera dreptul de proprietate asupra unui obiect, trebuie să aveţi:

- Autorizarea existenţă obiect pentru acel obiect
- Autorizarea *ALL sau dreptul de proprietate, dacă obiectul este o listă de autorizare
- Autorizarea de Adăugare pentru profilul de utilizator al noului proprietar
- Autorizarea de Ştergere pentru profilul de utilizator al proprietarului actual

Nu puteţi şterge un profil de utilizator care deţine obiecte. Subiectul “Ştergerea profilurilor de utilizator” la pagina 99 arată metode pentru manevrarea obiectelor deţinute la ştergerea unui profil.

Ecranul Work with Objects by Owner (Gestionare obiecte după proprietar) include obiecte din sistemul de fişiere integrat. Pentru aceste obiecte, coloana *Object* din ecran arată primele 18 caractere ale numelui căii. Dacă numele căii este mai lung de 18 caractere, atunci apare un simbol mai mare (>) la sfârşitul numelui căii. Pentru a vedea numele căii absolute, plasaţi cursorul oriunde în numele căii şi apăsaţi tasta F22.

Gestionarea autorizării de grup primar

Pentru a schimba grupul primar sau autorizarea grupului primar pentru un obiect, folosiţi una dintre următoarele comenzi:

Change Object Primary Group (CHGOBJPGP)

Work with Objects by Primary Group (WRKOBJPGP)

Change Primary Group (CHGPGP)

Când schimbaţi grupul primar al unui obiect, specificaţi ce autorizare are noul grup primar. De asemenea, puteţi revoca autorizarea vechiului grup primar. Dacă nu revocaţi autorizarea vechiului grup primar, atunci aceasta devine o autorizare privată.

Noul grup primar nu poate fi proprietarul obiectului.

Pentru a schimba grupul primar al unui obiect, trebuie să aveţi următoarele:

- autorizarea *OBJEXIST pentru obiect.
- Dacă obiectul este un fişier, o bibliotecă sau o descriere subsistem, vă trebuie autorizările *OBJOPR şi *OBJEXIST.
- Dacă obiectul este o listă de autorizare, vă trebuie autorizarea specială *ALLOBJ sau trebuie să fiţi proprietarul listei de autorizare.
- Dacă revocaţi autorizarea pentru vechiul grup primar, vă trebuie autorizarea *OBJMGT.
- Dacă este specificată o valoarea diferită de *PRIVATE, vă trebuie autorizarea *OBJMGT şi toate autorizările care sunt date.

Folosirea unui obiect referit

Atât ecranul Edit Object Authority (Editare autorizare obiect) cât şi comanda GRTOBJAUT vă permit să daţi autorizare pentru un obiect (sau grup de obiecte) pe baza autorizării unui obiect referit. Acesta este un instrument folositor în unele situaţii, dar ar trebui să evaluaţi de asemenea folosirea unei liste de autorizare pentru îndeplinirea cerinţelor dvs. Vedeţi “Planificarea listelor de autorizări” la pagina 206 pentru informaţii despre avantajele folosirii unei liste de autorizare.

Copierea autorizării de la un utilizator

Puteţi copia toate autorizările private dintr-un profil de utilizator la altul prin folosirea comenzii Grant User Authority (GRTUSRAUT). Această metodă poate fi folositoare în anumite situaţii. De exemplu, dacă sistemul nu vă permite să redenumiţi un profil de utilizator. Pentru a crea un profil identic dar cu alt nume sunt implicaţi câţiva paşi, incluzând copierea autorizărilor profilului original. “Redenumirea unui profil de utilizator” la pagina 103 arată un exemplu cum puteţi face asta.

Comanda GRTUSRAUT copiază doar autorizările private. Ea nu copiază autorizările speciale, şi nici nu transferă dreptul de proprietate asupra obiectului.

Comanda GRTUSRAUT nu ar trebui folosită în locul creării profilurilor de grup. GRTUSRAUT creează un set duplicat de autorizări private, ceea ce creşte timpul necesar pentru a salva sistemul şi face gestiunea autorizărilor mult mai dificilă. GRTUSRAUT copiază autorizările care există la un moment dat. Dacă este necesară autorizarea pentru noi obiecte pe viitor, atunci fiecare profil trebuie să primească autorizarea în mod individual. Profilul de grup oferă această funcţie în mod automat.

Pentru a folosi comanda GRTUSRAUT, trebuie să aveţi toate autorizările care sunt copiate. Dacă nu aveţi o autorizare, atunci acea autorizare nu este acordată profilului destinaţie. Sistemul emite câte un mesaj pentru fiecare autorizare care este acordată sau nu este acordată profilului de utilizator destinaţie. Tipăriţi istoricul de job pentru a avea evidenţa completă. Pentru a evita copierea unui set parţial de autorizări, comanda GRTUSRAUT ar trebui rulată de un utilizator care are autorizarea specială *ALLOBJ.

Gestionarea listelor de autorizare

Setarea unei liste de autorizare necesită trei paşi:

1. Crearea listei de autorizare.
2. Adăugarea utilizatorilor la lista de autorizare.
3. Securizarea obiectelor cu lista de autorizare.

Paşii 2 şi 3 pot fi făcuţi în orice ordine.

Crearea unei liste de autorizare

Nu vă trebuie nici o autorizare pentru biblioteca QSYS pentru a crea o listă de autorizare în acea bibliotecă. Folosiţi comanda Create Authorization List (CRTAUTL):

```
                    Create Authorization List (CRTAUTL)

Type choices, press Enter.

Authorization list . . . . . .   custlst1
Text 'description' . . . . . .   Files cleared at month-end

                           Additional Parameters

Authority  . . . . . . . . . .   *use
```

Parametrul AUT setează autorizarea publică pentru orice obiecte securizate de către listă. Autorizarea publică din lista de autorizare este folosită doar atunci când autorizarea publică pentru un obiect securizat de listă este *AUTL.

Acordarea către utilizatori a autorizării pentru o listă de autorizare

Pentru a lucra cu autorizarea pe care o au utilizatorii asupra listei de autorizare, trebuie să aveţi autorizarea *AUTLMGT (authorization list management - gestiune listă de autorizare), precum şi autorizările specifice pe care le acordaţi. Vedeţi subiectul “Gestionarea listei de autorizare” la pagina 116 pentru o descriere completă.

Puteţi folosi ecranul Edit Authorization List (EDTAUTL) pentru a schimba autorizarea utilizatorului asupra listei de autorizare sau pentru a adăuga noi utilizatori la listă:

```
                          Edit Authorization List

Object . . . . . :   CUSTLST1        Owner  . . . . . :   PGMR1
  Library  . . . . . :     QSYS          Primary group  . . . :   *NONE

Type changes to current authorities, press Enter.

            Object    List
User        Authority  Mgt
*PUBLIC     *USE
PGMR1       *ALL        X
```

Pentru a acorda noilor utilizatori autorizare asupra listei de autorizare, apăsaţi F6 (Adăugare noi utilizatori):

```
                              Add New Users

Object . . . . . :   CUSTLST1     Owner . . . PGMR1
  Library  . . . . . :     QSYS

Type new users, press Enter.

            Object    List
User        Authority  Mgt
AMES        *CHANGE
SMITHR      *CHANGE
```

Autorizarea fiecărui utilizator asupra listei este de fapt stocată ca o autorizare privată în profilul acelui utilizator. Puteţi folosi de asemenea comenzi pentru a lucra cu utilizatori ai listei de autorizare, ori în mod interactiv, ori în lot (batch):

- Folosiţi Add Authorization List Entry (ADDAUTLE) pentru a defini autorizarea pentru utilizatori suplimentari

- Folosiţi Change Authorization List Entry (CHGAUTLE) pentru a schimba autorizarea pentru utilizatorii care au deja autorizare asupra listei
- Folosiţi Remove Authorization List Entry (RMVAUTLE) pentru a şterge autorizarea unui utilizator asupra listei.

Securizarea obiectelor cu o listă de autorizare

Pentru a securiza un obiect cu o listă de autorizare, trebuie să fiţi proprietarul obiectului, să aveţi autorizarea *ALL asupra lui, sau să aveţi autorizarea specială *ALLOBJ .

Folosiţi ecranul Edit Object Authority sau comanda GRTOBJAUT pentru a securiza un obiect cu o listă de autorizare:

```
                          Edit Object Authority

Object . . . . . :   ARWRK1       Owner  . . . . . . . :   PGMR1
  Library  . . . . :   TESTLIB     Primary group. . . . :   *NONE
Object type  . . . :   *FILE       ASP device . . . . . :   *SYSBAS

Type changes to current authorities, press Enter.

  Object secured by authorization list  . . . . . . . . . .   ARLST1

            Object
User        Authority
*PUBLIC     *AUTL
PGMR1       *ALL
```

Setaţi autorizarea publică pentru obiect la *AUTL dacă vreţi ca autorizarea publică să vină din lista de autorizare.

În ecranul Editare listă de autorizare, puteţi folosi F15 (Display authorization list objects - Afişare obiecte din lista de autorizare) pentru a lista toate obiectele securizate de către listă:

```
                    Display Authorization List Objects

Authorization list . . . . . . . . . :   CUSTLST1
  Library  . . . . . . . . . . . . . :   CUSTLIB
Owner  . . . . . . . . . . . . . . . :   OWNAR
Primary group  . . . . . . . . . . . :   DPTAR

                                              Primary
Object      Library     Type      Owner       group       Text
CUSTMAS     CUSTLIB     *FILE     OWNAR
CUSTADDR    CUSTLIB     *FILE     OWNAR
```

Aceasta este doar o listă informativă. Nu puteţi adăuga sau şterge obiecte din listă. Puteţi folosi de asemeanea comanda Display Authorization List Objects (DSPAUTLOBJ) pentru a vizualiza sau tipări o listă cu toate obiectele securizate de către listă.

Ştergerea unei liste de autorizare

Nu puteţi şterge o listă de autorizare dacă este folosită pentru a securiza obiecte. Folosiţi comanda DSPAUTLOBJ pentru lista tuturor obiectelor securizate de către listă. Folosiţi ori ecranul Editare autorizare obiect ori comanda Revocare autorizare obiect (RVKOBJAUT) pentru a schimba autorizarea pentru fiecare obiect. Când lista de autorizare nu mai securizează nici un obiect, folosiţi comanda DLTAUTL (Delete Authorization List - Ştergere listă de autorizare) pentru a o şterge.

Cum verifică sistemul autorizarea

Când un utilizator încearcă să efectueze o operaţie asupra unui obiect, sistemul verifică dacă utilizatorul are autorizarea adecvată pentru operaţie. Sistemul verifică mai întâi autorizarea pentru biblioteca sau calea director care conţine obiectul. Dacă autorizarea pentru bibliotecă sau director este adecvată, sistemul verifică autorizarea asupra obiectului însuşi. În cazul fişierelor bază de date, verificarea autorizării este făcută la momentul deschiderii fişierului, nu când este efectuată fiecare operaţie individuală asupra fişierului.

În timpul procesului de verificare a autorizării, când este găsită o autorizare (chiar dacă nu este adecvată pentru operaţia cerută) verificarea autorizării se opreşte şi accesul este acordat sau respins. Funcţia de autorizare adoptată este o excepţie de la această regulă. Autorizarea adoptată poate trece peste orice autorizare specifică (şi inadecvată) care este găsită. Vedeţi subiectul “Obiecte care adoptă autorizarea proprietarului” la pagina 123 pentru mai multe informaţii despre autorizarea adoptată.

Sistemul verifică autorizarea unui utilizator asupra unui obiect în următoarea ordine:

1. Autorizarea asupra obiectului - calea rapidă
2. Autorizarea specială *ALLOBJ a utilizatorului
3. Autorizarea specifică a utilizatorului asupra obiectului
4. Autorizarea utilizatorului asupra listei de autorizare care securizează obiectul
5. Autorizarea specială *ALLOBJ a grupurilor
6. Autorizarea grupurilor asupra obiectului
7. Autorizarea grupurilor asupra listei de autorizare care securizează obiectul
8. Autorizarea publică specificată pentru obiect sau pentru lista de autorizare care securizează obiectul
9. Autorizarea proprietarului programului, dacă este folosită autorizarea adoptată

Notă: Autorizarea de la unul sau mai multe dintre grupurile utilizatorului poate fi acumulată pentru a găsi o autorizare suficientă pentru obiectul accesat.

Diagramele de flux pentru verificarea autorizării

În continuare sunt date nişte diagrame, descrieri şi exemple legate de modul în care este verificată autorizarea. Folosiţi-le pentru a răspunde la întrebări specifice legate de funcţionarea unei scheme de autorizare particulară sau pentru a diagnostica probleme legate de definiţiile dvs. de autorizare. Diagramele evidenţiază de asemenea tipurile de autorizare care produc cel mai mare efect asupra performanţelor.

Procesul de verificare a autorizării este împărţit într-o diagramă de flux primară şi mai multe diagrame de flux mai mici care arată părţi specifice ale procesului. În funcţie de combinaţia de autorizări pentru un obiect, paşii din unele diagrame de flux pot fi repetaţi de mai multe ori.

Numerele din partea stânga sus a figurilor din diagramele de flux sunt folosite în exemplele care urmează după diagramele de flux.

Paşii care reprezintă căutarea autorizărilor private ale unui profil sunt evidenţiaţi:

Pasul 6 din Organigrama 3 la pagina 146

Pasul 6 din Organigrama 6 la pagina 152

Pasul 2 din Organigrama 8 B la pagina 157

Repetarea acestor paşi este probabil să cauzeze probleme de performanţă în procesul de verificare a autorizării.

Organigrama 1: Procesul principal de verificare a autorizării

Paşii din Organigrama 1 arată procesul principal pe care sistemul îl urmează la verificarea autorizării pentru un obiect.

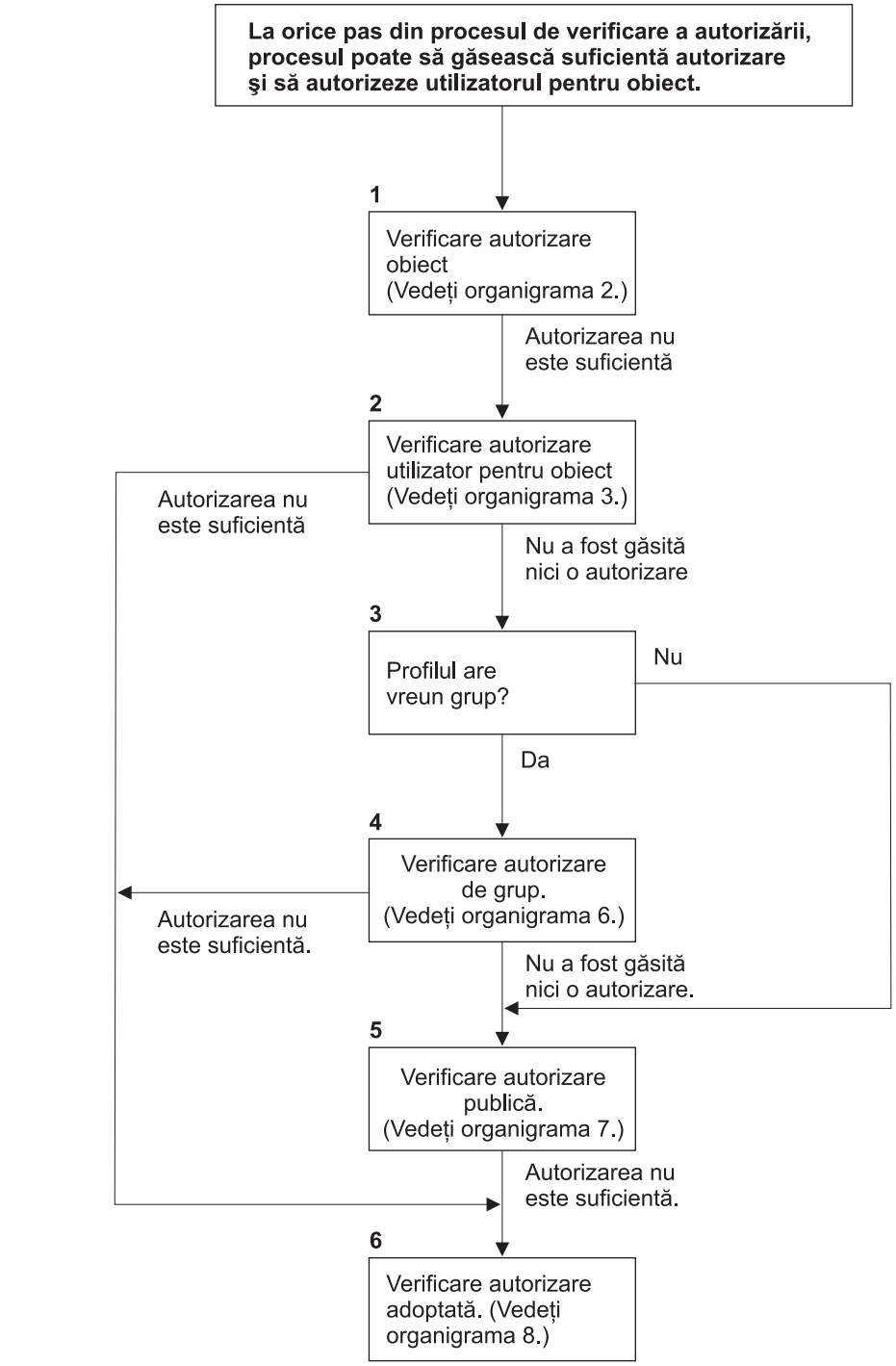

Figura 13. Organigrama 1: Procesul principal de verificare a autorizării

Descrierea pentru Organigrama 1: Procesul principal de verificare a autorizării

Notă: La orice pas din cadrul procesului de verificare a autorizării, sistemul poate găsi o autorizare suficientă şi poate autoriza utilizatorul să acceseze obiectul.

1. Sistemul verifică autorizarea obiectului. (Vedeţi diagrama de flux 2: Calea rapidă pentru verificarea autorizării obiectului.) Dacă sistemul găseşte că autorizarea este insuficientă, el continuă cu Pasul 2.
2. Sistemul verifică autorizarea utilizatorului asupra obiectului. (Vedeţi diagrama de flux 3: Cum este verificată autorizarea utilizatorului asupra unui obiect.) Dacă sistemul descoperă că utilizatorul nu are autorizare pentru obiect, el continuă cu Pasul 3. Dacă sistemul găseşte că autorizarea utilizatorului este insuficientă, el continuă cu Pasul 6.
3. Sistemul verifică dacă profilul de utilizator aparţine vreunui grup. Dacă da, sistemul continuă cu Pasul 4. Dacă nu, sistemul continuă cu Pasul 5.
4. Sistemul determină autorizarea grupului. (Vedeţi diagrama de flux 6). Dacă sistemul descoperă că grupul nu are autorizare pentru obiect, el continuă cu Pasul 5. Dacă sistemul determină că grupul nu are suficientă autorizare pentru obiect, el continuă cu Pasul 6.
5. Sistemul verifică autorizarea publică pentru obiect. (Vedeţi diagrama de flux 7.) Dacă sistemul găseşte că autorizarea publică este insuficientă, el continuă cu Pasul 6.
6. Sistemul verifică autorizarea adoptată pentru obiect. (Vedeţi diagrama de flux 8.)

Dacă utilizatorul nu este autorizat, se întâmplă una sau mai multe dintre următoarele:

- Este trimis un mesaj către utilizator sau program
- Programul eşuează
- Este scrisă o intrare AF în jurnalul de audit

Organigrama 2: Calea rapidă pentru verificarea autorizării obiectului

Paşii din Organigrama 2 sunt efectuaţi folosind informaţiile stocate cu obiectul. Aceasta este cea mai rapidă metodă de autorizare a unui utilizator pentru un obiect.

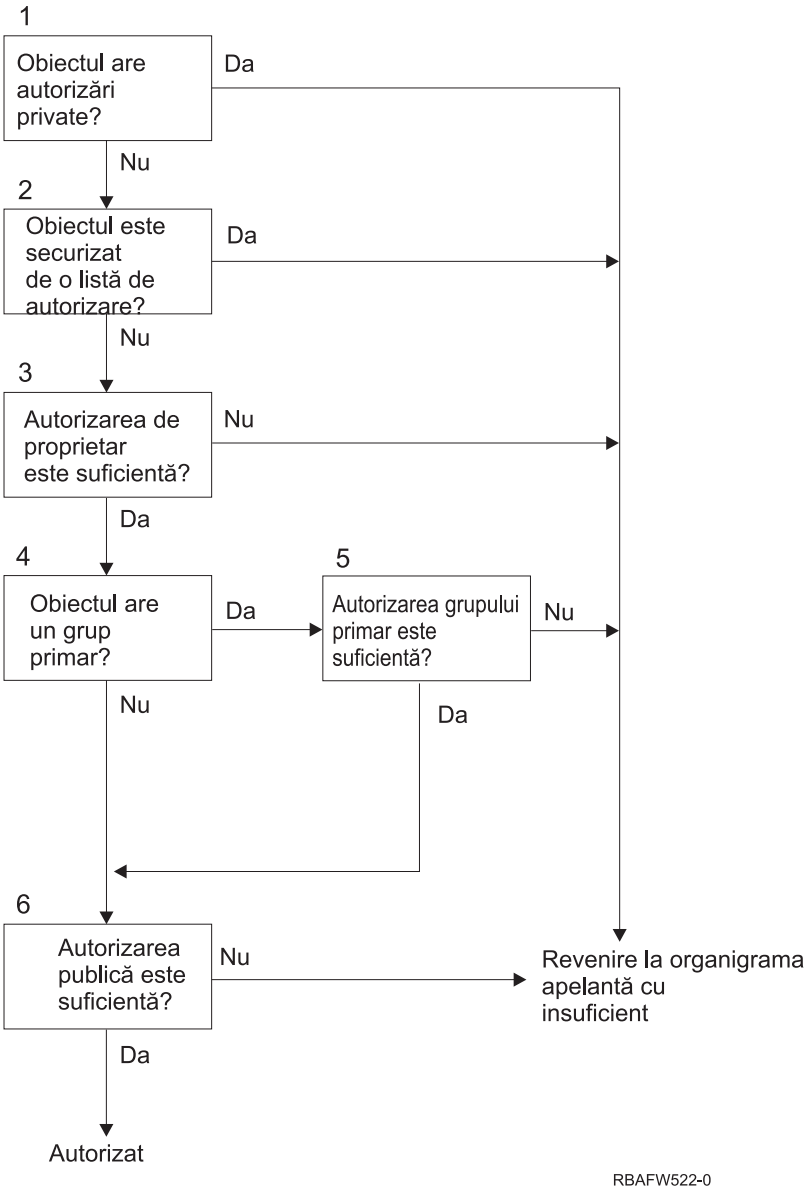

Figura 14. Organigrama 2: Calea rapidă pentru autorizarea obiectului

Descrierea lui Organigrama 2: Calea rapidă pentru autorizarea obiectului

1. Sistemul determină dacă obiectul are autorizări private. Dacă are, sistemul se întoarce la diagrama de flux apelantă cu insuficient. Dacă nu are, sistemul continuă cu Pasul 2.
2. Sistemul determină dacă obiectul este securizat de o listă de autorizare. Dacă este, sistemul se întoarce la diagrama de flux apelantă cu insuficient. Dacă nu este, sistemul continuă cu Pasul 3.
3. Sistemul determină dacă proprietarul obiectului are autorizare suficientă. Dacă are, sistemul se întoarce la diagrama de flux apelantă cu insuficient. Dacă nu este, sistemul continuă cu Pasul 4.
4. Sistemul determină dacă obiectul are un grup primar. Dacă are, sistemul continuă cu Pasul 5. Dacă nu are, sistemul continuă cu Pasul 6.
5. Sistemul determină dacă grupul primar al obiectului are autorizare suficientă. Dacă are, sistemul continuă cu Pasul 6. Dacă nu are, sistemul se întoarce la diagrama de flux apelantă cu insuficient.
6. Sistemul determină dacă autoritea publică este suficientă. Dacă este, atunci obiectul este autorizat. Dacă nu este, atunci sistemul se întoarce la diagrama de flux apelantă cu insuficient.

Organigrama 3: Cum este verificată autorizarea utilizatorului asupra unui obiect

Paşii din Organigrama 3 sunt efectuaţi pentru profilul de utilizator individual.

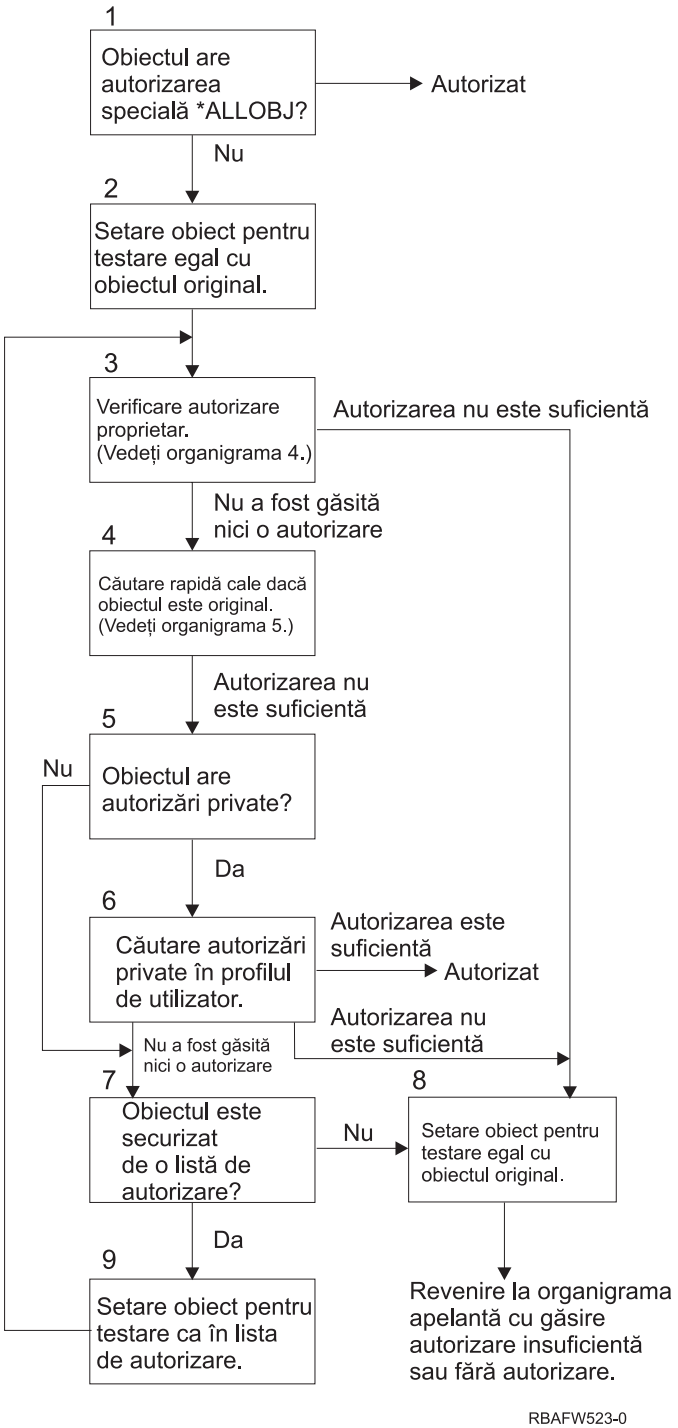

Figura 15. Organigrama 3: Verificare autorizare utilizator

Descrierea pentru Organigrama 3: Verificare autorizare utilizator

1. Sistemul determină dacă profilul de utilizator are autorizarea *ALLOBJ. Dacă profilul are autorizarea *ALLOBJ, atunci profilul este autorizat. Dacă nu are autorizarea *ALLOBJ, atunci verificarea autorizării continuă cu Pasul 2.
2. Sistemul setează autorizarea pentru obiect egală cu cea a obiectului original. Verificarea autorizării continuă cu Pasul 3.

3. Sistemul verifică autorizarea proprietarului. Dacă autorizarea este insuficientă, atunci el continuă cu Pasul 8. Dacă nu este găsită nici o autorizare, atunci el continuă cu Pasul 4.
4. Sistemul efectuează o verificare a autorizării obiectului original pe calea rapidă. (Vedeţi diagrama de flux 6). Dacă autorizarea este insuficientă, atunci verificarea autorizării continuă cu Pasul 5.
5. Sistemul determină dacă obiectul are autorizări private. Dacă are, atunci verificarea autorizării continuă cu Pasul 6. Dacă nu sunt autorizări private, atunci verificarea autorizării merge la Pasul 7.
6. Sistemul caută autorizări private pentru profilul de utilizator. Dacă autorizarea este suficientă, atunci utilizatorul este autorizat. Dacă autorizarea nu este suficientă, atunci verificarea autorizării continuă cu Pasul 8. Dacă nu este găsită nici o autorizare, atunci verificarea autorizării continuă cu Pasul 7.
7. Sistemul determină dacă obiectul este securizat de o listă de autorizare. Dacă nu este, atunci verificarea autorizării continuă cu Pasul 8. Dacă este securizat de o listă de autorizare, atunci verificarea autorizării continuă cu Pasul 9.
8. Sistemul setează obiectul pentru a fi testat egal cu obiectul original şi se întoarce la diagrama de flux apelantă cu autorizare insuficientă sau nici o autorizare găsită.
9. Sistemul setează obiectul testat egal cu lista de autorizare şi se întoarce la Pasul 3.

Organigrama 4: Cum este verificată autorizarea proprietarului

Figura 16 arată procesul pentru verificarea autorizării proprietarului. Numele profilului de utilizator care este proprietar, precum şi autorizarea proprietarului asupra unui obiect sunt stocate cu obiectul.

Există mai multe posibilităţi pentru utilizarea autorizării proprietarului pentru a accesa un obiect:

- Profilul de utilizator deţine obiectul.
- Profilul de utilizator deţine lista de autorizare.
- Profilul de grup al utilizatorului deţine obiectul.
- Profilul de grup al utilizatorului deţine lista de autorizare.
- Este folosită autorizarea adoptată şi proprietarul programului deţine obiectul.
- Este folosită autorizarea adoptată şi proprietarul programului deţine lista de autorizare.

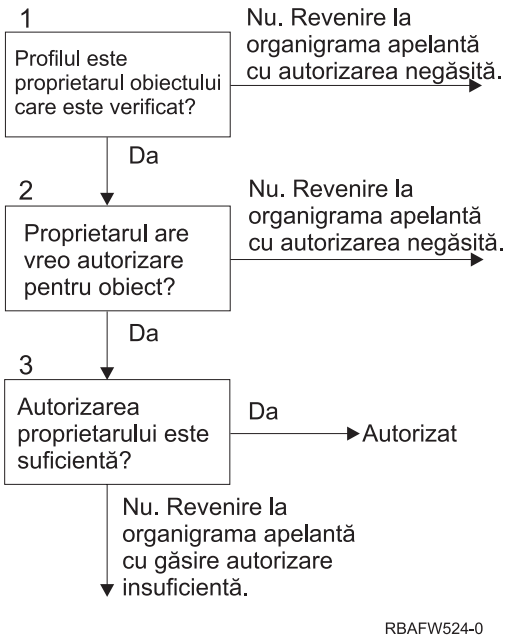

Figura 16. Organigrama 4: Verificarea autorizării proprietarului

Descrierea diagramei de flux 4: Verificarea autorizării proprietarului

1. Sistemul determină dacă profilul de utilizator deţine obiectul care este verificat. Dacă profilul de utilizator deţine într-adevăr obiectul, atunci sistemul trece la Pasul 2. Dacă profilul de utilizator nu deţine obiectul, atunci sistemul revine la diagrama de flux apelantă cu nici o autorizare găsită.
2. Dacă profilul de utilizator nu deţine obiectul, atunci sistemul determină dacă proprietarul are autorizare asupra obiectului. Dacă el sau ea este proprietarul, atunci verificarea autorizării continuă cu Pasul 3. Dacă sistemul descoperă că proprietarul nu are autorizare asupra obiectului, atunci sistemul se întoarce la diagrama de flux apelantă cu nici o autorizare găsită.
3. Dacă proprietarul are autorizare asupra obiectului, atunci sistemul determină dacă această autorizare este sau nu suficientă pentru a accesa obiectul. Dacă autorizarea este suficientă, atunci proprietarul este autorizat să acceseze obiectul. Dacă nu este suficientă, atunci sistemul se întoarce la diagrama de flux apelantă cu autorizare insuficientă găsită.

Organigrama 5: Calea rapidă pentru verificarea autorizării utilizatorului

Figura 17 la pagina 149 arată calea rapidă pentru testarea autorizării utilizatorului fără a căuta printre autorizările private.

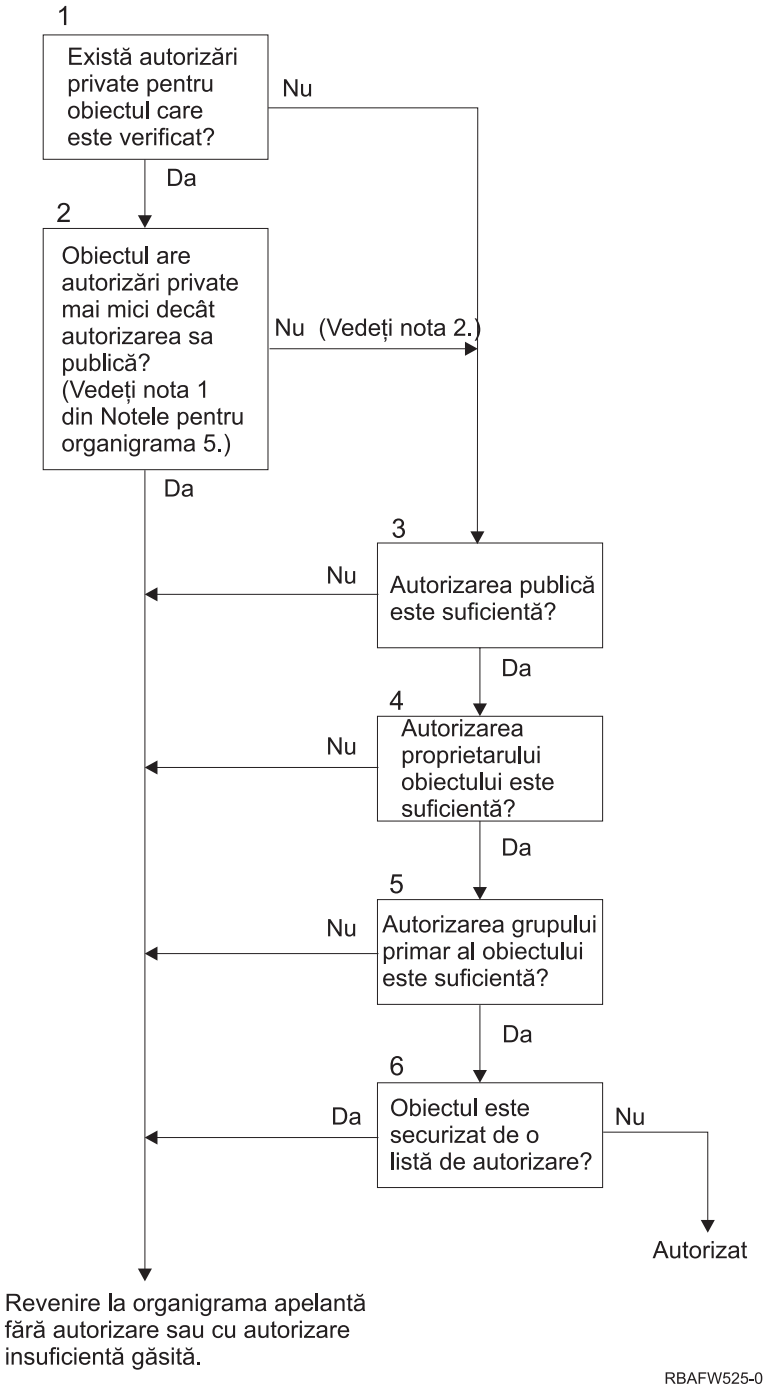

Figura 17. Organigrama 5: Calea rapidă pentru autorizarea utilizatorului

Note pentru Organigrama 5:

1. Autorizarea este considerată mai mică decât publică dacă orice autorizare care este prezentă pentru *PUBLIC nu este prezentă pentru alt utilizator. În exemplul arătat în Tabela 115, publicul are autorizările *OBJOPR, *READ şi *EXECUTE pentru obiect. WILSONJ are autorizarea *EXCLUDE şi nu are nici una dintre autorizările pe care le are publicul. De aceea, acest obiect are o autorizare privată mai mică decât autorizarea publică. (OWNAR are de asemenea o autorizare mai mică decât publicul, dar autorizarea proprietarului este considerată autorizare privată.)

Tabela 115. Autorizarea publică contra autorizarea privată

	Utilizatori			
Autorizare	**OWNAR**	**DPTMG**	**WILSONJ**	***PUBLIC**
Autorizări obiect:				
*OBJOPR		X		X
*OBJMGT	X			
*OBJEXIST				
*OBJALTER				
*OBJREF				
Autorizări de date				
*READ		X		X
*ADD		X		
*UPD		X		
*DLT		X		
*EXECUTE		X		X
*EXCLUDE			X	

2. Această cale oferă o metodă pentru folosirea autorizării publice, dacă este posibil, chiar dacă există autorizări private pentru un obiect. Sistemul se asigură să nu apară ceva mai târziu în procesul de verificare a autorizării care ar putea respinge accesul la obiect. Dacă rezultatul acestor teste este *Suficient*, atunci poate fi evitată căutarea printre autorizările private.

Descrierea diagramei de flux 5: Calea rapidă pentru autorizarea utilizatorului

Această diagramă de flux arată calea rapidă pentru testarea autorizării utilizatorului fără a căuta printre autorizările private.

1. Sistemul determină dacă există autorizări private pentru obiectul care este verificat. Dacă există autorizări private pentru obiect atunci verificarea autorizării continuă cu Pasul 2. Dacă nu există nici o autorizare privată, atunci verificarea autorizării continuă cu Pasul 3.
2. Dacă există autorizări private, atunci sistemul determină dacă obiectul are autorizări private care sunt mai mici decât autorizarea lui publică. (Vedeţi nota 1.) Dacă obiectul are autorizări private care sunt mai mici decât autorizarea lui publică, atunci sistemul se întoarce la diagrama de flux apelantă cu găsit nici o autorizare sau o autorizare insuficientă. Dacă obiectul nu are autorizări private care sunt mai mici decât autorizarea lui publică, (vedeţi nota 2), atunci verificarea autorizării continuă cu Pasul 3.
3. Dacă obiectul nu are autorizări private care sunt mai mici decât autorizarea lui publică, atunci sistemul determină dacă autorizarea publică este suficientă. Dacă autorizarea publică este suficientă, atunci verificarea autorizării continuă cu Pasul 4. Dacă public autorizarea publică este insuficientă, atunci sistemul se întoarce la diagrama de flux apelantă cu găsit nici o autorizare sau o autorizare insuficientă.
4. Dacă autorizarea publică este suficientă, atunci sistemul determină dacă autorizarea proprietarului obiectului este suficientă. Dacă autorizarea proprietarului obiectului este suficientă, atunci verificarea autorizării continuă cu Pasul 5. Dacă autorizarea proprietarului obiectului este insuficientă, atunci sistemul se întoarce la diagrama de flux apelantă cu găsit nici o autorizare sau o autorizare insuficientă.
5. Dacă autorizarea proprietarului obiectului este suficientă, atunci sistemul determină dacă autorizarea grupului primar al obiectului este suficientă. Dacă autorizarea grupului primar al obiectului este suficientă, atunci verificarea autorizării continuă cu Pasul 6. Dacă autorizarea grupului primar al obiectului este insuficientă, atunci sistemul se întoarce la diagrama de flux apelantă cu găsit nici o autorizare sau o autorizare insuficientă.
6. Dacă autorizarea grupului primar al obiectului este suficientă, atunci sistemul determină dacă obiectul este securizat de o listă de autorizare. Dacă obiectul este securizat de o listă de autorizare, atunci sistemul se întoarce la diagrama de flux apelantă cu găsit nici o autorizare sau o autorizare insuficientă. Dacă obiectul nu este securizat de o listă de autorizare, atunci utilizatorul este autorizat să acceseze obiectul.

Organigrama 6: Cum este verificată autorizarea grupului

Un utilizator poate fi membru al până la 16 grupuri. Un grup poate avea autorizare privată asupra unui obiect, sau poate fi grupul primar pentru un obiect.

Autorizarea de la unul sau mai multe dintre grupurile utilizatorului poate fi acumulată pentru a găsi o autorizare suficientă pentru obiectul accesat. De exemplu, WAGNERB are nevoie de autorizarea *CHANGE pentru fişierul CRLIM. Autorizarea *CHANGE include *OBJOPR, *READ, *ADD, *UPD, *DLT şi *EXECUTE. Tabela 116 arată autorizările pentru fişierul CRLIM:

Tabela 116. Autorizarea de grup acumulată

	Utilizatori			
Autorizare	**OWNAR**	**DPT506**	**DPT702**	***PUBLIC**
Autorizări obiect:				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
Autorizări de date				
*READ	X	X	X	
*ADD	X	X		
*UPD	X	X	X	
*DLT	X		X	
*EXECUTE	X	X	X	
*EXCLUDE				X

Lui WAGNERB îi trebuie atât DPT506 cât şi DPT702 pentru a avea o autorizare suficientă pentru fişierul CRLIM. Lui DPT506 îi lipseşte autorizarea *DLT, şi lui DPT702 îi lipseşte autorizarea *ADD.

Organigrama 6 la pagina 152 arată paşii de la verificarea autorizării de grup.

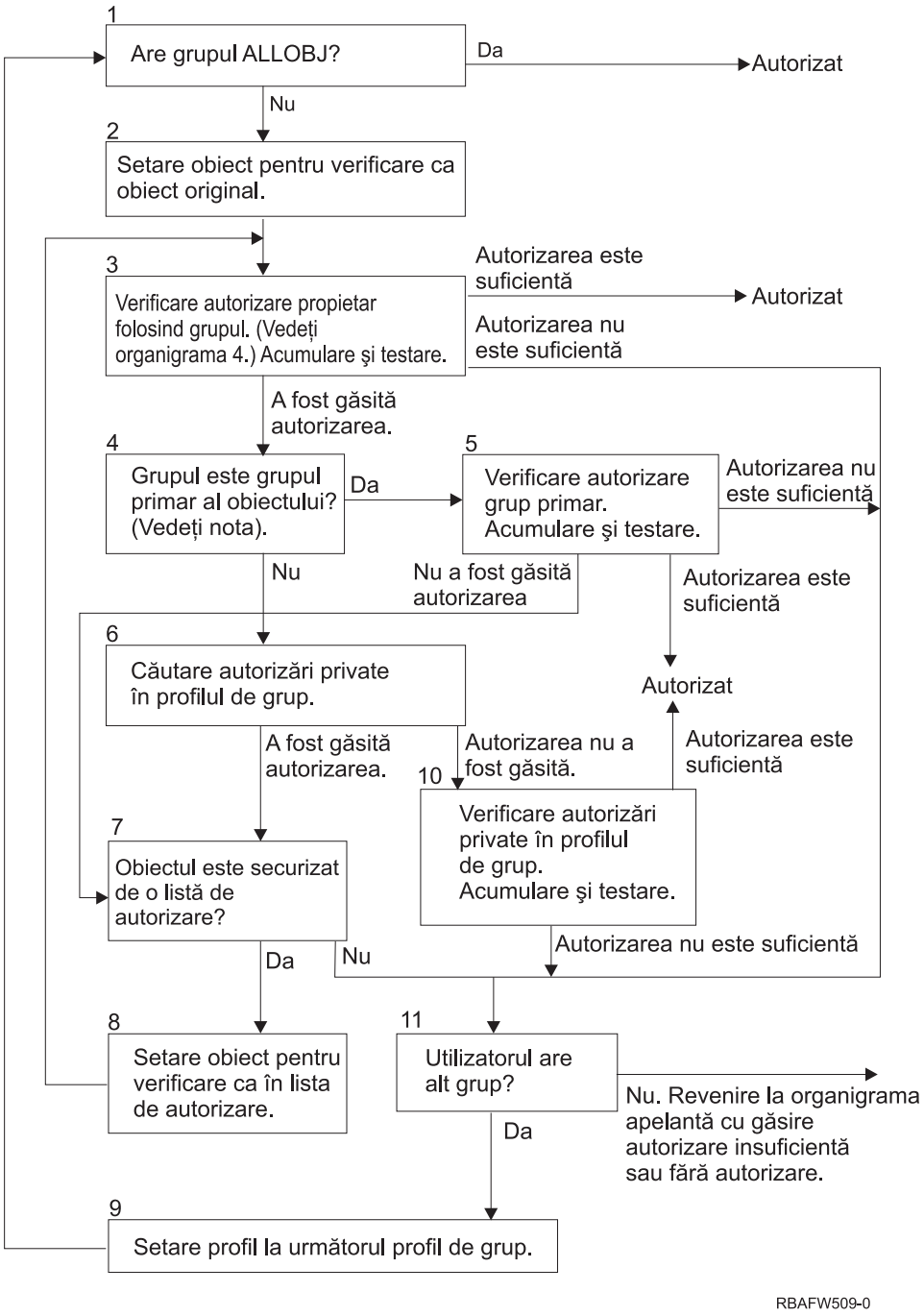

Figura 18. Organigrama 6: Verificarea autorizării de grup

Notă: Dacă utilizatorul a intrat în sistem cu profilul care este grupul primar pentru un obiect, atunci utilizatorul nu poate primi autorizare asupra obiectului prin intermediul grupului primar.

Descrierea diagramei de flux 6: Verificarea autorizării de grup

1. Sistemul determină dacă grupul are autorizarea ALLOBJ. Dacă are, atunci grupul este autorizat. Dacă nu are, atunci verificarea autorizării continuă cu Pasul 2.
2. Dacă grupul nu are autorizarea ALLOBJ, atunci sistemul setează obiectul care este verificat să fie egal cu obiectul original.

3. După ce sistemul setează obiectul la original, el verifică autorizarea proprietarului (Vedeţi Diagrama de flux 4) Dacă autorizarea este suficientă, atunci grupul este autorizat. Dacă autorizarea nu este suficientă, atunci verificarea autorizării trece la Pasul 7. Dacă autorizarea nu este găsită, atunci verificarea autorizării continuă cu Pasul 4.
4. Dacă autorizarea proprietarului nu este găsită, atunci sistemul verifică dacă grupul este grupul primar al obiectului.

   Notă: Dacă utilizatorul a intrat în sistem cu profilul care este grupul primar pentru un obiect, atunci utilizatorul nu poate primi autorizare asupra obiectului prin intermediul grupului primar.

   Dacă grupul este grupul primar al obiectului, atunci verificarea autorizării continuă cu Pasul 5. Dacă grupul nu este grupul primar al obiectului, atunci verificarea autorizării continuă cu Pasul 6.
5. Dacă grupul este grupul primar al obiectului, atunci sistemul verifică şi testează autorizarea grupului primar. Dacă autorizarea grupului primar este suficientă, atunci grupul este autorizat. Dacă autorizarea grupului primar este insuficientă sau nu este găsită, atunci verificarea autorizării trece la Pasul 7.
6. Dacă grupul nu este grupul primar al obiectului, atunci sistemul caută printre autorizările private din profilul de grup. Dacă este găsită autorizarea atunci verificarea autorizării merge la Pasul 10. Dacă nu este găsită autorizarea, atunci verificarea autorizării continuă cu Pasul 7.
7. Dacă nu este găsită nici o autorizare pentru autorizările private pentru profilul de grup atunci sistemul verifică dacă obiectul este securizat de o listă de autorizare. Dacă obiectul este securizat de o listă de autorizare, atunci verificarea autorizării continuă cu Pasul 8. Dacă obiectul nu este securizat de o listă de autorizare, atunci verificarea autorizării merge la Pasul 11.
8. Dacă obiectul este securizat de o listă de autorizare, atunci sistemul setează obiectul de verificat să fie egal cu lista de autorizare şi verificarea autorizării revine la Pasul 3.
9. Dacă utilizatorul aparţine altui profil de grup, atunci sistemul setează acest profil la următorul profil de grup şi revine la Pasul 1 pentru a porni din nou procesul de verificare a autorizării.
10. Dacă este găsită autorizarea pentru autorizările private din cadrul profilului de grup, atunci autorizările private sunt verificate şi testate în profilul de grup. Dacă autorizările sunt suficiente, atunci profilul de grup este autorizat. Dacă nu sunt suficiente atunci verificarea autorizării merge la Pasul 7.
11. Dacă un obiect nu este securizat de o listă de autorizare, atunci sistemul verifică dacă utilizatorul este asociat cu alt profil de grup. Dacă utilizatorul aparţine altui profil de grup, atunci sistemul merge la Pasul 9. Dacă utilizatorul nu aparţine altui profil de grup, atunci sistemul se întoarce la diagrama de flux apelantă cu autorizare insuficientă sau nici o autorizare găsită.

Organigrama 7: Cum este verificată autorizarea publică

Când este verificată autorizarea publică, sistemul trebuie să determine dacă va folosi autorizarea publică pentru obiect sau va folosi lista de autorizare. Organigrama 7 arată procesul:

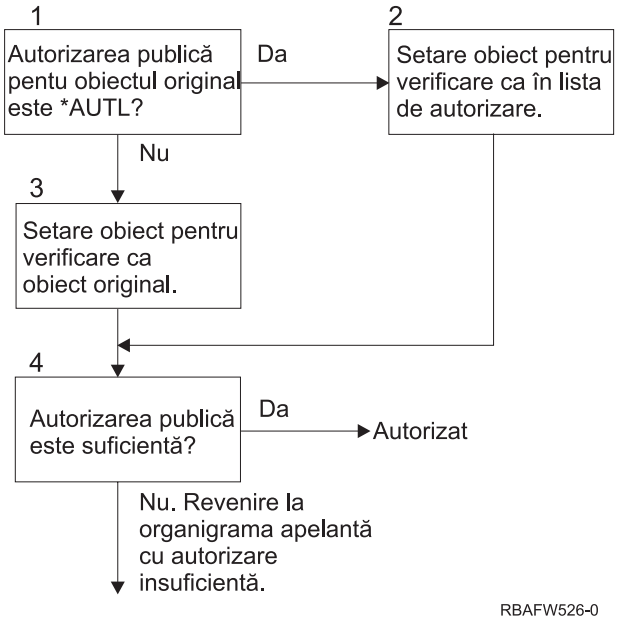

Figura 19. Organigrama 7: Verificarea autorizării publice

Descrierea pentru Organigrama 7: Verificarea autorizării publice

Diagrama de flux 7 arată cum trebuie sistemul să determine dacă va folosi autorizarea publică pentru obiect sau dacă va folosi lista de autorizare.

1. Sistemul determină dacă autorizarea publică pentru obiectul original este *AUTL. Dacă autorizarea publică pentru obiectul original este *AUTL, atunci sistemul continuă cu Pasul 2. Dacă autorizarea publică pentru obiectul original nu este *AUTL, atunci sistemul continuă cu Pasul 3.
2. Dacă autorizarea publică pentru obiectul original este *AUTL, atunci sistemul setează obiectul care este verificat să fie egal cu lista de autorizare şi continuă cu Pasul 4.
3. Dacă autorizarea publică pentru obiectul original nu este *AUTL, atunci sistemul setează obiectul care este verificat să fie egal cu obiectul original şi continuă cu Pasul 4.
4. Dacă obiectul care este verificat a fost setat egal cu lista de autorizare sau cu obiectul original, sistemul determină dacă autorizarea publică este suficientă. Dacă autorizarea publică este suficientă, atunci utilizatorul este autorizat pentru obiect. Dacă autorizarea publică nu este suficientă atunci sistemul se întoarce la diagrama de flux apelantă cu autorizare insuficientă.

Organigrama 8: Cum este verificată autorizarea adoptată

Dacă este găsită o autorizare insuficientă la verificarea autorizării utilizatorului, atunci sistemul verifică autorizarea adoptată. Sistemul poate folosi autorizarea adoptată de la programul original pe care utilizatorul l-a apelat sau de la programele anterioare din stiva program. Pentru a oferi cele mai bune performanţe şi pentru a minimiza numărul de câte ori sunt căutate autorizările private, procesul pentru verificarea autorizării adoptate verifică dacă proprietarul programului are autorizarea specială *ALLOBJ sau dacă deţine obiectul care este testat. Aceasta este repetată pentru fiecare program din stivă care foloseşte autorizarea adoptată.

Dacă nu este găsită o autorizarea suficientă, atunci sistemul verifică dacă proprietarul programului are autorizare privată pentru obiectul care este verificat. Aceasta este repetată pentru fiecare program din stivă care foloseşte autorizarea adoptată.

Figura 20 la pagina 155 şi Figura 21 la pagina 157 arată procesul pentru verificarea autorizării adoptate.

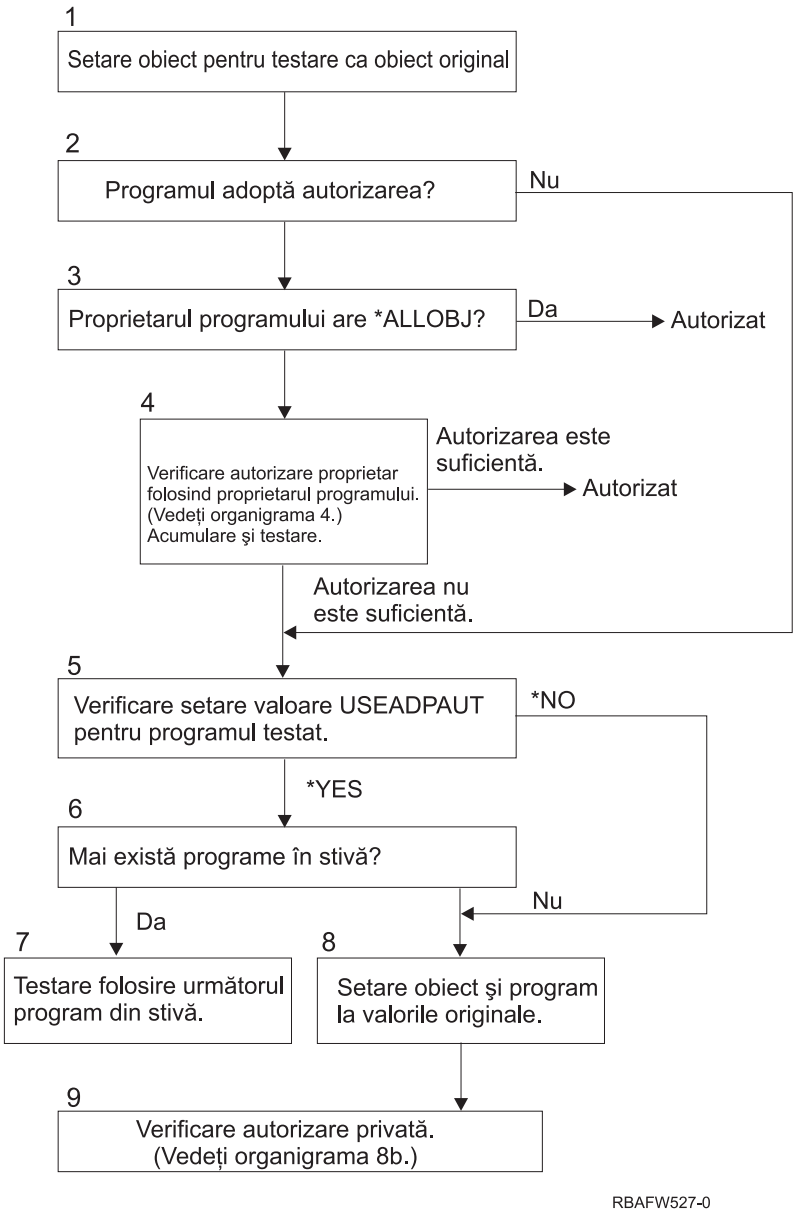

*Figura 20. Organigrama 8 A: Verificarea autorizării adoptate Utilizator *ALLOBJ şi Proprietar*

Descrierea pentru Organigrama 8 A: Verificarea autorizării adoptate Utilizator *ALLOBJ şi Proprietar

Organigrama 8 A descrie cum verifică sistemul autorizarea adoptată când a fost găsită o autorizare insuficientă la verificarea autorizării utilizatorului.

1. Sistemul setează obiectul care este verificat să fie egal cu obiectul original şi continuă cu Pasul 2.
2. Sistemul determină dacă programul adoptă autorizarea. Dacă programul adoptă autorizarea atunci verificarea autorizării continuă cu Pasul 3. Dacă programul nu adoptă autorizarea şi autorizarea este insuficientă, atunci verificarea autorizării merge la Pasul 5.
3. Dacă programul adoptă autorizarea, atunci sistemul determină dacă proprietarul programului are autorizarea *ALLOBJ. Dacă proprietarul programului are autorizarea *ALLOBJ, atunci utilizatorul este autorizat. Dacă proprietarul programului nu are autorizarea *ALLOBJ, atunci verificarea autorizării continuă cu Pasul 4.
4. Dacă proprietarul programului nu are autorizarea *ALLOBJ, atunci sistemul verifică şi testează autorizarea proprietarului. Dacă autorizarea este suficientă, atunci utilizatorul este autorizat. Dacă autorizarea este insuficientă atunci verificarea autorizării continuă cu Pasul 5.

5. Sistemul verifică valoarea USEADPAUT pentru programul care este testat. Dacă valoarea este egală cu *NO atunci verificarea autorizării continuă cu Pasul 8. Dacă valoarea este egală cu *YES atunci verificarea autorizării continuă cu Pasul 6.
6. Dacă valoarea USEADPAUT este egală cu *YES, atunci sistemul determină dacă sunt mai multe programe care aşteaptă în stivă. Dacă sunt mai multe programe în stivă, atunci verificarea autorizării continuă cu Pasul 7. Dacă nu mai sunt programe care aşteaptă în stivă, atunci verificarea autorizării merge la Pasul 8.
7. Dacă sunt mai multe programe în stivă, sistemul testează următorul program din stivă.
8. Dacă nu mai sunt programe în stivă sau dacă valoarea USEADPAUT este egală cu *NO, atunci sistemul setează obiectul şi programul la valorile originale şi continuă cu Pasul 9.
9. Sistemul verifică autorizarea privată. Aceasta este descrisă în Organigrama 8 B: Verificarea autorizării adoptate folosind autorizări private.

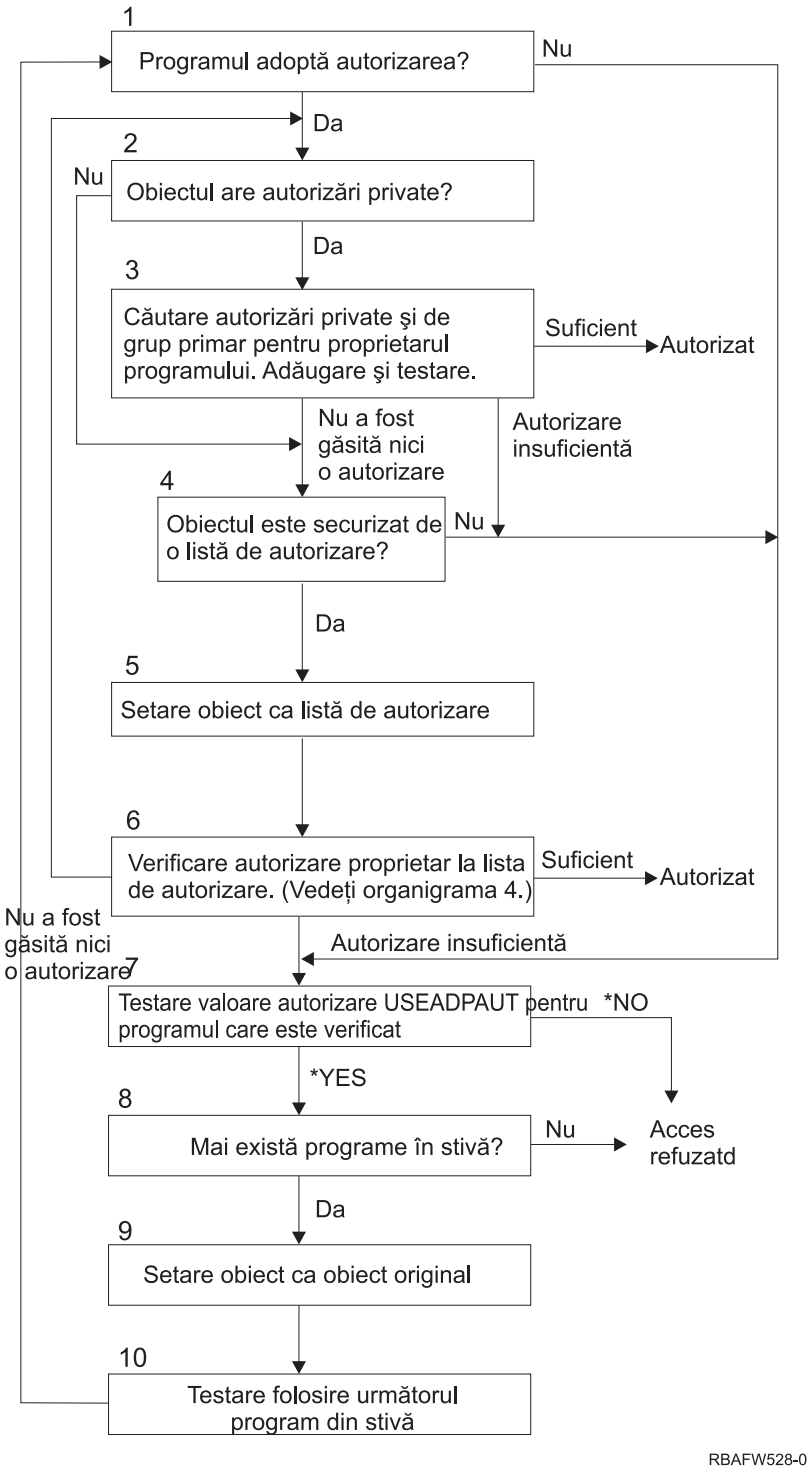

Figura 21. Organigrama 8 B: Verificarea autorizării adoptate folosind autorizări private

Descrierea pentru Organigrama 8 B: Verificarea autorizării adoptate folosind autorizări private

1. Sistemul determină dacă programul poate adopta autorizarea. Dacă da, continuă cu Pasul 2. Dacă nu, continuă cu Pasul 7.
2. Sistemul determină dacă obiectul are autorizări private. Dacă da, continuă cu Pasul 3. Dacă nu, continuă cu Pasul 4.

3. Sistemul verifică autorizările private şi ale grupului primar pentru proprietarul programului. Dacă autorizarea este suficientă, programul este autorizat. Dacă este găsită o autorizare insuficientă, continuă cu Pasul 7. Dacă nu este găsită nici o autorizare, continuă cu Pasul 4.
4. Sistemul determină dacă obiectul este securizat de o listă de autorizare. Dacă da, continuă cu Pasul 5. Dacă nu, continuă cu Pasul 7.
5. Sistemul setează obiectul egal cu lista de autorizare şi apoi continuă cu Pasul 6.
6. Sistemul verifică autorizarea proprietarului asupra listei de autorizare. (Vedeţi diagrama de flux 7.) Dacă nu este găsită nici o autorizare, revine la Pasul 2. Dacă este găsită autorizare suficientă, atunci programul este autorizat.
7. Sistemul testează valoarea de autorizare USEADPAUT pentru programul care este verificat. Dacă *YES, continuă cu Pasul 8. Dacă *NO, acces interzis.
8. Sistemul verifică dacă mai sunt programe în stivă. Dacă da, continuă cu Pasul 9. Dacă nu, acces interzis.
9. Sistemul setează obiectul la valoarea obiectului original şi continuă cu Pasul 10.
10. Text folosind următorul program din stivă şi reporneşte de la Pasul 1.

Exemple de verificare a autorizării

În continuare sunt mai multe exemple de verificare a autorizării. Aceste exemple demonstrează paşii pe care sistemul îi foloseşte pentru a determina dacă unui utilizator îi este permis un acces cerut la un obiect. Aceste exemple sunt destinate să arate cum funcţionează verificarea autorizării şi unde pot apare potenţiale probleme de performanţă.

Figura 22 arată autorizările pentru fişierul PRICES. După figură urmează mai multe exemple de acces cerut la acest fişier şi procesul de verificare a autorizării. În exemple, căutarea printre autorizările private (Organigrama 4, pasul 6) este evidenţiată deoarece aceasta este partea din procesul de verificare a autorizării care poate produce probleme de performanţă dacă este repetată de mai multe ori.

```
                          Display Object Authority

Object . . . . . :   PRICES          Owner  . . . . . :   OWNCP
  Library  . . . . . :   CONTRACTS       Primary group  . . . :   *NONE
Object type    . . . :   *FILE          ASP device . . . . . :   *SYSBAS

Object secured by authorization list  . . . . . . . . . . . . :   *NONE

                        Object
User        Group       Authority
OWNCP                   *ALL
DPTSM                   *CHANGE
DPTMG                   *CHANGE
WILSONJ                 *USE
*PUBLIC                 *USE
```

Figura 22. Autorizarea pentru fişierul PRICES

Cazul 1: Folosirea autorizării private de grup

Utilizatorul ROSSM doreşte accesul la fişierul PRICES folosind programul CPPGM01. CPPGM01 necesită autorizarea *CHANGE pentru fişier. ROSSM este un membru al profilului de grup DPTSM. Nici ROSSM nici DPTSM nu au autorizarea specială *ALLOBJ. Sistemul efectuează aceşti paşi pentru a determina dacă să-i permită lui ROSSM accesul la fişierul PRICES:

1. Organigrama 1, pasul 1.
   a. Organigrama 2, pasul 1.
2. Organigrama 1, pasul 2.
   a. Organigrama 3, paşii 1 şi 2. Obiectul de verificat = CONTRACTS/PRICES *FILE.

b. Organigrama 3, pasul 3.
   1) Organigrama 4, pasul 1. Revenire la Organigrama 3 cu nici o autorizare găsită. ROSSM nu deţine fişierul PRICES.
c. Organigrama 3, pasul 4.
   1) Organigrama 5, paşii 1, 2 şi 3. Public nu este suficient.
d. Organigrama 3, pasul 5.
e. **Organigrama 3, pasul 6**. ROSSM nu are autorizare privată pentru fişierul PRICES.
f. Organigrama 3, paşii 7 şi 8. Fişierul PRICES nu este securizat de o listă de autorizare. Revenire la Organigrama 1 cu nici o autorizare găsită.

3. Organigrama 1, paşii 3 şi 4. DPTSM este profilul de grup pentru ROSSM.
   a. Organigrama 6, paşii 1, 2 şi 3.
      1) Organigrama 4, pasul 1. DPTSM nu deţine fişierl PRICES.
   b. Organigrama 6, pasul 4. DPTSM nu este grupul primar pentru fişierul PRICES.
   c. **Organigrama 6, pasul 6**. Autorizat. (DPTSM are autorizarea *CHANGE.)

Rezultat: ROSSM este autorizat deoarece profilul de grup DPTSM are autorizarea *CHANGE.

Analiză: Folosirea autorizării de grup în acest exemplu este o bună metodă pentru gestiunea autorizărilor. Ea reduce numărul de autorizări private din sistem şi este uşor de înţeles şi de auditat. Însă folosirea autorizării private de grup cauzează de obicei două căutări de autorizări private (pentru utilizator şi pentru grup) când autorizarea publică nu este adecvată. O căutare a autorizării private poate fi evitată făcând ca DPTSM să fie grupul primar pentru fişierul PRICES.

Cazul 2: Folosirea autorizării grupului primar

ANDERSJ are nevoie de autorizarea *CHANGE pentru fişierul CREDIT. ANDERSJ este un membru al grupului DPTAR. Nici ANDERSJ nici DPTAR nu au autorizarea specială *ALLOBJ. Figura 23 arată autorizările pentru fişierul CREDIT.

```
                          Display Object Authority

Object . . . . . :   CREDIT          Owner  . . . . . :   OWNAR
  Library  . . . . :   ACCTSRCV      Primary group  . . :   DPTAR
Object type    . . :   *FILE         ASP device . . . . :   *SYSBAS

Object secured by authorization list  . . . . . :   *NONE

                        Object
User        Group       Authority
OWNAR                   *ALL
DPTAR                   *CHANGE
*PUBLIC                 *USE
```

Figura 23. Autorizarea pentru fişierul CREDIT

Sistemul efectuează aceşti paşi pentru a determina dacă să îi permită lui ANDERSJ accesul *CHANGE la fişierul CREDIT:

1. Organigrama 1, pasul 1.
   a. Organigrama 2, pasul 1. Autorizarea lui DPTAR este autorizarea de grup primar, nu autorizarea privată.
   b. Organigrama 2, paşii 2, 3, 4, 5 şi 6. Autorizarea publică nu este suficientă.
2. Organigrama 1, pasul 2.
   a. Organigrama 3, paşii 1 şi 2. Obiectul de verificat = ACCTSRCV/CREDIT *FILE.
   b. Organigrama 3, pasul 3.

1) Organigrama 4, pasul 1. ANDERSJ nu deţine fişierl CREDIT. Revenire la Organigrama 3 cu nici o autorizare găsită.

c. Organigrama 3, pasul 4.

1) Organigrama 5, pasul 1. Fişierul CREDIT nu are autorizări private.

2) Organigrama 5, pasul 3. Autorizarea publică nu este suficientă. Revenire la Organigrama 3 cu nici o autorizare găsită.

d. Organigrama 3, paşii 5, 7 şi 8. Fişierul CREDIT nu este securizat de o listă de autorizare. Revenire la Organigrama 1 cu nici o autorizare găsită.

3. Organigrama 1, paşii 3 şi 4. ANDERSJ este un membru al profilului de grup DPTAR.

a. Organigrama 6, paşii 1 şi 2. Obiectul de verificat = ACCTSRCV/CREDIT *FILE.

b. Organigrama 6, pasul 3.

1) Organigrama 4, pasul 1. DPTAR nu deţine fişierul CREDIT. Revenire la Organigrama 6 cu nici o autorizare găsită.

c. Organigrama 6, paşii 1 şi 2. Autorizat. DPTAR este grupul primar pentru fişierul CREDIT şi are autorizarea *CHANGE.

Rezultat: ANDERSJ este autorizat deoarece DPTAR este grupul primar pentru fişierul CREDIT şi are autorizarea *CHANGE.

Analiză: Dacă folosiţi autorizarea de grup primar, atunci performanţele verificării autorizării sunt mai bune decât dacă specificaţi autorizare privată pentru grup. Acest exemplu nu necesită nici o căutare de autorizări private.

Cazul 3: Folosirea autorizării publice

Utilizatorul JONESP doreşte accesul la fişierul CREDIT folosind programul CPPGM06. CPPGM06 necesită autorizarea *USE pentru fişier. JONESP este membru al profilului de grup DPTSM şi nu are autorizarea specială *ALLOBJ. Sistemul efectuează aceşti paşi pentru a determina dacă să-i permită lui JONESP accesul la fişierul CREDIT:

1. Organigrama 1, pasul 1.

a. Organigrama 2, pasul 1. Fişierul CREDIT nu are autorizări private. Autorizarea lui DPTAR este autorizarea de grup primar, nu autorizarea privată.

b. Organigrama 2, paşii 2 şi 3. Autorizarea proprietarului (OWNAR) este suficientă.

c. Organigrama 2, paşii 4 şi 5. Autorizarea grupului primar (DPTAR) este suficientă.

d. Organigrama 2, pasul 6. Autorizat. Autorizarea publică este suficientă.

Analiză: Acest exemplu arată câştigul de performanţă obţinut când evitaţui definirea vreunei autorizări private pentru un obiect.

Cazul 4: Folosirea autorizării publice fără căutarea autorizării private

Utilizatorul JONESP doreşte accesul la fişierul PRICES folosind programul CPPGM06. CPPGM06 necesită autorizarea *USE pentru fişier. JONESP este membru al profilului de grup DPTSM şi nu are autorizarea specială *ALLOBJ. Sistemul efectuează aceşti paşi pentru a determina dacă să-i permită lui JONESP accesul la fişierul PRICES:

1. Organigrama 1, pasul 1.

a. Organigrama 2, pasul 1. Fişierul PRICES are autorizări private.

2. Organigrama 1, pasul 2.

a. Organigrama 3, paşii 1 şi 2. Obiectul de verificat = CONTRACTS/PRICES *FILE.

b. Organigrama 3, pasul 3.

1) Organigrama 4, pasul 1. JONESP nu deţine fişierul PRICES. Revenire la Organigrama 3 cu nici o autorizare găsită.

c. Organigrama 3, pasul 4.

1) Organigrama 5, paşii 1, 2 şi 3. Autorizarea publică este suficientă.

2) Organigrama 5, pasul 4. Autorizarea proprietarului este suficientă. (OWNCP are *ALL.)
3) Organigrama 5, pasul 5. Fişierul PRICES nu are un grup primar.
4) Organigrama 5, pasul 6. Autorizat. (Fişierul PRICES nu este securizat de o listă de autorizare.)

Analiză: Acest exemplu arată câştigul de performanţă obţinut când evitaţi definirea vreunor autorizări private pentru un obiect care sunt mai mici decât autorizarea publică. Deşi există autorizări private pentru fişierul PRICES, autorizarea publică este suficientă pentru această cerere şi poate fi folosită fără a căuta autorizări private.

Cazul 5: Folosirea autorizării adoptate

Utilizatorul SMITHG doreşte accesul la fişierul PRICES folosind programul CPPGM08. SMITHG nu este membru al unui grup şi nu are autorizarea specială *ALLOBJ. Programul CPPGM08 necesită autorizarea *CHANGE pentru fişier. CPPGM08 este deţinut de profilul OWNCP şi adoptă autorizarea proprietarului (USRPRF este *OWNER).

1. Organigrama 1, pasul 1.
   a. Organigrama 2, pasul 1.
2. Organigrama 1, pasul 2.
   a. Organigrama 3, paşii 1 şi 2. Obiectul de verificat = CONTRACTS/PRICES *FILE.
   b. Organigrama 3, pasul 3.
      1) Organigrama 4, pasul 1. SMITHG nu deţine fişierul PRICES. Revenire la Organigrama 3 cu nici o autorizare găsită.
   c. Organigrama 3, pasul 4.
      1) Organigrama 5, paşii 1, 2 şi 3. Public nu este suficient.
   d. Organigrama 3, pasul 5.
   e. **Organigrama 3, pasul 6**. SMITHG nu are autorizare privată.
   f. Organigrama 3, paşii 7 şi 8. Fişierul PRICES nu este securizat de o listă de autorizare. Revenire la Organigrama 1 cu nici o autorizare găsită.
3. Organigrama 1, pasul 3. SMITHG nu are un grup.
4. Organigrama 1, pasul 5.
   a. Organigrama 7, pasul 1. Autorizarea publică nu este *AUTL.
   b. Organigrama 7, pasul 3. Obiectul de verificat = CONTRACTS/PRICES *FILE.
   c. Organigrama 7, pasul 4. Autorizarea publică nu este suficientă.
5. Organigrama 1, pasul 6.
   a. Organigrama 8 A, pasul 1. Obiectul de verificat = CONTRACTS/PRICES *FILE.
   b. Organigrama 8 A, paşii 2 şi 3. OWNCP nu are autorizarea *ALLOBJ.
   c. Organigrama 8 A, pasul 4.
      1) Organigrama 4, paşii 1, 2 şi 3. Autorizat. OWNCP deţine fişierul PRICES şi are suficientă autorizare.

Analiză: Acest exemplu demonstrează avantajele de performanţă la folosirea autorizării adoptate când proprietarul programului deţine de asemenea şi obiectele aplicaţiei.

Numărul de paşi necesari pentru a efectua verificarea autorizării nu are aproape nici un efect asupra performanţei, deoarece majoritatea paşilor nu necesită extragerea de noi informaţii. În acest exemplu, deşi sunt efectuaţi mulţi paşi, autorizările private sunt căutate o singură dată (pentru utilizatorul SMITHG).

Comparaţi aceasta cu Cazul 1 de la pagina “Cazul 1: Folosirea autorizării private de grup” la pagina 158.

- Dacă aţi schimba Cazul 1 astfel încât profilul de grup DPTSM deţine fişierul PRICES şi are autorizarea *ALL asupra lui, caracteristicile de performanţă ale celor două exemple ar fi aceleaşi. Oricum, facerea ca un profil de grup să deţină obiecte aplicaţie poate reprezenta un risc de securitate. Membrii grupului au întotdeauna autorizarea grupului (proprietar), doar dacă nu acordaţi în mod specific membrilor grupului o autorizare mai mică. Când folosiţi autorizarea adoptată, puteţi controla situaţiile în care este folosită autorizarea proprietarului.

- Puteţi de asemenea schimba Cazul 1 astfel încât DPTSM este grupul primar pentru fişierul PRICES şi are autorizare *CHANGE asupra lui. Dacă DPTSM este primul grup pentru SMITHG (specificat în parametrul GRPPRF al profilului de utilizator al lui SMITHG), caracteristicile de performanţă ar fi la fel ca în Cazul 5.

Cazul 6: Autorizarea de utilizator şi de grup

Utilizatorul WILSONJ doreşte să acceseze fişierul PRICES folosind programul CPPGM01, care necesită autorizarea *CHANGE. WILSONJ este membru al profilului de grup DPTSM şi nu are autorizarea specială *ALLOBJ. Programul CPPGM01 nu foloseşte autorizarea adoptată, şi ignoră orice autorizare adoptată anterior (USEADPAUT este *NO).

1. Organigrama 1, pasul 1.
   a. Organigrama 2, pasul 1. PRICES are autorizări private.
2. Organigrama 1, pasul 2.
   a. Organigrama 3, paşii 1 şi 2. Obiectul de verificat = CONTRACTS/PRICES *FILE.
   b. Organigrama 3, pasul 3.
      1) Organigrama 4, pasul 1. WILSONJ nu deţine fişierul PRICES. Revenire la Organigrama 3 cu nici o autorizare găsită.
   c. Organigrama 3, pasul 4.
      1) Organigrama 5, paşii 1, 2 şi 3. Public nu este suficient.
   d. Organigrama 3, pasul 5.
   e. **Organigrama 3, pasul 6**. WILSONJ are autorizarea *USE, care nu este suficientă.
   f. Organigrama 3, pasul 8. Obiectul de testat = CONTRACTS/PRICES *FILE. Revenire la Organigrama 1 cu autorizare insuficientă.
3. Organigrama 1, pasul 6.
   a. Organigrama 8 A, pasul 1. Obiectul de verificat = CONTRACTS/PRICES *FILE.
   b. Organigrama 8 A, pasul 2. Programul CPPGM01 nu adoptă autorizarea.
   c. Organigrama 8 A, pasul 5. Parametrul *USEADPAUT pentru programul CPPGM01 este *NO.
   d. Organigrama 8 A, paşii 8 şi 9.
      1) Organigrama 8 B, pasul 1. Programul CPPGM01 nu adoptă autorizarea.
      2) Organigrama 8 B, pasul 7. Parametrul *USEADPAUT pentru programul CPPGM01 este *NO. Accesul este interzis.

Analiză: Acest exemplu demonstrează că unui utilizator îi poate fi interzis accesul la un obiect chiar dacă grupul utilizatorului are autorizare suficientă.

Acordarea pentru un utilizator a aceleiaşi autorizării ca şi publicul dar mai mică decât grupul utilizatorului nu afectează performanţele verificării autorizării pentru alţi utilizatori. Oricum, dacă WILSONJ ar avea autorizarea *EXCLUDE (mai mică decât publicul), atunci aţi pierde beneficiile de performanţă arătate în Cazul 4.

Deşi acest exemplu are mulţi paşi, autorizările private sunt căutate o singură dată. Aceasta ar oferi performanţe acceptabile.

Cazul 7: Autorizarea publică fără autorizare privată

Informaţiile de autorizare pentru fişierul ITEM arată astfel:

```
                          Display Object Authority

Object . . . . . :   ITEM           Owner  . . . . . :   OWNIC
  Library  . . . . :   ITEMLIB       Primary group  . . :   *NONE
Object type  . . . :   *FILE         ASP device   . . . :   *SYSBAS

Object secured by authorization list  . . . . . . . . . . . :   *NONE

                       Object
User        Group      Authority
OWNIC                  *ALL
*PUBLIC                *USE
```

Figura 24. Display Object Authority - Afişare autorizare obiect

ROSSM are nevoie de autorizarea *USE pentru fişierul ITEM. ROSSM este membru al profilului de grup DPTSM. Aceştia sunt paşii verificării autorizării:

1. Organigrama 1, pasul 1.
   a. Organigrama 2, paşii 1, 2 şi 3. Autorizarea lui OWNIC este suficientă.
   b. Organigrama 2, pasul 4. Fişierul ITEM nu are un grup primar.
   c. Organigrama 2, pasul 6. Autorizat. Autorizarea publică este suficientă.

Analiză: Autorizarea publică oferă cele mai bune performanţe când este folosită fără autorizări private. În acest exemplu, autorizările private nu sunt căutate deloc.

Cazul 8: Autorizarea adoptată fără autorizare privată

Pentru acest exemplu, toate programele din aplicaţie sunt deţinute de profilul OWNIC. Orice program din aplicaţie care necesită o autorizare mai mare decât *USE adoptă autorizarea proprietarului. Aceştia sunt paşii pentru ca utilizatorul WILSONJ să obţină autorizarea *CHANGE pentru fişierul ITEM când foloseşte programul ICPGM10, care adoptă autorizarea:

1. Organigrama 1, pasul 1.
   a. Organigrama 2, paşii 1, 2, 3, 4 şi 6. Autorizarea publică nu este suficientă.
2. Organigrama 1, pasul 2.
   a. Organigrama 3, paşii 1 şi 2. Obiectul de verificat = ITEMLIB/ITEM *FILE.
   b. Organigrama 3, pasul 3.
      1) Organigrama 4, pasul 1. WILSONJ nu deţine fişierul ITEM. Revenire la Organigrama 3 cu nici o autorizare găsită.
   c. Organigrama 3, pasul 4.
      1) Organigrama 5, paşii 1 şi 3. Autorizarea publică nu este suficientă. Revenire la Organigrama 3 cu nici o autorizare găsită.
   d. Organigrama 3, paşii 5, 7 şi 8. Fişierul ITEM nu este securizat de o listă de autorizare. Revenire la Organigrama 1 cu nici o autorizare găsită.
3. Organigrama 1, paşii 3 şi 5. (WILSONJ nu are un profil de grup.)
   a. Organigrama 7, paşii 1, 3 şi 4. Publicul are autorizarea *USE, care nu este suficientă.
4. Organigrama 1, pasul 6.
   a. Organigrama 8 A, pasul 1. Obiectul de verificat = ITEMLIB/ITEM *FILE.
   b. Organigrama 8 A, paşii 2, 3 şi 4. Profilul OWNIC nu are autorizarea *ALLOBJ.
      1) Organigrama 4, paşii 1, 2 şi 3. Autorizat. OWNIC are autorizare suficientă pentru fişierul ITEM.

Analiză: Acest exemplu arată beneficiile folosirii autorizării adoptate fără autorizarea privată, în special dacă proprietarul programelor deţine de asemenea obiectele aplicaţiei. Acest exemplu nu a necesitat căutarea de autorizări private.

Cazul 9: Folosirea unei liste de autorizare

Fişierul ARWKR01 din biblioteca CUSTLIB este securizat de lista de autorizare ARLST1. Figura 25 şi Figura 26 arată autorizările:

```
                        Display Object Authority

Object . . . . . :   ARWRK01       Owner  . . . . . :   OWNAR
  Library  . . . . :   CUSTLIB      Primary group  . . :   *NONE
Object type  . . . :   *FILE        ASP device . . . . :   *SYSBAS

Object secured by authorization list. . . . . . . . . . . :   ARLST1

                       Object
User        Group      Authority
OWNCP                  *ALL
*PUBLIC                *USE
```

Figura 25. Autorizarea pentru fişierul ARWRK01

```
                         Display Authorization List

Object . . . . . :   ARLST1      Owner  . . . . . :   OWNAR
  Library  . . . . :   QSYS       Primary group  . . :   *NONE

                       Object     List
User        Group      Authority  Mgt
OWNCP                  *ALL
AMESJ                  *CHANGE
*PUBLIC                *USE
```

Figura 26. Autorizarea pentru lista de autorizare ARLST1

Utilizatorul AMESJ, care nu este membru al unui profil de grup, necesită autorizarea *CHANGE pentru fişierul ARWRK01. Aceştia sunt paşii verificării autorizării:

1. Organigrama 1, pasul 1.
   a. Organigrama 2, paşii 1 şi 2. Fişierul ARWRK01 este securizat de o listă de autorizare.
2. Organigrama 1, pasul 2.
   a. Organigrama 3, paşii 1 şi 2. Obiectul de verificat = CUSTLIB/ARWRK01 *FILE.
   b. Organigrama 3, pasul 3.
      1) Organigrama 4, pasul 1. AMESJ nu deţine fişierl ARWRK01. Revenire la Organigrama 2 cu nici o autorizare găsită.
   c. Organigrama 3, pasul 4.
      1) Organigrama 5, paşii 1 şi 3. Autorizarea publică nu este suficientă. Revenire la Organigrama 3 cu nici o autorizare găsită.
   d. Organigrama 3, paşii 5, 7 şi 9. Obiectul de verificat = ARLST1 *AUTL.
   e. Organigrama 3, pasul 3.

1) Organigrama 4, pasul 1. AMESJ nu deţine lista de autorizare ARLST1. Revenire la Organigrama 3 cu nici o autorizare găsită.

f. Organigrama 3, paşii 4 şi 5.

g. **Organigrama 3, pasul 6**. Autorizat. AMESJ are autorizarea *CHANGE pentru lista de autorizare ARLST1.

Analiză: Acest exemplu demonstrează că listele de autorizare pot face ca autorizările să fie mai uşor de gestionat şi oferă performanţe bune. Acest lucru este adevărat mai ales dacă obiectele securizate de lista de autorizare nu au autorizări private.

Dacă AMESJ ar fi fost membru al unui profil de grup, aceasta ar adăuga paşi suplimentari la acest exemplu, dar nu ar adăuga o căutare suplimentară a autorizărilor private, atâta vreme cât nu sunt definite autorizări private pentru fişierul ARWRK01. Problemele de performanţă este cel mai probabil să apară când autorizările private, listele de autorizare şi profilurile de grup sunt combinate, ca în “Cazul 11: Combinarea metodelor de autorizare” la pagina 166.

Cazul 10: Folosirea mai multor grupuri

WOODBC necesită autorizarea *CHANGE pentru fişierul CRLIM. WOODBC este membru al trei grupuri: DPTAR, DPTSM şi DPTMG. DPTAR este primul profil de grup (GRPPRF). DPTSM şi DPTMG sunt profiluri de grup suplimentare (supplemental group profiluris - SUPGRPPRF). Figura 27 arată autorizările pentru fişierul CRLIM:

```
                          Display Object Authority

Object . . . . . :   CRLIM          Owner  . . . . . :   OWNAR
  Library  . . . . :   CUSTLIB       Primary group  . . :   DPTAR
Object type    . . :   *FILE         ASP device . . . . :   *SYSBAS

 Object secured by authorization list  . . . . . . . . . . . :   *NONE

                       Object
User        Group      Authority
OWNAR                  *ALL
DPTAR                  *CHANGE
DPTSM                  *USE
*PUBLIC                *EXCLUDE
```

Figura 27. Autorizarea pentru fişierul CRLIM

Aceştia sunt paşii verificării autorizării:

1. Organigrama 1, pasul 1.
   a. Organigrama 2, pasul 1. Revenire la diagrama de flux apelantă cu autorizare insuficientă.
2. Organigrama 1, pasul 2.
   a. Organigrama 3, paşii 1 şi 2. Obiectul de verificat = CUSTLIB/CRLIM *FILE.
   b. Organigrama 3, pasul 3.
      1) Organigrama 4, pasul 1. WOODBC nu deţine fişierul CRLIM. Revenire la Organigrama 3 cu nici o autorizare găsită.
   c. Organigrama 3, pasul 4.
      1) Organigrama 5, paşii 1, 2 şi 3. Autorizarea publică nu este suficientă.
   d. Organigrama 3, pasul 5.
   e. **Organigrama 3, pasul 6**. WOODBC nu are nici o autorizare pentru fişierul CRLIM.
   f. Organigrama 3, paşii 7 şi 8. Fişierul CRLIM nu este securizat de o listă de autorizare. Revenire la Organigrama 1 cu nici o autorizare găsită.
3. Organigrama 1, paşii 3 şi 4. Primul grup pentru WOODBC este DPTAR.

a. Organigrama 6, paşii 1 şi 2. Obiectul de verificat = CUSTLIB/CRLIM *FILE.
b. Organigrama 6, pasul 3.
   1) Organigrama 4, pasul 1. DPTAR nu deţine fişierul CRLIM. Revenire la Organigrama 6 cu nici o autorizare găsită.
c. Organigrama 6, paşii 4 şi 5. Autorizat. DPTAR este grupul primar şi are autorizare suficientă.

Cazul 11: Combinarea metodelor de autorizare

WAGNERB necesită autorizarea *ALL pentru fişierul CRLIMWRK. WAGNERB este membru al acestor grupuri: DPTSM, DPT702 şi DPTAR. Primul grup (first group - GRPPRF) al lui WAGNERB este DPTSM. Figura 28 arată autorizarea pentru fişierul CRLIMWRK.

```
                          Display Object Authority

Object . . . . . :   CRLIMWRK        Owner  . . . . . :   OWNAR
  Library  . . . . . :   CUSTLIB         Primary group  . . . :   *NONE
Object type    . . . :   *FILE          ASP device . . . . . :   *SYSBAS

Object secured by authorization list  . . . . . . . . . . . :   CRLST1

                        Object
User        Group       Authority
OWNAR                   *ALL
DPTSM                   *USE
WILSONJ                 *EXCLUDE
*PUBLIC                 *USE
```

Figura 28. Autorizarea pentru fişierul CRLIMWRK

Fişierul CRLIMWRK este securizat de lista de autorizare CRLST1. Figura 29 arată autorizarea pentru lista de autorizare CRLST1.

```
                        Display Authorization List

Object . . . . . :   CRLST1        Owner  . . . . . :   OWNAR
  Library  . . . . . :     QSYS        Primary Group  . . . :   DPTAR

                        Object    List
User        Group       Authority  Mgt
OWNAR                   *ALL        X
DPTAR                   *ALL
*PUBLIC                 *EXCLUDE
```

Figura 29. Autorizarea pentru Lista de autorizare CRLST1

Acest exemplu arată multe dintre posibilitpţile de verificare a autorizării. De asemenea el demonstrează cum folosirea a prea multe opţiuni de autorizare pentru un obiect poate conduce la performanţe scăzute.

În continuare sunt paşii necesari pentru a verifica autorizarea lui WAGNERB pentru fişierul CRLIMWRK:

1. Organigrama 1, pasul 1.
   a. Organigrama 2, pasul 1.
2. Organigrama 1, pasul 2.
   a. Organigrama 3, paşii 1 şi 2. Obiectul de verificat = CUSTLIB/CRLIMWRK *FILE.

b. Organigrama 3, pasul 3.
   1) Organigrama 4, pasul 1. WAGNERB nu deţine fişierul CRLIMWRK. Revenire la Organigrama 3 cu nici o autorizare găsită.
c. Organigrama 3, pasul 4.
   1) Organigrama 5, paşii 1 şi 2. WILSONJ are autorizarea *EXCLUDE, care este mai mică decât autorizarea publică *USE.
d. Organigrama 3, paşii 5 şi 6 (**se caută mai întâi autorizările private**). WAGNERB nu are autorizare privată.
e. Organigrama 3, paşii 7 şi 9. Obiectul de verificat = CRLST1 *AUTL.
f. Organigrama 3, pasul 3.
   1) Organigrama 4, pasul 1. WILSONJ nu deţine CRLST1. Revenire la Organigrama 3 cu nici o autorizare găsită.
g. Organigrama 3, paşii 4 şi 5.
h. Organigrama 3, pasul 6 (**a doua căutare a autorizărilor private**). WAGNERB nu are autorizare privată pentru CRLST1.
i. Organigrama 3, paşii 7 şi 8. Obiectul de verificat = CUSTLIB/CRLIMWRK *FILE.

3. Organigrama 1, paşii 3 şi 4. Primul profil de grup al lui WAGNERB este DPTSM.
   a. Organigrama 6, paşii 1 şi 2. Obiectul de verificat = CUSTLIB/CRLIMWRK *FILE.
   b. Organigrama 6, pasul 3.
      1) Organigrama 4, pasul 1. DPTSM nu deţine fişierul CRLIMWRK. Revenire la Organigrama 6 cu nici o autorizare găsită.
   c. Organigrama 6, pasul 4. DPTSM nu este grupul primar pentru fişierul CRLIMWRK.
   d. Organigrama 6, pasul 6 (**a treia căutare a autorizărilor private**). DPTSM are autorizarea *USE pentru fişierul CRLIMWRK, care nu este suficientă.
   e. Organigrama 6, pasul 6 continuat. Autorizarea *USE este adăugată la autorizările deja găsite pentru grupurile lui WAGNERB (nici una). Nu a fost încă găsită o autorizare suficientă.
   f. Organigrama 6, paşii 9 şi 10. Următorul grup al lui WAGNERB este DPT702.
   g. Organigrama 6, paşii 1 şi 2. Obiectul de verificat = CUSTLIB/CRLIMWRK *FILE.
   h. Organigrama 6, pasul 3.
      1) Organigrama 4, pasul 1. DPT702 nu deţine fişierul CRLIMWRK. Revenire la Organigrama 6 cu nici o autorizare găsită.
   i. Organigrama 6, pasul 4. DPT702 nu este grupul primar pentru fişierul CRLIMWRK.
   j. Organigrama 6, pasul 6 (**a patra căutare a autorizărilor private**). DPT702 nu are autorizare pentru fişierul CRLIMWRK.
   k. Organigrama 6, paşii 7 şi 8. Obiectul de verificat = CRLST1 *AUTL
   l. Organigrama 6, pasul 3.
      1) Organigrama 5, pasul 1. DPT702 nu deţine lista de autorizare CRLST1. Revenire la Organigrama 6 cu nici o autorizare găsită.
   m. Organigrama 6, paşii 4 şi 6. (**a cincea căutare a autorizărilor private**). DPT702 nu are autorizare pentru lista de autorizare CRLST1.
   n. Organigrama 6, paşii 7, 9 şi 10. DPTAR este următorul profil de grup al lui WAGNERB.
   o. Organigrama 6, paşii 1 şi 2. Obiectul de verificat = CUSTLIB/CRLIMWRK *FILE.
   p. Organigrama 6, pasul 3.
      1) Organigrama 4, pasul 1. DPTAR nu deţine fişierul CRLIMWRK. Revenire la Organigrama 6 cu nici o autorizare găsită.
   q. Organigrama 6, paşii 4 şi 6. (**a şasea căutare a autorizărilor private**). DPTAR nu are autorizare pentru fişierul CRLIMWRK.
   r. Organigrama 6, paşii 7 şi 8. Obiectul de verificat = CRLST1 *AUTL

s. Organigrama 6, pasul 3.
   1) Organigrama 4, pasul 1. DPTAR nu deţine lista de autorizare CRLST1. Revenire la Organigrama 6 cu nici o autorizare găsită.
t. Organigrama 6, paşii 4 şi 5. Autorizat. DPTAR este grupul primar pentru lista de autorizare CRLST1 şi are autorizarea *ALL.

Rezultat: WAGNERB este autorizat să efectueze operaţia cerută folosind autorizarea grupului primar al lui DPTAR pentru lista de autorizare CRLIST1.

Analiză: Acest exemplu demonstrează o proiectare slabă a autorizărilor, atât din punct de vedere al gestiunii, cât şi din punct de vedere al performanţelor. Sunt folosite prea multe opţiuni, ceea ce face dificilă înţelegerea, modificarea şi auditarea. Autorizările private sunt căutate de 6 ori, ceea ce poate produce probleme de performanţă observabile:

Profil	Obiect	Tip	Rezultat
WAGNERB	CRLIMWRK	*FILE	Nici o autorizare găsită
WAGNERB	CRLST1	*AUTL	Nici o autorizare găsită
DPTSM	CRLIMWRK	*FILE	Autorizare *USE (insuficientă)
DPT702	CRLIMWRK	*FILE	Nici o autorizare găsită
DPT702	CRLST1	*AUTL	Nici o autorizare găsită
DPTAR	CRLIMWRK	*FILE	Nici o autorizare găsită

Schimbarea secvenţei profilurilor de grup ale lui WAGNERB ar schimba caracteristicile de performanţă ale acestui exemplu. Să presupunem că DPTAR este primul profil de grup al lui WAGNERB (first group profiluri - GRPPRF). Sistemul ar căuta autorizările private de 3 ori înainte de a găsi autorizarea grupului primar al lui DPTAR pentru lista de autorizare CRLST1.

- Autorizarea lui WAGNERB pentru fişierul CRLIMWRK
- Autorizarea lui WAGNERB pentru lista de autorizare CRLST1
- Autorizarea lui DPTAR pentru fişierul CRLIMWRK

Planificarea cu grijă a profilurilor de grup şi a listelor de autorizare este esenţială pentru performanţe bune ale sistemului.

Cache-ul de autorizări

În Versiunea 3, Ediţia 7, sistemul creează un cache de autorizări pentru un utilizator prima dată când utilizatorul accesează un obiect. De fiecare dată când obiectul este accesat, sistemul caută autorizarea în cache-ul utilizatorului înainte de a căuta în profilul utilizatorului. Aceasta rezultă într-o verificare mai rapidă a autorizării private.

Cache-ul de autorizare conţine până la 32 autorizări private pentru obiecte şi până la 32 autorizări private pentru listele de autorizare. Cache-ul este actualizat când o autorizare este acordată sau revocată utilizatorului. Toate cache-urile utilizator sunt curăţate când este efectuat IPL-ul sistemului.

Cât timp este recomandată folosirea limitată a autorizărilor private, cache-ul oferă flexibilitate. De exemplu, puteţi alege cum să securizaţi obiecte cu mai puţină grijă legată de impactul asupra performanţelor sistemului. Acest lucru este adevărat în mod special dacă utilizatorii accesează aceleaşi obiecte în mod repetat.

Capitolul 6. Securitate control funcţionare

Acest capitol discută probleme de securitate asociate cu controlul funcţionării in sistem:

- Iniţiere job
- Staţii de lucru
- Descrieri de subsitem
- Descrieri de job
- Liste de biblioteci
- Tipărire
- Atribute reţea
- Reglare performanţă

Pentru informaţii complete despre subiectele de control funcţionare, vedeţi cartea *Work Management*.

Iniţiere job

Când porniţi un job în sistem, obiectele sunt asociate cu jobul, cum ar fi o coadă de ieşire, o descriere de job şi bibliotecile din lista de biblioteci. Autorizarea pentru unele dintre aceste obiecte este verificată înainte de a se permite jobului să pornească şi este verificată pentru alte obiecte după ce porneşte jobul. Autorizarea necorespunzătoare poate cauza erori sau oprirea jobului.

Obiectele care sunt parte a structurii jobului pot fi specificate în descrierea de job, profilul utilizator şi în comanda SBMJOB (Submit Job - Lansare job) pentru un job batch.

Pornirea unui job interactiv

Următoarea este o descriere a activităţii de securitate realizate când un job interactiv este pornit. Pentru că există multe posibilităţi pentru specificarea obiectelor folosite de către un job, acesta este doar un exemplu.

Când un eşec de autorizare survine în timpul procesului de semnare, în partea de jos a ecranului de Semnare apare un mesaj care descrie eroarea. Unele eşecuri de autorizare cauzează de asemenea scrierea în istoricul jobului. Dacă un utilizator nu poate să se semneze din cauza unui eşec de autorizare, modificaţi fie profilul utilizator pentru a specifica un obiect diferit sau acordaţi autorizarea utilizator pentru obiect.

După ce utilizatorul introduce un ID utilizator şi parola, aceşti paşi sunt realizaţi înainte de pornirea efectivă a unui job în sistem:

1. Sunt verificate profilul utilizator şi parola. Starea profilului utilizator trebuie să fie *ENABLED. Profilul utilizator care este specificat pe ecranul de semnare trebuie să aibă autorizările *OBJOPR şi *CHANGE.
2. Autorizarea utilizator de folosit la verificarea staţiei de lucru. Vedeţi “Staţii de lucru” la pagina 171 pentru detalii.
3. Sistemul verifică autorizarea pentru valorile din profilul utilizator şi din descrierea de job utilizator care sunt folosite pentru a construi structura jobului, cum este:
   - Descriere de job
   - Coadă de ieşire
   - Bibliotecă curentă
   - Biblioteci în lista de biblioteci

   Dacă oricare dintre aceste obiecte nu există sau utilizatorul nu are autorizarea corespunzătoare, este afişat un mesaj în partea de jos a ecranului de Semnare şi utilizatorul nu poate să se semneze. Dacă autorizarea este verificată cu succes pentru aceste obiecte, jobul este pornit în sistem.

Notă: Autorizarea pentru dispozitivul de tipărire şi coada de joburi nu este verificată până când utilizatorul nu încearcă să le folosească.

După ce este pornit jobul, sunt realizaţi aceşti paşi înainte ca utilizatorul să vadă primul ecran sau meniu:

1. Dacă intrarea de rutare pentru job specifică un program utilizator, verificarea autorizării normale este făcută pentru program, biblioteca program şi orice obiecte folosite de către program. Dacă autorizarea nu este corespunzătoare, este trimis un mesaj utilizatorului pe ecranul de Semnare şi se opreşte jobul.
2. Dacă intrare de rutare specifică comanda procesor (QCMD):
   a. Verificarea de autorizare este făcută pentru programul procesor QCMD, biblioteca program şi orice obiecte folosite aşa cum este descris la pasul 1.
   b. Autorizarea utilizator pentru programul şi biblioteca tratare-tastă-atenţie este verificată. Dacă autorizarea nu este corespunzătoare, este trimis un mesaj utilizatorului şi este scris în istoricul jobului. Procesarea continuă.

      Dacă autorizarea este corespunzătoare, programul tratare-tastă-atenţie este activat. Programul nu este pornit până la prima apăsare a tastei Atenţie de către utilizator. La acel moment, este făcută verificarea autorizării normale pentru obiectele folosite de către program.
   c. Verificarea autorizării normale este făcută pentru programul iniţial (şi obiectele sale asociate) specificate în profilul utilizator. Dacă autorizarea este corespunzătoare, programul este pornit. Dacă autorizarea nu este corespunzătoare, este trimis un mesaj utilizatorului şi este scris în istoricul jobului. Jobul se opreşte.
   d. Verificarea autorizării normale este făcută pentru meniul iniţial (şi obiectele sale asociate) specificate în profilul utilizator. Dacă autorizarea este corespunzătoare, meniul este afişat. Dacă autorizarea nu este corespunzătoare, este trimis un mesaj utilizatorului şi este scris în istoricul jobului. Jobul se opreşte.

Pornirea unui job batch

Următoarea este o descriere a activităţii de securitate realizate când un job batch este pornit. Deoarece există mai multe metode pentru lansarea de joburi batch şi pentru specificarea obiectelor folosite de către job, aceasta este doar linie de îndrumare. Acest exemplu foloseşte un job lansat de la un job interactiv folosind comanda SBMJOB (submit job - lansare job).

Când introduceţi comanda SBMJOB, această verificare este realizată înainte ca jobul să fie adăugat în coada de joburi:

1. Dacă specificaţi un profil utilizator în comanda SBMJOB, trebuie să aveţi autorizarea *USE pentru profilul utilizator.
2. Autorizarea este verificată pentru obiectele specificate ca parametrii în comanda SBMJOB şi în descrierea de job. Autorizarea este verificată pentru profilul utilizator sub care rulează jobul.
3. Dacă nivelul de securitate este 40 şi comanda SBMJOB specifică USER(*JOBD), utilizatorul care lansează jobul trebuie să aibă autorizarea *USE pentru profilul utilizator din descrierea de job.
4. Dacă autorizarea nu este corespunzătoare, este trimis un mesaj utilizatorului şi jobul nu este lansat.

Când sistemul selectează jobul din coada de joburi şi încearcă să pornească jobul, the job, secvenţa de verificare autorizare este similară cu secvenţa pentru pornirea unui job interactiv.

Autorizarea adoptată şi joburile batch

Când este pornit un job nou, este creată o nouă stivă program pentru job. Autorizarea adoptată nu poate avea efect până când primul program este adăugat în stiva program. Autorizarea adoptată nu poate fi folosită pentru a obţine acces la orice obiecte, cum este o coadă de ieşire sau o descriere de job, care sunt adăugate la structura jobului înainte ca jobul să fie rutat. Prin urmare, chiar dacă jobul dumneavoastră interactiv rulează sub autorizare adoptată când lansaţi jobul, acea autorizare adoptată nu este folosită când autorizarea este verificată pentru obiectele din cererea dumneavoastră SBMJOB.

Puteţi modifica caracteristicile unui job batch când aşteaptă să ruleze, folosind comanda CHGJOB (Change Job - Modifică job). Vedeţi 353 pentru autorizarea care este necesară pentru a modifica parametrii pentru un job.

Staţii de lucru

O **descriere de dispozitiv** conţine informaţii despre un dispozitiv particular sau o unitate logică care este ataşată sistemului. Când vă semnaţi în sistem, staţia dumneavoastră de lucru este ataşată fie la o descriere de dispozitiv fizic sau virtual. Pentru a semna cu succes, trebuie să aveţi autorizarea *CHANGE pentru descrierea de dispozitiv.

Valoarea de sistem QLMTSECOFR (limită responsabil cu securitatea) controlează dacă utilizatorii cu autorizarea specială *ALLOBJ sau *SERVICE trebuie să fie autorizaţi specific pentru descrierile de dispozitiv.

Figura 30 la pagina 172 arată logica pentru a determina dacă unui utilizator îi este permis să se semneze la un dispozitiv:

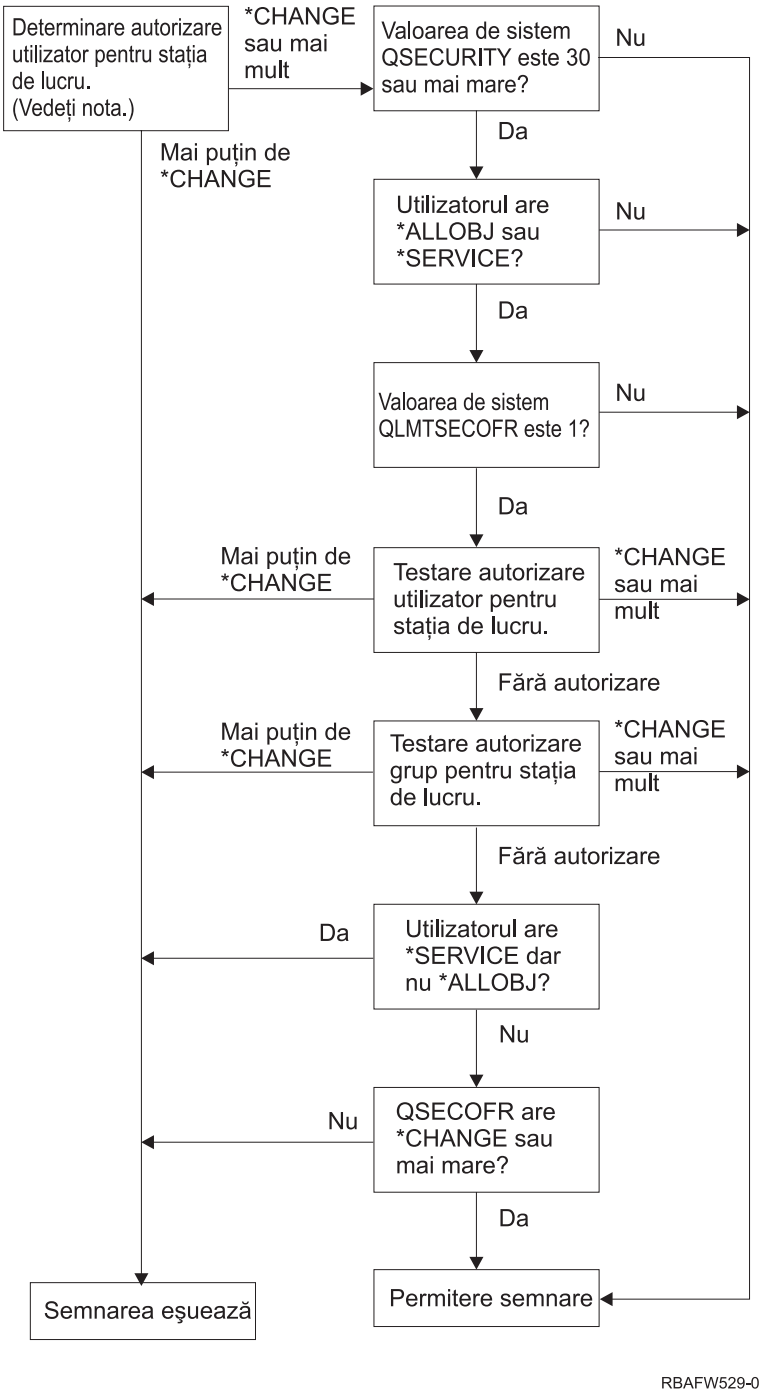

Figura 30. Verificare autorizare pentru Staţii de lucru

Notă: Verificarea autorizării normale este realizată pentru a determina dacă un utilizator are cel puţin autorizarea *CHANGE pentru o descriere de dispozitiv. Autorizarea *CHANGE poate fi găsită utilizând următoarele:

- Autorizarea specială *ALLOBJ din profilul utilizator, profilul de grup sau profilurile de grup suplimentare.
- Autorizarea privată pentru descrierea de dispozitiv din profilul utilizator, profilul de grup sau profilurile de grup suplimentare.
- Autorizarea pentru o listă de autorizăţii folosită pentru a securiza descrierea de dispozitiv.
- Autorizarea pentru o listă de autorizăţii folosită pentru a securiza autorizarea publică.

Verificarea de autorizare pentru descrierea de dispozitiv este făcută înainte ca orice programe să fie în stiva program pentru job; de aceea autorizarea adoptată nu se aplică.

Descrierea Verificării autorizare pentru Staţiile de lucru

Sistemul determină autorizarea utilizator pentru staţia de lucru. (Vedeţi nota 1) Dacă autorizarea este mai puţin decât *CHANGE atunci semnarea eşuează. Dacă autorizarea este *CHANGE sau mai mare atunci sistemul verifică pentru a vedea dacă nivelul de securitate al sistemului este 30 sau mai înalt. Dacă nu este, atunci utilizatorului îi este permis să se semneze.

Dacă nivelul de securitate este 30 sau mai înalt, sistemul verifică dacă utilizatorul are autorizările speciale *ALLOBJ sau *SERVICE. Dacă utilizatorul nu are nici una din aceste autorizări speciale, atunci semnarea este permisă.

Dacă utilizatorul are una din autorizările speciale *ALLOBJ sau *SERVICE, atunci sistemul verifică dacă valoarea de sistem QLMTSECOFR este setată la 1. Dacă nu este setată la 1, atunci semnarea este permisă.

Dacă valoarea de sistem QLMTSECOFR este setată la 1, atunci sistemul va testa autorizarea utilizator pentru staţia de lucru. Dacă autorizarea utilizator este *CHANGE sau mai înaltă, atunci semnarea este permisă. Dacă autorizarea utilizator este mai puţin decât *CHANGE, semnarea eşuează. Dacă utilizatorul nu are nici o autorizare pentru staţia de lucru, sistemul verifică autorizarea de grup utilizator pentru staţia de lucru.

Dacă autorizarea de grup utilizator este *CHANGE sau mai înaltă, atunci semnarea este permisă. Dacă autorizarea de grup utilizator este mai puţin decât *CHANGE, semnarea eşuează. Dacă utilizatorul nu are nici o autorizare pentru staţia de lucru, sistemul verifică dacă utilizatorul are sau nu autorizarea specială *SERVICE, dar nu şi autorizarea specială *ALLOBJ.

Dacă utilizatorul are autorizarea specială *SERVICE, dar nu are autorizarea specială *ALLOBJ atunci semnarea eşuează. Dacă utilizatorul are autorizarea specială *SERVICE, dar nu are autorizarea specială *ALLOBJ, atunci sistemul verifică dacă QSECOFR are *CHANGE sau mai înaltă.

Dacă QSECOFR nu are *CHANGE sau mai înaltă, semnarea eşuează. Dacă QSECOFR are *CHANGE sau mai înaltă, atunci semnarea este permisă.

Profilurilor utilizator responsabil cu securitatea (QSECOFR), service (QSRV), service de bază (QSRVBAS) li se permite întotdeauna să se semneze la consolă. Valoarea de sistem QCONSOLE (consolă) este folosită pentru a determina care dispozitiv este consola. Dacă profilurile QSRV sau QSRVBAS încearcă să se semneze la consolă şi nu au autorizarea *CHANGE, sistemul acordă autorizarea *CHANGE profilului şi îi permite să se semneze.

Proprietatea asupra descrierilor de dispozitiv

Autorizarea publică implicită pentru comenzile CRTDEVxxx este *LIBCRTAUT. Dispozitivele sunt create în biblioteca QSYS, care este livrată cu o valoare CRTAUT a *SYSVAL. Valoroarea livrată pentru valoarea de sistem QCRTAUT este *CHANGE.

Pentru a limita utilizatorii care se pot semna la o staţie de lucru, setaţi autorizarea publică pentru staţia de lucru la *EXCLUDE şi daţi autorizarea *CHANGE grupurilor sau utilizatorilor specifici.

Responsabil cu securitatea (QSECOFR) nu este autorizarea dată anume pentru orice dispozitiv. Dacă valoarea de sistem QLMTSECOFR este setată la 1 (YES), trebuie să daţi autorizarea responsabil cu securitatea *CHANGE dispozitivelor. Oricine cu autorizarea *OBJMGT şi *CHANGE pentru un dispozitiv poate da autorizarea *CHANGE altui utilizator.

Dacă o descriere de dispozitiv este creată de către responsabilul cu securitatea, acesta deţine acel dispozitiv şi îi este data autorizarea specifică *ALL pentru acel dispozitiv. Când sistemul configurează automat dispozitive, cele mai multe dintre ele sunt deţinute de către profilul QPGMR. Dispozitivele create de programul QLUS (dispozitive tip *APPC) sunt deţinute de către profilul QSYS.

Dacă planificaţi să folosiţi valoarea de sistem QLMTSECOFR pentru a limita unde să se poată semna responsabilul cu securitatea, orice dispozitive pe care le creaţi trebuie să fie deţinute de un alt profil decât QSECOFR.

Pentru a modifica dreptul de proprietate al unei descrieri de dispozitiv afişare, dispozitivul trebuie să fie alimentat şi activat. Semnaţi-vă la dispozitiv şi modificaţi dreptul de proprietate folosind comanda CHGOBJOWN. Dacă nu sunteţi semnat la dispozitiv, trebuie să alocaţi dispozitivul înainte să modificaţi dreptul de proprietate, folosind comnada ALCOBJ (Allocate Object - Alocare obiect). Puteţi aloca dispozitivul doar dacă nimeni nu îl foloseşte. După ce aţi modificat dreptul de proprietate, dezalocaţi dispozitivul folosind comanda DLCOBJ (Deallocate Object - Dezalocare obiect).

Fişierul de afişare pentru ecranul de semnare

Administratorul de sistem poate modifica ecranul de semnare sistem pentru a adăuga text sau logo-ul companiei. Trebuie să aveţi grijă pentru a fi sigur că numele câmpului sau lungimile buffer-ului fişierului de afişare nu sunt modificate când se adaugă text la fişierul de afişare. Modificarea numelor câmpului sau a lungimilor buffer-ului poate cauza eşecul semnării.

Modificarea afişării ecranului de semnare

Codul sursă pentru fişierul de afişare semnare este livrat cu sistemul de operare. Sursa este livrată în fişierul QSYS/QAWTSSRC. Acest cod sursă poate fi modificat pentru a adăuga text la afişarea ecranului de semnare. Numele de câmp şi lungimile buffer-ului nu trebuie modificate.

Sursa fişierului de afişare pentru ecranul de semnare

Sursa pentru fişierul de afişare semnare este livrată ca un membru (QDSIGNON sau QDSIGNON2) în fişierul fizic QSYS/QAWTSSRC. QDSIGNON conţine sursa pentru sursa ecranul de semnare folosit când valoarea de sistem QPWDLVL este setată la 0 sau la 1. Membrul QDSIGNON2 conţine sursa ecranului de semnare folosit când valoarea de sistem QPWDLVL este setată la 2 sau la 3.

Fişierul QSYS/QAWTSSRC este **şters sau restaurat** de fiecare dată când sistemul de operare OS/400 este instalat. Dacă planificaţi să creaţi propria dumneavoastră versiune a ecranului de semnare, atunci trebuie mai întâi să copiaţi fişierul membru sursă corespunzător, fie QDSIGNON fie QDSIGNON2 în fişierul dumnevoastră sursă şi să faceţi modificări în copia din fişierul dumneavoastră sursă.

Modificarea fişierului de afişare pentru semnare

Pentru a modifica formatul ecranului de afişare:

1. Crearea unui fişier de afişare semnare modificat.

   Un câmp ascuns în fişierul de afişare numit UBUFFER poate fi modificat pentru a gestiona câmpurile mai mici. UBUFFER are 128 de octeţi lungime şi este stabilit ca ultimul câmp din fişierul de afişare. Acest câmp poate fi modificat pentru a funcţiona ca un buffer de intrare/ieşire astfel încât datele specificate în acest câmp al ecranului vor fi disponibile pentru programul aplicaţie când este pornit jobul interactiv. Puteţi modifica câmpul UBUFFER pentru a conţine câte câmpuri mai mici aveţi nevoie dacă sunt îndeplinite următoarele cerinţe:

   - Noile câmpuri trebuie să urmeze toate celelalte câmpuri din fişierul de afişare. Locaţia câmpurilor din ecran nu contează atâta timp cât ordinea în care sunt puse în specificaţiile descrierii de date (DDS) îndeplineşte această cerinţă.
   - Lungimea trebuie să fie în total 128. Dacă lungimea câmpurilor este mai mult de 128, unele date nu vor fi transmise.
   - Toate câmpurile trebuie să fie de intrare/ieşire (tipul B în sursă DDS) sau ascunse (tipul H în sursă DDS).
2. Ordinea în care câmpurile din fişierul de afişare semnare sunt declarate nu trebuie modificată. Poziţia în care ele sunt arătate pe ecran poate fi modificată. Nu modificaţi numele de câmp existente din sursa pentru fişierul de afişare ecran de semnare.
3. Nu modificaţi dimensiunea totală a buffer-lor de intrare sau ieşire. Pot apărea probleme serioase dacă ordinea sau dimensiunea buffer-lor este modificată.
4. Nu folosiţi funcţia de ajutor specificaţii descrieri de date (DDS) din fişierul de afişare semnare.

5. Modificaţi o descriere de subsistem pentru a folosi fişierul de afişare modificat în locul valorii implicite sistem a QSYS/QDSIGNON. Puteţi modifica descrierile de subsistem pentru subsistemele pe care vreţi să folosiţi noul ecran. Pentru a modifica descrierea de subsistem:
   a. Folosiţi comanda CHGSBSD (Change Subsystem Description - Modificare descriere de subsistem).
   b. Specificaţi noul fişier de afişare în parametrul SGNDSPF.
   c. Folosiţi o versiune de test a subsistemului pentru a verifica dacă ecranul este valid înainte de a încerca să modificaţi subsistemul de control.
6. Testaţi modificarea.
7. Modificaţi alte descrieri de subsistem.

Note:

1. Lungimea buffer-ului pentru fişierul de afişare trebuie să fie 318. Dacă este mai puţin decât 318, subsistemul foloseşte ecranul de afişare implicit QDSIGNON din biblioteca QSYS când valoarea de sistem QPWDLVL este 0 sau 1 şi QDSIGNON2 din biblioteca QSYS când QPWDLVL este 2 sau 3.
2. Linia de copyright nu poate fi ştearsă.

Descrierile de subsistem

Control descrieri de subsistem:

Cum intră joburi-le în sistemul dumneavoastră

Cum sunt pornite joburi-le

Caracteristici de performanţă ale joburi-lor

Doar câţiva utilizatori trebuie să fie autorizaţi pentru a modifica descrieri de subsistem şi modificările trebuie monitorizate cu atenţie.

Controlarea felului în care intră joburile în subsistem

Mai multe descrieri de subsistem sunt livrate cu sistemul dumneavoastră. După ce aţi modificat nivelul dumneavoastră de securitate (valoarea de sistem QSECURITY) la nivelul 20 sau mai sus, semnarea fără a introduce un ID utilizator şi o parolă nu este permisă cu subsistemele livrate de IBM.

Totuşi, definirea unei combinaţii de descriere de subsistem şi descriere de job care permite semnarea implicită (nici un ID utilizator şi nici o parolă) este posibilă şi reprezintă o expunere de securitate. Când sistemul rutează un job interactiv, priveşte intrarea staţiei de lucru din descrierea de subsistem pentru o descriere de job. Dacă descrierea de job specifică USER(*RQD), utilizatorul trebuie să introducă un ID utilizator valid (şi parola) în ecranul de Semnare. Dacă descrierea de job specifică un profil utilizator în câmpul *Utilizator*, oricine poate apăsa tasta Enter pentru a se semna ca acel utilizator.

La nivelurile de securitate 30 sau mai înalte, sistemul înregistrează în istoric o intrare (tip AF, sub-tip S) în jurnalul de auditare, dacă este încercată semnarea implicită şi funcţia de auditare este activă. La nivelul de securitate 40 şi mai sus, sistemul nu permite semnarea implicită, chiar dacă o combinaţie de intrare de staţie de lucru şi descriere de job există şi ar permite semnarea implicită. Vedeţi “Semnarea fără ID de utilizator şi parolă” la pagina 14 pentru informaţii suplimentare.

Fiţi sigur că toate intrările staţiei de lucru pentru subsistemele interactive se referă la descrierile de job cu USER(*RQD). Controlaţi autorizarea pentru modificarea descrierile de job şi monitorizaţi orice modificări care sunt făcute descrierilor de job. Dacă funcţia de auditare este activă, sistemul scrie o intrare jurnal de tip JD de fiecare dată când parametrul USER dintr-o descriere de job este modificat.

Intrările de comunicaţii dintr-o descriere de subsistem controlează felul cum joburi-le de comunicaţii intră în sistemul dumneavoastră. O intrare de coumunicaţii pointează spre un profil utilizator implicit, care permite unui job să fie pornit fără un ID utilizator şi o parolă. Aceasta reprezintă o potenţială expunere de securitate. Evaluaţi intrările de comunicaţii

din sistemul dumneavoastră şi folosiţi atribute de reţea pentru a controla felul cum joburi-le de comunicaţii intră în sistemul dumneavoastră. “Atributele de reţea” la pagina 183 discutaţi atributele de reţea care sunt importante pentru securitate.

Descrieri de job

O descriere de job este o unealtă valoroasă pentru securitate şi controlul funcţionării. Puteţi de asemenea să setaţi o descriere de job pentru un grup de utilizatori care necesită aceeaşi listă de biblioteci iniţială, coadă de ieşiere şi coadă de job. Puteţi seta o descriere de job pentru un grup de joburi batch care au cerinţe similare.

O descriere de job reprezintă o potenţială expunere de securitate. În unele cazuri, o descriere de job care specifică un nume de profil pentru parametrul USER poate permite unui job să intre în sistem fără verificări de securitate adecvate. “Controlarea felului în care intră joburile în subsistem” la pagina 175 discutaţi cum poate fi aceasta împiedicată pentru joburi-le interactive şi de comunicaţii.

Când un job batch este lansat, jobul poate rula folosind un profil diferit de cel al utilizatorului care a lansat jobul. Profilul poate fi specificat în comanda SBMJOB sau poate veni de la parametrul USER al descrierii de job. Dacă sistemul dumneavoastră este la nivelul de securitate 30 (valoare de sistem QSECURITY) sau mai jos, utilizatorul care lansează un job necesită autorizare pentru descrierea de job, dar nu şi pentru profilul utilizator specificat în descrierea de job. Aceasta reprezintă o expunere de securitate. La nivelul de securitate 40 şi mai înalt, cel care lansează jobul necesită autorizare atât pentru descrierea de job cât şi pentru profilul utilizator.

De exemplu:

- USERA nu este autorizat pentru fişierul PAYROLL.
- USERB are autorizarea *USE pentru fişierul PAYROLL şi pentru programul PRLIST, care listează fişierul PAYROLL.
- Descrierea de job PRJOBD specifică USER(USERB). Autorizarea publică pentru PRJOBD este *USE.

La nivelul de securitate 30 sau mai jos, USERA poate lista fişierul stat de plată prin lansarea unui job batch:

```
SBMJOB RQSDTA("Apelaţi PRLIST") JOBD(PRJOBD) +
                      USER(*JOBD)
```

Puteţi preveni aceasta prin folosirea nivelului de securitate 40 sau prin controlarea autorizării pentru descrierile de job care specifică un profil utilizator.

Uneori, un nume de profil utilizator specific într-o descriere de job este necesar pentru anumite tipuri de lucru batch pentru a funcţiona cum trebuie. De exemplu, descrierea de job QBATCH este livrată cu USER(QPGMR). Această descriere de job este livrată cu autorizarea publică *EXCLUDE.

Dacă sistemul dumneavoastră este la nivelul de securitate 30 sau mai jos, orice utilizator din sistem care are autorizare pentru comanda SBMJOB (Submit Job - Lansare job) sau pentru comenzile de pornire cititor şi are autorizarea *USE pentru descrierea de job QBATCH, poate lansa lucrul sub profilul utilizator programator (QPGMR), indiferent dacă utilizatorul are sau nu autorizarea pentru profilul utilizator QPGMR. La nivelul de securitate 40 sau mai înalt, autorizarea *USE pentru profilul QPGMR este de asemenea necesară.

Coada de mesaje operator sistem

Meniul iSeries Asistent operaţional (ASSIST) furnizează o opţiune pentru a gestiona sistemul dumneavoastră, utilizatorii şi dispozitivele. Meniul Gestionare sistem, utilizatori şi dispozitive furnizează o opţiune pentru a lucru cu mesajele operatorului sistem. S-ar putea să vreţi să împiedicaţi utilizatorii de la a răspunde la mesaje în coada de mesaje QSYSOPR (operator sistem). Răspunsurile incorecte la mesajele operatorului sistem pot cauza probleme în sistemul dumneavoastră.

Răspunderea la mesaje necesită autorizările *USE and *ADD pentru coada de mesaje. Înlăturarea mesajelor necesită autorizările *USE şi *DLT. (Vedeţi 376.) Daţi autorizarea de a răspunde la mesaje şi de înlătura mesaje în QSYSOPR doar utilizatorilor cu responsabilitate operator sistem. Autorizarea publică pentru QSYSOPR trebuie să fie *OBJOPR şi *ADD, care permit adăugarea de mesaje noi la QSYSOPR.

Atenţie: Toate joburi-le necesită abilitatea de a adăuga mesaje noi în coada de mesaje QSYSOPR. Nu faceţi autorizarea publică pentru QSYSOPR *EXCLUDE.

Lista de biblioteci

Lista de biblioteci pentru un job indică care biblioteci sunt căutate şi ordinea în care ele vor fi căutate. Când un program specifică un obiect, obiectul poate fi specificat cu un nume calificat, care include atât numele obiectului cât şi numele bibliotecii. Sau biblioteca pentru obiect poate fi specificată ca *LIBL (listă de biblioteci). Bibliotecile din lista de biblioteci sunt căutate în ordine până când este găsit obiectul.

Tabela 117 rezumă parţile din lista de biblioteci şi cum sunt ele construite în timpul unui job. Secţiunile care urmează discută riscurile şi măsurile de protecţie pentru lista de biblioteci.

Tabela 117. Părţi ale listei de biblioteci. Lista de biblioteci este căutată în această ordine:

Parte	Cum este construită
Porţiune sistem 15 intrări	Construită iniţial folosind valoarea de sistem QSYSLIBL. Poate fi modificată în timpul unui job folosind comanda CHGSYSLIBL.
Porţiune bibliotecă produs 2 intrări	Blanc iniţial. O bibliotecă este adăugată la porţiunea bibliotecă produs a listei de biblioteci când o comandă sau un meniu rulat au fost create cu o bibliotecă în parametrul PRDLIB. Biblioteca rămâne în porţiunea bibliotecă produs a listei de biblioteci până când comanda sau meniul se termină.
Biblioteca curentă 1 intrare	Specificată în profilul utilizator sau pe ecranul de semnare. Poate fi modificată când o comandă sau un meniu rulat specifică o bibliotecă pentru parametrul CURLIB. Poate fi modificată în timpul jobului cu comanda CHGCURLIB.
Porţiune utilizator 250 intrări	Construită iniţial prin folosirea listei de biblioteci iniţiale din descrierea jobului utilizatorului. Dacă descrierea de job specifică *SYSVAL, este folosită valoarea de sistem QUSRLIBL. În timpul unui job, porţiunea utilizator a listei de biblioteci poate fi modificată cu comenzile ADDLIBLE, RMVLIBLE, CHGLIBL şi EDTLIBL.

Riscurile de securitate ale listelor de biblioteci

Listele de biblioteci reprezintă o potenţială expunere de securitate. Dacă un utilizator este capabil să modifice ordinea bibliotecilor în lista de biblioteci sau să adauge biblioteci suplimentare în listă, poate fi capabil să realizeze funcţii care să încalce cerinţele dumneavoastră de securitate.

“Securitatea bibliotecii şi listele de biblioteci” la pagina 113 furnizează unele informaţii generale despre problemele asociate cu listele de biblioteci. Acest subiect oferă mai multe exemple specifice de expuneri posibile şi modul cum pot fi evitate.

Următoarele două exemple arată cum modificările dintr-o listă de biblioteci pot duce la încălcarea cerinţelor de securitate:

Modificarea funcţiei

Figura 31 la pagina 178 arată o bibliotecă de aplicaţie. Programul A apelează Programul B, despre care se aşteaptă să fie în LIBA. Programul B realizează actualizări în Fişierul A. Programul B este apelat fără un nume calificat, astfel încât lista de biblioteci este căutată până când este găsit Program B.

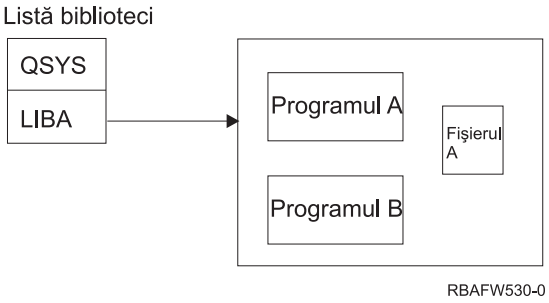

Figura 31. Lista de biblioteci–Mediu aşteptat

Un programator sau alt utilizator informat poate pune alt Program B în biblioteca LIBB. Programul înlocuit poate realiza funcţii diferite ca facerea unei copii a informaţiilor confidenţiale sau actualizarea fişierelor incorect. Dacă LIBB este plasată înainte de LIBA în lista de biblioteci, este rulat Program B înlocuit în locul Programului B original, deoarece programul este apelat fără un nume calificat:

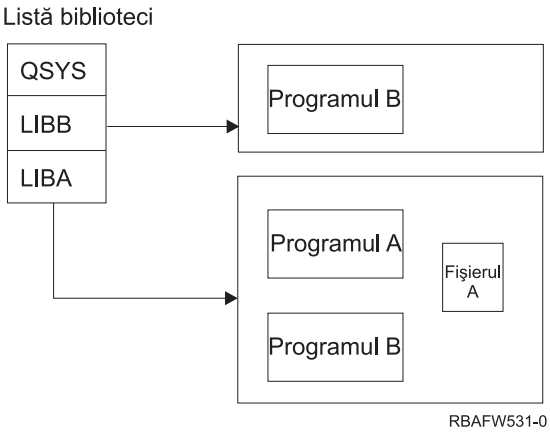

Figura 32. Lista de biblioteci–Mediu real

Accesul neautorizat la informaţii

Să presupunem că Programul A din Figura 31 adoptă autorizarea USER1, care are autorizarea *ALL pentru Fişierul A. Să presupunem că Programul B este apelat de Programul A (autorizarea adoptată rămâne în vigoare). Un utilizator informat poate crea un Program B înlocuitor care apelează pur şi simplu procesorul de comandă. Utilizatorul va avea o linie de comandă şi acces total la Fişierul A.

Recomandări pentru porţiunea de sistem a listei de biblioteci

Porţiunea sistem a listei de biblioteci este intenţionată pentru biblioteci livrate de IBM. Bibliotecile aplicaţie care sunt controlate cu grijă pot fi de asemenea plasate în porţiunea sistem a listei de biblioteci. Porţiunea sistem a listei de biblioteci reprezintă cea mai mare expunere de securitate, deoarece bibliotecile din această parte a listei sunt căutate primele.

Doar un utilizator cu autorizările speciale *ALLOBJ şi *SECADM poate modifica valoarea sitem QSYSLIBL. Controlaţi şi monitorizaţi orice modificări la porţiunea sistem a listei de biblioteci. Urmaţi aceste linii de ghidare când adăugaţi biblioteci:

- Doar bibliotecile care sunt controlate specific sunt plasate în această listă.
- Publicul nu trebuie să aibă autorizarea *ADD la aceste biblioteci.
- Puţine biblioteci livrate de IBM cum este QGPL sunt livrate cu autorizarea publică *ADD din motive de producţie. Monitorizaţi regulat ce obiecte (programe particulare, fişiere sursă şi comenzi) sunt adăugate la aceste biblioteci.

Comanda CHGSYSLIBL este livrată cu autorizarea publică *EXCLUDE. Doar utilizatorii cu autorizarea *ALLOBJ sunt autorizaţi la comandă, doar dacă dumneavoastră acordaţi autorizare către alţi utilizatori. Dacă lista de biblioteci sistem necesită să fie modificată temporar în timpul unui job, puteţi folosi tehnica descrisă în subiectul “Modificarea listei de biblioteci de sistem” la pagina 196.

Recomandări pentru biblioteca de produs

Porţiunea bibliotecii de produs a listei de biblioteci este căutată înainte de porţiunea de utilizator. Un utilizator informat poate crea o comandă sau un meniu care inserează o bibliotecă produs în lista de biblioteci. De exemplu, această declaraţie creează CMDX, care rulează programul PGMA:

```
CRTCMD CMDX PGM(PGMA) PRDLIB(LIBB)
```

Cât timp CMDX rulează, LIBB este în porţiunea produs a listei de biblioteci.

Folosiţi aceste măsuri pentru a proteja porţiunea produs a listei de biblioteci:

- Controlaţi autorizarea pentru comenzile CRTCMD (Create Command - Comandă creare), CHGCMD (Change Command - Comandă modificare), CRTMNU (Create Menu - Meniu creare) şi CHGMNU (Change Menu - Meniu modificare).
- Când creaţi comenzi şi meniuri, specicaţi PRDLIB(*NONE), care înlătură toate intrările prezente în porţiunea produs a listei de biblioteci. Aceasta vă protejează de la a avea căutate biblioteci necunoscute înaintea bibliotecii pe care o aşteptaţi când comanda sau meniul dumenavoastră rulează.

  Notă: Valoarea implicită când creaţi o comandă sau un meniu este PRDLIB(*NOCHG). *NOCHG înseamnă că atunci când comanda sau meniul rulează, porţiunea bibliotecă produs a listei de biblioteci nu este modificată.

Recomandări pentru biblioteca curentă

Biblioteca curentă poate fi utilizată de către uneltele suport-decizie cum este Query/400. Orice programe de interogare create de către un utilizator sunt plasate implicit în biblioteca curentă a utilizatorului. Când creaţi un meniu sau o comandă, puteţi specifica o bibliotecă curentă pentru a fi utilizată în timp ce meniul este activ.

Biblioteca curentă furnizează o metodă uşoară pentru utilizator şi programator pentru a crea obiecte noi, cum sunt programele de interogare, fără a vă îngrijora despre unde vor fi ele localizate. Totuşi, biblioteca curentă ridică un risc de securitate, deoarece este căutată înaintea porţiunii utilizator a listei de bibioteci. Puteţi lua mai multe prevederi pentru a proteja securitatea sistemului dumneavoastră în timp ce încă vă folosiţi de capabilităţile bibliotecii curente:

- Specificaţi *YES pentru câmpul *Limitare capabilităţi* din profilul utilizator. Aceasta împiedică un utilizator de a modifica biblioteca curentă în ecranul de Semnare sau de la a folosi comanda CHGPRF.
- Restricţionaţi autorizarea pentru comenzile CHGCURLIB (Change Current Library - Modificare bibliotecă curentă), CRTMNU (Create Menu - Meniu creare), CHGMNU (Change Menu - Meniu modificare), CRTCMD (Create Command - Comandă creare) şi CHGCMD (Change Command - Comandă modificare).
- Folosiţi tehnica descrisă în “Controlarea listei de biblioteci de utilizator” la pagina 195 pentru a seta biblioteca curentă în timpul procesării aplicaţiei.

Recomandări pentru porţiunea de utilizator a listei de biblioteci

Porţiunea utilizator a listei de biblioteci modifică de obicei mai mult decât alte porţiuni şi este mai dificil de controlat. Multe programe de aplicaţie modifică lista de biblioteci. Descrierile de job afectează de asemenea lista de biblioteci pentru un job.

Următoarele sunt unele sugestii alternative pentru controlarea porţiunii utilizator a listei de biblioteci pentru a fi sigur că biblioteci neautorizate cu programe şi fişiere înlocuitoare nu sunt folosite în timpul procesării:

- Restricţionarea utilizatorilor aplicaţiilor de producţie la un mediu meniu. Setaţi câmpul *Limitare capabilităţi* din profilurile utilizator la *YES pentru a restricţiona abilitatea lor de a introduce comenzi. “Planificarea meniurilor” la pagina 197 furnizează un exemplu al acestui mediu.
- Folosiţi nume calificate (obiect sau bibliotecă) în aplicaţia dumneavoastră. Aceasta împiedică sistemul de la a căuta lista de biblioteci pentru a găsi un obiect.

- Controlaţi abilitatea de a modifica descrierile de job, deoarece descrierea de job setează lista de biblioteci iniţială pentru un job.
- Folosiţi comanda ADDLIBLE (Add Library List Entry - Adăugare intrare lista de biblioteci) la începutul programului pentru a vă asigura că obiectele dorite sunt la începutul porţiunii utilizator a listei de biblioteci. La sfârşitul programului, biblioteca poate fi înlăturată.

  Dacă biblioteca este deja în lista de biblioteci, dar nu sunteţi sigur că este la începutul listei, trebuie să înlăturaţi biblioteca şi să o adăugaţi. Dacă ordinea listei de biblioteci este importantă pentru alte aplicaţii din sistem, folosiţi în locul ei următoarea metodă.
- Folosiţi un program care extrage şi salvează lista de biblioteci pentru un job. Înlocuiţi lista de biblioteci cu lista dorită pentru aplicaţie. Când se termină aplicaţia, întoarceţi lista de biblioteci la setarea originală. Vedeţi “Controlarea listei de biblioteci de utilizator” la pagina 195 pentru un exemplu al acestei tehnici.

Tipărire

Cele mai multe informaţii care sunt tipărite în sistemul dumneavoastră sunt memorate ca fişier spool într-o coadă de ieşire în timp ce se aşteaptă tipărirea. Doar dacă controlaţi securitatea cozilor de ieşire din sistemul dumneavoastră, utilizatorii neautorizaţi pot afişa, tipări şi chiar copia informaţii confidenţiale care aşteaptă să fie tipărite.

O metodă de a proteja ieşirea confidenţială este de a crea o coadă de ieşire specială. Trimiteţi ieşirea confidenţială la coada de ieşire şi controlaţi cine poate vizualiza şi manevra fişierele spool în coada de ieşire.

Pentru a determina unde merge ieşirea, sistemul priveşte în ordine fişierul imprimantă, atributele jobului, profilul utilizator, descrierea dispozitivului staţie de lucru şi valoarea de sistem dispozitiv de tipărire (QPRTDEV). Dacă sunt folosite valori implicite, este folosită coada de ieşire asociată cu imprimanta QPRTDEV. Cartea *Printer Device Programming* furnizează exemple despre cum se face direcţionarea ieşirii spre o anumită coadă de ieşire.

Securizarea fişiereleor spool

Un fişier spool este un tip special de obiect în sistem. Nu puteţi acorda direct şi revoca autorizarea de a vizualiza şi manevra un fişier spool. Autorizarea pentru un fişier spool este controlată de mai mulţi parametri din coada de ieşire care păstrează fişierul spool.

Când creaţi un fişier spool, sunteţi proprietarul acelui fişier. Puteţi vizualiza şi manevra întotdeauna orice fişier spool pe care îl deţineţi, indiferent cum este definită autorizarea pentru coada de ieşire. Trebuie să aveţi autorizarea *READ pentru a adăuga intrări noi într-o coadă de ieşire. Dacă este înlăturată autorizarea pentru o coadă de ieşire, puteţi accesa încă orice intrări pe care le deţineţi în acea coadă folosind comanda WRKSPLF (Work with Spooled Files - Gestionare fişiere spool).

Parametrii de securitate pentru o coadă de ieşire sunt specificaţi folosind comanda CRTOUTQ (Create Output Queue - Creare coadă de ieşire) sau comanda CHGOUTQ (Change Output Queue - Modificare coadă de ieşire). Puteţi afişa parametrii de securitate pentru o coadă de ieşire folosind comanda WRKOUTQD (Work with Output Queue Description - Gestiune descriere coadă de ieşire).

Atenţie: Un utilizator cu autorizarea specială *SPLCTL poate realiza toate funcţiile pe toate intrările în ciuda felului cum este definită coada de ieşire. Unii parametrii din coada de ieşire permit unui utilizator cu autorizarea specială *JOBCTL să vizualizeze conţinutul intrărilor din coada de ieşire.

Parametrul Afişare date (DSPDTA) al cozii de ieşire

Parametrul DSPDTA este proiectat pentru a proteja conţinutul unui fişier spool. Determină ce autorizare este necesară pentru a realiza următoarele funcţii pe fişierele spool deţinute de alţi utilizatori:

- comanda DSPSPLF (View the contents of a spooled file - Vizualizarea conţinutului unui fişier spool)
- comanda CPYSPLF(Copy a spooled file - Copierea unui fişier spool)
- comanda SNDNETSPLF (Send a spooled file - Trimiterea unui fişier spool)
- comanda CHGSPLFA (Move a spooled file to another output queue - Mutarea unui fişier spool în altă coadă de ieşire)

Valori posibile pentru DSPDTA

***NO**	Un utilizator nu poate afişa, trimite sau copia fişiere spool deţinute de alţi utilizatori decât dacă utilizatorul are una din următoarele: • autorizarea specială *JOBCTL dacă parametrul OPRCTL este *YES. • autorizare *READ, *ADD şi *DLT pentru coada de ieşire dacă parametrul *AUTCHK este *DTAAUT. • Dreptul de proprietate al cozii de ieşire dacă parametrul *AUTCHK este *OWNER.
***YES**	Orice utilizator cu autorizarea *READ pentru coada de ieşire poate afişa, copia sau trimite datele fişierelor spool deţinute de alţii.
***OWNER**	Doar proprietarul unui fişier spool sau un utilizator cu *SPLCTL (control spool) poate afişa, copia sau trimite fişierul. Dacă valoarea OPRCTL este *YES, utilizatorii cu autorizarea specială *JOBCTL pot reţine, modifica, şterge şi elibera fişierele spool din coada de ieşire, dar ei nu pot afişa, copia, trimite sau muta fişierele spool. Aceasta este concepută pentru a permite operatorilor să gestioneze o coadă de ieşire fără a fi capabili să vizualizeze conţinutul.

Parametrul Autorizare pentru verificare (AUTCHK) al cozii de ieşire

Parametrul AUTCHK determină dacă autorizările *READ, *ADD şi *DLT pentru coada de ieşire permit unui utilizator să modifice şi să şteargă fişierele spool deţinute de alţi utilizatori.

Valori posibile pentru AUTCHK

***OWNER**	Doar utilizatorul care deţine coada de ieşire poate modifica sau şterge fişierele spool deţinute de alţii.
***DTAAUT**	Specifică dacă orice utilizator cu autorizările *READ, *ADD şi *DLT pentru coada de ieşire poate modifica sau şterge fişierele spool deţinute de alţii.

Parametrul Control operator (OPRCTL) al cozii de ieşire

Parametrul OPRCTL determină dacă un utilizator cu autorizarea specială *JOBCTL poate controla coada de ieşire.

Valori posibile pentru OPRCTL

***YES**	Un utilizator cu autorizarea specială *JOBCTL poate realiza toate funcţiile pe fişierele spool doar dacă valoarea DSPDTA este *OWNER. Dacă valoarea DSPDTA este *OWNER, autorizarea specială *JOBCTL nu permite utilizatorului să afişeze, copieze, trimită sau să mute fişierele spool.
***NO**	Autorizarea specială *JOBCTL nu dă utilizatorului orice autorizare de a realiza operaţii asupra cozii de ieşire. Regulile autorizării normale se aplică utilizatorului.

Coada de ieşire şi Parametrul Autorizări necesar pentru tipărire

Tabela 118 la pagina 182 arată ce combinaţie între parametrii cozii de ieşire şi autorizarea pentru coada de ieşire este necesară pentru a realiza funcţiile de gestiune tipărire din sistem. Pentru unele funcţii este menţionată mai mult de o combinaţie. Proprietarul unui fişier spool poate realiza întotdeauna toate funcţiile pe acel fişier. Pentru informaţii suplimentare vedeţi “Comenzile pentru scriitor” la pagina 426.

Autorizarea şi parametrii cozii de ieşire pentru toate comenzile asociate cu fişire spool sunt listate pe “Comenzile pentru fişier spool” la pagina 412. Comenzile cozii de ieşire sunt listate pe “Comenzile pentru coadă de ieşire” la pagina 388.

Atenţie: Un utilizator cu autorizarea specială *SPLCTL (control spool) nu este subiectul nici unor restricţii de autorizare asociate cu cozile de ieşire. Autorizarea specială *SPLCTL permite utilizatorului să realizeze toate operaţiile pe toate cozile de ieşire. Evaluaţi cu grijă acordarea autorizării speciale *SPLCTL pentru orice utilizator.

Tabela 118. Autorizarea necesară pentru a realiza funcţii de tipărire

Funcţie de tipărire	Parametrii cozii de ieşire			Autorizarea coadă de ieşire	Autorizarea specială
	DSPDTA	AUTCHK	OPRCTL		
Adăugare fişiere spool în coadă [1]				*READ	Nimic
			*YES		*JOBCTL
Vizualizaţi lista de fişiere spool (comanda WRKOUTQ [2])				*READ	Nimic
			*YES		*JOBCTL
Afişare, copiere sau trimitere fişiere spool (DSPSPLF, CPYSPLF, SNDNETSPLF, SNDTCPSP[2])	*YES			*READ	Nimic
	*NO	*DTAAUT		*READ, *ADD, *DLT	Nimic
	*NO	*OWNER		Proprietar [3]	Nimic
	*YES		*YES		*JOBCTL
	*NO		*YES		*JOBCTL
	*OWNER				
Modificare, ştergere, reţinere şi eliberare fişier spool (CHGSPLFA, DLTSPLF, HLDSPLF, RLSSPLF [2])		*DTAAUT		*READ, *ADD, *DLT	Nimic
		*OWNER		Proprietar [3]	Nimic
			*YES		*JOBCTL
Modificare, curăţare, reţinere şi eliberare coada de ieşire (CHGOUTQ, CLROUTQ, HLDOUTQ, RLSOUTQ [2])		*DTAAUT		*READ, *ADD, *DLT	Nimic
		*OWNER		Proprietar [3]	Nimic
			*YES		*JOBCTL
Porniţi un scriitor pentru coada de ieşire (STRPRTWTR, STRRMTWTR [2])		*DTAAUT		*CHANGE	Nimic
			*YES		*JOBCTL

1 Aceasta este autorizarea necesară pentru a direcţiona ieşirea dumneavoastră spre o coadă de ieşire.

2 Folosirea acestor comenzi sau a opţiunilor echivalente de la un ecran.

3 Trebuie să fiţi proprietarul cozii de ieşire.

4 Necesită de asemenea autorizarea *USE pentru descrierea de dispozitiv de tipărire.

5 *CHGOUTQ necesită autorizarea *OBJMGT pentru coada de ieşire, în plus la autorizările *READ, *ADD şi *DLT.

Exemple: Coada de ieşire

Următoarele sunt mai multe exemple de setare a parametrilor de securitate pentru cozile de ieşire astfel încât să îndeplinească cerinţe diferite:

- Creaţi o coadă de ieşire cu scop-general. Toţi utilizatorii au permisiunea de a afişa toate fişierele spool. Operatorilor sistem le este permis să gestioneze coada şi să modifice fişierele spool:

```
CRTOUTQ OUTQ(QGPL/GPOUTQ) DSPDTA(*YES) +
        OPRCTL(*YES) AUTCHK(*OWNER) AUT(*USE)
```

- Creaţi o coadă de ieşire pentru o aplicaţie. Doar membrilor profilului de grup GRPA le este permisă folosirea cozii de ieşire. Toţi utilizatorii autorizaţi ai cozii de ieşire au permisiunea de a afişa toate fişierele spool. Operatorilor sistem nu le este permisă gestionarea cozii de ieşire:

```
CRTOUTQ OUTQ(ARLIB/AROUTQ) DSPDTA(*YES) +
        OPRCTL(*NO) AUTCHK(*OWNER) AUT(*EXCLUDE)
GRTOBJAUT OBJ(ARLIB/AROUTQ) OBJTYP(*OUTQ) +
        USER(GRPA)  AUT(*CHANGE)
```

- Creaţi o coadă de ieşire confidenţială pentru responsabilii cu securitatea pentru a o folosi când tipăriţi informaţii despre profilurile şi autorizările utilizator. Coada de ieşire este creată şi deţinută de profilul QSECOFR.

```
CRTOUTQ OUTQ(QGPL/SECOUTQ) DSPDTA(*OWNER) +
        AUTCHK(*DTAAUT) OPRCTL(*NO) +
        AUT(*EXCLUDE)
```

Chiar dacă responsabilii cu securitatea dintr-un sistem au autorizarea specială *ALLOBJ, ei nu sunt capabili să acceseze fişierele spool deţinute de alţi utilizatori ai cozii de ieşire SECOUTQ.

- Creaţi o coadă de ieşire care este partajată de utilizatorii care tipăresc fişiere şi documente confidenţiale. Utilizatorii pot gestiona doar propriile fişire spool. Operatorii sistem pot gestiona fişierele spool, dar nu pot afişa conţinutul acestor fişiere.

  ```
  CRTOUTQ OUTQ(QGPL/CFOUTQ) DSPDTA(*OWNER) +
          AUTCHK(*OWNER) OPRCTL(*YES) AUT(*USE)
  ```

Atributele de reţea

Atributele de reţea controlează felul cum sistemul dumneavoastră comunică cu alte sisteme. Unele atribute de reţea controlează felul cum sunt tratate cererile la distanţă de procesare joburi şi acces la informaţii. Aceste atribute de reţea afectează direct securitatea din sistemul dumneavoastră şi sunt discutate în subiectele care urmează:

Acţiune job (JOBACN)

Cerere client acces (PCSACC)

cerere DDM acces (DDMACC)

Sunt arătate valorile posibile pentru fiecare atribut de reţea. Valoarea implicită este subliniat. Pentru a seta valoarea unui atribut de reţea, folosiţi comanda CHGNETA (Change Network Attribute - Modificare atribut reţea).

Atributul de reţea Acţiune job (JOBACN)

Atributul de reţea JOBACN determină cum procesează sistemul cererile de intrare pentru a rula joburi.

Valori posibile pentru JOBACN:

***REJECT**	Fluxul de intrare este refuzat. Un mesaj care a pornit fluxul de intrare şi a fost refuzat, este trimis atât emiţătorului cât şi receptorului intenţionat.
***FILE**	Fluxul de intrare este introdus în coada fişierelor de reţea pentru utilizatorul ce recepţionează. Acest utilizator poate afişa, anula sau recepţiona fluxul de intrare într-un fişier de bază de date sau îl poate lansa într-o coadă de job. Un mesaj care porneşte fluxul de intrare care a fost umplut, este trimis atât emiţătorului cât şi receptorului.
***SEARCH**	Tabela job de reţea controlează acţiunile prin folosirea valorilor din tabelă.

Recomandări

Dacă nu vă aşteptaţi să primiţi cereri de joburi la distanţă în sistemul dumneavoastră, setaţi atributul de reţea JOBACN la *REJECT.

Pentru informaţii suplimentare despre atributul JOBACN, referiţi-vî la cartea *SNA Distribution Services*.

Atributul de reţea Acces Cerere client (PCSACC)

Atributul de reţea PCSACC determină modul în care programul licenţiat iSeries Access pentru Windows procesează cererile de la calculatoarele personale ataşate pentru accesarea obiectelor. Atributul de reţea PCSACC controlează dacă joburile calculator personal pot accesa obiecte în sistem şi nu dacă calculatorul personal iSeries poate folosi emularea staţiei de lucru.

Notă: Atributul de reţea PCSACC controlează doar clienţii DOS şi OS/2. Acest atribut nu are nici un efect pe alt client iSeries Access.

Valori posibile pentru PCSACC:

***REJECT**	iSeries Access refuză toate cererile de la calculatorul personal pentru a accesa obiecte din sistem iSeries. Un mesaj de eroare este trimis aplicaţiei PC.
***OBJAUT**	Programele iSeries Access din sistem verifică autorizările obiect normal pentru fiecare obiect cerut de un program PC. De exemplu, dacă este cerut transferul fişierului, este verificată autorizarea de a copia date din fişierul bază de date.
***REGFAC**	Sistemul foloseşte facilitatea de înregistrare a sistemului pentru a determina ce program de ieşire (dacă e vreunul) să ruleze. Dacă nu este definit nici un program de ieşire pentru un punct de ieşire şi această valoare este specificată, este folosit *OBJAUT.
nume program- calificat-	Programul iSeries Access apelează acest program de ieşire scriitor-utilizator pentru a determina dacă cererea PC-ului trebuie să fie refuzată. Programul de ieşire este aplelat doar dacă verificarea de autorizare normală pentru obiect are succes. Programul iSeries Access transmite informaţii despre utilizator şi funcţia cerută programului de ieşire. Programul întoarce un cod care indică dacă cererea trebuie permisă sau refuzată. Dacă codul retur indică că cererea trebuie refuzată sau dacă apare o eroare, un mesaj de eroare este trimis calculatorului personal.

Riscuri şi recomandări

Măsurile de securitate normale în sistemul dumneavoastră s-ar putea să nu fie protecţia suficientă dacă programul iSeries Access este instalat în sistemul dumnevoastră. De exemplu, dacă un utilizator are autorizarea *USE pentru un fişier şi atributul de reţea PCSACC este *OBJAUT, utilizatorul poate folosi programul iSeries Access şi un program din calculatorul personal pentru a transfera tot acel fişier pe calculatorul personal. Utilizatorul poate copia datele pe o dischetă sau o bandă PC şi le poate înlătura din punctul de plecare.

Sunt disponibile mai multe metode pentru a împiedica iSeries ca un utilizator staţie de lucru cu autorizarea *USE pentru un fişier, să copieze acel fişier:

- Setare LMTCPB(*YES) în profilul utilizator.
- Restricţionaţi autorizarea pentru comenzile care copiază fişiere.
- Restricţionaţi autorizarea pentru comenzile folosite de iSeries Access.
- Nu daţi autorizarea utilizator *ADD pentru orice bibliotecă. Autorizarea *ADD este necesară pentru a crea un fişier nou într-o bibliotecă.
- Nu daţi accesul utilizator pentru orice dispozitiv *SAVRST.

Nici una din aceste metode nu funcţionează pentru utilizatorul PC al programul cu licenţă iSeries Access. Folosirea unui program de ieşire pentru a verifica toate cererile este singura măsură de protecţie adecvată.

Programul iSeries Access transmite informaţii programului de ieşire utilizator apelat de atributul de reţea PCSACC, pentru următoarele tipuri de acces:

Transfer fişier

tipărire virtuală

Mesaj

Folder partajat

Pentru informaţii suplimentare despre iSeries Access, consultaţi Centrul de informare (vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii).

Atributul de reţea Acces cerere DDM (DDMACC)

Atributul de reţea DDMACC determină cum procesează sistemul cererile de la alte sisteme pentru a accesa date folosind gestiunea de date distribuită (DDM) sau funcţia bază de date relaţională distribuită.

Valori posibile pentru DDMACC:

***REJECT**	Sistemul nu permite orice DDM sau orice cereri DRDA de la sistemele la distanţă. *REJECT nu împiedică acest sistem de la a funcţiona ca sistemul care cere şi a trimite cereri către alte sisteme server.
***OBJAUT**	Cererile la distanţă sunt controlate de autorizarea obiect din sistem.
nume- program- calificat-	Acest program scriitor-utilizator este apelat după ce a fost verificată autorizarea obiect normală. Programul de ieşire este apelat doar pentru fişierele DDM, nu pentru funcţiile bază de date relaţională distribuită. Programul de ieşire este transmis parametru lista, construit de sistemul la distanţă, care identifică utilizatorul sistem local şi cererea. Programul evaluează cererea şi trimite un cod retur, acordă sau refuză accesul cerut.

Pentru informaţii suplimentare despre atributul de reţea DDMACC şi despre problemele de securitate asociate cu DDM, vedeţi Centrul de informare (vedeţi "Cerinţe preliminare şi informaţii înrudite" la pagina xvi pentru detalii).

Operaţiile de salvare şi restaurare

Abilitatea de a salva obiecte din sistemul dumneavoastră sau de a restaura obiecte în sistemul dumneavoastră reprezintă o expunere pentru organizarea dumneavoastră.

De exemplu, programatorii au adesea autorizarea *OBJEXIST pentru programae, deoarece această autorizare este necesară pentru a recompila un program (şi şterge vechea copie). Autorizarea *OBJEXIST este de asemenea necesară pentru a salva un obiect. Prin urmare, programatorul tipic poate face o copie bandă a programelor, care pot reprezenta o investiţie financiară substanţială.

Un utilizator cu autorizarea *OBJEXIST pentru un obiect poate de asemenea restaura o copie nouă a unui obiect peste un obiect existent. În cazul unui program, programul restaurat poate fi creat pe un sistem diferit. Poate realiza funcţii diferite. De exemplu, presupuneţi ca programul original a lucrat cu date confidenţiale. Noua versiune poate realiza aceleaşi funcţii, dar poate scrie de asemenea o copie a informaţiilor confidenţiale într-un fişier secret din biblioteca proprie a programatorului. Programatorul nu are nevoie de autorizare pentru datele confidenţiale, deoarece utilizatorii obişnuiţi ai programului vor accesa datele.

Restricţionarea operaţiilor de salvare şi restaurare

Puteţi controla abilitatea de a salva şi restaura obiecte în mai multe căi:

- Restricţionaţi accesul fizic de a salva şi restaura dispozitive, cum sunt unităţi bandă, unitaţi optice şi unităţi de dischetă.
- Restricţionaţi autorizarea pentru obiectele descrieri de dispozitiv pentru a salva şi restaura dispozitive. Pentru a salva un obiect pe o unitate bandă, trebuie să aveţi autorizarea *USE pentru descrierea de dispozitiv pentru unitatea bandă.
- Restricţionaţi comenzile de salvare şi restaurare. Aceasta vă permite să controlaţi ce este salvat din sistemul dumnevoastră şi restaurat în sistemul dumneavoastră prin toate interfeţele - prin includerea fişierelor de salvare. Vedeţi "Exemplu: Restricţionarea comenzilor de salvare şi restaurare" pentru un exemplu de cum se face aceasta. Sistemul setează comenzile de restaurare la PUBLIC(*EXCLUDE) când vă instalaţi sistemul.
- Daţi autorizarea specială *SAVSYS doar utilizatorilor de încredere.

Exemplu: Restricţionarea comenzilor de salvare şi restaurare

Următorul este un exemplu al paşilor pe care puteţi să-i folosiţi pentru a restricţiona operaţiile de salvare şi restaurare din sistemul dumnevoastră:

1. Pentru a crea o listă de autorizaţii pe care puteţi să o folosiţi pentru a da autorizare comenzilor pentru operatorii sistem, tastaţi următoarele:

   ```
   CRTAUTL AUTL(SRLIST) TEXT('Listă salvare şi restaurare')
   AUT(*EXCLUDE)
   ```

2. Pentru a folosi lista de autorizaţii pentru a securiza comenzile de salvare, tastaţi următoarele:

   ```
   GRTOBJAUT OBJ(SAV*) OBJTYPE(*CMD) AUTL(SRLIST)
   ```

3. Pentru a vă asigura că autorizarea *PUBLIC vine din lista de autorizaţii, tastaţi următoarele:

```
GRTOBJAUT OBJ(SAV*) OBJTYPE(*CMD) USER(*PUBLIC)
   AUT(*AUTL)
```

4. Pentru a folosi lista de autorizaţii pentru a securiza comenzile de restaurare, tastaţi următoarele:

```
GRTOBJAUT OBJ(RST*) OBJTYPE(*CMD) AUTL(SRLIST)
```

5. Pentru a vă asigura că autorizarea *PUBLIC vine din lista de autorizaţii, tastaţi următoarele:

```
GRTOBJAUT OBJ(RST*) OBJTYPE(*CMD) USER(*PUBLIC)
   AUT(*AUTL)
```

6. Deşi operatorii sistem care sunt responsabili pentru salvarea sistemului au autorizarea specială *SAVSYS, ei trebuie acum să aibă dată autorizare explicită pentru comenzile SAVxxx. Faceţi aceasta prin adăugarea operatorilor sistem în lista de autorizaţii:

```
ADDAUTLE AUTL(SRLIST) USER(USERA USERB) AUT(*USE)
```

   Notă: Puteţi vrea ca operatorii sistem ai dumneavoastră să aibă autorizare doar pentru comenzile de salvare. În acest caz, securizaţi comenzile de salvare şi restaurare cu două liste de autorizaţii separate.

7. Pentru a restricţiona API-urile de salvare şi restaurare şi a le securiza cu lista de autorizaţii, tastaţi următoarele comenzi:

```
GRTOBJAUT OBJ(QSRSAVO) OBJTYPE(*PGM) AUTL(SRLIST)
GRTOBJAUT OBJ(QSRSAVO) OBJTYPE(*PGM) USER(*PUBLIC)
   AUT(*AUTL)
GRTOBJAUT OBJ(QSRLIB01) OBJTYPE(*SRVPGM) AUTL(SRLIST)
GRTOBJAUT OBJ(QSRLIB01) OBJTYPE(*SRVPGM) USER(*PUBLIC)
   AUT(*AUTL)
```

Ajustarea performanţei

Monitorizarea şi ajustarea performanţei nu este responsabilitatea unui responsabil cu securitatea. Totuşi, responsabilul cu securitatea trebuie să se asigure că utilizatorii nu alterează caracteristicile de performanţă ale sistemului pentru a mări viteza propriilor joburi pe socoteala altora.

Mai multe obiecte de control funcţionare afectează performanţa joburi-lor din sistem:

- Clasa setează prioritatea de rulare şi felia de timp pentru un job.
- Intrarea de rutare din descrierea de subsistem determină clasa şi pool-ul de stocare pe care le foloseşte jobul.
- Descrierea de job poate determina coada de ieşire, prioritatea de ieşire, coada de joburi şi prioritatea job.

Utilizatorii informaţi cu autorizare corespunzătoare pot crea propriile lor medii în sistem şi să-şi dea singuri performanţă mai bună decât alţi utilizatori. Controlaţi aceasta prin limitarea autorizării de a crea şi modifica obiecte de control funcţionare. Setaţi autorizarea publică pentru comenzile de control funcţionare la *EXCLUDE şi acordaţi autorizarea pentru puţini utilizatori de încredere.

Caracteristicile de performanţă ale sistemului pot fi de asemenea modificate interactiv. De exemplu, ecranul WRKSYSSTS (Work with System Status - Gestiune stare sistem) poate fi folosit pentru a modifica dimensiunea pool-urilor de stocare şi a nivelurilor de activitate. De asemenea, un utilizator cu autorizarea specială *JOBCTL (job control) poate modifica prioritatea de planificare a oricărui job din sistem, subiect al limitei de prioritate (PTYLMT) din profilul utilizator. Alocaţi cu grijă autorizarea specială *JOBCTL şi PTYLMT în profilurile utilizator.

Pentru a permite utilizatorilor să vizualizeze informaţiile de performanţă folosind comanda WRKSYSSTS, dar să nu o modifice, faceţi următoarele:

```
GRTOBJAUT OBJ(CHGSHRPOOL) OBJTYPE(*CMD) +
          USER(*PUBLIC)   AUT(*EXCLUDE)
```

Autorizaţi utilizatorii responsabili cu ajustarea sistemului să modifice caracteristicile de performanţă:

```
GRTOBJAUT OBJ(CHGSHRPOOL) OBJTYPE(*CMD) +
          USER(USRTUNE)   AUT(*USE)
```

Restricţionarea joburilor la batch

Puteţi crea sau modifica comenzi pentru a restricţiona anumite joburi să fie rulate doar într-un mediu batch. De exemplu, s-ar putea să vreţi să rulaţi anumite rapoarte sau compilări program în batch. Un job care rulează în batch afectează de obicei performanţa de sistem mai puţin decât acelaşi job rulând interactiv.

De exemplu, pentru a restricţiona comanda care rulează programul RPTA la batch, faceţi următoarele:

- Creaţi o comandă pentru a rula RPTA şi specificaţi că acea comandă poate fi rulată doar în batch:
  ```
  CRTCMD CMD(RPTA) PGM(RPTA) ALLOW(*BATCH *BPGM)
  ```

Pentru a restricţiona compilările la batch, faceţi următoarele pentru a crea comanda pentru fiecare tip de program:

```
CHGCMD CMD(CRTxxxPGM) ALLOW(*BATCH *BPGM)
```

Capitolul 7. Proiectarea securităţii

Protejarea informaţiilor este o parte importantă a majorităţii aplicaţiilor. Securitatea ar trebui considerată, împreună cu alte cerinţe, la momentul la care e proiectată aplicaţia. De exemplu, când vă decideţi cum să organizaţi informaţiile aplicaţiei în biblioteci, încercaţi să echilibraţi cerinţele de securitate cu alte considerente, cum ar fi performanţa aplicaţiei şi salvare de rezervă şi recuperare.

Acest capitol conţine linii de ghidare care să ajute dezvoltatorii de aplicaţie şi manegerii de sistem să includă securitatea ca parte a proiectării generale. De asemenea conţine exemple de tehnici pe care le puteţi folosi pentru a îndeplini obiectivele de securitate din sistemul dumneavoastră. Unele din exemplele din acest capitol conţin programe exemplu. Aceste programe sunt incluse doar cu scop ilustrativ. Multe dintre ele nu vor putea fi compilate sau rulate aşa cum sunt, nici nu includ tratarea de mesaje şi recuperarea erorii.

Subiectul Securitatea de bază a sistemului şi planificarea din Centrul de informare este menit pentru administratorul de securitate. El conţine formulare, exemple şi linii de ghidare pentru planificarea securităţii pentru aplicaţii care au fost deja dezvoltate. Dacă sunteţi responsabil pentru proiectarea unei aplicaţii, veţi găsi folositoare revederea formularelor şi exemplelor din Centrul de informare (vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii). Vă pot ajuta să vă vedeţi aplicaţia din perspectiva unui administrator de securitate şi să înţelegeţi ce informaţii e nevoie să furnizaţi.

Subiectul Securitatea de bază a sistemului şi planificarea din Centrul de informare foloseşte de asemenea un set de aplicaţii exemplu pentru o companie fictivă numită Compania de jucării JKL. Acest capitol discută considerente de proiectare pentru acelaşi set de aplicaţii exemplu. Figura 33 arată relaţia dintre grupuri de utilizator, aplicaţii şi biblioteci pentru Compania de jucării JKL:

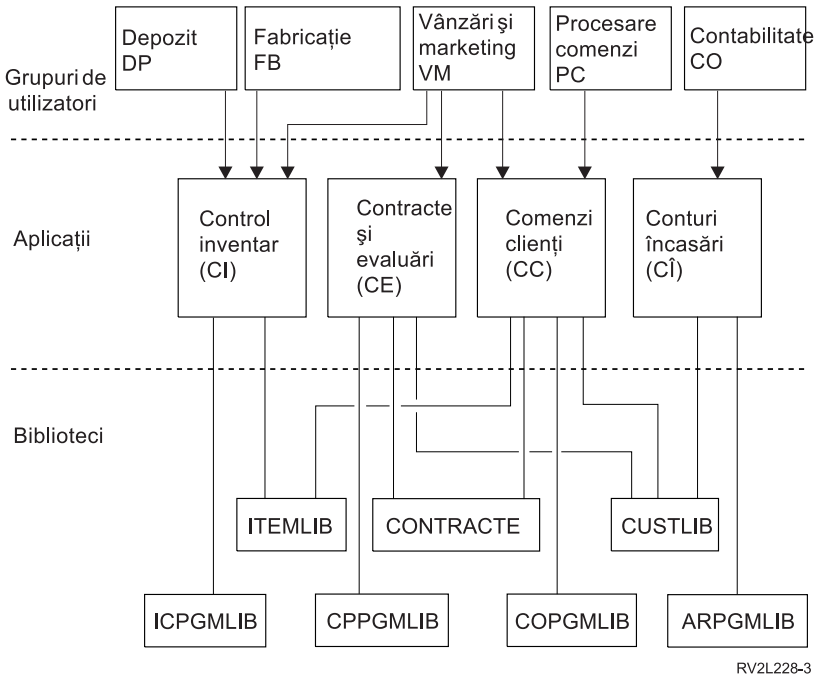

Figura 33. Aplicaţii exemplu

Descriere grafic

Acest grafic vă arată cum cinci seturi de grupuri de utilizatori accesează aplicaţii şi biblioteci pe sistem la Compania JKL Toy. Grupurile de utilizatori includ Depozit, Producţie, Vânzări şi Marketing, Procesare comandă şi Contabilitate.

Grupurile de utilizatori Depozit, Producţie şi Vânzări şi Marketing pot accesa toate aplicaţiile din Control inventar. Grupul de utilizatori Vânzări şi Marketing au de asemenea acces la aplicaţia Contracte şi Preţuri şi la aplicaţia Personalizare comandă. Grupul de utilizatori Procesare comandă poate de asemenea accesa aplicaţia Personalizare comandă. Grupul de utilizatori Contabilitate foloseşte aplicaţia Conturi de primit.

Recomandări generale

Recomandările din acest capitol şi din subiectul Securitatea de bază a sistemului şi planificarea din Centrul de informare se bazează pe un principiu important: simplitatea. Păstrarea proiectării securităţii cât mai simple face mai uşoară gestionarea şi auditarea ei. De asemenea îmbunătăţeşte performanţele aplicaţiei şi ale copiei de rezervă.

Urmează o listă de recomandări generale pentru proiectarea securităţii:

- Folosiţi securitatea resurselor împreună cu metodele disponibile, cum ar fi capabilităţi limitate în profilul utilizator şi restricţionarea utilizatorilor la un set de meniuri, pentru a proteja informaţiile.

  Atenţie: Nu e suficient să folosiţi doar capabilităţile limitate în profilul de utilizator şi controlul accesului la meniu pentru a vă securiza sistemul dacă folosiţi un produs cum ar fi iSeries Access sau aveţi linii de comunicaţie ataşate sistem. Trebuie să folosiţi securitatea resurselor pentru a securiza acele obiecte care vreţi să nu fie accesibile din aceste interfeţe.
- Securizaţi doar acele obiecte care chiar necesită securitate. Analizaţi o biliotecă pentru a determina care obiecte, cum ar fi fişierele de date, sunt confidenţiale şi securizaţi-le. Folosiţi autorizare publică pentru alte obiecte, cum ar fi zone de date şi cozi de mesaje.
- Mutaţi din general în specific:
  - Planificaţi securitatea pentru biblioteci şi directoare. Lucraţi cu obiecte individuale doar când e necesar.
  - Planificaţi autorizarea publică întâi, urmată de autorizarea de grup şi cea individuală.
- Faceţi autorizarea publică pentru obiecte noi într-o bibliotecă (parametrul CRTAUT) acceaşi ca autorizarea publică pentru majoritatea obiectelor existente în bibliotecă.
- Pentru a face auditarea mai uşoară şi a îmbunătăţi performanţa verificării autorizării, evitaţi definirea autorizării private care e mai puţin decât autorizarea publică pentru un obiect.
- Folosiţi listele de autorizaţii pentru a grupa obiecte cu aceleaşi cerinţe de securitate. Listele de autorizaţii sunt mai simplu de gestionat decât autorizările individuale şi ajută la recuperarea informaţiilor de securitate.

Planificarea modificărilor nivelului de parolă

Modificarea nivelurilor parolei ar trebui planificată cu atenţie. Operaţiile cu alte sisteme pot eşua sau este posibil ca utilizatorii să nu se poată semna în sistem dacă nu aţi planificat corespunzător modificarea nivelului parolei. Înainte de a modifica valoarea de sistem QPWDLVL, asiguraţi-vă că v-aţi salvat datele de securitate folosind comanda SAVSECDTA sau SAVSYS. Dacă aveţi o copie de rezervă curentă, veţi putea reseta parolele pentru toate profilurile utilizator dacă trebuie să vă întoarceţi la un nivel al parolei inferior.

Produsele pe care le folosiţi în sistem şi pe clienţii cu care sistemul interfaţează, pot avea probleme când valoarea de sistem pentru nivelul parolei (QPWDLVL) este setată la 2 sau 3. Orice produs sau client care trimite parole la sistem într-o formă criptată, mai degrabă decât in forma necriptată în care le introduce un utilizator într-un ecran de semnare, trebuie modernizat pentru a lucra nu noile reguli de criptare a parolei pentru QPWDLVL 2 sau 3. Trimiterea parolei criptate e cunoscută ca substituiţia parolei. Sustituţia parolei este folosită pentru a preveni ca o parolă să fie capturată în timpul transmisiei printr-o reţea. Înlocuirile parolei generate de clienţi mai vechi care nu suportă noul algoritm pentru QPWDLVL 2 sau 3, chiar dacă caraterele specifice introduse sunt corecte, nu vor fi acceptate. Asta se aplică de asemenea oricărui acces peer iSeries la iSeries care foloseşte valorile criptate pentru a autentifica de la un sistem la altul.

Problema este generată de faptul că anumite produse afectate (cum ar fi IBM Toolbox for Java) sunt furnizate ca middleware. Un produs terţ care incorporează o versiune anterioară a unuia din aceste produse nu va lucra corespunzător până ce nu e reconstruit folosind o versiune actualizată a middleware.

Dându-se acesta şi alte scenarii, este uşor de văzut de ce e necesară planificarea cu atenţie înainte de modificarea valorii de sistem QPWDLVL.

Considerente pentru modificarea QPWDLVL de la 0 la 1

Nivelul de parolă 1 permite ca pe un sistem care nu trebuie să comunice cu produsul Windows 95/98/ME iSeries Client Support for Windows Network Neighborhood (NetServer) să fie eliminate parolele NetServer. Eliminarea parolelor criptate nenecesare din sistem creşte securitatea generală a sa.

La QPWDLVL 1, toate mecanismele curente, pre-V5R1 de înlocuire şi autorizare a parolei vor continua să funcţioneze. Probabilitatea de a apărea probleme este foarte mică, cu excepţia funcţiilor/serviciilor care necesită parola NetServer.

Printre funcţiile/serviciile care necesită parola NetServer se numără:

- iSeries Support for Windows Network Neighborhood, ediţia Windows 95/98/ME, (NetServer)

Considerente pentru modificarea QPWDLVL de la 0 sau 1 la 2

Nivelul de parolă 2 introduce folosirea parolelor sensibile la majuscule cu lungime de până la 128 de caractere (numite şi passphrases) şi furnizează abilitatea maximă de a reveni la QPWDLVL 0 sau 1.

Indiferent de nivelul de parolă al sistemului, parolele din nivelul 2 şi 3 sunt create oricând este modificată o parolă sau când semnează un utilizator în sistem. Deţinerea unei parole de nivel 2 şi 3 create când sistemul este încă la nivelul 0 sau 1 ajută la pregătirea modificării la nivelul de parolă 2 sau 3.

Înainte de a modifica QPWDLVL la 2, administratorul de sistem ar trebui să folosească comanda PRTUSRPRF TYPE(*PWDLVL) pentru a localiza toate profilurile utilizator care nu au o parolă care nu poate fi folosită la nivelul 2. În funcţie de profilurile localizate, administratorul îşi poate dori să folosească unul din următoarele mecanisme pentru a adăuga un nivel de parolă 2 şi 3 la profiluri.

- Modificaţi parola pentru profilul utilizator folosind comanda CHGUSRPRF sau CHGPWD CL sau API-ul QSYCHGPW API. Asta va face ca sistemul să modifice parola care poate fi folosită la nivelurile 0 şi 1; şi sistemul de asemenea creează două parole sensibile la majuscule echivalente care pot fi folosite la nivelurile 2 şi 3. Sunt create versiuni doar de majuscule şi doar cu litere mici ale parolei pentru folosire la nivelurile 2 sau 3.

  De exemplu, modificare parolei în C4D2RB4Y rezultă în generarea de către sistem a parolelor C4D2RB4Y şi c4d2rb4y de nivel 2.
- Semnaţi în sistem printr-un mecanism care prezintă parola în text clar (nu foloseşte înlocuirea parolei). Dacă parola e validă şi profilul utilizator nu are o parolă care poate fi folosită la nivelurile 2 şi 3, sistemul creează două parole sensibile la majuscule echivalente care pot fi folosite la nivelurile 2 şi 3. Sunt create versiuni doar de majuscule şi doar de litere mici pentru folosirea la nivelurile de parolă 2 sau 3.

Absenţa unei parole care poate fi folosită la nivelul 2 sau 3 poate fi o problemă oricând profilul utilizator nu are o parolă care poate fi folosită la nivelurile 0 şi 1 sau când utilizatorul încearcă să semneze printr-un produs care foloseşte înlocuirea parolei. În aceste cazuri, utilizatorul nu va fi capabil să semneze când nivelul parolei este modificat la 2.

Dacă un profil de utilizator nu are o parolă care poate fi folosită la nivelurile 2 şi 3, profilul de utilizator nu are o parolă care poate fi folosită la nivelurile 0 şi 1 şi utilizatorul semnează printr-un produs care trimite parole în text clar, atunci sistemul validează utilizatorul cu parola de la nivelul 0 de parolă şi creează două parole de nivel 2 (aşa cum au fost descrise mai sus) pentru profilul utilizator. Următoarele semnări vor fi validate cu parolele din nivelul 2.

Orice client/serviciu care foloseşte înlocuirea parolei nu va funcţiona corect la QPWDLVL 2 dacă clientul/serviciul nu a fost actualizat pentru a folosi noua schemă (passphrase) de înlocuire a parolei. Administratorul ar trebui să verifice dacă e necesar un client/serviciu care nu a fost actualizat pentru noua schemă de înlocuire a parolei.

Clienţii/serviciile care folosesc înlocuirea parolei includ:

- TELNET
- iSeries Access

- iSeries Servere gazdă
- QFileSrv.400
- Suportul iSeries NetServer Print
- DDM
- DRDA
- SNA LU6.2

Se recomandă insistent ca datele de securitate să fie salvate înainte de a se modifica la QPWDLVL 2. Asta poate ajuta la facerea mai uşoară a tranziţiei înapoi la QPWDLVL 0 sau 1 dacă e necesar.

Se recomandă ca celelaltele valori de sistem ale parolei, cum ar fi QPWDMINLEN şi QPWDMAXLEN să nu fie modificate decât după o testare a QPWDLVL 2. Asta va face mai uşoară tranziţia înapoi la QPWDLVL 1 sau 0 dacă e necesar. Totuşi, valoarea de sistem QPWDVLDPGM trebuie să specifice fie *REGFAC fie *NONE înainte ca sistemul să permită ca QPWDLVL să fie modificată la 2. Aşadar, dacă folosiţi un program de validare a parolei, veţi dori să scrieţi unul nou care poate fi înregistrat pentru punctul de ieşire QIBM_QSY_VLD_PASSWRD folosind comanda ADDEXITPGM.

Parolele NetServer sunt suportate în continuare la QPWDLVL 2, astfel că orice funcţie/serviciu care necesită o parolă NetServer ar trebui de asemenea să funcţioneze corect.

După ce administratorul s-a familiarizat cu rularea sistemului la QPWDLVL 2, puteţi începe să modificaţi valorile de sistem ale parolei pentru a exploata parole mai lungi. Totuşi, administratorul trebuie să ştie că parolele mai lungi vor avea următoarele efecte:

- Dacă sunt specificate parole mai mari de 10 caractere, nivelurile de parolă 0 şi 1 sunt curăţate. Acest profil utilizator nu va putea semna dacă sistemul este returnat la nivelul de parolă 0 sau 1.
- Dacă parolele conţin caractere speciale sau nu urmează regulile de compoziţie pentru nume de obiecte simple (excluzând sensibilitatea la majuscule), parola de nivel 0 şi 1 e ştearsă.
- Dacă sunt specificate parole mai mari de 14 caractere, este ştearsă parola NetServer pentru profilul de utilizator.
- Valorile de sistem ale parolei se aplică doar la valoarea 2 a nivelului de parolă, nu şi la parolele de nivel 0 şi 1 generate de sistem sau valorile parolelor NetServer (dacă sunt generate).

Considerente pentru modificarea QPWDLVL de la 2 la 3

După ce rulaţi sistemul la QPWDLVL 2 pentru o perioadă de timp, administratorul poate lua în considerare mutarea la QPWDLVL 3 pentru a maximiza protecţia securităţii prin parole.

La QPWDLVL 3, toate parolele NetServer sunt şterse, aşa că un sistem nu ar trebui mutat la QPWDLVL 3 decât atunci când nu mai este necesară folosirea parolelor NetServer.

La QPWDLVL 3, toate parolele de nivel 0 şi 1 sunt curăţate. Administratorul poate folosi comenzile DSPAUTUSR sau PRTUSRPRF pentru a localiza profilurile utilizator care nu au parole de nivel 2 sau 3 asociate cu ele.

Trecerea la un nivel de parolă mai scăzut

Întoarcerea la o valoare QPWDLVL mai mică, chiar dacă e posibilă, nu e aşteptată ca o operaţie lipsită de probleme. În general, ar trebui să fie un singur sens de la valori QPWDLVL mai mici la valori QPWDLVL mai mari. Totuşi, pot fi cazuri în care o valoare QPWDLVL mai mică trebuie să fie refăcută.

Următoarele secţiuni discută munca necesară pentru a vă întoarce la un nivel de parolă mai mic.

Considerente pentru modificarea QPWDLVL de la 3 la 2

Această modificare e relativ uşoară. După ce s-a setat QPWDLVL la 2, administratorul trebuie să determine dacă este necesar ca vreun profil de utilizator să conţină parole NetServer sau parole de nivel 0 sau 1 şi, dacă este aşa, să modifice parola profilului de utilizator la o valoare permisă.

În plus, poate fi necesară schimbarea înapoi a valorilor de sistem pentru parolă, la valorile compatibile cu parolele NetServer şi nivelul de parolă 0 sau 1, dacă sunt necesare aceste parole.

Considerente pentru modificarea QPWDLVL de la 3 la 1 sau 0

Din cauza potenţialului foarte mare de a cauza probleme pentru sistem (cum ar fi faptul că nimeni nu poate semna deoarece toate parolele de nivel 0 şi 1 au fost curăţate), această modificare nu e suportată direct. Pentru a modifica de la QPWDLVL 3 la QPWDLVL 1 sau 0, sistemul trebuie să facă mai întâi modificarea intermediară la QPWDLVL 2.

Considerente pentru modificarea QPWDLVL de la 2 la 1

Înainte de la modifica QPWDLVL la 1, administratorul trebuie să folosească comanda DSPAUTUSR sau PRTUSRPRF TYPE(*PWDINFO) pentru a localiza profilurile de utilizator care nu au o parolă de nivel 0 sau 1. Dacă profilul de utilizator va necesita o parolă după ce se modifică QPWDLVL, administratorul trebuie să se asigure că e creată o parolă de nivel 0 şi 1 pentru profil folosind unul din următoarele mecanisme:

- Modificaţi parola pentru profilul utilizator folosind comanda CHGUSRPRF sau CHGPWD CL sau API-ul QSYCHGPW API. Asta va face ca sistemul să modifice parola care poate fi folosită la nivelurile 2 şi 3; şi sistemul de asemenea creează două parole sensibile la majuscule echivalente care pot fi folosite la nivelurile 0 şi 1. Sistemul e capabil să creeze parola de nivel 0 şi 1 doar dacă sunt îndeplinite următoarele condiţii:
  - Parola are o lungime de 10 caratere sau mai puţin.
  - Parola poate fi convertită la caractere cu majuscule EBCDIC A-Z, 0-9, @, #, $ şi liniuţă de subliniere.
  - Parola nu începe cu un caracter numeric sau liniuţă de subliniere.

  De exemplu, modificarea parolei la o valoare de RainyDay va rezulta în generarea de către sistem a parolei de nivel 0 şi 1 RAINYDAY. Dar modificarea valorii parolei la Rainy Days In April va face ca sistemul să cureţe parola de nivel 0 şi 1 (deoarece parola e prea lungă şi conţine spaţii).

  Nu e produs nici un mesaj sau indicaţie dacă parola de nivel 0 sau 1 nu a putut fi creată.
- Semnaţi în sistem printr-un mecanism care prezintă parola în text clar (nu foloseşte înlocuirea parolei). Dacă parola e validă şi profilul utilizator nu are o parolă care poate fi folosită la nivelurile 0 şi 1, sistemul creează două parole sensibile la majuscule echivalente care pot fi folosite la nivelurile 0 şi 1. Sistemul e capabil să creeze parola de nivel 0 şi 1 doar dacă condiţiile de mai sus sunt îndeplinite.

Adminstratorul poate apoi modifica QPWDLVL la 1. Toate parolele NetServer sunt curăţate când modificarea la QPWDLVL 1 devine efectivă (la următorul IPL).

Considerente pentru modificarea QPWDLVL de la 2 la 0

Considerentele sunt identice cu cele de la modificarea de la QPWDLVL 2 la 1, cu excepţia că toate parolele NetServer sunt reţinute când modificarea devine efectivă.

Considerente pentru modificarea QPWDLVL de la 1 la 0

După modificarea QPWDLVL la 0, administratorul trebuie să folosească comanda DSPAUTUSR sau PRTUSRPRF pentru a localiza profilurile de utilizator care nu au o parolă NetServer. Dacă profilul de utilizator necesită o parolă NetServer, ea poate fi creată modificând parola utilizatorului sau semnând printr-un mecanism care prezintă parola în text clar.

Administratorul poate apoi modifica QPWDLVL la 0.

Planificarea bibliotecilor

Mulţi factori afectează modul în care alegeţi să grupaţi informaţiile aplicaţiilor dumneavoastră în biblioteci şi să le gestionaţi. Acest subiect adresează unele din problemele de securitate asociate proiectării bibliotecii.

Pentru a accesa un obiect, aveţi nevoie de autorizare pentru obiectul însuşi şi pentru biblioteca care îl conţine. Puteţi restricţiona accesul la un obiect restricţionând obiectul insuşi, biblioteca care îl conţine sau ambele.

O bibiotecă este ca un director folosit pentru a localiza obiectele din ea. Autorizarea *USE pentru o bibliotecă vă permite să folosiţi directorul pentru a găsi obiecte în ea. Autorizarea pentru obiectul însuşi determină *cum* puteţi folosi

obiectul. Autorizarea *USE pentru o bibliotecă e suficientă pentru a realiza majoritatea operaţiilor asupra obiectelor din ea. Vedeţi “Securitatea bibliotecii” la pagina 112 pentru informaţii suplimentare despre relaţia dintre autorizarea bibliotecă şi obiect.

Folosirea autorizării publice pentru obiecte şi restricţionarea accesului la biblioteci poate fi o tehnică de securitate simplă, eficace. Punerea programelor într-o bibliotecă separată faţă de alte obiecte aplicaţie poate de asemnea simplifica panificarea securităţii. Aceasta este adevărată mai ales dacă fişierele sunt partajate de mai mult de o aplicaţie. Puteţi utiliza autorizarea de folosire pentru bibliotecile care conţin programe aplicaţie pentru a controla cine poate realiza funcţii asupra aplicaţiilor.

Urmează două exemple de folosire a securităţii bibliotecii pentru aplicaţiile Compania de jucării JKL. (Vedeţi Figura 33 la pagina 189 pentru o diagramă a aplicaţiilor.)

- Informaţiile din biblioteca CONTRACTS sunt considerate confidenţiale. Autorizarea publică pentru toate obiectele din bibliotecă este suficientă pentru a realiza funcţiile aplicaţiei Preţ şi contracte (*CHANGE). Autorizarea publică pentru biblioteca CONTRACTS este *EXCLUDE. Doar utilizatorilor sau grupurilor autorizate pentru aplicaţia Preţ şi contracte le este acordată autorizare *USE pentru bibliotecă.
- Compania de jucării JKL este o companie mică cu o abordare nerestrictivă asupra securităţii, cu excepţia informaţiilor despre contracte şi preţuri. Tuturor utilizatorilor sistemului le e permis să vadă informaţiile despre client şi inventar, deşi doar utilizatorii autorizaţi le pot modifica. Bibliotecile CUSTLIB şi ITEMLIB şi obiectele din biblioteci, au autorizarea publică *USE. Utilizatorii pot vedea informaţii din aceste biblioteci prin aplicaţia lor primară sau folosind Query. Bibliotecile programului au autorizarea publică *EXCLUDE. Doar utilizatorii cărora le e permis să modifice informaţiile despre inventar au acces la ICPGMLIB. Programele care modifică informaţiile despre inventar adoptă autorizarea proprietarului aplicaţiei (OWNIC) şi astfel au autorizare *ALL pentru câmpurile din biblioteca ITEMLIB.

Securitatea bibliotecii este eficientă doar când sunt urmate aceste reguli:

- Bibliotecile conţin obiecte cu cerinţe de securitate similare.
- Utilizatorilor nu le e permis să adauge obiecte noi la biblioteci restricţionate. Modificările asupra programelor din bibliotecă sunt controlate. Bibliotecile aplicaţiei trebuie să aibă autorizare publică *USE sau *EXCLUDE mai puţin în cazul în care utilizatorii au nevoie să creeze obiecte direct în bibliotecă.
- Listele de biblioteci sunt controlate.

Planificarea aplicaţiilor pentru a împiedica profilurile mari

Din cauza impactului poteţial asupra performanţelor şi securităţii, IBM **recomandă insistent** următoarele pentru ca profilurile să nu devină prea plin:

- Să nu aveţi un profil care să deţină totul pe sistemul dumneavoastră.

  Creaţi profiluri utilizator speciale pentru a deţine aplicaţii. Profilurile proprietar care sunt specifice unei aplicaţii fac mai uşoară recuperarea lor şi mutarea acestora între sisteme. De asemenea, informaţiile despre autorizări private sunt împrăştiate prin mai multe profiluri, ceea ce îmbunătăţeşte performanţele. Folosind mai multe profiluri utilizator, puteţi preveni ca un profil să devină prea mare din cauza prea multor obiecte. Profilurile proprietar de asemenea vă permit să adoptaţi autorizarea profilului proprietar decât un profil mai puternic care furnizează autorizare nenecesară.
- Evitaţi deţinerea de aplicaţii deţinute de profiluri utilizator furnizate de IBM, cum ar fi QSECOFR sau QPGMR.

  Aceste profiluri deţin un număr mare de obiecte furnizate de IBM şi pot deveni foarte greu de gestionat. Păstrarea de aplicaţii deţinute de profiluri utilizator livrate de IBM poate cauza de asemenea şi probleme de securitate atunci când sunt mutate aplicaţiile de pe un sistem pe altul. Aplicaţiile deţinute de profilurile de utilizator livrate de IBM pot afecta de asemenea performanţele comenzilor, cum ar fi CHKOBJITG şi WRKOBJOWN.
- Folosiţi liste de autorizaţii pentru a securiza obiecte.

  Dacă acordaţi autorizări private multor obiecte pentru mai mulţi utilizatori, ar trebui să consideraţi folosirea unei liste de autorizări pentru a securiza obiectele. Listele de autorizaţii vor cauza o intrare autorizare privată pentru lista de autorizaţii din profilul utilizatorului mai degrabă decât o intrare de autorizare privată pentru fiecare obiect. Din profilul proprietarului obiectului, listele de autorizări cauzează o intrare obiect autorizată pentru fiecare utilizator căruia i-a fost acordată autorizare la lista de autorizare mai degrabă decât o intrare obiect neautorizată pentru fiecare obiect multiplicat cu numărul utilizatorilor cărora le este acordată autorizarea privată.

Listele de biblioteci

Lista de bilioteci pentru un job furnizează flexibilitate. De asemenea reprezintă o expunere a securităţii. Această expunere este importantă mai ales dacă folosiţi autorizare publică pentru obiecte şi vă bazaţi pe securitatea bibliotecii ca principalul mijloc de protejare a informaţiilor. în acest caz, un utilizator care primeşte acces la o bibliotecă are acces necontrolat la informaţiile din ea. Subiectul “Lista de biblioteci” la pagina 177 furnizează o discuţie despre problemele de securitate asociate listelor de biblioteci.

Pentru a evita riscurile de securitate ale listelor de biblioteci, aplicaţiile dumneavoastră pot folosi nume calificate. Atunci când atât numele obiectului cât şi biblioteca sunt specificate, sistemul nu caută lista de biblioteci. Aceasta împiedică un potenţial intrus de la folosirea listei de biblioteci pentru a dejuca securitatea.

Totuşi, alte cerinţe de proiectare a aplicaţiei vă pot împiedica să folosiţi nume calificate. Dacă aplicaţiile dumneavoastră se bazează pe liste de biblioteci, tehnica descrisă în următoarea secţiune poate reduce expunerea securităţii.

Controlarea listei de biblioteci de utilizator

Ca o precauţie de securitate, poate vreţi să vă asiguraţi că poarţiunea utilizator a listei de biblioteci are intrările corecte în secvenţa aşteptată înainte de rularea unui job. O metodă de a face asta este să folosiţi un program CL pentru a salva lista de biblioteci a utilizatorului, să o înlocuiţi cu lista dorită şi să o restauraţi la sfârşitul aplicaţiei. Urmează un program exemplu pentru a face asta:

```
          PGM
          DCL      &USRLIBL *CHAR LEN(2750)
          DCL      &CURLIB  *CHAR LEN(10)
          DCL      &ERROR *LGL
          DCL      &CMD *CHAR LEN(2800)
          MONMSG   MSGID(CPF0000)  +
                   EXEC(GOTO SETERROR)
          RTVJOBA  USRLIBL(&USRLIBL) +
                   CURLIB(&CURLIB)
          IF COND(&CURLIB=('*NONE')) +
             THEN(CHGVAR &CURLIB '*CRTDFT  ')
          CHGLIBL  LIBL(QGPL) CURLIB(*CRTDFT)
          /*********************************/
          /*                               */
          /*     Normal processing         */
          /*                               */
          /*********************************/
          GOTO     ENDPGM
SETERROR: CHGVAR   &ERROR '1'
ENDPGM:   CHGVAR   &CMD +
                     ('CHGLIBL LIBL+
                     (' *CAT &USRLIBL *CAT')  +
                     CURLIB(' *CAT &CURLIB *TCAT ' )')
                   CALL     QCMDEXC PARM(&CMD 2800)
                   IF       &ERROR SNDPGMMSG MSGID(CPF9898) +
                            MSGF(QCPFMSG) MSGTYPE(*ESCAPE) +
                            MSGDTA('The xxxx error occurred')
                   ENDPGM
```

Figura 34. Program pentru a înlocui şi restaura lista de biblioteci

Note:

1. Indiferent de modul în care se termină programul (normal sau anormal), lista de biblioteci este returnată la versiunea pe care o reţinea când programul a fost apelat, deoarece tratarea erorii include restaurarea listei de biblioteci.
2. Deoarece comanda CHGLIBL necesită o listă de nume de biblioteci, nu poate fi rulată direct. Comanda RTVJOBA, aşadar, extrage bibliotecile folosite pentru a contrui comanda CHGLIBL ca o variabilă. Variabile este pasată ca un parametru funcţiei QCMDEXC.

3. Dacă ieşiţi într-o funcţie necontrolată (de exemplu, un program utilizator, un meniu care permite introducerea de comenzi sau ecranul Introducere comanzi) în mijlocul unui program, acesta ar trebui să înlocuiască lista de biblioteci la întoarcere, pentru a asigura control adecvat.

Modificarea listei de biblioteci de sistem

Dacă aplicaţia dumneavoastră are nevoie să adauge intrări în porţiunea sistem a listei de biblioteci, puteţi folosi un program CL similar celui arătat în Figura 34 la pagina 195, cu următoarele modificări:

- În loc să folosiţi comanda RTVJOBA, folosiţi comanda RTVSYSVAL (Retrieve System Values - Extragere valori de sistem) pentru a extrage valoarea de sistem QSYSLIBL.
- Folosiţi comanda CHGSYSLIBL (Change System Library List - Modificare listă de biblioteci sistem) pentru a modifica porţiunea sistem a listei de biblioteci la valoarea dorită
- La sfârşitul programului dumneavoastră, folosiţi comanda GSYSLIBL din nou pentru a restaura porţiunea sistem a listei de biblioteci la valoarea sa originală.
- Comanda CHGSYSLIBL este livrată cu autorizarea publică *EXCLUDE. Pentru a folosi această comandă în programul dumneavoatră, faceţi una din următoarele:
  - Acordaţi proprietarului programului autorizare *USE pentru comanda CHGSYSLIBL şi folosiţi use autorizarea adoptată.
  - Acordaţi utilizatorilor care rulează programul autorizare *USE pentru comanda CHGSYSLIBL.

Descrierea securităţii bibliotecii

Ca un proiectant de aplicaţii, trebuie să furnizaţi informaţii despre o bibliotecă pentru administratorul de securitate. Administratorul de securitate foloseşte aceste informaţii pentru a decide cum să securizeze bliblioteca şi obiectele ei. Informaţiile tipice necesare sunt:

- Orice funcţii ale aplicaţiei care adaugă obiecte în bibliotecă.
- Dacă sunt şterse obiecte din bibliotecă în timpul procesării aplicaţiei.
- Ce profil deţine biblioteca şi obiectele sale.
- Dacă biblioteca ar trebui inclusă în lista de biblioteci.

Figura 35 furnizează un format exemplu pentru furnizarea acestor informaţii:

Nume bibliotecă: ITEMLIB

Autorizare publică pentru bibliotecă: *EXCLUDE

Autorizare publică pentru obiectele bibliotecă: *CHANGE

Autorizare publică pentru obiectele noi (CRTAUT): *CHANGE

Proprietar bibliotecă: OWNIC

Se include în lista de biblioteci? Nu. Biblioteca este adăugată în lista de biblioteci de programul aplicaţie iniţial sau programul de interogare iniţial.

Listare orice funcţii care necesită autorizare *ADD pentru bibliotecă:

Nu sunt adăugate obiecte în bibliotecă în timpul procesării normale a aplicaţiei. Listaţi orice obiect care necesită autorizare *OBJMGT sau *OBJEXIST şi ce funcţii au nevoie de acea autorizare:

Toate fişierele de lucru, ale căror nume încep cu caracterele ICWRK, sunt curăţate la sfârşit de lună. Asta necesită autorizare *OBJMGT.

Figura 35. Format pentru descrierea securităţii bibliotecii

Planificarea meniurilor

Meniurile sunt o metodă bună pentru furnizarea de acces controlat la sistemul dumneavoastră. Puteţi folosi meniuri pentru a restricţiona un utilizator la un set de funcţii controlate strict specificând capabiblităţi limitate şi un meniu iniţial în profilul utilizator.

Pentru a folosi meniuri ca o unealtă de control al accesului, urmaţi aceste linii la proiectarea lor:

- Nu furnizaţi o linie de comandă sau meniuri proiectate pentru utilizatori restricţionaţi.
- Evitaţi să aveţi funcţii cu cerinţe de securitate diferite în acelaşi meniu. De exemplu, dacă unor utilizatori ai unei aplicaţii le e permis doar să vadă informaţii, nu o modificaţi, furnizaţi un meniu care are doar opţiuni de vizualizare şi tipărire pentru acei utilizatori.
- Asiguraţi-vă că setul de meniuri furnizează toate legăturile necesare între meniuri astfel încât utilizatorul să nu aibă nevoie de o linie de comandă pentru a cere una.
- Furnizaţi acces la câteva funcţiie de sistem, cum ar fi vizualizarea ieşirii imprimantei. Meniul sistem ASSIST să această capabilitate şi poate fi definit în profilul utilizator ca programul Attention-key-handling program. Dacă profilul utilizator are o clasă *USER şi are capabilităţi limitate, utilizatorul nu poate vedea ieşirea sau joburile altor utilizatori.
- Furnizaţi acces la unelte de suport decizie din meniuri. Subiectul “Folosirea autorizării adoptate în proiectarea meniului” dă un exemplu cum să faceţi asta.
- Consideraţi controlarea accesului la Meniul System Request sau la unele din opţiunile acestui meniu. Vedeţi “Meniul Cerere sistem” la pagina 201 pentru informaţii suplimentare.
- Pentru utilizatorii cărora le e permis să ruleze doar o singură funcţie, evitaţi complet meniurile şi specificaţi un program iniţial în profilul utilizator. Specificaţi *SIGNOFF ca meniu iniţial.

La Compania de jucării JKL, toţi utilizatorii văd un meniu de interogare care permite accesul la majoritatea fişierelor. Pentru utilizatorii cărora nu le e permis să modifice informaţii, acesta este meniul iniţial. Opţiunea de întoarcere din meniu deconectează utilizatorul. Pentru alţi utilizatori, acest meniu este apelat de o opţiune de interogare din meniurile aplicaţiei. Apăsând F12 (Întoarcere), utilizatorul se întoarce la meniul de apelare. Deoarece se foloseşte securitatea bibliotecilor pentru bibliotecile program, acest meniu şi programul pe care îl apelează sunt păstrate în biblioteca QGPL:

```
  INQMENU       Inquiry Menu

          1. Item Descriptions
          2. Item Balances
          3. Customer Information
          4. Query
          5. Office

Enter option ==>
F1=Help  F12=Return
```

Figura 36. Exemplu de meniu de interogare

Folosirea autorizării adoptate în proiectarea meniului

Disponibilitatea uneltelor de suport decizie, cum ar fi Query/400, pune probleme es pentru proiectarea securităţii. Poate vreţi ca utilizatorii să fie capabili să vadă informaţii din fişiere folosind o unealtă de interogare, dar probabil vreţi să vă asiguraţi că fişierele sunt modificate doar de programe aplicaţie testate.

Nu există nici o metodă în definiţiile de securitate ale resursei pentru ca un utilizator să aibă autorizare diferită pentru un fişier în circumstanţe diferite. Totuşi, folosirea autorizării adoptate vă permite să definiţi autorizare pentru a îndeplini cerinţe diferite.

Notă: “Obiecte care adoptă autorizarea proprietarului” la pagina 123 descrie cum funcţionează autorizare adoptată. “Organigrama 8: Cum este verificată autorizarea adoptată” la pagina 154 descrie cum verifică sistemul autorizarea adoptată.

Figura 37 arată un meniu iniţial exemplu care foloseşte autorizare adoptată pentru a furnize acces controlat la fişiere folosind unelte de interogare:

```
MENU1         Initial Menu

        1.  Inventory Control (ICSTART)
        2.  Customer Orders   (COSTART)
        3.  Query             (QRYSTART)
        4.  Office            (OFCSTART)

(no command line)
```

Figura 37. Meniu exemplu iniţial

Programele care pornesc aplicaţii (ICSTART şi COSTART) adoptă autorizarea profilului care deţine obiectele aplicaţie. Programele adaugă biblioteci aplicaţie la lista de biblioteci şi afişează meniul aplicaţiei iniţiale. Urmează un exemplu de program de cotrol inventar (ICSTART).

```
PGM
ADDLIBLE ITEMLIB
ADDLIBLE ICPGMLIB
GO ICMENU
RMVLIBLE ITEMLIB
RMVLIBLE ICPGMLIB
ENDPGM
```

Figura 38. Program aplicaţie iniţială exemplu

Programul care porneşte Query (QRYSTART) adoptă autorizarea unui profil (QRYUSR) furnizat pentru a permite acces la fişiere pentru interogări. Figura 39 arată programul QRYSTART:

```
PGM
ADDLIBLE ITEMLIB
ADDLIBLE CUSTLIB
STRQRY
RMVLIBLE ITEMLIB
RMVLIBLE CUSTLIB
ENDPGM
```

Figura 39. Program exemplu pentru interogare cu autorizare adoptată

Sistemul meniu foloseşte trei tipuri de profiluri utilizator, arătate în Tabela 119. Tabela 120 la pagina 199 descrie obiectele folosite de sistemul meniu.

Tabela 119. Profiluri utilizatori pentru sistem meniu

Tip profil	Descriere	Parolă	Limitare capabilităţi	Autorizări speciale	Meniu iniţial
Proprietar aplicaţie	Deţine toate obiectele aplicaţie şi are autorizare *ALL. OWNIC deţine aplicaţia Control inventar.	*NONE	Nu se aplică	Aşa cum e necesar aplicaţiei	Nu se aplică
Utilizator aplicaţie [1]	Profil exemplu pentru oricine care foloseşte sistemul meniu	Da	*YES	Nimic	MENU1
Profil interogare	Folosit pentru a furniza acces la biblioteci pentru interogare	*NONE	Nu se aplică	Nimic	Nu se aplică

Tabela 119. Profiluri utilizatori pentru sistem meniu (continuare)

Tip profil	Descriere	Parolă	Limitare capabilităţi	Autorizări speciale	Meniu iniţial
[1]	Biblioteca curentă specificată în profilul utilizator al aplicaţiei e folosită pentru a memora orice interogări create. Programul Attention-key-handling este *ASSIST, dându-i acces utilizatorului la funcţiile de bază ale sistemului.				

Tabela 120. Obiecte folosite de sistem meniu

Nume obiect	Proprietar	Autorizare publică	Autorizări provate	Informaţii suplimentare
MENU1 în biblioteca QGPL	Vedeţi Nota	*EXCLUDE	Autorizare *USE pentru orice utilizator căruia îi e permis să folosească meniul	În biblioteca QGPL deoarece utilizatorii nu au autorizare pentru bibliotecile aplicaţiei
Programul ICSTART din QGPL	OWNIC	*EXCLUDE	Autorizare *USE pentru utilizatorii autorizaţi pentru aplicaţia Control inventar	Creat cu USRPRF(*OWNER) pentru a adopta autorizare OWNIC
Programul QRYSTART din QGPL	QRYUSR	*EXCLUDE	Autorizare *USE pentru utilizatorii autorizaţi să creeze sau să ruleze interogări	Creat cu USRPRF(*OWNER) pentru a adopta autorizare QRYUSR
ITEMLIB	OWNIC	*EXCLUDE	QRYUSR are *USE	
ICPGMLIB	OWNIC	*EXCLUDE		
Fişiere disponibile pentru Interogare în ITEMLIB	OWNIC	*USE		
Fişiere nedisponibile pentru Interogare în ITEMLIB	OWNIC	*EXCLUDE		
Programe din ICPGMLIB	OWNIC	*USE		

Notă: Un profil profrietar special poate fi creat pentru obiecte folosite de aplicaţii multiple.

Când USERA selectează opţiunea 1 (Inventory Control) din MENU1, rulează programul ICSTART. Programul adoptă autorizarea lui OWNIC, dând autorizare *ALL obiectelor de control al inventarului din ITEMLIB şi programelor din ICPGMLIB. USERA este astfel autorizată să facă modificări asupra fişierelor de control al inventarului în timp de folosesc opţiuni din ICMENU.

Când USERA iese din ICMENU şi se întoarce la MENU1, bibliotecile ITEMLIB şi ICPGMLIB sunt înlîturate din lista de biblioteci USERA şi programul ICSTART este înlăturat din stiva de programe. USERA nu mai rulează sub autorizarea adoptată.

Când USERA selectează opţiunea 3 (Query) din MENU1, rulează programul QRYSTART. Programul adoptă autorizarea lui QRYUSR, dând autorizare *USE bibliotecii ITEMLIB. Autorizarea publică pentru fişierele din ITEMLIB determină care fişiere are voie USERA să le interogheze.

Această tehnică are avantajul de a minimiza numărul de autorizări private şi de a furniza performanţe bune la verificarea autorizării:

- Obiectele din bibliotecile aplicaţiei nu au autorizări private. Pentru unele funcţii ale aplicaţie, autorizarea publică este adecvată. Dacă autorizarea publică nu e adecvată, e folosită autorizarea proprietar. “Cazul 8: Autorizarea adoptată fără autorizare privată” la pagina 163 arată paşii de verificare a autorizării.
- Accesul la fişierele pentru interogare foloseşte autorizare publică pentru fişiere. Profilul QRYUSR este doar specific autorizat pentru biblioteca ITEMLIB.
- Implicit, programele de interogare create sunt puse în biblioteca curentă a utilizatorului. Biblioteca curentă ar trebui să fie deţinută de utilizator şi utilizatorul ar trebui să aibă autorizare *ALL.
- Utilizatorii individuali au nevoie doar să fie autorizaţi pentru MENU1, ICSTART şi QRYSTART.

Consideraţi aceste riscuri şi precauţii când folosiţi această tehnică:

- USERA are autorizare *ALL pentru toate obiectele de control inventar din ICMENU. Asiguraţi-vă că meniul nu permite acces la o linie de comandă sau permite funcţii de ştergere şi actualizare nedorite.
- Multe unelte de suport decizie permit acces la o linie de comandă. Profilul QRYUSR ar trebui să fie un utilizator cu capabilitate limitată fără autorizări speciale pentru a preveni funcţii neautorizate.

Ignorarea autorizării adoptate

Folosirea autorizării adoptate în proiectarea meniului arată o tehnică pentru furnizarea capabilităţii de interogare fără a permite modificări necontrolate asupra fişierelor aplicaţie. Această tehnică necesită ca utilizatorul să se întoarcă la meniul iniţial înainte de a rula interogări. Dacă vreţi să furnizaţi oportunitatea de pornire a interogării din meniurile aplicaţiei precum şi din meniul iniţial, puteţi seta programul QRYSTART să ignore autorizarea adoptată.

Notă: "Programe care ignoră autorizarea adoptată" la pagina 126 furnizează informaţii suplimentară despre ignorarea autorizării adoptate. "Organigrama 8: Cum este verificată autorizarea adoptată" la pagina 154 descrie cum verifică sistemul autorizarea adoptată.

Figura 40 arată un meniu de aplicaţie care include programul QRYSTART:

```
ICMENU       Inventory Control Menu

             1.  Issues (ICPGM1)
             2.  Receipts (ICPGM2)
             3.  Purchases (ICPGM3)
             4.  Query  (QRYSTART)

(no command line)
```

Figura 40. Meniu de aplicaţie exemplu cu Query

Informaţiile de autorizare pentru programul QRYSTART sunt aceleaşi ca cele arătate în Tabela 120 la pagina 199. Programul este creat cu parametrul de autorizare adoptată de utilizare (USEADPAUT) setat pe *NO, pentru a ignora autorizarea adoptată a programelor anterioare din stivă.

Urmează comparaţii ale stivelor de programe când USERA selectează interogare din MENU1 (vedeţi Figura 37 la pagina 198) şi din ICMENU:

Stiva de programe când se selectează interogare din MENU1

MENU1 (fără autorizare adoptată)

QRYSTART (autorizare adoptată QRYUSR)

Stiva de programe când se selectează interogare din ICMENU

MENU1 (fără autorizare adoptată)

ICMENU (autorizare adoptată OWNIC)

QRYSTART (autorizare adoptată QRYUSR)

Specificând programul QRYSTART cu USEADPAUT(*NO), autorizarea oricărui program anterior din stivă nu e folosită. Asta permite USERA să ruleze interogare din ICMENU fără a avea abilitatea de a modifica şi şterge fişiere, deoarece autorizarea lui OWNIC nu e folosită de programul QRYSTART.

Când USERA termină interogarea şi se întoarce la ICMENU, autorizarea adoptată este din nou activă. Autorizarea adoptată este ignorată doar atâta timp cât programul QRYSTART este activ.

Dacă autorizarea publică pentru programul QRYSTART este *USE, specificaţi USEADPAUT(*NO) ca o precauţie de securitate. Aceasta împiedică pe oricine care rulează sub autorizarea adoptată de la apelarea programului QRYSTART şi realizarea funcţiilor neautorizate.

Meniul de interogare (Figura 36 la pagina 197) de la Compania de jucării JKL de asemenea foloseşte această tehnică, deoarece poate fi apelată din meniuri în biblioteci aplicaţie diferite. Ea adoptă autorizarea lui QRYUSR şi ignoră orice altă autorizare adoptată din stiva de programe.

Descrierea securităţii meniului

Ca un proiectant de aplicaţii, trebuie să furnizaţi informaţii despre un meniu pentru administratorul de securitate. Administratorul de securitate foloseşte aceste informaţii pentru a decide cine ar trebui să aibă acces la meniu şi ce autorizări sunt necesare. Informaţiile tipice necesare sunt:

- Dacă oricare din opţiunile din meniu necesită autorizări speciale, cum ar fi *SAVSYS sau *JOBCTL.
- Dacă opţiunile din meniu apelează programe care adoptă autorizare.
- Ce autorizare pentru obiecte e necesară pentru fiecare opţiune din meniu. Ar trebui să aveţi nevoie doar să identificaţi acele autorizări care sunt mai mari decât autorizarea publică normală.

Figura 41 arată un format exemplu pentru furnizarea acestor informaţii.

Nume meniu: MENU1 Bibliotecă: QGPL Număr opţiune: 3 Descriere: Query

Program apelat: QRYSTART Bibliotecă: QGPL

Autorizare adoptată: QRYUSR

Autorizare specială necesară: None

Autorizări obiect necesare: Utilizatorul trebuie să aibă autorizarea *USE pentru programul QRYSTART. QRYUSR trebuie să aibă autorizare *USE pentru bibliotecile conţinând fişiere care vor fi interogate. Utilizatorul, QRYUSR sau public trebuie să aibă autorizare *USE pentru fişierele care sunt interogate.

Figura 41. Cerinţe format pentru securitate meniu

Meniul Cerere sistem

Un utilizator poate folosi funcţia de cerere sistem pentru a suspenda jobul curent şi a afişa Meniul cerere sistem. Meniul cerere sistem permite utilizatorului să trimită şi să afişeze mesaje, să trasfere la un al doilea job sau să oprească jobul curent.

Când e livrat sistemul dumneavoastră, autorizarea publică pentru Meniul cerere sistem e *USE. Cea mai uşoară cale de a împiedica utilizatorii să acceseze acest meniu este prin restricţionarea autorizării la grupul de panouri QGMNSYSR:

- Pentru a împiedica anumiţi utilizatori să vadă Meniul cerere sistem, specificaţi autorizarea *EXCLUDE pentru acei utilizatori:

```
GRTOBJAUT OBJ(QSYS/QGMNSYSR) +
          OBJTYPE(*PNLGRP)   +
          USER(USERA) AUT(*EXCLUDE)
```

- Pentru a împiedica majoritatea utilizatorilor să acceseze Meniul cerere sistem, anulaţi autorizarea publică şi acordaţi autorizare *USE pentru utilizatori specifici:

```
RVKOBJAUT OBJ(QSYS/QGMNSYSR) +
          OBJTYPE(*PNLGRP) +
          USER(*PUBLIC) AUT(*ALL)
GRTOBJAUT OBJ(QSYS/QGMNSYSR) +
          OBJTYPE(*PNLGRP)   +
          USER(USERA) AUT(*USE)
```

| Unele din comenzile reale folosite pentru meniul cerere sistem vin din mesajul CPX2313 din fişierul de mesaje
| QCPFMSG. Începând cu V5R3, aceste comenzi sunt calificate după bibliotecă cu valori *NLVLIBL şi *SYSTEM din
| mesajul CPX2373. Cineva ar putea folosi comanda OVRMSGF (Override Message File - Înlocuire fişier de mesaje)
| pentru a modifica comenzile care le folosesc opţiunile meniului cerere sistem. Pentru a împiedica utilizatorii să
| înlocuiască comenzile folosire de opţiunile meniului cerere sistem, acordaţi autorizare publică *EXCLUDE pentru
| comanda OVRMSGF:

```
| GRTOBJAUT OBJ(QSYS/OVRMSGF) OBJTYPE(*CMD) USER(*PUBLIC) AUT(*EXCLUDE)
```

Puteţi împiedica utilizatorii să selecteze opţiuni specifice din Meniul cerere sistem restricţionând autorizarea pentru comenzile asociate. Tabela 121 arată comenzile asociate cu opţiunile meniului:

Tabela 121. Opţiuni şi comenzi pentru Meniul cerere sistem

Opţiune	Comandă
1	Transferare job secundar (TFRSECJOB)
2	Terminare cerere (ENDRQS)
3	Afişare job (DSPJOB)
4	Afişare mesaj (DSPMSG)
5	Trimitere mesaj (SNDMSG)
6	Afişare mesaj (DSPMSG)
7	Afişare utilizator staţie de lucru (DSPWSUSR)
10	Pornire cerere sistem la sistemul precedent (TFRPASTHR). (Vedeţi nota de mai jos.)
11	Transferare la sistemul anterior (TFRPASTHR). (Vedeţi nota de mai jos.)
12	Afişare opţiuni de emulare 3270 (Vedeţi nota de mai jos.)
13	Pornire cerere sistem pe sistemul home (TFRPASTHR). (Vedeţi nota de mai jos.)
14	Transferare la sistemul home (TFRPASTHR). (Vedeţi nota de mai jos.)
15	Transferare la sistemul capăt (TFRPASTHR). (Vedeţi nota de mai jos.)
50	Terminare cerere pe sistemul la distanţă (ENDRDBRQS). (Vedeţi nota de mai jos.)
80	Deconectare job (DSCJOB)
90	Sign-Off (SIGNOFF)

Note:

1. Opţiunile 10, 11, 13, 14 şi 15 sunt afişate doar dacă passthrough-ul staţiei de afişare a fost pornit cu comanda STRPASTHR (Start Pass-Through - Pornire passthrough). Opţiunile 10, 13 şi 14 sunt afişate doar pe sistemul destinaţie.
2. Opţiunea 12 e afişată doar unde emularea 3270 este activă.
3. Opţiunea 50 este afişată doar dacă un job la distanţă e activ.
4. Unele din opţiuni au restricţii pentru mediul System/36.

De exemplu, pentru a împiedica utilizatorii să transfere la un job interavtiv alternativ, anulaţi autorizarea publică pentru comanda TFRSECJOB (Transfer to Secondary Job - Transfer la un job secundar) şi acordaţi autorizare doar utilizatorilor specifici:

```
RVKOBJAUT OBJ(TFRSECJOB) OBJTYPE(*CMD)
          USER(*PUBLIC) AUT(*ALL)
GRTOBJAUT OBJ(TFRSECJOB) OBJTYPE(*CMD)
          USER(USERA) AUT(*USE)
```

Dacă un utilizator selectează o opţiune pentru care nu are autorizare, e afişat un mesaj.

Dacă vreţi să împiedicaţi utilizatorii de la folosirea generală a comenzilor din meniul cerere sistem dar tot vreţi să fie capabili să ruleze o comandă la un moment specific (cum ar fi la sign-off), puteţi crea un program CL care adoptă autorizarea unui utilizator autorizat şi rulează comanda.

Planificarea securităţii comenzii

Securitatea meniului e o tehnica buna pentru utilizatorii care au nevoie de aplicaţii şi de funcţii sistem limitate. Unii utilizatori au nevoie de un mediu mai flexibil şi de capabilitatea de a rula comenzi. Când sistemul dumneavoastră ajunge, abilitatea de folosire comenzi e setată să îndeplinească nevoile de securitate ale majorităţii instalărilor. Unele comenzi pot fi rulate doar de un responsabil cu securitatea. Altele necesită o autorizare specială, cum ar fi *SAVSYS. Majoritatea comenzilor pot fi folosite de oricine pe sistem.

Puteţi modifica autorizarea pentru comenzi pentru a îndeplini cerinţele dumneavoastră de securitate. De exemplu, poate vreţi să împiedicaţi majoritatea utilizatorilor de pe sistemul dumneavoastră să lucreze cu comunicaţii. Puteţi seta autorizarea publică pe *EXCLUDE pentru toate comenzile care lucrează cu obiecte de comunicaţie, cum ar fi comenzile CHGCTLxxx, CHGLINxxx, şi CHGDEVxxx.

Dacă aveţi nevoie să controlaţi care comenzi pot fi rulate de utilizatori, puteţi folosi autorizarea obiect pentru comenzile inseşi. Fiecare comandă de pe sistem are tipul obiect *CMD şi poate fi autorizată pentru public sau orice utilizator specific. Pentru a rula o comandă, utilizatorul are nevoie de autorizare *USE pentru ea. Anexa C listează toate comenzile care sunt livrate cu autorizarea publică setată pe *EXCLUDE.

Dacă folosiţi biblioteca System/38, aveţi nevoie să restricţionaţi comenzile relative pentru securitate de asemenea în acea bibliotecă. Sau aţi putea restricţiona accesul la întreaga bibliotecă. Dacă folosiţi una sau mai multe versiuni de limbă naţionalăOS/400 a programului licenţiat pe sistemul dumneavoastră, aveţi nevoie să restricţionaţi comenzile în bibliotecile QSYSxxx suplimentare din sistemul dumneavoastră de asemenea.

O altă masură de securitate folositoare este să modificaţi valorile implicite pentru unele comenzi. Comanda CHGCMDDFT (Change Command Default - Modificare valoare implicită a comenzii) vă permite să faceţi asta.

Planificarea securităţii fişierului

Informaţiile conţinute în fişierele de bază de date sunt de obicei cele mai importante bunuri de pe sistemul dumneavoastră. Securitatea resursei vă permite să controlaţi cine poate vedea, modifica şi şterge informaţii dintr-un fişier. Dacă utilizatorii necesită autorizări diferite pentru fişiere în funcţie de situaţie, puteţi folosi autorizarea adaptivă. “Folosirea autorizării adoptate în proiectarea meniului” la pagina 197 dă un exemplu pentru această metodă.

Pentru fişiere critice de pe sistemul dumneavoatră, păstraţi o evidenţă a utilizatorilor care au autorizare pentru fişier. Dacă folosiţi autorizare de grup şi liste de autorizare, trebuie să ţineţi evidenţa utilizatorilor care au autorizare prin aceste metode, precum şi a celor care sunt autorizaţi direct. Dacă folosiţi autorizare adoptată, puteţi lista programe care adoptă autorizarea unui utilizator particular folosind comanda DSPPGMADP (Display Program Adopt - Afişare program adoptare).

Puteţi folosi de asemnea funcţia de jurnalizare de pe sistem pentru a monitoriza activitatea unui fişier critic. Deşi intenţia primară a unui jurnal este să recupereze informaţii, poate fi folosit ca o unealtă de securitate. El conţine o înregistrare a celor care au accesat un fişier şi în ce fel. Puteţi folosi comanda DSPJRN (Display Journal - Afişare jurnal) pentru a vedea un exemplu de intrări jurnal periodic.

Securizarea fişierelor logice

Securitatea resursei din sistem suportă securitate la nivel de câmp a unui fişier. Puteţi de asemenea folosi fişiere logice pentru a proteja câmpuri pecifice sau înregistrări dintr-un fişier. Vedeţi subiectul Baza de date universală DB2 pentru iSeries din Centrul de informare pentru informaţii suplimentare. Vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii.

Un fişier logic poate fi folosit pentru a specifica un subset de *înregistrări* pe care un utilizator le poate accesa (folosind logică de selecţie şi omitere). Aşadar, utilizatori specifici pot fi împiedicaţi să acceseze anumite tipuri de înregistrări. Un fişier logic poate fi folosit pentru a specifica un subset de *câmpuri* într-o înregistrare pe care o poate accesa un utilizator. Aşadar, utilizatori specifici pot fi împiedicaţi să acceseze anumite câmpuri dintr-o înregistrare.

Un fişier logic nu conţine nici o dată. Este o vizualizare particulară a unui sau mai multor fişiere care conţin datele. Furnizarea accesului la informaţiile definite de un fişier logic necesită autorizare de date atât pentru fişierul logic cât şi pentru fişierele fizice asociate.

Figura 42 la pagina 204 arată un exemplu de fişier fizic şi trei fişiere logice diferite asociate cu el.

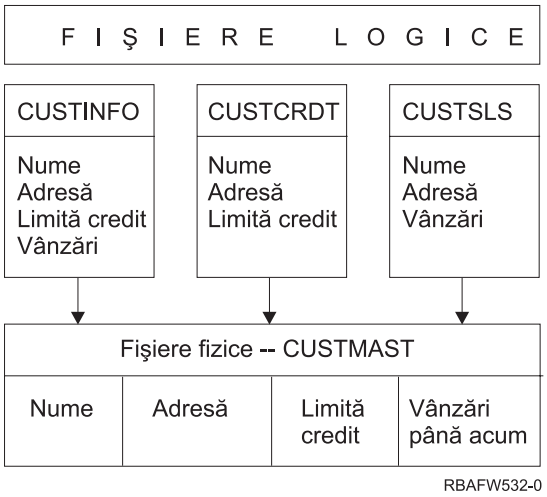

Figura 42. Folosire fişier logic pentru securitate

Membrilor departamentului de vânzări (profilul de grup DPTSM) le e permis să vadă toate câmpurile, dar nu pot modifica limita de credit. Membrilor departamentului conturi de primit (profil de grup DPTAR) le e permis să vadă toate câmpurile, dar nu pot modifica câmpul vânzări. Autorizarea pentru fişierul fizic arată astfel:

Tabela 122. Exemplu filier fizic: Fişier CUSTMAST

Autorizare	**Utilizatori: *PUBLIC**
Autorizări obiect	
*OBJOPR	
*OBJMGT	
*OBJEXIST	
*OBJALTER	
*OBJREF	
Autorizări pentru date	
*READ	X
*ADD	X
*UPD	X
*DLT	X
*EXECUTE	X
*EXCLUDE	

Publicul ar trebui să aibă toate autorizările pentru date, dar nu şi autorizare de operare asupra obiectelor din fişierul fizic CUSTMAST. Publicul nu poate accesa fişierul CUSTMAST direct, deoarece este necesară autorizarea *OBJOPR pentru a deschide un fişier. Autorizarea publicului face ca toate drepturile asupra datelor să fie potenţial disponibile pentru utilizatorii fişierului logic.

Autorizarea pentru fişierul logic arată astfel:

```
                        Display Object Authority

Object . . . . . :   CUSTINFO      Owner  . . . . . :   OWNAR
  Library  . . . . . :   CUSTLIB       Primary group  . . . :   *NONE
Object type  . . . . :   *FILE         ASP device . . . . . :   *SYSBAS

Object secured by authorization list  . . . . . . . . . . . :   *NONE

                       Object
User        Group      Authority
*PUBLIC                *USE
```

```
                        Display Object Authority

Object . . . . . :   CUSTCRDT      Owner  . . . . . :   OWNAR
  Library  . . . . . :   CUSTLIB       Primary group  . . . :   DPTAR
Object type  . . . . :   *FILE         ASP device . . . . . :   *SYSBAS

Object secured by authorization list  . . . . . . . . . . . :   *NONE

                       Object
User        Group      Authority
DPTAR                  *CHANGE
*PUBLIC                *USE
```

```
                        Display Object Authority

Object . . . . . :   CUSTSLS       Owner  . . . . . :   OWNSM
  Library  . . . . . :   CUSTLIB       Primary group  . . . :   DPTSM
Object type  . . . . :   *FILE         ASP device . . . . . :   *SYSBAS

Object secured by authorization list  . . . . . . . . . . . :   *NONE

                       Object
User        Group      Authority
DPTSM                  *CHANGE
*PUBLIC                *USE
```

Pentru ca această schemă de autentificare să funcţioneze nu este necesar ca profilul de grup, cum ar fi DPTSM, să fie făcut grup primar pentru fişierul logic. Totuşi, folosirea autorizării de grup primar elimină căutarea autorizărilor private atât pentru utilizatorul care încearcă să acceseze fişierul, cât şi pentru grupul utilizatorului. “Cazul 2: Folosirea autorizării grupului primar” la pagina 159 arată cum folosirea autorizării de grup primar afectează autorizarea care verifică procesul.

Puteţi specifica autorizări de date pentru fişiere logice începând cu V3R1 a programului OS/400 licenţiat. Când vă mutaţi la V3R1 de la o versiune anterioară, sistemul converteşte fişierele dumneavoastră logice când e instalat. Prima dată când e accesat un fişier logic, sistemul dă toate autorizările de date.

Pentru a folosi fişiere logice ca unealtă de securitate, faceţi următoarele:

- Acordaţi toate autorizările de date fişierelor fizice subliniate.
- Anulaţi *OBJOPR de la fişierele fizice. Asta împiedică utilizatorii să acceseze fişierele fizice direct.

- Acordaţi autorizările de date corespunzătoare pentru fişierele logice. Anulaţi orice autorizare pe care n-o vreţi.
- Acordaţi *OBJOPR pentru fişierele logice.

Înlocuirea fişierelor

Comenzile de înlocuire pot fi folosite pentru ca un program să utilizeze un fişier diferit cu acelaşi format. De exemplu, presupuneţi că un program din aplicaţia contracte şi preţuri din Compania de jucării JKL scrie informaţii despre preţ într-un fişier de lucru înainte de a face modificările de preţ. Un utilizator cu acces la o linie de comandă care dorea să captureze informaţii confidenţiale poate folosi o comandă de înlocuire pentru a face ca programul să scrie date într-un fişier diferit într-o bibliotecă controlată de utilizator. Vă puteţi asigura că un program procesează fişierele corecte folosind comenzi de înlocuire cu SECURE(*YES) înainte ca programul să ruleze.

Securitatea fişierului şi SQL

SQL (Structured Query Language) foloseşte fişiere cross-reference pentru a ţine evidenţa fişierelor bază de date şi relaţiile dintre ele. La aceste fişiere se referă colectiv drept catalog SQL. Autorizarea publică pentru catalogul SQL este *READ. Asta înseamnă că orice utilizator care are acces la interfaţa SQL poate afişa numele şi descrierile text pentru toate fişierele de pe sistemul dumneavoastră. Catalogul SQL nu afectează autorizarea normală necesară pentru a accesa conţinutul fişierelor bază de date.

Ar trebui să aveţi grijă când folosiţi un program CL care adoptă autorizare pentru a porni SQL sau Query Manager. Aceste două programe de interogare permit utilizatorilor să specifice un nume de fişier. Utilizatorul poate, aşadar, să acceseze orice fişier la care profilul adoptat are autorizare.

Planificarea listelor de autorizări

O listă de autorizaţii are aceste avantaje:

- Listele de autorizaţii simplifică destionarea autorizaţiilor. Autorizarea utilizatorului e definită pentru lista de autorizaţii, nu pentru obiectele individuale din listă. Dacă un obiect nou e securizat de lista de autorizaţii, utilizatorii din listă primesc autorizare pentru el.
- O operaţie poate fi folosită pentru a da unui utilizator autorizare pentru toate obiectele din listă.
- Listele de autorizaţii reduc numărul autorizărilor private din sistem. Fiecare utilizator are o autorizare privată pentru un obiect, lista de autorizaţii. Aceasta îi dă utilizatorului autorizare pentru toate obiectele din listă. Reducerea numărului de autorizări private din sistem are următoarele avantaje:
  - Reduce dimensiunea profilului utilizator.
  - Îmbunătăţeşte performanţele la salvarea sistemului (SAVSYS) sau salvarea datelor de securitate (SAVSECDTA).
- Listele de autorizaţii furnizează o cale bună de a securiza fişiere. Dacă folosiţi autorizări private, fiecare utilizator va avea o autorizate privată pentru fiecare membru fişier. Dacă folosiţi o listă de autorizaţii, fiecare utilizator va avea doar o autorizare. De asemenea, fişierele care sunt deschise nu pot să aibă autorizare acordată sau anulată din fişier. Dacă securizaţi fişierul cu o listă de autorizaţii, puteţi modifica autorizările, chiar când fişierul e deschis.
- Listele de autorizaţii furnizează o cale de a memora autorizările când este salvat un obiect. Când este salvat un obiect care e securizat de o listă de autorizaţii, numele listei e salvat cu obiectul. Dacă obiectul e şters şi restaurat pe **acelaşi** sistem, e legat automat din nou la lista de autorizaţii. Dacă obiectul e restaurat pe un sistem diferit, lista de autorizaţii nu e legată, decât dacă se specifică ALWOBJDIF(*ALL) în comanda de restaurare.

Avantajele folosirii unei liste de autorizări

Din punctul de vedere al gestionării securităţii, o listă de autorizaţii este metoda preferată pentru a gestiona obiectele care au aceleaşi cerinţe de securitate. Chiar şi când sunt doar câteva obiecte care vor securizate de listă, mai e totuşi un avantaj să folosiţi o listă de autorizaţii în loc să folosiţi autorizări private pentru obiect. Deoacere autorizările sunt într-un loc (lista de autorizaţii), este mai uşor să modificaţi cine e autorizat pentru obiecte. De asemenea e mai uşor să securizaţi orice obiecte noi cu aceleaşi autorizări ca obiectele existente.

Dacă folosiţi liste de autorizaţii, atunci nu ar trebui să aveţi autorizări private pentru obiect. Sunt necesare două căutări ale autorizărilor private ale utilizatorului în timpul verificării lor dacă obiectul are autorizări private şi obiectul e de

asemenea securizat cu o listă de autorizaţii. Prima căutare este pentru autorizările private pentru obiect; cea de-a doua e pentru autorizările private din lista de autorizaţii. Două căutări necesită utilizarea resurselor sistemului; aşadar, performanţele pot fi alterate. Dacă folosiţi doar lista de autorizaţii, se realizează doar o căutare. De asemenea, deoarece folosirea cache-ului autorizării cu lista de autorizaţii, performaţa pentru verificarea autorizării va fi aceeaşi ca cea pentru verificarea doar a autorizărilor private pentru obiect.

La Compania de jucării JKL, o listă de autorizaţii este folosită pentru a securiza toate fişierele de lucru folosite în procesare inventarului la sfârşit de lună. Aceste fişiere de lucru sunt curăţate, ceea ce necesită autorizare *OBJMGT. Pe măsură ce cerinţele aplicaţiei se modifică, mai multe fişiere de lucru pot fi adăugate aplicaţiei. De asemenea, pe măsură ce responsabilităţile jobului se modifică, utilizatori diferiţi rulează procesarea de la sfârşit de lună. O listă de autorizaţii face mai simplă gestionarea acestor modificări.

Urmează paşii pentru a seta lista de autorizaţii:

1. Creaţi lista de autorizaţii:
   ```
   CRTAUTL ICLIST1
   ```
2. Securizaţi toate fişierele de lucru cu lista de autorizaţii:
   ```
   GRTOBJAUT OBJ(ITEMLIB/ICWRK*) +
             OBJTYP(*FILE) AUTL(ICLIST1)
   ```
3. Adăugaţi utilizatori la listă care realizează procesare la sfârşit de lună:
   ```
   ADDAUTLE AUTL(ICLIST1) USER(USERA) AUT(*ALL)
   ```

Planificarea profilurilor de grup

Un profil de grup este o unealtă folositoare când mai mulţi utilizatori au cerinţe de securitate similare. Sunt folositoare în special când cerinşele jobului şi apartenenţa la grup se modifică. De exemplu, dacă membrii unui departament au responsabilitate pentru o aplicaţie, un profil de grup poate fi setat pentru departament. Pe măsură de utilizatorii întră sau părăsesc departamentul, câmpul profil de grup din profilurile lor utilizator se pot modifica. Aceasta este mai uşor de gestionat decât înlăturarea autorizărilor individuale din profiluri utilizator.

Puteţi crea profiluri specific pentru a fi profiluri de grup sau puteţi face unul existent într-un profil de grup. Un profil de grup este un tip special de profil utilizator. El devine un profil de grup când se întâmplă una din următoarele:

- Alt profil îl desemnează ca profil de grup
- Îi asignaţi un număr de identificare a grupului (gid).

De exemplu:

1. Creaţi un profil numit GRPIC:
   ```
   CRTUSRPRF GRPIC
   ```
2. Când profilul e creat, e un profil obişnuit, nu unul de grup.
3. Desemnaţi GRPIC ca profilul de grup pentru alt profilul de grup:
   ```
   CHGUSRPRF USERA GRPPRF(GRPIC)
   ```
4. Sistemul acum tratează GRPIC ca un profil de grup şi îi asignează un gid.

Planificarea grupurilor primare pentru obiecte

Orice obiect de pe sistem poate avea un grup primar. Autorizarea pentru grupul primar poate furniza un avantaj în performanţe dacă grupul primar este primul pentru majoritatea utilizatorilor unui obiect.

Deseori, un grup de utilizatori e responsabil pentru unele informaţii din sistem, cum ar fi informaţiile despre client. Acel grup necesită mai multă autorizare pentru informaţii decât alţi utilizatori ai sistemului. Folosind autorizare pentru grup primar, puteţi seta acest tip de schemă de autorizare fără a afecta performanţele verificării autorizării. “Cazul 2: Folosirea autorizării grupului primar” la pagina 159 arată un exemplu pentru asta.

Planificarea profilurilor de grup multiple

Un utilizator poate fi membru a până la 16 grupuri: primul grup (parametrul GRPPRF din profilul utilizator) şi 15 grupuri suplimentare (parametrul SUPGRPPRF din profilul utilizator). Folosind profiluri de grup, puteţi gestiona autorizarea mai eficient şi reduce numărul de autorizări private individuale pentru obiecte. Însă folosirea greşită a profilurilor de grup poate avea un efect negativ asupra performanţelor verificării autorizării.

Urmaţi aceste sugestii la folosirea profilurilor de grup multiple:

- Încercaţi să folosiţi grupuri multiple în combinaţie cu autorizarea grupului primar şi eliminaţi autorizarea privată pentru obiecte.
- Planificaţi cu atenţie ordinea în care profilurile de grup sunt asignate unui utilizator. Primul grup al utilizatorului trebuie să se refere la asignarea primară a utilizatorului şi la obiectele folosite mai des. De exemplu, să presupunem că un utilizator numit WAGNERB lucrează de obicei la inventariere şi din când la introducerea comenzilor. Profilul necesar pentru autorizarea de inventar (DPTIC) trebuie să fie primul grup al lui WAGNERB. Profilul necesar pentru introducerea de comenzi (DPTOE) trebuie să fie grupul suplimentar al lui WAGNERB.

  Notă: Ordinea în care sunt specificate autorizările private pentru un obiect nu are nici un efect asupra performanţelor verificării autorizării.
- Dacă intenţionaţi să folosiţi grupuri multiple, studiaţi procesul de verificare a autorizării descris în “Cum verifică sistemul autorizarea” la pagina 142. Asiguraţi-vă că înţelegeţi cum folosirea grupurilor multiple în combinaţie cu alte tehnici de autorizare, cum ar fi liste de autorizare, vă poate afecta performaţa sistemului.

Acumularea autorizărilor speciale pentru membrii profilurilor de grup

Autorizările speciale ale profilurilor de grup sunt disponibile membrilor acelui grup. Profilurile utilizator care sunt membri a unul sau mai multor grupuri au propriile autorizări speciale, plus autorizările speciale ale oricărui profil de grup pentru care utilizatorul e mumbru. Autorizările speciale sunt cumulative pentru utilizatorii care sunt membri ale grupurilor multiple. De exemplu, presupuneţi că profilul GROUP1 are *JOBCTL, profilul GROUP3 are *AUDIT şi profilul GROUP16 au autorizările speciale *IOSYSCFG. Un profil utilizator care are toate cele trei profiluri ca profilurile sale de grup are autorizările speciale *JOBCTL, *AUDIT şi *IOSYSCFG.

Notă: ATENŢIE

Dacă un membru de grup deţine un program, acesta adoptă doar autorizarea deţinătorului. Autorizările grupului sunt **not** adoptate.

Folosirea unui profil individual ca profil de grup

Crearea profilurilor specific pentru a fi profiluri de grup este preferabilă transformării profilurilor existente în profiluri de grup. Puteţi găsi că un utilizator specific are toate autorizările necesare pentru un grup de utilizatori şi poate fi tentat să facă acel profil utilizator un profil de grup. Totuşi, folosirea unui profil individual ca profil de grup poate cauza probleme în viitor:

- Dacă utilizatorul al cărui profil este folosit ca profil de grup modifică responsabilităţile, un nou profil necesită să fie desemnat ca profil de grup, autorizările necesită să fie modificate şi dreptul de proprietate necesită să fie transferat.
- Toţi membriii grupului automat au autorizare pentru orice obiect creat de profilul de grup. Utilizatorul al cărui profil este profilul de grup pierde abilitatea de a avea obiecte private, doar dacă acel utilizatorul nu exclude specific alţi utilizatori.

Încercaţi să planificaţi profiluri de grup în avans. Creaţi profiluri de grup specifice cu parola *NONE. Dacă descoperiţi după ce o aplicaţie a rulat că un utilizator are autorizări care ar trebui să aparţină unui grup de utilizatori, faceţi următoarele:

1. Creaţi un profil de grup.
2. Folosiţi comanda GRTUSRAUT pentru a da autorizările utilizatorului pentru profilul de grup.
3. Înlăturaţi autorizările private din utilizator, deoarece ele nu mai sunt necesare. Folosiţi comanda RVKOBJAUT sau EDTOBJAUT.

Comparaţie între profilurile de grup şi listele de autorizări

Profilurile de grup sunt folosite pentru a simplifica gestionarea profilurilor utilizator care au cerinţe de securitate similare. Listele de autorizaţii sunt folosite pentru a securiza obiecte cu cerinţe de securitate similare. Tabela 123 arată caracteristicile celor două metode:

Tabela 123. Comparaţie între lista de autorizaţii şi profilul de grup

Articolul comparat	Listă de autorizaţii	Profil de grup
Folosit pentru a securiza obiecte multiple	Da	Da
Utilizatorul poate apaţine mai multora	Da	Da
Autorizarea privată înlocuieşte altă autorizare	Da	Da
Utilizatorului trebuie să-i fie asignată autorizare independent	Da	Nu
Autorizările specificate sunt aceleaşi pentru toate obiectele	Da	Nu
Obiectul poate fi securizat de mai mult de unul	Nu	Da
Autorizarea poate fi specificată când este creat obiectul	Da	Da [1]
Poate securiza toate tipurile de obiecte	Nu	Da
Asocierea cu obiectul este ştearsă când obiectul este şters	Da	Da
Asocierea cu obiectul este salvată când obiectul este salvat	Da	Nu [2]

1 Profilului de grup îi poate fi acordată autorizare când este crea un obiect folosind parametrul GRPAUT din profilul utilizatorului care îl creează.

2 Autorizarea de grup primar este salvată cu obiectul.

Planificarea securităţii pentru programatori

Programtorii reprezintă o problemă pentru responsabilul cu securitatea. Cunoştinţele lor îi pot face să ocolească procedurile de securitate care nu sunt proiectate cu atenţie. Ei pot acoli securitatea pentru a accesa date de care au nevoie pentru testare. De asemenea ei pot dejuca procedurile normale care alocă resurse ale sistemului pentru a realiza performanţe mai bune pentru propriile joburi. Securitatea e deseori vazută de ei ca un obstacol pentru realizarea task-urilor cerute de jobul lor, cum ar fi testarea aplicaţiilor. Totuşi, acordarea de prea multe autorizări programatorilor din sistem contrazice principiul de securitate al datoriilor separate. Ea permite de asemenea unui programator să instaleze programe nedorite.

Urmaţi aceste linii când csetaţi un mediu pentru programatorii de aplicaţii:

- Nu acordaţi **toate** autorizările speciale programatorilor. Totuşi, dacă trebuie să le daţi autorizări speciale, daţi-le **doar** autorizarea specială necesară pentru a realiza joburile sau task-urile asignate programatorului.
- Nu folosiţi profilul utilizator QPGMR ca un profil de grup pentru programatori.
- Folosiţi biblioteci de test şi împiedicaţi accesul la bibliotecile de producţie.
- Creaţi biblioteci ale programatorilor şi folosiţi un program care adoptă autorizare pentru a copia datele de producţie selectate în bibliotecile programatorului pentru testare.
- Dacă performanţele interactive sunt o problemă, consideraţi modificarea comenzilor pentru crearea programelor să ruleze doar în batch:

  ```
  CHGCMD CMD(CRTxxxPGM) ALLOW(*BATCH *BPGM)
  ```

- Realizaţi auditarea securităţii funcţiei aplicaţiei înainte de mutarea aplicaţiilor sau a modificărilor de program din bibliotecile de testare în cele de producţie.
- Folosiţi tehnica de profil de grup când e dezvoltată o aplicaţie. Toate programele aplicaţie să fie deţinute de un profil de grup. Faceţi programatorii care lucrează la aplicaţie membri ai grupului şi definiţi profilurile utilizator ale programatorului ca grupul să deţină orice obiecte noi create (OWNER(*GRPPRF)). Când un programator se mută de la un proiect la altul, puteţi modifica informaţiile de grup din profilul său. Vedeţi “Dreptul de proprietate al grupului asupra obiectelor” la pagina 118 pentru informaţii suplimentare.
- Dezvoltaţi un plan pentru asignarea dreptului de proprietate asupra aplicaţiilor când sunt mutate la producţie. Pentru a controla modificările asupra unei aplicaţii de producţie, toate obiectele aplicaţiei, inclusiv programele trebuie să fie deţinute de profilul utilizator proiectat pentru aplicaţie.

Obiectele aplicaţiei nu ar trebui deţinute de un programator deoarece acesta ar avea acces necontrolat la ele într-un mediu de producţie. Profilul care deţine aplicaţia poate fi cel al individului responsabil pentru aplicaţie sau poate fi profilul creat specific ca deţinător al aplicaţiei.

Gestionarea fişierelor sursă

Fişierele sursă sunt importante pentru integritatea sistemului dumneavoastră. Ele pot fi de asemenea un bun valoros al companiei, dacă aţi dezvoltat sau obţinut aplicaţii personalizate. Fişierele sursă ar trebui să fie protejate ca şi alte fişiere importante de pe sistem. Consideraţi punerea fişierelor sursă în biblioteci separate şi controlarea celor care le pot actualiza şi muta la producţie.

Când e creat un fişier sursă pe sistem, autorizarea publică implicită este *CHANGE, care permite oricărui utilizator să actualizeze orice mumbru sursă. Implicit, doar proprietarul fişierului sursă sau un utilizator cu autorizarea specială*ALLOBJ poate adăuga sau înlătura membri. În majoritatea cazurilor, această autorizare implicită pentru fişiere sursă fizice ar trebui modificată. Programatorii care lucrează la o aplicaţie au nevoie de autorizarea *OBJMGT pentru fişierele sursă pentru a adăuga membri noi. Autorizarea publică ar trebui probabil să fie redusă la *USE sau *EXCLUDE, doar dacă fişierele nu sunt într-o bibliotecă controlată.

Planificarea securităţii pentru programatori de sistem sau manageri

Majoritatea sistemelor au pe cineva responsabil pentru funcţii de administrare. Această persoană monitorizează folosirea resurselor sistemului, în special spaţiul de stocare de pe disc, pentru a se asigura că utilizatorii înlătură regulat obiectele nefolosite pentru a elibera spaţiu. Programatorii de sistem au nevoie de autorizare mare pentru a observa toate obiectele din sistem. Totuşi, nu au nevoie să vadă conţinutul acelor obiecte.

Puteţi folosi autorizare adoptată pentru a furniza un set de comenzi de afişare pentru programatorii de sistem, mai degrabă decât să daţi autorizări speciale în profilurile lor utilizator.

Planificarea folosirii obiectelor din lista de validare

Obiectele listei de validare sunt un nou tip de obiect în Versiunea 4, Ediţia 1, care furnizează o metodă pentru aplicaţii de a memora sigur informaţiile de autentificare utilizator.

De exemplu, ICS (Internet Connection Server) foloseşte liste de validare pentru a implementa conceptul de **utilizator Internet**. Pentru Versiunea 4, Ediţia 1, ICS poate realiza **autentificare de bază** înainte să fie servită o pagină web. Autentificarea de bază necesită ca utilizatorii să furnizeze un tip de informaţii de autentificare, cum ar fi parolă, PIN sau număr de cont. Numele utilizatorului şi informaţiile de autentificare pot fi memorate sigur într-o listă de validare. ICS poate folosi informaţiile din listele de validare mai degrabă decât să ceară ca toţi utilizatorii săi să aibă iSeries un id utilizator şi o parolă.

Unui utilizator de internet îi poate fi permis sau refuzat accesul la iSeries de pe serverul web. Utilizatorul, totuşi, nu are nici o autorizare pentru iSeries nici o resursă sau autorizare să semneze sau să ruleze joburi. Un iSeries profil utilizator nu e niciodată creat pentru utilizatori internet.

Pentru a crea şi şterge listele de validare, puteţi folosi comenzile CL CRTVLDL (Create Validation List - Creare listă de validare) şi DLTVLDL (Delete Validation List - Ştergere listă de validare). Sunt furnizate de asemenea API-uri (Application Programming Interfaces) pentru a permite aplicaţiilor să adauge, modifice, înlăture, verifice (autentifice) şi să găsească intrări într-o listă de validare. Pentru informaţii suplimentare şi exemple, vedeţi subiectul API-uri din Centrul de informare (vedeţi“Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii).

Obiectele listei de validare sunt disponibile pentru folosirea de către toate aplicaţiile. De exemplu, dacă o aplicaţie necesită o parolă, parolele aplicaţiei pot fi memorate într-un obiect al listei de validare mai degrabă decât într-un fişier bază de date. Aplicaţia poate folosi API-urile listei de validare pentru a averifica parola unui utilizator, care e criptată, mai degrabă decât ca aplicaţia să realizeze verificarea însăşi.

În Versiunea 4, Ediţia 1, informaţiile de autentificare (parolă, PIN, număr de cont) care sunt asociate cu o listă de validare sunt mereu păstrate într-o formă care nu poate fi decripată, ce nu poate fi returnată utilizatorului.

În Versiunea 4, Ediţia 2, puteţi alege să memoraţi informaţiile de autentificare într-o formă decriptabilă. Dacă un utilizator are securitatea corespunzătoare, informaţiile de autentificare pot fi descriptate şi returnate utilizatorului. Pentru informaţii despre controlarea memorării datelor decriptibile în liste de validare, vedeţi “Reţinerea informaţiilor de securitate server (QRETSVRSEC)” la pagina 27.

Limitarea accesului la funcţia programului

Limitarea accesului la funcţia programului vă permite să definiţi cine poate folosi o aplicaţie, părţi din ea sau funcţiile dintr-un program. Acest suport **nu** e o înlocuire a securităţii resursei. Funcţia de limitare a accesului la program nu împiedică un utilizator să acceseze o resursă (cum ar fi un fişier sau program) din altă interfaţă.

Suportul funcţiei de limitare a accesului la program furnizează API-uri pentru a :

- Înregistra o funcţie
- Extrage informaţii despre funcţie
- Defini cine poate şi cine nu o poate folosi
- Verifica dacă utilizatorului îi e permis să folosească funcţia

Pentru a folosi acest suport în interiorul aplicaţiei, furnizorul ei trebuie să înregistreze funcţiile când e instalată aplicaţia. Funcţia înregistrată corespunde unui bloc de cod pentru funcţii specifice din aplicaţie. Când utilizatorul rulează aplicaţia, ea apelează API-urile de folosire pentru a vedea dacă utilizatorului îi e permis să folosească funcţia care e asociată cu blocul de cod, înainte de a-l apela. Dacă utilizatorului îi e permis să folosească funcţia înregistrată, este rulat blocul de cod. Dacă utilizatorului nu îi e permis să folosească funcţia, utilizatorul este împiedicat să ruleze blocul de cod.

Administratorul de sistem specifică cui îi e permis sau refuzat accesul la o funcţie. Administratorul poate fie să folosească comanda WRKFCNUSG (Work with Function Usage Information - Gestionare informaţii folosire funcţie) pentru a gestiona accesul la funcţia programului fie să folosească Navigatorul iSeries.

Capitolul 8. Salvarea de rezervă şi recuperarea informaţiilor de securitate

În acest capitol este discutată relaţia dintre securitate şi salvarea de rezervă şi recuperarea pe sistemul dumneavoastră:

- Modul în care informaţiile despre securitate sunt salvate şi restaurate
- Modul în care securitatea afectează salvarea şi restaurarea obiectelor
- Probleme de securitate asociate cu autorizarea speciale *SAVSYS

Această *Backup and Recovery* carte furnizează informaţii suplimentare despre copierea de rezervă şi recuperare. Puteţi de asemenea să consultaţi subiectele Copierea de rezervă şi recuperarea din Centrul de informare iSeries (consultaţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii).

Salvarea informaţiilor dumneavoastră de securitate este la fel de importantă ca salvarea datelor dumneavoastră. În anumite ssituaţii, este posibil să fie nevoie să recuperaţi profiluri de utilizator, autorizări de obiecte şi date pe sistemul dumneavoastră. În cazul în care nu aveţi salvate informaţiile dumneavoastră de securitate, va trebui să reconstruiţi manual profilurile utilizator şi autorizările de obiecte. Aceasta poate fi o activitate consumatoare de timp şi poate duce la erori şi la probleme de securitate.

Planificarea procedurilor corespunzătoare de copiere de rezervă şi recuperare pentru informaţiile de securitate necesită înţelegerea modului în care informaţiile sunt stocate, salvate şi restaurate.

Tabela 124 arată comenzile folosite pentru a salva şi restaura informaţiile de securitate. Această secţiune discută despre salvarea şi recuperarea datelor de securitate în detaliu.

Tabela 124. Modul în care informaţiile de securitate sunt salvate şi restaurate

	Comenzi de salvare şi restaurare				
Informaţiile de securitate salvate şi restaurate	**SAVSECDTA SAVSYS**	**SAVCHGOBJ SAVOBJ SAVLIB SAVDLO SAVCFG**	**RSTUSRPRF**	**RSTOBJ RSTLIB RSTDLO RSTCFG**	**RSTAUT**
Profiluri de utilizator	X		X		
Dreptul de proprietate [1]		X		X	
Grup primar [1]		X		X	
Autorizări publice [1]		X		X	
Autorizări private	X				X
Liste de autorizare	X		X		
Deţinător de autoruzare	X		X		
Legătura cu lista de autorizare şi deţinătorii de autorizare		X		X	
Valoare auditare obiect		X		X	
Informaţii înregistrare funcţie [2]		X		X	
Informaţii de folosire funcţie	X		X		X

1 Comenzile SAVSECDTA, SAVSYS şi RSTUSRPRF salvează şi restaurează drepuri de proprietate, grupuri primare, autorizări de grup primare şi autorizări publice pentru aceste tipuri de obiecte: Profil utilizator (*USRPRF), listă de autorizare(*AUTL), şi deţinător de autorizare (*AUTHLR).

2 Obiectul de salvat/restaurat este QUSEXRGOBJ, tip *EXITRG din biblioteca QUSRSYS.

Modul în care sunt stocate informaţiile de securitate

Informaţiile de securitate sunt stocate cu obiecte, profiluri utilizator şi liste de autorizare:

Informaţii de autorizare stocate cu obiecte:

Autorizare publică

Nume proprietar

Autorizarea proprietarului la obiect

Nume grup primar

Autorizarea grupului primar la obiect

Nume listă autorizare

Valoare auditare obiect

Dacă există autorizare privată

Dacă orice autorizare privată este mai puţin de public

Informaţii de autorizare stocate cu profilul utilizatorului:

Informaţii antet

Atributele profilului utilizator afişate în ecranul Create User Profile - Creare profil utilizator.

uid şi gid.

Informaţii autorizare privată

Autorizare privată la obiecte. Aceasta include autorizarea privată la liste de autorizare.

Informaţii despre proprietate

Lista obiectelor deţinute

Pentru fiecare obiect, o listă a utilizatorilor cu autorizare privată la obiect.

Informaţii grup primar

Lista obiectelor pentru care profilul este grup primar.

Informaţii de auditare:

Valoare auditare acţiune

Valoare auditare obiect

Informaţii utilizare funcţie:

Setările de utilizare pentru funcţiile înregistrate.

Informaţii de autorizare stocate cu liste de autorizare:

Informaţii de autorizare normală stocate cu orice obiect, cum ar fi autorizare publică şi proprietar.

Lista obiectelor securizate de lista de autorizare.

Salvarea informaţiilor de securitate

Informaţiile de securitate sunt stocate diferenţiat pe acelaşi mediu de stocare pe care este stocat sistemul dumneavoastră. Atunci când salvaţi profilurile utilizator, informaţiile de autorizare privată stocate cu profilul utilizator sunt formatate într-o tabelă de autorizare. O tabelă de autorizare este construită şi salvată pentru fiecare profil utilizator care are autorizări private. Această reformatare şi salvare a informaţiior de securitate poate fi de durată în cazul în care aveţi multe autorizări private pe sistemul dumneavoastră.

Acesta este modul în care informaţiile de securitate sunt stocate pe mediul de stocare:

Informaţii de autorizare salvate cu obiect:

Autorizare publică

Nume proprietar

Autorizarea proprietarului la obiect

Nume grup primar

Autorizarea grupului primar la obiect

Nume listă autorizare

Câmp nivel autorizări

Valoare auditare obiect

Dacă există autorizare privată

Dacă orice autorizare privată este mai puţin de public

Informaţii de autorizare salvate cu liste de autorizare:

Informaţii de autorizare normală stocate cu orice obiect, cum ar fi autorizare publică, proprietar şi grup primar.

Informaţii de autorizare salvate cu profilul utilizatorului:

Atributele profilului utilizator afişate în ecranul Create User Profile - Creare profil utilizator.

Tabela de autorizare salvată asociată cu profilul utilizatorului:

Câte o înregistrare pentru fiecare autorizare privată a profilului utilizator, incluzând setări de folosire pentru funcţiile înregistrate.

Informaţii înregistrare funcţie salvate cu obiectul QUSEXRGOBJ:

Informaţiile de înregistrare a funcţiei pot fi salvate prin salvarea obiectului QUSEXRGOBJ *EXITRG din QUSRSYS.

Recuperare informaţiilor de securitate

Recuperarea sistemului dumneavoastră înseamnă restaurarea datelor şi a informaţiilor de securitate asociate. Secvenţa obişnuită de recuperare este:

1. Reataurare profiluri de utilizator şi liste de autorizare (RSTUSRPRF USRPRF(*ALL)).
2. Restaurare obiecte (RSTLIB, RSTOBJ sau RSTCFG).
3. Restaurare autorizări private la obiecte (RSTAUT).

Cartea *Backup and Recovery* furnizează mai multe informaţii despre planificarea recuperării.

Reataurarea profilurilor de utilizator

Unele modificări pot fi efectuate asupra unui profil utilizator atunci când este restaurat. Se aplică următoarele:

- Dacă profilurile ce sunt restaurate individual (RSTUSRPRF USRPRF(*ALL) nu este specificat), SECDTA(*PWDGRP) nu este solicitat şi profilul ce este restaurat nu există pe sistem, aceste câmpuri se modifică în *NONE:
  - Nume profil grup (GRPPRF)
  - Parolă (PASSWORD)
  - Parolă a documentului (DOCPWD)
  - Profiluri suplimentare de grup (SUPGRPPRF)

  Parolele produsului sunt modificate în *NONE, astfel încât ele vor fi incorecte după restaurarea unui profil utilizator individual care nu există pe sistem.
- Dacă profilurile ce sunt restaurate individual (RSTUSRPRF USRPRF(*ALL) nu este specificat), SECDTA(*PWDGRP) nu este solicitat şi profilul există pe sistem, parola, parola document şi profilul grupului nu se modifică.

  Profilurile utilizatorului pot fi restaurate individual cu parola şi informaţiile de grup restaurate de pe mediul de salvare, prin specificarea parametrului SECDTA(*PWDGRP) în comanda RSTUSRPRF. Autorizările speciale *ALLOBJ şi *SECADM sunt cerute pentru a restaura parola şi informaţiile de grup, când se restaurează profilurile

individuale. Parolele produsului restaurate cu profilul utilizator vor fi incorecte după restaurarea unui profil utilizator individual care există pe sistem, doar dacă nu este specificat parametrul SECDTA(*PWDGRP) în comanda RSTUSRPRF.

- Dacă toate profilurile utilizator sunt restaurate pe sistemul dumneavoastră, toate câmpurile din orice profil care există deja pe sistem, sunt restaurate de pe mediul de salvare, inclusiv parola.

  Atenţie: Profilurile utilizator salvate de pe sistem cu un nivel diferit de parolare (QPWDLVL variabilă de sistem) faţă de cel al sistemului ce este restaurat pot determina constituirea unei parole care nu este validă pe sistemul restaurat. De exemplu, dacă profilul utilizator ce este salvat vine de pe un sistem pe care rulează un nivel 2 de parolare, utilizatorul ar putea obţine o parolă de tipul ″Aceasta este parola mea″. Această parolă nu ar fi validă pe un sistem pe care rulează nivelul de parolare 0 sau 1.

  Atenţie: Păstraţi o înregistrare a parolei responsabilului cu securitatea (QSECOFR) asociată cu fiecare versiune a informaţiilor dumneavoastră de securitate ce sunt salvate pentru a vă asigura că puteţi să vă logaţi pe sistemul dumneavoastră, dacă trebuie să realizaţi o operaţie completă de restaurare.

  Puteţi folosi DST (Dedicated Service Tools - Instrumente dedicate de service) pentru a reseta parola pentru profilul QSECOFR. Consultaţi subiectul Instrumente pentru service din Centrul de informare, în legătură cu instrucţiunile. Vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru informaţii suplimentare asupra accesării, Centrul de informare.
- Dacă există un profil pe sistem, operaţia de restaurare nu modifică uid sau gid.
- Dacă nu există un profil pe sistem, uid şi gid pentru un profil sunt restaurate din mediul de salvare. Dacă atât uid cât şi gid există deja pe sistem, sistemul generează o nouă valoare şi compune un mesaj (CPI3810).
- Autorizarea specială *ALLOBJ este înlăturată din profilurile utilizator ce sunt restaurate pe un sistem la nivelul de securitate 30 sau mai înalt în oricare din situaţiile acestea:
  - Profilul a fost salvat de pe un sistem diferit şi utilizatorul ce realizează RSTUSRPRF nu are autorizările speciale *ALLOBJ şi *SECADM.
  - Profilul a fost salvat de pe acelaşi sistem la nivelul de securitate 10 sau 20.

  ATENŢIE: Sistemul foloseşte numărul de serie al maşinii de pe sistem şi de pe mediul de salvare pentru a determina dacă obiectele sunt restaurate pe acelaşi sistem sau pe un alt sistem.

  Autorizarea specială *ALLOBJ **nu** este înlăturată de pe aceste profiluri furnizate de IBM:

  profil utilizator QSYS (sistem)

  profil utilizator QSECOFR (responsabil de securitate)

  profil utilizator QLPAUTO (instalare automată a programului licenţiat)

  profil utilizator QLPINSTALL (instalare a programului licenţiat)

Restaurarea obiectelor

Când restauraţi un obiect pe un sistem, sistemul foloseşte informaţiile de autorizare stocate cu obiectul. Se aplică securităţii obiectului restaurat următoarele :

Drept de propietate a obiectului:

- Dacă profilul care deţine obiectul este pe sistem, dreptul de propietate este restaurat pe acel profil.
- Dacă propietarul profilului nu există pe sistem, dreptul de propietate al obiectului este cedat profilului utilizator QDFTOWN (proprietar implicit).
- Dacă obiectul există pe sistem şi proprietarul sistemului este diferit faţă de proprietarul mediului de salvare, obiectul nu este restaurat dacă nu este specificat ALWOBJDIF(*ALL). În acest caz, obiectul este restaurat şi proprietarul sistemului este folosit.
- Vedeţi “Restaurarea programelor” la pagina 219 pentru informaţii suplimentare, la restaurarea programelor.

Grup primar:

Pentru un obiect care nu există pe sistem:

- Dacă profilul care este grup primar pentru obiect este pe sistem, variabila grup primar şi autorizarea sunt restaurate pentru obiect.
- Dacă profilul care este grup primar este pe sistem:
  - Grupul primar pentru obiect este setat pe nimic.
  - Autorizarea grup primar este setată pe fără autorizare.

Când un obiect existent este restaurat, grupul primar pentru obiect nu este restaurat de operaţia de restaurare.

Autorizare publică:
- Dacă obiectul ce este restaurat nu există pe sistem, autorizarea publică este setată pe autorizarea publică a obiectului salvat.
- Dacă obiectul ce este restaurat nu există pe sistem şi este înlocuit, autorizarea publică nu este modificată. Autorizarea publică de la versiunea salvată a obiectului nu este folosită.
- CRTAUT pentru bibliotecă nu ete folosit când se face restaurarea obiectelor la bibliotecă.

Lista de autorizare:
- Dacă un obiect, altul decât un document sau fişier, există deja pe sistem şi este legat de o listă de autorizare, parametrul ALWOBJDIF determină rezultatul:
  - Dacă este specificat ALWOBJDIF(*NONE), obiectul existen trebuie să aibă aceeaşi listă de autorizare precum obiectul salvat. Dacă nu, obiectul nu este restaurat.
  - Dacă este specificat ALWOBJDIF(*ALL), obiectul este restaurat. Obiectul este legat de lista de autorizare asociată cu obiectul existent.
- Dacă un document sau un fişier ce există deja pe sistem este restaurat, lista de autorizare asociată cu obiectul de pe sistem este folosită. Lista de autorizare de pe documentul sau fişierul salvat nu este folosită.
- Dacă nu există lista de autorizare pe sistem, obiectul este restaurat fără a fi legat de lista de autorizare şi autorizarea publică este modificată la *EXCLUDE.
- Dacă obiectul ce este restaurat pe acelaşi sistem de pe care a fost salvat, obiectul este legat din nou de lista de autorizare.
- Dacă obiectul ce este restaurat pe un sistem diferit, parametrul ALWOBJDIF, la comanda de restaurare, este folosit să determine dacă obiectul este legat la lista de autorizare:
  - Dacă este specificat ALWOBJDIF(*ALL), obiectul este legat la lista de autorizare.
  - Dacă nu este specificat ALWOBJDIF(*NONE), atunci obiectul nu este legat de lista de autorizare şi autorizarea publică a obiectului este modificată la *EXCLUDE.

Autorizări private:
- Autorizarea privată este salvată cu profilurile utilizator, nu cu obiecte.
- Dacă profilurile utilizator au autorizare privată pentru un obiect ce se restaurează, acele autorizări private nu sunt, de obicei, afectate. Restaurarea anumitor tipuri de programe poate determina revocarea autorizărilor private. Vedeţi “Restaurarea programelor” la pagina 219 pentru informaţii suplimentare.
- Dacă este şters un obiect din sistem şi apoi restaurat din versiunea salvată, autorizarea privată a obiectului nu mai există deja pe sistem. Când este şters un obiect, toate autorizările private ale obiectului sunt înlăturate din profilul utilizator.
- Dacă autorizările private trebuie să fie recuperate, comanda RSTAUT (Restore Authority - Restaurare autorizare) trebuie folosită. Secvenţa obişnuită este:
  1. Restaurare profiluri utilizator
  2. Restaurare obiecte
  3. Restaurare autorizare

Auditare obiect:

- Dacă obiectul ce este restaurat nu există pe sistem, variabila auditare obiect (OBJAUD) a obiectului salvat este restaurată.
- Dacă obiectul ce este restaurat nu există pe sistem şi este înlocuit, variabila auditare obiect nu este modificată. Valoarea OBJAUD de la versiunea salvată a obiectului nu este restaurată.
- Dacă obiectul ce este restaurat nu există pe sistem, variabila creare auditare obiect (CRTOBJAUD) pentru bibliotecă este restaurată.
- Dacă o bibliotecă ce este restaurată există şi este înlocuită, variabila CRTOBJAUD pentru bibliotecă nu este restaurată. Variabila CRTOBJAUD pentru biblioteca existentă este folosită.

Deţinător de autorizare:
- Dacă un fişier este restaurat şi un deţinător de autorizare există pentru acel nume de fişier la care este restaurat, fişierul este legat la deţinătorul de autorizare.
- Informaţiile de autorizare asociate cu deţinătorul de autorizare înlocuiesc autorizarea publică şi informaţiile deţinătorului salvate cu fişierul.

Obiecte din domeniul utilizator:
- Pentru sisteme ce rulează Versiunea 2 Ediţia 3 sau ulterioară a OS/400 programului licenţiat, sistemul restricţionează obiectele domeniu utilizator (*USRSPC, *USRIDX şi *USRQ) la bibliotecile specificate în variabla de sistem QALWUSRDMN. Dacă o bibliotecă este înlăturată din variabila de sistem QALWUSRDMN după ce este salvat un obiect domeniu utilizator de tipul *USRSPC, *USRIDX sau *USRQ, sistemul modifică obiectul la domeniul de sistem când este restaurat.

Informaţii înregistrare funcţie:
- Informaţiile de înregistrare a funcţiei pot fi restaurate prin restaurarea obiectului QUSEXRGOBJ *EXITRG din QUSRSYS. Aceasta restaurează toate funcţiile înregistrate. Aceste informaţii de utilizare sunt asociate cu funcţii şi sunt restaurate când profilurile utilizator şi autorizările sunt restaurate.

Aplicaţii care folosesc înregistrarea certificatelor
- Aplicaţiile care folosesc informaţii de înregistrare a certificatelor pot fi restaurate prin restaurarea obiectului QUSEXRGOBJ *EXITRG din QUSRSYS. Aceasta restaurează toate aplicaţiile înregistrate. Asocierea aplicaţiei la informaţiile ei de certificare poate fi restaurată prin restaurarea obiectului QYCDCERTI *USRIDX din QUSRSYS.

Restaurarea autorizării

Când este restaurată informaţia de securitate, autorizările private trebuie să fie reconstruite. Când se restaurează un profil de utilizator care are o tabelă de autorizare, este restaurată şi tabela de autorizare pentru profil.

Comanda Restaurare autorizare (RSTAUT) reconstruieşte autorizarea privată în profilul de utilizator folosind informaţiile din tabela de autorizare. Operaţia de acordare a autorizării este rulată pentru fiecare autorizare privată din tabela de autorizare. Dacă autorizarea este restaurată pentru multe profiluri şi multe autorizări private există în tabelele autorizare, acesta poate fi un proces de durată.

Comenzile RSTUSRPRF şi RSTAUT pot fi rulate pentru un profil singular, o listă de profiluri, un nume generic de profil sau toate profilurile. Sistemul caută mediul de salvare sau fişierele de salvare create de comanda SAVSECDTA sau SAVSYS sau API-ul QSRSAVO pentru a găsi profilurile pe care doriţi dumneavoastră să le restauraţi.

Restaurare a autorizării câmpului:

Următorii paşi se cer pentru a restaura autorizări câmp privat pentru fişiere bază de date care nu există încă pe sistem:
- Restauraţi sau creaţi profilurile utilizator necesare.
- Restaurare fişiere.
- Rulare a comenzii RSTAUT (Restore Authority - Restaurare autorizare)

Autorizările câmp privat nu sunt restaurate în totalitate până când autorizările obiect privat pe care ele le restricţionează, nu sunt din nou restabilite.

Restaurarea programelor

Restaurarea programelor pe sistemul dumneavoastră ce sunt obţinute de la o sursă necunoscută pun o problemă de securitate. Programele pot realiza operaţii care întrerup cererile de securitate. De o atenţie deosebită se bucură programele care conţin instrucţiuni restricţionate, programele care adoptă propria lor autorizare şi programele care au fost dotate cu aceasta. Aceasta include tipurile de obiect *PGM, *SRVPGM, *MODULE şi *CRQD. Puteţi folosi variabilele de sistem QVFYOBJRST, QFRCCVNRST şi QALWOBJRST pentru a preveni aceste tipuri de obiecte de la a fi restaurate pe sistemul dumneavoastră. Consultaţi Variabile de sistem restaurare referitoare la securitate pentru informaţii suplimentare despre aceste variabile de sistem.

Sistemul fofloseşte o variabilă de validare pentru a ajuta la protejarea programelor. Această variabilă este stocată cu un program şi recalculată când este restaurat programul. Acţiunile sistemului sunt determinate de parametrul ALWOBJDIF din comanda de restaurare şi forţează conversia pentru restaurarea variabilei de sistem (QFRCCVNRST).

Notă: Programele ce sunt create pentru Versiunea 5 Ediţia 1 iSeries sau una ulterioară conţin informaţii care permit programului să fie recreat la momentul restaurării, dacă este necesar. Informaţiile necesare pentru a recrea programul rămân cu programul, chiar dacă atunci când observabilitatea programului este înlăturată. Dacă este determinată o eroare de validare program la momentul restaurării programului, programul va fi recreat pentru a corecta eroarea de validare a programului. Acţiunea de recreere a programului la momentul restaurării nu este ceva nou în iSeries Version 5 Release 1. În ediţiile anterioare, orice eroare de validare a programului întâlnită în momentul restaurării rezulta în recrearea programului dacă era posibil acest lucru (dacă exista observabilitate în programul de restaurat). Diferenţa dintre iSeries Version 5 Release 1 şi programele ulterioare este aceea că informaţiile necesare pentru recrearea programului rămân chiar si atunci când observabilitatea a fost înlăturată din program.

Restaurarea programelor care adoptă autorizarea proprietarului:

Atunci când un program este restaurat şi adoptă autorizarea deţinătorului, dreptul de proprietate şi autorizarea la program pot fi modificate. Se aplică următoarele reguli:

- Profilul utilizatorului ce realizează operaţiunea de restaurare rtebuie fie să deţină programul, fie să aibă autorizările speciale *ALLOBJ şi *SECADM.
- Profilul utilizatorului ce realizează operaţiunea de restaurare poate primi autorizarea de a restaura programul dacă
  - Este deţinătorul programului.
  - Este un membru al profilului de grup care deţine programul (în cazul în care nu aveţi autorizare privată asupra programului).
  - Are autorizările speciale *ALLOBJ şi *SECADM.
  - Este un membru al profilului de grup care are autorizările speciale *ALLOBJ şi *SECADM.
  - Rulează sub o autorizare adoptată care îndeplineşte unul din testele de mai sus.
- În cazul în care profilul care restaurează nu are autorizarea adecvată, toate autorizările publice şi private asupra programului sunt revocate şi autorizarea publică este modificată în *EXCLUDE.
- În cazul în care deţinătorul programului nu există în sistem, dreptul de proprietate este dat profilului utilizator QDFTOWN. Autorizarea publică este modificată în *EXCLUDE şi lista de autorizare este înlăturată.

Restaurarea programelor licenţiate

Comanda Restore Licensed Programs (RSTLICPGM) este folosită pentru a instala programele furnizate de IBM pe sistemul dumneavoastră. Poate fi folosită de asemenea pentru ainstala programe non-IBM create folosind programul licenţiat SystemView* System Manager/400*.

La furnizarea sistemului dumneavoastră, doar utilizatorii cu autorizarea specială *ALLOBJ pot folosi comanda RSTLICPGM. Apelurile de procedură ale RSTLICPGM apelează un program ieşire pentru a instala programe care nu sunt furnizate de IBM.

Pentru a proteja securitatea pe sistemul dumneavoastră, programul de ieşire nu trebuie să ruleze folosind un profil cu autorizarea specială *ALLOBJ. Folosiţi un program care adoptă autorizarea specială *ALLOBJ pentru a rula comanda RSTLICPGM, în loc de a avea un utilizator cu autorizarea *ALLOBJ care să ruleze direct comanda.

Urmează un exemplu pentru această tehnică. Programul de instalat folosind comanda RSTLICPGM este numit CPAPP (Contracts and Pricing).

1. Creaţi un profil de utilizator cu autorizare suficientă pentru a instala cu succes aplicaţia. Nu acordaţi acestui profil autorizarea specială *ALLOBJ. Pentru acest exemplu, profilul de utilizator este numit OWNCP.
2. Scrieţi un program pentru a instala aplicaţia. De exemplu, programul este numit CPINST:

   ```
   PGM
   RSTLICPGM CPAPP
   ENDPGM
   ```

3. Creaţi programul CPINST pentru a adopta autorizarea unui utilizator cu autorizarea specială *ALLOBJ, cum ar fi QSECOFR şi autorizaţi OWNCP la program:

   ```
   CRTCLPGM QGPL/CPINST USRPRF(*OWNER) +
            AUT(*EXCLUDE)
   GRTOBJAUT OBJ(CPINST) OBJTYP(*PGM) +
             USER(OWNCP)  AUT(*USE)
   ```

4. Semnaţi ca OWNCP şi apelaţi programul CPINST. Atunci când programul CPINST rulează comanda RSTLICPGM, rulaţi sub autorizarea QSECOFR. Atunci când programul ieşire rulează pentru a instala programele CPAPP, aruncă autorizarea adoptată. Programele apelate de programul ieşire rulează sub autorizarea OWNCP.

Restaurarea listelor de autorizare

Listele de autorizare sunt salvate fie de comanda SAVSECDTA, fie de comanda SAVSYS. Listele de autorizare sunt restaurate de comanda:

```
RSTUSRPRF USRPRF(*ALL)
```

Nu există nici o metodă pentru restaurarea listelor de autorizare individuale.

La restaurarea unei liste de autorizare, autorizarea şi dreptul de proprietate sunt stabilite aşa cum sunt ele pentru orice alt obiect care este restaurat. Legătura dintre listele de autorizare şi obiecte este stabilită dacă obiectele sunt restaurate după lista de autorizare. Consultaţi “Restaurarea obiectelor” la pagina 216 pentru mai multe informaţii. Autorizările private ale utilizatorilor la listă sunt restaurate folosdind comanda RSTAUT.

Recuperarea dintr-o listă de autorizare deteriorată

Atunci când un obiect este securizat de o listă de autorizare şi lista de autorizare este deteriorată, accesul la obiect este limitat la utilizatorii care au autorizarea specială *ALLOBJ.

Pentru a recupera dintr-o listă de autorizare deteriorată, sunt necesari doi paşi.

1. Recuperarea utilizatorilor şi a autorizărilor lor din lista de autorizare.
2. Recuperarea asociaţiilor listei de autorizare cu obiecte.

Aceşti paşi trebuie făcuţi de un utilizator cu autorizarea specială *ALLOBJ.

Recuperarea listei de autorizare: În cazul în care autorizările utilizatorilor la lista de autorizare sunt cunoscute, ştergeţi lista de autorizare, creaţi-o din nou şi apoi adăugaţi la ea utilizatori.

Dacă nu este posibil să creaţi din nou lista de autorizare pentru că nu ştiţi toate autorizările utilizatorilor, lista de autorizare poate fi restaurată şi utilizatorii restauraţi la lista de autorizare folosind ultimile benzi SAVSYS sau SAVSECDTA. Pentru a restaura lista de autorizare, efectuaţi următoarele:

1. Ştergeţi lista de autorizare deteriorată folosind comanda DLTAUTL (Delete Authorization List - Ştergere listă de autorizare).
2. Restauraţi lista de autorizare prin restaurarea profilurilor utilizator:

   ```
   RSTUSRPRF USRPRF(*ALL)
   ```

3. Restauraţi autorizările private ale utilizatorilor la listă folosind comanda RSTAUT .

Atenţie: Această procedură restaurează valorile profilului utilizator de pe mediul de salvare. Consultaţi “Reataurarea profilurilor de utilizator” la pagina 215 pentru informaţii suplimentare.

Recuperarea asociaţiilor de obiecte la lista de autorizare: Atunci când lista de autorizare deteriorată este ştearsă, obiectele securizate de lista de autorizare trebuie adăugate la noua listă de autorizare. Efectuaţi următoarele:

1. Găsiţi obiectele care erau asociate cu lista de autorizare deteriorată folosind comanda Reclaim Storage (RCLSTG). Reclamarea spaţiului de stocare asociază obiectele care erau asociate cu lista de autorizare la lista de autorizare QRCLAUTL.
2. Folosiţi comanda DSPAUTLOBJ (Display Authorization List Objects - Afişare obiecte ale listei de autorizare) pentru a afişa obiectele asociate cu lista de autorizare QRCLAUTL.
3. Folosiţi comanda GRTOBJAUT (Grant Object Authority - Acordare autorizare obiect) pentru a securiza fiecare obiect cu lista de autorizare corectă.

```
GRTOBJAUT OBJ(nume-bibliotecă/nume-obiect) +
          OBJTYPE(tip-obiect) +
          AUTL(nume-listă-autorizare)
```

Notă: Dacă un număr mare de obiecte sunt asociate cu lista de autorizare QRCLAUTL, creaţi un fişier bază de date prin specificarea OUTPUT(*OUTFILE) în comanda DSPAUTLOBJ. Puteţi scrie un program CL pentru a rula comanda GRTOBJAUT pentru fiecare obiect din fişier.

Restaurarea sistemului de operare

La efectuarea unui IPL manual pe sistemul dumenavoastră, meniul IPL sau Instalare sistem furnizează o opţiune de instalare a sistemului de operare. Funcţia DST (dedicated service tools - unelte serviciu dedicat) furnizează abilitatea de a cere oricui care foloseşte acest meniu parola de securitate DST. Puteţi folosi aceasta pentru a preveni situaţia în care cineva restaurează o copie neautorizată a sistemului de operare.

Pentru a securiza instalarea sistemului dumneavoastră de operare, faceţi următoarele:

1. Realizaţi un IPL manual.
2. Selectaţi DST de la un IPL sau de la meniul Instalarea sistemului.
3. Din meniul Folosire DST, selectaţi opţiunea de lucru cu mediul DST.
4. Selectaţi opţiunea de modificare a parolelor.
5. Selectaţi opţiunea de modificare a securităţii de instalare a sistemului de operare.
6. Specificare 1 (securizare).
7. Apăsaţi F3 (ieşire) până când vă întoarceţi la IPL sau la meniul Instalare a sistemului.
8. Completaţi manualul IPL şi lăsaţi cheia IPL la poziţia sa normală.

Note:

1. Dacă nu mai doriţi să securizaţi instalarea sistemului de operare, faceţi paşii următori şi specificaţi 2 (nesecurizat).
2. Puteţi, de asemenea, preveni instalarea sistemului de operare prin păstrarea întrerupătorului cheii dumneavoastră IPL în poziţia normală şi înlăturarea cheii.

Autorizarea specială *SAVSYS

Pentru a salva sau restaura un obiect, trebuie să aveţi autorizarea *OBJEXIST pentru obiect sau autorizarea specială *SAVSYS. Un utilizator cu autorizarea specială *SAVSYS nu are nevoie de nici o autorizare suplimentară pentru un obiect ca să-l salveze sau să-l restaureze.

Autorizarea specială *SAVSYS dă unui utilizator capabilitatea de a salva un obiect şi de a-l lua pe un sistem diferit spre a fi restaurat sau pentru a afişa (dump) mediul ca să vadă datele. De asemenea, dă unui utilizator capabilitatea de a

salva un obiect şi de a face o memorare liberă chiar şi ştergând datele din obiect. Când salvaţi documentele, un utilizator cu autorizarea specială *SAVSYS are opţiunea de a şterge acele documente. Autorizarea specială *SAVSYS trebuie să fie acordată cu atenţie.

Auditarea operaţiilor de salvare şi restaurare

Este scrisă o înregistrare de auditare a securităţii pentru fiecare operaţie de restaurare dacă variabila de auditare acţiune (variabila de sistem QAUDLVL sau AUDLVL din profilul de utilizator) include *SAVRST. Când folosiţi o comandă care restaurează un număr mare de obiecte, precum RSTLIB, este scrisă o înregistrare de auditare pentru fiecare obiect restaurat. Aceasta poate determina probleme legate de dimensiunea receptorului jurnalului de auditare, în particular, dacă restauraţi mai multe biblioteci.

Comanda RSTCFG nu creează o înregistrare de auditare pentru fiecare obiect restaurat. Dacă doriţi să aveţi o înregistrare de auditare pentru această comandă, setaţi auditarea obiect pentru comandă. Se va scrie o înregistrare de auditare de fiecare dată când este rulată comanda.

Comenzile care salvează un număr foarte mare de obiecte, cum ar fi SAVSYS, SAVSECDTA şi SAVCFG nu creează înregistrări individuale de auditare pentru obiectele salvate, chiar dacă obiectele salvate au activă auditarea. Pentru a monitoriza aceste comenzi, setaţi auditarea obiect pentru aceste comenzi.

Capitolul 9. Auditarea securităţii pe sistemul iSeries

Acest capitol descrie tehnici de auditare a eficienţei securităţii pe sistem. Auditarea sistemului se face din mai multe motive:

- Pentru a se evalua dacă planul de securitate este complet.
- Pentru a se asigura că se află în locul potrivit controalele de securitate planificate şi că funcţionează. Acest tip de auditare este realizat de responsabilul cu securitatea ca parte a administrării zilnice a securităţii. Se realizează de asemenea, uneori şi mai amănunţit, ca parte a examinării periodice a securităţii de către auditorii interni sau externi.
- Pentru a se asigura că securitatea sistemului se armonizează cu modificările mediului sistem. Unele exemple de modificări ce afectează securitatea sunt:
  - Obiecte noi create de utilizatori ai sistemului
  - Utilizatori noi admişi în sistem
  - Modificarea dreptului de proprietate a unui obiect (autorizare ne potrivită)
  - Modificarea a responsabilităţilor (grup de utilizatori modificat)
  - Autorizare temporară (nerevocată în timp)
  - Produse noi instalate
- Pentru a face pregătirea pentru un eveniment viitor, precum instalarea unei noi aplicaţii, mutarea spre un nivel mai ridicat de securitate sau setarea unei reţele de comunicare.

Tehnicile descrise în acest capitol sunt potrivite pentru toate aceste situaţii. Ce lucruri şi cât de des le auditaţi, depinde de dimensiunea şi nevoile de securitate ale organizaţiei dumneavoastră. Scopul acestui capitol este, mai de grabă, de a discuta ce informaţii sunt disponibile, cum se obţin şi de ce sunt necesare, decât de a oferi îndrumări pentru frecvenţa auditărilor.

Acest capitol are trei părţi:

- O listă de elemente de securitate ce pot fi planificate şi auditate.
- Informaţii despre setarea şi utilizarea jurnalului de auditare furnizat de sistem.
- Alte tehnici care sunt disponibile pentru a culege informaţii de securitate privind sistemul.

Auditarea securităţii implică utilizarea comenzilor pe sistemul iSeries şi accesarea informaţiilor despre sistem din istoric şi din jurnal. Este posibil să doriţi să creaţi un profil special pentru a fi utilizat de cineva pentru realizarea unei auditări a securităţii sistemului dumneavoastră. Profilul de auditare va necesita autorizarea specială *AUDIT pentru a fi capabil să modifice caracteristicile de auditare ale sistemului dumneavoastră. Unele operaţii de auditare sugerate în acest capitol, necesită un profil utilizator cu autorizarea specială *ALLOBJ şi *SECADM. Asiguraţi-vă că setaţi parola pentru profilul de auditare la *NONE, când s-a terminat perioada de auditare.

Listă de verificare pentru responsabilii cu securitatea şi auditori

Această listă de verificare poate fi folosită, atât pentru planificare, cât şi pentru auditare a securităţii sistemului. În timp ce planificaţi securitatea, alegeţi elementele din listă, care împlinesc cererile dumneavoastră de securitatea. Când auditaţi securitatea sistemului dumneavoastră, folosiţi lista pentru evaluarea controalelor pe care le aveţi pe poziţii şi determinaţi dacă sunt necesare controale suplimentare.

Aceasta listează servere ca o sinteză a informaţiei din această carte. Lista conţine descrieri pe scurt ale modului în care se face fiecare element şi cum se monitorizează ceea ce s-a făcut, inclusiv ce intrări se vor căuta în jurnalul QAUDJRN. Detalii despre elementele acestea se găsesc în carte.

Securitatea fizică

Notă: Subiectul Securitatea de bază a sistemului şi planificarea din Centrul de informare conţine o prezentare completă problemelor legate de securitatea fizică pe sistemul iSeries. Vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii.

Unitatea sistem şi consola se află într-o locaţie sigură.

Mediul cu copia de rezervă este protejat faţă de deteriorare şi furt.

Comutatorul cheie IPL de pe unitatea procesor este în poziţia Secure sau Auto. Cheia este înlăturată. Cheile se păstrează separat, amândouă, sub securitate fizică strictă. Consultaţi Centrul de informare pentru informaţii suplimentare despre comutatorul cheie IPL (vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii).

Accesul la staţiile de lucru localizate public şi la consolă este restricţionat. Utilizaţi comanda DSPOBJAUT pentru a vedea cine are autorizarea *CHANGE la staţiile de lucru. Căutaţi în jurnalul de auditare intrări AF ce au câmpul pentru tipul obiectului egal cu *DEVD, pentru a găsi încercări de semnare pe staţiile de lucru restricţionate.

Logarea pentru utilizatori cu autorizarea apecială *ALLOBJ sau *SERVICE este limitată la câteva staţii de lucru. Faceţi verificarea pentru a vedea dacă variabila de sistem QLMTSECOFR este 1. Folosiţi comanda DSPOBJAUT pentru dispozitive, în scopul de a afla dacă profilul QSECOFR are autorizare *CHANGE.

Valorile de sistem

Valorile de sistem pentru securitate urmează liniile generale recomandate. Pentru a tipări valorile de sistem pentru securitate, introduceţi: WRKSYSVAL *SEC OUTPUT(*PRINT). Două valori de sistem importante de auditat sunt:

- QSECURITY, care trebuie setată la 40 sau mai mult.
- QMAXSIGN, care nu trebuie să fie mai mare de 5.

Notă: Dacă funcţia de auditare este activă, o intrare SV este scrisă în jurnalul QAUDJRN, ori de câte ori este modificată o variabilă de sistem.

Deciziile asupra variabilelor de sistem sunt revăzute periodic, mai ales când mediul de sistem se modifică, cum ar fi instalarea unei aplicaţii noi sau unei reţele de comunicaţie.

Profilurile de utilizator furnizate de IBM

Parola s-a modificat pentru profilul de utilizator QSECOFR. Acest profil este livrat cu parola setată pe QSECOFR, astfel încât dumneavoastră vă puteţi loga pentru a instala sistemul dumneavoastră. Parola **trebuie** să fie modificată prima dată când vă logaţi pe sistemul dumneavoastră şi, periodic, după instalare.

Verificaţi dacă a fost modificată controlând într-o listă DSPAUTUSR data la care parola QSECOFR a fost modificată şi încercând să vă logaţi cu o parolă implicită diferită.

Notă: Vedeţi “Profiluri utilizator livrate de IBM” la pagina 105 şi Anexa B pentru informaţii suplimentare despre profiluri utilizator furnizate de IBM.

Parolele IBM pentru DST sunt modifcate. Profilurile DST nu apar într-o listă DSPAUTUSR. Pentru a verifica dacă ID-urile şi parolele utilizator sunt modificate, porniţi DST şi încercaţi să folosiţi valorile implicite. Vedeţi subiectul “Gestionarea ID-urilor de utilizator unelte de service” la pagina 106 pentru informaţii suplimentare.

Nu este recomandată logarea cu profiluri utilizator furnizate de IBM, cu excepţia lui QSECOFR. Aceste profiluri furnizate de IBM sunt proiectate pentru a deţine obiecte sau a rula funcţii de sistem. Folosiţi o listă DSPAUTUSR pentru a verifica dacă următoarele profiluri utilizator furnizate de IBM au o parolă *NONE:

| QAUTPROF
| QBRMS
| QCLUMGT
| QCLUSTER
| QCOLSRV
| QDBSHR
| QDBSHRDO
| QDFTOWN
| QDIRSRV
| QDLFM
| QDOC
| QDSNX
| QEJB
| QFNC
| QGATE
| QIPP
| QLPAUTO
| QLPINSTALL
| QMGTC
| QMSF
| QNETSPLF
| QNFSANON
| QNTP
| QPEX
| QPGMR
| QPM400
| QRJE
| QSNADS
| QSPL
| QSPLJOB
| QSRV
| QSRVAGT
| QSRVBAS
| QSYS
| QSYSOPR
| QTCM
| QTCP
| QTFTP
| QTMHHTP1
| QTMHHTTP
| QTSTRQS
| QUSER
| QYCMCIMOM
| QYPSJSVR

Controlul parolei

Utilizatorii pot schimba propriile parole. Permisiunea acordată utilizatorilor de a defini propriile parole reduce nevoia utilizatorilor de a nota parolele proprii. Utilizatorii trebuie să aibă acces la comanda CHGPWD sau la funcţia Modificare parolă din meniul Securitate (GO SECURITY - PORNIRE SECURITATE).

Este necesară modificare a parolei conform regulilor de securitate ale organizaţiei, de exemplu la un interval între 30 şi 90 de zile. Variabila de sistem QPWDEXPITV este setată pentru a respecta ghidul de securitate.

Dacă un profil de utilizator are un interval de expirare a parolei care este diferit de variabila de sistem, el se conformează ghidului de securitate. Revedeţi profilurile de utilizator pentru o valoare PWDEXPITV alta decât *SYSVAL.

Parolele simple sunt împiedicate prin utilizarea variabilelor de sistem pentru a seta regulile de parole şi prin folosirea unui program de aprobare a parolelor. Folosiţi comanda WRKSYSVAL *SEC şi uitaţi-vă la setările pentru valori începând cu QPWD.

Profilurile de grup au parola *NONE. Utilizaţi comanda DSPAUTUSR pentru a verifica dacă există profiluri de grup care au parole.

Oricând sistemul nu operează la nivel de parolare 3 şi utilizatorii îşi modifică parola lor, sistemul va încerca să creeze o parolă echivalentă care este utilizabilă la alte niveluri de parolare, dacă este posibil. Puteţi utiliza comanda PRTUSRPRF TYPE(*PWDLVL) pentru a vedea ce profiluri utilizator au parole care sunt utilizabile la diverse niveluri de parolare.

Notă: Parola echivalentă este cea mai bună încercare de a crea o parolă utilizabilă pentru alte niveluri de parolare, dar este posibil să nu fi trecut de toate regulile de parolare, dacă celălalt nivel de parolare era activ. De exemplu, dacă o parolă BbAaA3x este specificată la nivelul 2 de parolare, sistemul va crea o parolă echivalentă BBAAA3X pentru utilizare la nivelurile 0 şi 1 de parolare. Aceasta ar fi adevărată chiar dacă variabila de sistem QPWDLMTCHR îl include pe ’A’ ca pe unul din caracterele limitate (QPWDLMTCHR nu este impus la nivelul 2 de parolare) sau variabila de sistem QPWDLMTREP a specificat că nu pot fi caracterele consecutive la fel (deoarece verificarea este sensibilă la majuscule, la nivelul 2 de parolare dar insensibile la majusculă la nivelurile 0 şi 1 de parolare.)

Profilurile de utilizator şi de grup

Fiecărui utilizator îi este alocat un profil de utilizaor unic. Variabila de sistem QLMTDEVSSN trebuie setată la 1. Chiar dacă limitarea fiecări utilizator la o sesiune dispozitiv la un moment dat nu previne partajarea profilurilor utilizator, descurajează aceast fapt.

Profilurile de utilizator cu autorizarea specială *ALLOBJ sunt limitate şi nu sunt utilizate ca profiluri de grup. Comanda DSPUSRPRF poate fi utilizată pentru a verifica autorizările speciale pentru profilurile utilizator şi pentru a determina care profiluri sunt profiluri de grup. Subiectul “Tipărirea profilurilor de utilizator selectate” la pagina 259 arată cum se foloseşte un fişier de ieşire şi o interogare pentru a determina aceasta.

Câmpul *Capabilităţi limită* estes *YES în profilurile utilizatorilor, care ar trebui să fie restricţionate la un set de meniuri. Subiectul “Tipărirea profilurilor de utilizator selectate” la pagina 259 oferă un exemplu despre modul în care se determină aceasta.

Programatorii sunt restricţionaţi de bibliotecile de producţie. Folosiţi comanda DSPOBJAUT pentru a determina autorizările publice şi private pentru bibliotecile de producţie şi obiectele critice din biblioteci.

“Planificarea securităţii pentru programatori” la pagina 209are mai multe informaţii despre securitate şi mediul de programare.

Apartenenţa la un profil de grup este modificată când responsabilităţile de job se modifică. Pentru a verifica apartenenţa la grup, utilizaţi una din aceste comenzi:

```
DSPAUTUSR SEQ(*GRPPRF)
DSPUSRPRF nume-profil *GRPMBR
```

Dumneavoastră trebuie să utilizaţi o convenţie de denumire pentru un profil de grup. Când sunt afişate autorizările, puteţi recunoaşte atunci cu uşurinţă profilul de grup.

Administrarea profilurilor de utilizatori este organizată adecvat. Nici un profil de utilizator nu are numere mari ca autorizare privată. Subiectul “Examinarea profilurilor mari de utilizatori” la pagina 259 discută modul în care se găseşte şi se examinează profilurile mari de utilizatori de pe sistemul dumneavoastră.

Angajaţii sunt înlăturaţi din sistem imediat când sunt transferaţi sau eliberaţi. Revedeţi în mod regulat lista DSPAUTUSR pentru a vă asigura de faptul că numai angajaţii activi au acces la sistem. Intrările DO (Delete Object - Ştergere obiect) din jurnalul de auditare pot fi revăzute pentru a vă asigura că profilurile de utilizator sunt şterse imediat după ce pleacă utilizatorii.

Gestiunea verifică în mod regulat utilizatorii autorizaţi pe sistem. Dumneavoastră puteţi folosi comanda DSPAUTUSR pentru această informaţie.

Parola pentru un angajat inactiv este setată la *NONE. Utilizaţi comanda DSPAUTUSR pentru a verifica faptul că profilurile de utilizatori inactivi nu au parole.

Gestiunea verifică în mod regulat utilizatorii cu autorizări speciale, în particular, *ALLOBJ *SAVSYS şi autorizări speciale *AUDIT. Subiectul “Tipărirea profilurilor de utilizator selectate” la pagina 259 oferă un exemplu despre modul în care se determină aceasta.

Controlul autorizării

Proprietarii datelor înţeleg obligaţia lor de autorizare a utilizatorilor pe principiul nevoii-de-cunoaştere.

Proprietarii obiectelor verifică în mod regulat autorizarea de utilizare a obiectelor, inclusiv autorizarea publică. Comanda WRKOBJOWN furnizează un ecran pentru lucrul cu autorizările pentru toate obiectele deţinute de un profil utilizator.

Date sensibile nu sunt publice. Verificare a autorizării pentru utilizator *PUBLIC pentru obiecte critice utilzând comanda DSPOBJAUT.

Autorizarea pentru profilurile de utilizator este controlată. Autorizarea publică pentru profilurile utilizator trebuie să fie *EXCLUDE. Aceasta previne lansarea de către utilizatori a joburilor ce rulează sub alt profil de utilizator.

Descrierile de joburi sunt controlate

- Descrierile de job cu autorizarea publică *USE sau mai mare sunt specificate ca USER(*RQD). Aceasta înseamnă că joburile lansate folosind descrierea de job trebuie să ruleze folosind profilul lansatorului.
- Descrieri de job care specifică un utilizator au o autorizare publică *EXCLUDE. Autorizarea de a folosi aceste descrieri de job este controlată. Aceasta împiedică utilizatorii neautorizaţi să lanseze joburi care rulează folosind autorizarea altui profil.

Pentru a afla ce descrieri de job sunt pe sistem, introduceţi:

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

Pentru a verifica paramentrul *Utilizator* al descrierii de job, folosiţi comanda DSPJOBD (Display Job Description - Afişare descriere de job) Pentru a verifica autorizarea pentru o descriere de job, folosiţi comanda DSPOBJAUT.

Notă: La nivelul de securitate 40 sau 50, un utilizator ce trimite un job folosind o descriere de job care specifică un nume de profil utilizator, trebuie să aibă autorizarea *USE atât pentru descrierea de job, cât şi pentru profilul

de utilizator. La toate nivelurile de securitate, o încercare de a trimite sau a programa un job fără autorizarea *USE unui utilizator specificat în descriere, determină o intrarea AF cu tipul de violare J din jurnalul de auditare.

Utilizatorilor nu li se permite să se logeze prin apăsarea tastei Introducere de pe ecranul Logare. Asiguraţi-vă că nici o intrare de staţie de lucru din descrierile subsistem nu specifică o descriere de job care are un nume de profil utilizator specificat pentru parametrul USER.

Logarea implicită este prevenită la nivelul 40 sau 50 de securitate, chiar dacă o descriere de subsistem o permite. La toate nivelurile de securitate, o intrare AF cu un tip de violare S este scrisă într-un jurnal de audit, dacă logarea implicită se încearcă şi este definită o descriere de subsistem pentru a o permite.

Lista de biblioteci din programele aplicaţie este controlată pentru a preveni o bibliotecă ce conţine un program similar de la a fi adăugat înainte de bilbiotecile de producţie. Subiectul “Lista de biblioteci” la pagina 177 discută metode pentru controlul listei de biblioteci.

Programele care adoptă autorizarea sunt folosite doar când sunt cerute şi sunt controlate cu atenţie. Vedeţi subiectul “Analizarea programelor care adoptă autorizarea” la pagina 260 pentru o explicaţie a modului în care se evaluează utilizarea funcţiei de adoptare a programului.

Interfeţele program aplicaţie (API-uri) sunt securizate.

Tehnicile bune de securitate a obiectului sunt folosite pentru a evita problemele de performanţă.

Accesul neautorizat

Evenimentele referitoare la securitate sunt înregistrate în jurnalul de auditare a securităţii (QAUDJRN), când funcţia de auditare este activă. Pentru a audita defectele de autorizare, folosiţi următoarele variabile de sistem şi setări:

- QAUDCTL trebuie să fie setat la *AUDLVL
- QAUDLVL trebuie să includă valorile *PGMFAIL şi *AUTFAIL.

Cea mai bună metodă de detectare a încercărilor neautorizate de a accesa informaţiile este aceea de a revedea intrările din jurnalul de auditare în mod regulat.

Variabila de sistem QMAXSIGN limitează numărul încercărilor consecutive de acces incorect la 5 sau mai puţin. Variabila de sistem QMAXSGNACN setată la 2 sau 3.

Coada mesaj QSYSMSG este creată şi monitorizată.

Jurnalul de auditare este auditat pentru încercări repetate ale unui utilizator. (Eşecurile de autorizare determină intrări de tipul AF în jurnalul auditare.)

Programele care încearcă să acceseze obiecte, folosind interfeţe care nu sunt suportate, eşuează. (Variabila de sistem QSECURITY este setată la 40 sau 50.)

ID-ul şi parola utilizatorului sunt cerute pentru logare. Nivelurile de securitate 40 şi 50 impun aceasta. La nivelul 20 sau 30, trebuie să vă asiguraţi că nici o descriere de subsistem nu are o intrare de staţie de lucru care utilizează o descriere de job ce are un nume de profil utilizator.

Programele neautorizate

Variabila de sistem QALWOBJRST este setată la *NONE pentru a împiedica pe oricine de la restaurarea programelor sensibile la securitate în sistem.

Comanda CHKOBJITG (Check Object Integrity - Verificare integritate a obiectului) rulează periodic pentru a detecta modificări neautorizate în scopul programării obiectelor. Această comandă este descrisă “Verificarea obiectelor ce au fost modificate” la pagina 261

Comunicaţiile

Comunicaţiile telefonice sunt protejate de proceduri apel-înapoi.

Criptarea este utilizată cu date sensibile.

Logarea de la diatanţă este controlată. Variabila de sistem QRMTSIGN este setată la *FRCSIGNON sau este folosit un program de validare passthrough.

Datele de acces de la alte sisteme, inclusiv computere personale, sunt controlate folosind atributele de reţea JOBACN, PCSACC şi DDMACC. Atributul de reţea JOBACN trebuie să fie *FILE.

Utilizarea jurnalului de auditare a securităţii

Jurnalul de auditare a securităţii este sursa primară de auditare a informaţiilor despre sistem. Un auditor de securitate din interiorul sau din afara organizaţiei dumneavoastră poate folosi funcţia de auditare furnizată de sistem pentru a strânge informaţii despre evenimente referitoare la securitate, ce apar pe sistem.

Puteţi defini auditarea pe sistemul dumneavoastră la trei niveluri diferite.

- Auditare largă a sistemului ce apare pentru toţi utilizatorii.
- Auditare ce are loc pentru obiecte specifice.
- Auditare ce are loc pentru utilizatori specifici.

Folosiţi variabile de sistem, parametrii profil utilizator şi parametrii obiect pentru a defini auditarea. “Planificarea auditării securităţii”descrie cum se face aceasta

Când un eveniment referitor la securitate, care poate fi auditat, apare, sistemul verifică dacă dumneavoastră aţi selectat acel eveniment pentru auditare. Dacă este aşa, sistemul scrie o intrare de jurnal în receptorul curent pentru jurnalul de auditare securitate (QAUDJRN din biblioteca QSYS).

Cînd doriţi să analizaţi informaţiile de auditare pe care le-aţi colectat în jurnalul QAUDJRN, puteţi folosi comanda Afişare jurnal (DSPJRN). Cu această comandă, informaţiile din jurnalul QAUDJRN pot fi scrise într-un fişier baze de date. Un program aplicaţie sau o unealtă de interogare pot fi folosite pentru a analiza datele.

Funcţia de auditare securitate este opţională. Trebuie să faceţi anumiţi paşi pentru a seta auditarea securităţii.

Următoarele secţiuni descriu modul în care se planifică, se setează şi se gestionează auditarea securităţii, ce informaţii sunt înregistrate şi cum se vizualizează acele informaţii. Anexa Farată machetele de înregistrare pentru intrările jurnal audit Anexa Edescrie care operaţii sunt auditate pentru fiecare tip de obiect.

Planificarea auditării securităţii

Pentru a planifica folosirea auditării securităţii pe sistemul dumneavoastră:

- Determinaţi ce evenimente relevante de securitate doriţi să înregistraţi pentru toţi urilizatorii sistemului. Auditarea evenimentelor relevante de securitate se numeşte **auditare acţiune**
- Verificaţi dacă aveţi nevoie de auditare suplimentară pentru utilizatori particulari.
- Decideţi dacă doriţi să auditaţi utilizarea obiectelor specifice pe sistem.
- Determinaţi dacă auditarea obiectului ar trebui folosită pentru toţi utilizatorii sau utilizatorii particulari.

Planificarea auditării acţiunilor

Variabila de sistem QAUDCTL (control audit), variabila de sistem QAUDLVL (nivel audit), variabila de sistem QAUDLVL2 (extensie nivel audit) şi parametrul AUDLVL (auditare acţiune) din profilurile utilizator lucrează împreună pentru a controla auditarea acţiunii:

- Variabila de sistem QAUDLVL specifică ce acţiuni sunt auditate pentru toţi utilizatorii sistemului.
- Variabila de sistem QAUDLVL2 specifică, de asemenea, ce acţiuni sunt auditate pentru toţi utilizatorii sistemului şi este folosită când mai mult de 16 valori de auditare sunt necesare.
- Parametrul AUDLVL din profilul utilizator determină ce acţiuni sunt auditate pentru un utilizator specific. Valorile pentru parametrul AUDLVL aplică *in addition to* valorile pentru variabilele de sistem QAUDLVL şi QAUDLVL2.
- Variabila de sistem QAUDCTL porneşte şi opreşte auditarea acţiune.

Evenimentele pe care le alegeţi pentru înregistrare în istoric depind atât de obiectivele dumneavoastră de securitate, cât şi de expunerile potenţiale. Tabela 125 la pagina 229 descrie valorile posibile de nivel auditare şi cum este posibil să le folosiţi Arată dacă acestea sunt disponibile ca variabilă de sistem, parametru profil utilizator sau ambele.

Tabela 126 la pagina 233furnizează informaţii suplimentare despre intrările jurnal care sunt scrise pentru valorile auditare acţiune specificate în variabilele de sistem QAUDLVL şi QAUDLVL2 şi în profilul utilizator. Arată:

- Tipul intrării scrise pentru jurnalul QAUDJRN.
- Fişierul extern bază de date model poate fi folosit pentru a defini înregistrarea când creaţi un fişier ieşire cu comanda DSPJRN. Machete complete pentru fişierele externe ale bazei de date model se găsesc în Anexa F.
- Tipul de intrare detaliat. Unele tipuri de intrare jurnal sunt folosite pentru a înregistra în istoric mai mult de un tip de eveniment. Câmpul tip de intrare detaliat din intrarea de jurnal identifică tipul de eveniment.
- ID-ul mesajului care poate fi utilizat pentru a defini informaţiile specifice intrării în intrarea de jurnal.

Tabela 125. Valori auditare acţiune

Valoare posibilă	Disponibil la variabilele de sistem QAUDLVL şi QAUDLVL2	Disponibil la comanda CHGUSRAUD	Descriere
*NONE	Da	Da	Dacă variabila de sistem QAUDLVL etse *NONE, nici o acţiune nu este înregistrată în istoric pe o bază lărgită a sistemului. Acţiunile sunt înregistrate în istoric pentru utilizatori individuali pe baza valorii AUDLVL din profilurile lor de utilizatori. Dacă valoarea AUDLVL dintr-un profil utilizator este *NONE, nu este realizată nici o auditare suplimentară de acţiune pentru acest utilizator. Orice acţiuni specificate pentru variabila de sistem QAUDLVL sunt înregistrate în sistem pentru acest utilizator.
*AUTFAIL	Da	Nu	**Autorizare eşecuri**: Încercările fără succes de logare la sistem şi de accesare a obiectelor sunt înregistrate în istoric. *AUTFAIL poate fi folosit în mod regulat pentru monitorizarea utilizatorilor ce încearcă să realizeze funcţii neautorizate pe sistem. *AUTFAIL poate fi folosit, de asemenea, pentru a ajuta migrarea spre un nivel de securitate mai înalt şi pentru a testa resursa de securitate pentru o nouă aplicaţie.
*CMD	Nu	Da	**Comenzi**: Şirurile de comandă pentru înregistrare în istoric, ale sistemului, rulate de un utilizator. Dacă o comandă rulează de la un program CL ce este creat cu LOG(*NO) şi ALWRTVSRC(*NO), doar numele comandă şi numele de bibliotecă sunt înregistrate. *CMD poate fi utilizat pentru a înregistra acţiunile unui utilizator particular, precum responsabilul de securitate.
*CREATE	Da	Da	**Creare obiecte**: Sistemul scrie o intrare de jurnal când este creat un obiect nou sau de înlocuire. *CREATE poate fi folosit pentru a monitoriza când sunt create sau recompilate programele.
*DELETE	Da	Da	**Ştergere de obiecte**: Sistemul scrie o intrare de jurnal când este şters un obiect.
*JOBDTA	Da	Da	**Operaţii ale jobului**: Acţiunile care afectează un job sunt înregistrate în istoric, precum pornirea şi oprirea jobului, păstrarea, eliberarea, anularea sau modificarea lui. *JOBDTA poate fi folosit pentru a monitoriza cine rulează joburile batch.
*NETBAS	Da	Nu	**Funcţii de bază reţea**: Acţiuni reguli IP, conexiuni socket-uri, filtru de căutare director APPN, filtru punct final APPN.

Tabela 125. Valori auditare acţiune (continuare)

Valoare posibilă	Disponibil la variabilele de sistem QAUDLVL şi QAUDLVL2	Disponibil la comanda CHGUSRAUD	Descriere
*NETCLU	Da	Nu	**Operaţii cluster sau grup de resurse** : Este scrisă o intrare de jurnal de auditare când apar aceste evenimente: • Un nod cluster sau un grup de resurse cluster este adăugat, creat sau şters. • Un nod cluster sau un grup de resurse cluster este pornit, oprit, actualizat sau înlăturat. • Eşecul automat al unui sistem care comută accesul la alt sistem. • Accesul este comutat manual de la un sistem la alt sistem, într-un cluster.
*NETCMN	Da	Nu	**Auditare comunicaţii reţea**: Violările detectate de suportul pentru filtrare APPN sunt înregistrate în jurnalul de auditare a securităţii când sunt auditate Filtrul de căutare director şi Filtrul de punct final. *NETCMN este compus din câteva valori pentru a vă permite să personalizaţi mai bine auditarea dumneavoastră. Următoarele valori compun *NETCMN: *NETBAS *NETCLU *NETFAIL *NETSCK
*NETFAIL	Da	Nu	**Eşecuri de reţea** : Este scrisă o intrare de jurnal de auditare când încercaţi să vă conectaţi la un port TCP/IP care nu există sau când încercaţi să trimiteţi informaţii unui port TCP/IP care nu este deschis sau disponibil.
*NETSCK	Da	Nu	**Operaţii socket-uri**: Este scrisă o intrare de jurnal de auditare când apar aceste evenimente: • Este acceptată o conexiune de intrare socket TCP/IP. • Este satbilită o conexiune de ieşire socket TCP/IP. • Este alocată o adresă IP prin DHCP (Dynamic Host Configuration Protocol). • O adresă IP este nedisponibilă pentru a fi alocată prin DHCP, deoarece toate adresele IP sunt folosite. • Paşta este filtrată sau refuzată.
*OBJMGT	Da	Da	**Operaţii de gestionare a obiectului** : Deplasare a unui obiect către o bibliotecă diferită sau redenumirea sa este înregistrată în istoric. *OBJMGT poate fi folosit pentru a detecta copierea informaţiilor cofidenţiale prin mutarea obiectului într-o bibliotecă diferită.
*OPTICAL	Da	Da	**Funcţii optice**: Toate funcţiile optice sunt auditate, inclusiv funcţiile referitoare la fişierele optice, directoarele optice, volumele optice şi cartuşele optice. *OPTICAL poate fi utilizat pentru a detecta încercările de creare sau ştergere a unui director optic.

Tabela 125. Valori auditare acţiune (continuare)

Valoare posibilă	Disponibil la variabilele de sistem QAUDLVL şi QAUDLVL2	Disponibil la comanda CHGUSRAUD	Descriere
*PGMADP	Da	Da	**Autorizare adoptată**: Sistemul scrie o intrare de jurnal când este folosită o autorizare adoptată pentru a câştiga accesul la un obiect. *PGMADP poate fi utilizat pentru a testa modul în care o aplicaţie nouă foloseşte o autorizare adoptată.
*PGMFAIL	Da	Nu	**Eşecuri de program**: Sistemul scrie o intrare de jurnal când este un program creează o eroare de integritate. *PGMFAIL poate fi folosit pentru a ajuta migrarea spre un nivel de securitate mai înalt şi pentru a testa o nouă aplicaţie.
*PRTDTA	Da	Nu	**Funcţii de tipărire**: Tipărirea unui fişier spool, tipărirea direct dintr-un program sau trimiterea unui fişier spool unei imprimante la distanţă sunt înregistrate în istoric. *PRTDTA poate fi folosit pentru a detecta tipărirea informaţiei confidenţiale.
*SAVRST	Da	Da	**Restaurare operaţii** : *SAVRST poate fi folosit pentru a detecta încercările de restaurare a obiectelor neautorizate.
*SECCFG	Da	Nu	**Configurare a securităţii**: Este scrisă o intrare de jurnal de auditare când apar aceste evenimente: • Sunt create, modificate, şterse sau restaurate profiluri utilizator. • Se aduc modificări programelor, variabilelor de sistem, rutării de subsistem sau atributelor de auditare ale unui obiect. • Parola QSECOFR este resetată la valoarea livrată. • Parola responsabilului cu securitatea uneltelor de service este implicită.
*SECDIRSRV	Da	Nu	**Funcţii Directory Services**: Este scrisă o intrare de jurnal de auditare când apar aceste evenimente: • Modificări sau actualizări se fac auditării, autorizării, parolelor şi dreptului de proprietate. • Legări şi dezlegări de succes.
*SECIPC	Da	Nu	**Comunicaţii interproces**: Este scrisă o intrare de jurnal de auditare când apar aceste evenimente: • Se fac modificări dreptului de proprietate sau autorizării unui obiect IPC. • O creare, ştergere sau obţinere a unui obiect IPC. • Ataşare de memorie partajată.

Tabela 125. Valori auditare acţiune (continuare)

Valoare posibilă	Disponibil la variabilele de sistem QAUDLVL şi QAUDLVL2	Disponibil la comanda CHGUSRAUD	Descriere
*SECNAS	Da	Nu	**Acţiuni de service autentificare în reţea**: Este scrisă o intrare de jurnal de auditare când apar aceste evenimente: • Tichet de serviciu valid. • Principalii serviciului nu se potrivesc. • Principalii clientului nu se potrivesc. • Nepotrivire adresă IP tichet. • Decriptarea tichetului a eşuat. • Decriptarea autorizării a eşuat. • Reagiunea nu este în cadrul clientului şi regiunilor locale. • Tichetul este o încercare de răspuns. • Tichetul nu este încă valid. • Nepotrivire adresă IP locală sau la distanţă. • Decriptare a erorii sumă de control KRB_AP_PRIV sau KRB_AP_SAFE. • Pentru KRB_AP_PRIV sau KRB_AP_SAFE: Eroare amprentă de timp, eroare de răspuns sau eroare de ordine a secvenţei. • Pentru acceptare GSS: acreditări expirate, eroare sumă de control sau legături de canal. • Pentru desfacere GSS sau verificare GSS: context expirat, decriptare/ decodificare, eroare sumă de control sau eroare de secvenţă.
*SECRUN	Da	Nu	**Funcţii de timp pentru rularea securităţii** : Modificrile dreptului de proprietate al obiectului, autoritatăţii şi grupului primar sunt scrise în jurnalul de auditare.
*SECSCKD	Da	Nu	**Descriptori socket**: Este scrisă o intrare de jurnal de auditare când apar aceste evenimente: • Un descriptor socket este acordat altui job. • Un descriptor socket este primit. • Un descriptor socket este inutilizabil.
*SECVFY	Da	Nu	**Funcţii de verificare**: Este scrisă o intrare de jurnal de auditare când apar aceste evenimente: • Este generat un mâner de profil sau un jeton. • Toate jetoanele profil au fost invalidate. • Numărul maxim de jetoane profil a fost generat. • Toate jetoanele profil pentru un utilizator au fost înlăturate. • Un profil utilizator a fost autentificat. • Un profil destinaţie a fost modificat în timpul unei sesiuni passthrough.

Tabela 125. Valori auditare acţiune (continuare)

Valoare posibilă	Disponibil la variabilele de sistem QAUDLVL şi QAUDLVL2	Disponibil la comanda CHGUSRAUD	Descriere
*SECVLDL	Da	Nu	**Operaţii de validare a listei**: Este scrisă o intrare de jurnal de auditare când apar aceste evenimente: • O adăugare, înlăturare sau găsire a intrării de listă de validare. • Verificare cu succes sau fără succes a intrării listei de validare.
*SECURITY	Da	Da	**Operaţii de securitate**: Evenimente relevante de securitate, precum modificarea unui profil de utilizator sau a variabilei de sistem, sunt înregistrate în istoric. *SECURITY poate fi utilizat pentru a păstra o înregistrare a tuturor activităţilor de securitate. *SECURITY este compus din câteva valori pentru a vă permite să personalizaţi mai bine auditarea dumneavoastră. Următoarele valori compun *SECURITY: *SECCFG *SECDIRSRV *SECIPC *SECNAS *SECRUN *SECSCKD *SECVFY *SECVLDL
*SERVICE	Da	Da	**Operaţii de service**: utilizarea uneltelor de service, precum DMPOBJ (Dump Object - Obiect dump) şi STRCPYSCN (Start Copy Screen - Pornire ecran de copiere), este înregistrată. *SERVICE poate fi utilizat pentru a detecta încercările de a circumscrie securitatea prin utilizarea uneltelor de service.
*SPLFDTA	Da	Da	**Operaţii în fişiere spool**: Acţiunile realizate într-un fişier spool sunt înregistrate, inclusiv crearea, copierea şi trimiterea. *SPLFDTA poate fi utilizat pentru a detecta încercările de tipărire sau trimitere a datelor confidenţiale.
*SYSMGT	Da	Da	**Operaţii de gestionare sisteme**: Sistemul scrie o intrare de jurnal pentru activităţile de gestionare a sistemelor, precum modificarea unei liste de răspuns sau a unei programări pornire/oprire. Se poate folosi *SYSMGT pentru a detecta încercările de utilizare a funcţiilor de gestionare a sistemelor pentru a trece peste controalele de securitate.

Tabela 126. Intrări jurnal auditare securitate

Valoare de auditare acţiune sau obiect	Tip de intrare jurnal	Model de fişier ieşire bază de date	Intrare detaliată	Descriere
Auditare acţiune:				

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acţiune sau obiect	Tip de intrare jurnal	Model de fişier ieşire bază de date	Intrare detaliată	Descriere
*AUTFAIL [1]	AF	QASYAFJE/J4/J5	A	Încercare făcută pentru a accesa un obiect pentru a realiza o operaţie pentru care utilizatorul nu a fost autorizat.
	X1	QASYX1J5	F	Eşuare jeton de identitate delega
			U	Primire utilizator de la jetonul identitate eşuat
			F	Eroare autorizare ICAPI
			G	Eroare autentificare ICAPI
			H	Final de scanare acţiune program
			J	Încercare făcută pentru a lansa sau programa un job sub o descriere de job care are un profil utilizator specificat. Lansatorul nu are autorizarea la profilul utilizator.
			N	Jetonul profil nu este un jeton profil regenerabil.
			P	Încercare făcută pentru a folosi un mâner profil care nu este valid pe API QWTSETP.
			S	Încercare făcută pentru logare fără introducerea unei parole sau a unui ID utilizator.
			T	Port TCP/IP neautorizat
			U	O cerere de permisiune utilizator nu a fost validă.
			V	Jetonul profil nu este valid pentru generarea unui jeton profil nou.
			W	Jetonul profil nu este valid pentru swap.
			Y	Nu este autorizat pentru câmpul JUID curent în timpul unei operaţii de ştergere JUID.
			Z	Nu este autorizat pentru câmpul JUID curent în timpul unei operaţii de setare JUID.
	CV	QASYCVJ4/J5	E	Conexiune finalizată anormal
	DI	QASYDIJ4/J5	AF	Eşuări de autorizare
			PW	Eşuări de parolă
			R	Conexiune refuzată
	GR	QASYGRJ4/J5	F	Operaţii de înregistrare a funcţiei.
	KF	QASYKFJ4/J5	P	A fost introdusă o parolă incorectă.
	IP	QASYIPJE/J4/J5	F	Eşuare autorizare pentru o cerere IPC.
	PW	QASYPWJE/J4/J5	A	Eşuare legătură APPC.
			D	A fost introdus un nume utilizator DST incorect.
			E	A fost introdusă o parolă DST incorectă.
			P	A fost introdusă o parolă incorectă.
			U	Nume utilizator nevalid
			X	Utilizatorul uneltelor de service este dezactivat
			Y	Utilizatorul uneltelor de service nu este valid
			Z	Parola uneltelor de service nu este validă

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acţiune sau obiect	Tip de intrare jurnal	Model de fişier ieşire bază de date	Intrare detaliată	Descriere
	VO	QASYVOJ4/J5	U	Verificare fără succes a unei intrări a listei de validare.
	VC	QASYVCJE/J4/J5	R	O conexiune a fost refuzată din cauza parolei incorecte.
	VN	QASYVNJE/J4/J5	R	O logare de reţea a fost refuzată din cauza contului expirat, a orelor incorecte, a id-ului utilizator incorect sau a parolei incorecte.
	VP	QASYVPJE/J4/J5	P	A fost folosită parolă incorectă de reţea.
*CMD [2]	CD	QASYCDJE/J4/J5	C	Rula o comandă.
			L	Rula o declaraţie limbaj de control S/36E.
			O	Era rulată o comandă control operator S/36E.
			P	Era rulată o procedură S/36E.
			S	Rularea comenzii a avut loc după substituirea comenzii.
			U	Era rulată o declaraţie de control utilitar S/36E.
*CREATE [3]	CO	QASYCOJE/J4/J5	N	Creare de obiect nou, cu excepţia creării obiectelor din biblioteca QTTEMP.
			R	Înlocuirea obiectului existent.
	DI	QASYDIJ4/J5	CO	Creare obiect
*DELETE [3]	DO	QASYDOJE/J4/J5	A	Obiect şters
			C	Aşteptare ştergere realizată
			D	Aşteptare creare rulare inversă
			P	Ştergere în curs
			R	Aşteptare ştergere rulare inversă
	DI	QASYDIJ4/J5	DO	Ştergere obiect
*JOBDTA	JS	QASYJSJE/J4/J5	A	Comanda ENDJOBABN a fost folosită.
			B	A fost trimis un job.
			C	A fost modificat un job.
			E	A fost oprit un job.
			H	A fost reţinut un job.
			I	A fost deconectat un job.
			M	Modificare profil sau profil de grup.
			N	Comanda ENDJOB a fost folosită.
			P	A fost ataşată o cerere de pornire a programului la jobul prestart.
			Q	Atributele interogării au fost modificate.
			R	A fost eliberat un job reţinut.
			S	A pornit un job.
			T	Modificare profil sau profil de grup folosind un jeton de profil.
			U	Comanda CHGUSRTRC
	SG	QASYSGJE/J4/J5	A	Proces de semnalizare asincron OS/400.
			P	Procesare de semnal asincron mediu de spaţiu adresă privată (Private Address Space Environment -(PASE).
	VC	QASYVCJE/J4/J5	S	A fost pornită o conexiune.
			E	O conexiune a fost terminată.
	VN	QASYVNJE/J4/J5	F	Cerere de delogare.
			O	Cerere de logare.

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acţiune sau obiect	Tip de intrare jurnal	Model de fişier ieşire bază de date	Intrare detaliată	Descriere
	VS	QASYVSJE/J4/J5	S	A pornit o sesiune de server.
			E	A fost terminată o sesiune de server.
*NETBAS	CV	QASYCVJE/J4/J5	C	Conexiune stabilită
			E	Conexiune finalizată normal
			R	Conexiune refuzată
	IR	QASYIRJ4/J5	L	Au fost încărcate reguli IP de pe un fişier.
			N	Reguli IP au fost descărcate pentru o conexiune securitate IP.
			P	Reguli IP au fost încărcate pentru o conexiune securitate IP.
			R	Reguli IP au fost citite şi copiate într-un fişier.
			U	Au fost descărcate (înlăturate) reguli.
	IS	QASYISJ4/J5	1	Faza 1 de negociere.
			2	Faza 2 de negociere.
	ND	QASYNDJE/J4/J5	A	A fost detectată o violare la suportul de APPN Filter când a fost auditat filtrul de căutare director.
	NE	QASYNEJE/J4/J5	A	A fost detectată o violare la suportul APPN Filter când a fost auditat filtrul punct de oprire.
*NETCLU	CU	QASYCUJE/J4/J5	M	Creare a unui obiect de către operaţia control cluster.
			R	Creare a unui obiect de către operaţia de gestiune Grup resursă cluster (*GRP).
*NETCMN	CU	QASYCUJE/J4/J5	M	Creare a unui obiect de către operaţia control cluster.
			R	Creare a unui obiect de către operaţia de gestiune Grup resursă cluster (*GRP).
	CV	QASYCVJ4/J5	C	Conexiune stabilită.
			E	Conexiune finalizată normal
	IR	QASYIRJ4/J5	L	Au fost încărcate reguli IP de pe un fişier.
			N	Reguli IP au fost descărcate pentru o conexiune securitate IP.
			P	Reguli IP au fost încărcate pentru o conexiune securitate IP.
			R	Reguli IP au fost citite şi copiate într-un fişier.
			U	Au fost descărcate (înlăturate) reguli.
	IS	QASYISJ4/J5	1	Phase 1 negotiation.
			2	Phase 2 negotiation.
	ND	QASYNDJE/J4/J5	A	A fost detectată o violare la suportul de APPN Filter când a fost auditat filtrul de căutare director.
	NE	QASYNEJE/J4/J5	A	A fost detectată o violare la suportul APPN Filter când a fost auditat filtrul punct de oprire.
	SK	QASYSKJ4/J5	A	Acceptare
			C	Conectare
			D	Adresă DHCP alocată
			F	Poştă filtrată
			P	Port nedisponibil

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acţiune sau obiect	Tip de intrare jurnal	Model de fişier ieşire bază de date	Intrare detaliată	Descriere
			R	Refuzare poştă
			U	Adresă DHCP refuzată
*NETFAIL	SK	QASYSKJ4/J5	P	Port nedisponibil
*NETSCK	SK	QASYSKJ4/J5	A	Acceptare
			C	Conectare
			D	Adresă DHCP alocată
			F	Poştă filtrată
			R	Refuzare poştă
			U	Adresă DHCP refuzată
*OBJMGT [3]	DI	QASYDIJ4/J5	OM	Redenumire obiect
	OM	QASYOMJE/J4/J5	M	A fost mutat un obiect la o altă bibliotecă.
			R	Un obiect a fost redenumit.
*OFCSRV	ML	QASYMLJE/J4/J5	O	A fost deschis un istoric de poştă.
	SD	QASYSDJE/J4/J5	S	A fost făcută o modificare directorului de distribiţie sistem.
*OPTICAL	O1	QASY01JE/J4/J5	R	Deschidere fişier sau director
			U	Modificare sau extragere atribute
			D	Ştergere director fişier
			C	Creare director
			X	Eliberare de fişier optic reţinut
	O2	QASY02JE/J4/J5	C	Copiere fişier sau director
			R	Redenumire fişier
			B	Copiere de rezervă fişier sau director
			S	Salvare de fişier optic reţinut
			M	Mutare fişier
	O3	QASY03JE/J4/J5	I	Iniţializare volum
			B	Copiere de rezervă volum.
			N	Redenumire volum
			C	Conversiune a volumului de rezervă la cel primar
			M	Importare
			E	Exportare
			L	Modificare listă de autorizare
			A	Modificare atribute ale volumului
			R	Citire absolută
*PGMADP	AP	QASYAPJE/J4/J5	S	A pornit un program care adoptă autorizarea proprietarului. Intrarea de pornire este scrisă prima dată când autorizarea adoptată este folosită pentru a câştiga accesul la un obiect, nu atunci când programul intră în stiva programului.
			E	A fost oprit un program care adoptă autorizarea proprietarului. Intrarea aeste scrisă când programul părăseşte stiva programului. Dacă acelaşi program apare mai mult de o dată în stiva program, intrarea oprire este scrisă când apariţia cea mai înaltă (ultima) a programului părăseşte stiva.
			A	Autorizarea adoptată a fost folosită în timpul activării programului.

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acţiune sau obiect	Tip de intrare jurnal	Model de fişier ieşire bază de date	Intrare detaliată	Descriere
*PGMFAIL [1]	AF	QASYAFJE/J4/J5	B	Un program rula o instrucţiune restricţionată de interfaţă de maşină.
			C	Un program care a eşuat verificările de validarea a programului de restaurare timp a fost restaurat. Informaţii despre eşec sunt în câmpul *Tip de violare valoare de validare* al ânregistrării.
			D	Un program accesează un obiect printr-o interfaţă nesuportată sau programul calabil este nelistat ca API calabil.
			E	Violare protecţie hardware spaţiu de stocare.
			R	Încercare făcută să actualizeze un obiect care este definit numai citire. (Protecţia hardware îmbunătăţită a spaţiului de stocare este înregistrată în istoric numai la nivelul de securitate 40 sau mai înalt)
*PRTDTA [1]	PO	QASYPOJE/J4/J5	D	Ieşirea imprimantei a fost tipărită direct la imprimantă.
			R	Ieşire trimisă sistemului de la distanţă pentru tipărire.
			S	Ieşirea imprimantei a fost spool sau tipărită.
*SAVRST [3]	OR	QASYORJE/J4/J5	N	Un obiect nou a fost restaurat pentru sistem.
			E	Un obiect a fost restaurat şi înlocuieşte un obiect existent.
	RA	QASYRAJE/J4/J5	A	Sistemul a modificat autorizarea unui obiect ce era restaurat. [4]
	RJ	QASYRJJE/J4/J5	A	O descriere de job ce conţine un nume de profil utilizatore a fost restaurată.
	RO	QASYROJE/J4/J5	A	Proprietarul obiectului a fost modificat la QDFTOWN în timpul operaţiei de restaurare.
	RP	QASYRPJE/J4/J5	A	A fost restaurat un program care adoptă autorizarea proprietarului.
	RQ	QASYRQJE/J4/J5	A	Un obiect *CRQD cu PROFILE(*OWNER) a fost restaurat.
	RU	QASYRUJE/J4/J5	A	Autorizarea a fost restaurată pentru un profil utilizator folosind comanda RSTAUT.
	RZ	QASYRZJE/J4/J5	A	Grupul primar pentru un obiect a fost modificat în timpul operaţiei de restaurare.
			O	Auditarea unui obiect a fost modificată cu comanda CHGOBJAUD.
			U	Auditarea pentru un utilizator a fost modificată cu comanda CHGUSRAUD.
*SECCFG	AD	QASYADJE/J4/J5	D	Auditarea unui DLO a fost modificată cu comanda CHGDLOAUD.
			S	Modificare atribut de scanare prin comanda CHGATR sau API Qp01SetAttr.
			O	Auditarea unui obiect a fost modificată cu comanda CHGOBJAUD.

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acţiune sau obiect	Tip de intrare jurnal	Model de fişier ieşire bază de date	Intrare detaliată	Descriere
			U	Auditarea pentru un utilizator a fost modificată cu comanda CHGUSRAUD.
	AU	QASYAUJ5	E	Modificare de configuraţie Mapare identitate întreprindere (Enterprise Identity Mapping - EIM)
	CP	QASYCPJE/J4/J5	A	Operaţia de creare, modificare sau restaurare a unui profil utilizator când API QSYSRESPA este folosit.
	CQ	QASYCQJE/J4/J5	A	Un obiect *CRQD a fost modificată.
	CY	QASYCYJ4/J5	A	Funcţie de Control acces
			F	Funcţie de Control facilitate
			M	Funcţie Cheie master
	DO	QASYDOJE/J4/J5	A	Obiectul nu a fost şters sub un control angajat
			C	O ştergere în aşteptare a obiectului a fost realizată
			D	O creare în aşteptare a obiectului a fost rulată înapoi.
			P	Ştergerea obiectului este în curs (ştergera a fost realizată sub controlul angajării)
			R	O ştergere în aşteptare a obiectului a fost rulată înapoi.
	DS	QASYDSJE/J4/J5	A	Cerere de resetare a parolei DST QSECOFR pentru valoarea implicită furnizată de sistem.
			C	Profil DST modificat.
	EV	QASYEVJ4/J5	A	Adăugare.
			C	Modificare.
			D	Ştergere.
	GR	QASYGRJ4/J5	A	Adăugare ieşire program
			D	Ieşire de program înlăturată.
			F	Operaţie de înregistrare a funcţiei.
			R	Ieşire de program înlocuită.
	JD	QASYJDJE/J4/J5	A	Parametrul USER al unei descrieri de job a fost modificat.
	KF	QASYKFJ4/J5	C	Certificare operaţie.
			K	Operaţie fişier inel de chei.
			T	Operaţie rădăcină de încredere.
	NA	QASYNAJE/J4/J5	A	A fost modificat un atribut de reţea.
	PA	QASYPAJE/J4/J5	A	A fost modificat un program pentru a adopta autorizarea proprietarului.
	SE	QASYSEJE/J4/J5	A	A fost modificată o intrare rutare de subsistem.
	SO	QASYSOJ4/J5	A	Adăugare intrare.
			C	Modificare intrare.
			R	Înlăturare intrare.
	SV	QASYSVJE/J4/J5	A	A fost modificată o variabilă de sistem.
			B	Atributele service au fost modificate.
			C	Modificare la ceasul de sistem.
	VA	QASYVAJE/J4/J5	S	Lista de control al accesului a fost modificată cu succes.

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acţiune sau obiect	Tip de intrare jurnal	Model de fişier ieşire bază de date	Intrare detaliată	Descriere
			F	Modificarea listei de control al accesului a eşuat.
			V	Verificare cu succes a unei intrări a listei de validare.
	VU	QASYVUJE/J4/J5	G	A fost modificată o înregistrare de grup.
			M	Informaţia globală a profilului utilizator a fost modificată.
			U	A fost modificată o înregistrare utilizator.
*SECDIRSRV	DI	QASYADJE/J4/J5	AD	Modificare auditare.
			BN	Legătură reuşită.
			CA	Modificare autorizare
			CP	Modificare parolă
			OW	Modificare drept de proprietate
			UB	Dezlegare reuşită
*SECIPC	IP	QASYIPJE/J4/J5	A	A fost modificat dreptul de proprietate sau autorizarea unui obiect IPC.
			C	Creare a unui obiect IPC.
			D	Ştergere a unui obiect IPC.
			G	Obţinere a unui obiect IPC.
*SECNAS	X0	QASYX0J4/J5	1	Tichet service valid.
			2	Principalii serviciului nu se potrivesc.
			3	Principalii clientului nu se potrivesc.
			4	Nepotrivire adresă IP tichet.
			5	Decriptarea tichetului a eşuat.
			6	Decriptarea autentificatorului a eşuat.
			7	Reagiunea nu este în cadrul clientului şi regiunilor locale.
			8	Tichetul este o încercare de repunere în funcţiune.
			9	Tichetul nu este încă valid.
			A	Decriptare a erorii sumă de control KRB_AP_PRIV sau KRB_AP_SAFE.
			B	Nepotrivire de adresă IP la distanţă
			C	Nepotrivire de adresă IP locală
			D	Eroare amprentă de timp KRB_AP_PRIV or KRB_AP_SAFE
			E	Eroare de repunere în funcţiune KRB_AP_PRIV or KRB_AP_SAFE
			F	Eroare de ordine secvenţială KRB_AP_PRIV KRB_AP_SAFE
			K	GSS credenţial acceptat - expirat
			L	GSS eroare sumă de control - acceptare
			M	GSS legături canal - acceptate
			N	GSS unwrap sau GSS verificare expirat
			O	GSS unwrap sau GSS verificare decriptare/decodificare
			P	GSS unwrap sau GSS verificare eroare sumă de control
			Q	GSS unwrap sau GSS verificare eroare secvenţială
*SECRUN	CA	QASYCAJE/J4/J5	A	Modificări ale listei de autorizare sau ale autorizăriii obiectului.

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acţiune sau obiect	Tip de intrare jurnal	Model de fişier ieşire bază de date	Intrare detaliată	Descriere
	OW	QASYOWJE/J4/J5	A	Dreptul de proprietate al obiectului a fost modificat.
	PG	QASYPGJE/J4/J5	A	Grupul primar pentru un obiect a fost modificat.
*SECSCKD	GS	QASYGSJE/J4/J5	G	Un descriptor socket a fost acordat altui job. (Înregistrarea de auditare GS este creată dacă nu este creată pentru jobul curent.)
			R	Primire descriptor.
			U	Imposibil de folosit descriptorul.
*SECURITY	AD	QASYADJE/J4/J5	D	Auditarea unui DLO a fost modificată cu comanda CHGDLOAUD.
			O	Auditarea unui obiect a fost modificată cu comanda CHGOBJAUD.
			U	Auditarea pentru un utilizator a fost modificată cu comanda CHGUSRAUD.
			S	Modificare atribut de scanare prin comanda CHGATR sau API Qp01SetAttr.
	X1	QASYADJE/J4/J5	D	Reuşiree jeton de identitate delegat
			G	Primire utilizator de la jetonul identitate reuşit
	AU	QASYAUJ5	E	Modificare de configuraţie Mapare identitate întreprindere (Enterprise Identity Mapping - EIM)
	CA	QASYCAJE/J4/J5	A	Modificări ale listei de autorizare sau ale autorizăriii obiectului.
	CP	QASYCPJE/J4/J5	A	Operaţia de creare, modificare sau restaurare a unui profil utilizator când API QSYRESPA este folosit.
	CQ	QASYCQJE/J4/J5	A	Un obiect *CRQD a fost modificată.
	CV	QASYCVJ4/J5	C	Conexiune stabilită.
			E	Conexiune finalizată normal
			R	Conexiune refuzată.
	CY	QASYCYJ4/J5	A	Funcţie de Control acces
			F	Funcţie de Control facilitate
			M	Funcţie Cheie master
	DI	QASYDIJ4/J5	AD	Modificare audit
			BN	Legătură reuşită.
			CA	Modificare autorizare
			CP	Modificare parolă
			OW	Modificare drept de proprietate
			UB	Dezlegare reuşită
	DO	QASYDOJE/J4/J5	A	Obiectul nu a fost şters sub un control angajat
			C	O ştergere în aşteptare a obiectului a fost realizată
			D	O creare în aşteptare a obiectului a fost rulată înapoi.
			P	Ştergerea obiectului este în curs (ştergera a fost realizată sub controlul angajării)
			R	O ştergere în curs de obiect a fost rulată înapoi.

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acţiune sau obiect	Tip de intrare jurnal	Model de fişier ieşire bază de date	Intrare detaliată	Descriere
	DS	QASYDSJE/J4/J5	A	Cerere de resetare a parolei DST QSECOFR pentru valoarea implicită furnizată de sistem.
			C	Profil DST modificat.
	EV	QASYEVJ4/J5	A	Adăugare.
			C	Modificare.
			D	Ştergere.
	GR	QASYGRJ4/J5	A	Adăugare ieşire program
			D	Ieşire de program înlăturată.
			F	Operaţie de înregistrare a funcţiei.
			R	Ieşire de program înlocuită.
	GS	QASYGSJE/J4/J5	G	Un descriptor socket a fost acordat altui job. (Înregistrarea de auditare GS este creată dacă nu este creată pentru jobul curent.)
			R	Primire descriptor.
			U	Imposibil de folosit descriptorul.
	IP	QASYIPJE/J4/J5	A	A fost modificat dreptul de proprietate sau autorizarea unui obiect IPC.
			C	Creare a unui obiect IPC.
			D	Ştergere a unui obiect IPC.
			G	Obţinere a unui obiect IPC.
	JD	QASYJDJE/J4/J5	A	Parametrul USER al unei descrieri de job a fost modificat.
	KF	QASYKFJ4/J5	C	Certificare operaţie.
			K	Operaţie fişier inel de chei.
			T	Operaţie rădăcină de încredere.
	NA	QASYNAJE/J4/J5	A	A fost modificat un atribut de reţea.
	OW	QASYOWJE/J4/J5	A	Dreptul de proprietate al obiectului a fost modificat.
	PA	QASYPAJE/J4/J5	A	A fost modificat un program pentru a adopta autorizarea proprietarului.
	PG	QASYPGJE/J4/J5	A	Grupul primar pentru un obiect a fost modificat.
	PS	QASYPSJE/J4/J5	A	Un profil utilizator destinaţie a fost modificat în timpul unei sesiuni passthrough.
			E	An office user ended work on behalf of another user.
			H	Un mâner de profil a fost generat prin QSYGETPH API.
			I	Toate jetoanele profil au fost invalidate.
			M	Numărul maxim de jetoane profil a fost generat.
			P	Jetonul profil generat pentru utilizator.
			R	Toate jetoanele profil pentru un utilizator au fost înlăturate.
			S	Un utilizator de tip office a început să lucreze în contul altui utilizator.
			V	Profil utilizator autentificat.
	SE	QASYSEJE/J4/J5	A	A fost modificată o intrare rutare de subsistem.

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acţiune sau obiect	Tip de intrare jurnal	Model de fişier ieşire bază de date	Intrare detaliată	Descriere
	SO	QASYSOJ4/J5	A	Adăugare intrare.
			C	Modificare intrare.
			R	Înlăturare intrare.
	SV	QASYSVJE/J4/J5	A	A fost modificată o variabilă de sistem.
			B	Atributele service au fost modificate.
			C	Modificare la ceasul de sistem.
	VA	QASYVAJE/J4/J5	S	Lista de control al accesului a fost modificată cu succes.
			F	Modificarea listei de control al accesului a eşuat.
	VO		V	Verificare cu succes a unei intrări a listei de validare.
	VU	QASYVUJE/J4/J5	G	A fost modificată o înregistrare de grup.
			M	Informaţia globală a profilului utilizator a fost modificată.
			U	A fost modificată o înregistrare utilizator.
	X0	QASYX0J4/J5	1	Tichet service valid.
			2	Principalii serviciului nu se potrivesc.
			3	Principalii clientului nu se potrivesc.
			4	Nepotrivire de adresă IP tichet.
			5	Decriptare a tichetului eşuat.
			6	Decriptare a autentificatorului eşuat.
			7	Reagiunea nu este în client şi regiunile locale.
			8	Tichetul este o încercare de repunere în funcţiune.
			9	Tichetul nu este încă valid.
			A	Decriptare a erorii sumă de control KRB_AP_PRIV sau KRB_AP_SAFE.
			B	Nepotrivire de adresă IP la distanţă
			C	Nepotrivire de adresă IP locală
			D	Eroare amprentă de timp KRB_AP_PRIV or KRB_AP_SAFE
			E	Eroare de repunere în funcţiune KRB_AP_PRIV or KRB_AP_SAFE
			F	Eroare de ordine secvenţială KRB_AP_PRIV KRB_AP_SAFE
			K	GSS credenţial acceptat - expirat
			L	GSS eroare sumă de control - acceptare
			M	GSS legături canal - acceptate
			N	GSS unwrap sau GSS verificare expirat
			O	GSS unwrap sau GSS verificare decriptare/decodificare
			P	GSS unwrap sau GSS verificare eroare sumă de control
			Q	GSS unwrap sau GSS verificare eroare secvenţială
*SECVFY	PS	QASYPSJE/J4/J5	A	Un profil utilizator destinaţie a fost modificat în timpul unei sesiuni passthrough.
	X1	QASYX1J5	D	Reuşiree jeton de identitate delegat

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acţiune sau obiect	Tip de intrare jurnal	Model de fişier ieşire bază de date	Intrare detaliată	Descriere
			G	Primire utilizator de la jetonul identitate reuşit
			E	An office user ended work on behalf of another user.
			H	Un mâner de profil a fost generat prin QSYGETPH API.
			I	Toate jetoanele profil au fost invalidate.
			M	Numărul maxim de jetoane profil a fost generat.
			P	Jetonul profil generat pentru utilizator.
			R	Toate jetoanele profil pentru un utilizator au fost înlăturate.
			S	Un utilizator de tip office a început să lucreze în contul altui utilizator.
			V	Profil utilizator autentificat.
*SECVLDL	VO		V	Verificare cu succes a unei intrări a listei de validare.
*SERVICE	ST	QASYSTJE/J4/J5	A	Unealta service a fost folosită.
	VV	QASYVVJE/J4/J5	C	The fost modificată starea serviciului.
			E	Serverul a fost oprit.
			P	Serverul a fost oprit.
			R	Serverul a fost repornit.
			S	Serverul a fost pornit.
*SPLFDTA	SF	QASYSFJE/J4/J5	A	Un fişier spool a fost citit de altcineva decât proprietarul.
			C	A fost creat un fişier spool.
			D	A fost şters un fişier spool.
			H	A fost reţinut un fişier spool.
			I	An fost creat un fişier inline.
			R	A fost şeliberat un fişier spool.
			U	A fost modificat un fişier spool.
*SYSMGT	DI	QASYDIJ4/J5	CF	Modificări de configurare
	SM	QASYSMJE/J4/J5	B	Opţiunile de copiere pentru rezervă au fost modificate foloisindxxxxxxxxxx
			C	Opţiunile de curăţare automată au fost modificate foloisindxxxxxxxxxx
			D	O modificare DRDA* a fost făcută.
			F	An fost modificat un fişier HFS.
			N	A fost realizată o operaţie fişier de reţea.
			O	O listă de copiere de rezervă a fost modificată foloisindxxxxxxxxxx
			P	O programare pornire/oprire a fost modificată folosind xxxxxxxxxx.
			S	Lista de răspunsuri sistem a fost modificată.
			T	Orele de recuperare a căii de acces au fost modificate.
	VL	QASYVLJE/J4/J5	A	Contul a expirat.
			D	Contul este dezactivat.
			L	Orele de logare au expirat.
			U	Necunoscut sau nedisponibil
			W	Staţie de lucru nevalidă

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acţiune sau obiect	Tip de intrare jurnal	Model de fişier ieşire bază de date	Intrare detaliată	Descriere
Auditare obiect:				
*CHANGE	DI	QASYDIJ4/J5	IM	Import director LDAP
	ZC	QASYZCJ4/J5	C	Modificări obiect
			U	Modernizare a accesului deschis către un obiect
	AD	QASYADJEJ4/J5	D	Auditarea unui obiect a fost modificată cu comanda CHGOBJAUD.
			O	Auditarea unui obiect a fost modificată cu comanda CHGOBJAUD.
			S	Modificare atribut de scanare prin comanda CHGATR sau API Qp01SetAttr.
			U	Auditarea pentru un utilizator a fost modificată cu comanda CHGUSRAUD.
	AU	QASYAUJ5	E	Modificare de configuraţie Mapare identitate întreprindere (Enterprise Identity Mapping - EIM)
	CA	QASYCAJE/J4/J5	A	Modificări ale listei de autorizare sau ale autorizăriii obiectului.
	OM	QASYOMJE/J4/J5	M	A fost mutat un obiect la o altă bibliotecă.
			R	Un obiect a fost redenumit.
	OR	QASYORJE/J4/J5	N	Un obiect nou a fost restaurat pentru sistem.
			E	Un obiect a fost restaurat şi înlocuieşte un obiect existent.
	OW	QASYOWJE/J4/J5	A	Dreptul de proprietate al obiectului a fost modificat.
	PG	QASYPGJE/J4/J5	A	Grupul primar pentru un obiect a fost modificat.
	RA	QASYRAJE/J4/J5	A	Sistemul a modificat autorizarea unui obiect ce era restaurat.
	RO	QASYROJE/J4/J5	A	Proprietarul obiectului a fost modificat la QDFTOWN în timpul operaţiei de restaurare.
	RZ	QASYRZJE/J4/J5	A	Grupul primar pentru un obiect a fost modificat în timpul operaţiei de restaurare.
	GR	QASYGRJ4/J5	F	Operaţii de înregistrare a funcţiei[6]
	LD	QASYLDJE/J4/J5	L	Legătură la un director.
			U	Dezlegare de la un director.
			K	Căutare a unui director.
	VF	QASYVFJE/J4/J5	A	Fişierul a fost închis din cauza deconectării administrative.
			N	Fişierul a fost închis din cauza deconectării client normal.
			S	Fişierul a fost închis din cauza sesiunii deconectării.
	VO	QASYVOJ4/J5	A	Adăugare intrare listă de validare.
			C	Modificare intrare listă de validare.
			F	Găsire intrare listă de validare.
			R	Înlăturare intrare listă de validare.
	VR	QASYVRJE/J4/J5	F	Resursă de acces eşuată.
			S	Resursa de acces a fost reuşită.
	YC	QASYYCJE/J4/J5	C	Un obiect bibliotecă document a fost modificat.

Tabela 126. Intrări jurnal auditare securitate (continuare)

Valoare de auditare acţiune sau obiect	Tip de intrare jurnal	Model de fişier ieşire bază de date	Intrare detaliată	Descriere
	ZC	QASYZCJE/J4/J5	C	Un obiect a fost modificat.
			U	Modernizare a accesului deschis către un obiect.
*ALL [5]	CD	QASYCDJ4/J5	C	Rulare comandă
	DI	QASYDIJ4/J5	EX	Export director LDAP
			ZR	Citire obiect
	GR	QASYGRJ4/J5	F	Operaţii de înregistrare a funcţiei[6]
	YR	QASYYRJE/J4/J5	R	Un obiect bibliotecă document a fost citit.
	ZR	QASYZRJE/J4/J5	R	Un obiect a fost citit.

[1] Această valoare poate fi specificată numai pentru variabila de sistem QAUDLVL. Nu este o valoare pentru parametrul AUDLVL al unui profil utilizator.

[2] Această valoare poate fi specificată numai pentru paramtrul AUDLVL al unui profil utilizator. Nu este o valoare pentru variabila de sistem QAUDLVL,

[3] Dacă auditarea de obiect este activă pentru un obiect, este scrisă o înregistrare de auditare pentru o operaţie de creare, ştergere, gestionare obiect sau restaurare, chiar dacă aceste acţiuni nu sunt incluse în nivelul de auditare.

[4] Vedeţi acest subiect “Restaurarea obiectelor” la pagina 216 pentru informaţii despre modificările de autorizare care pot apărea când un obiect este restaurat.

[5] Când este specificat *ALL, intrările pentru *CHANGE şi *ALL sunt scrise.

[6] Când obiectul QUSRSYS/QUSEXRGOBJ *EXITRG este auditat.

Planificarea auditării accesului la obiect

Sistemul furnizează abilitatea de a înregistra accesul la un obiect din jurnalul de auditare a securităţii. Aceasta se numeşte **auditare obiect**. Variabila de sistem QAUDCTL, valoarea OBJAUD pentru un obiect şi valoarea OBJAUD pentru un profil utilizator lucrează împreună pentru a controla auditarea obiectului. Valoarea OBJAUD pentru obiectul şi valoarea OBJAUD pentru utilizatorul care foloseşte acest obiect determină dacă un acces specific ar trebui să fie înregistrat. Variabila de sistem QAUDCTL porneşte şi opreşte funcţia de auditarea a obiectului.

Tabela 127arată cum lucrează împreună valorile OBJAUD pentru obiect şi profilul utilizator.

Tabela 127. Cum lucrează împreună un obiect şi o auditare utilizator.

Valoare pentru obiect OBJAUD	Valoare pentru utilizator OBJAUD		
	*NONE	*CHANGE	*ALL
*NONE	Nimic	Nimic	Nimic
*USRPRF	Nimic	Modificare	Modificare şi utilizare
*CHANGE	Modificare	Modificare	Modificare
*ALL	Modificare şi utilizare	Modificare şi utilizare	Modificare şi utilizare

Puteţi folosi auditarea obiectului pentru a reţine indicii depre toţi utilizatorii ce accesează un obiect critic pe sistem. Puteţi folosi, de asemenea, auditarea obiectului pentru a reţine indicii depre toate accesările obiect ale unui utilizator particular. Auditarea obiectului este o unealtă flexibilă ce vă permite să monitorizaţi acele accesări obiecte care sunt importante pentru organizaţia dumneavoastră.

Profitrea de capabilităţile auditării obiect necesită o planificare atentă. O auditare neglijent proiectată poate genera mult mai multe înregistrări de auditare decât puteţi analiza şi poate afecta semnificativ performanţa sistemului. De exemplu,

setarea unei valori OBJAUD la *ALL pentru o bibliotecă generează o intrare de auditare ce este scrisă de fiecare dată sistemul caută un obiect în acea bibliotecă. Pentru o bibliotecă utilizată des într-un sistem aglomerat, aceasta ar genera un foarte mare număr de intrări de jurnal de auditare.

Ceea ce urmează sunt câteva exemple asupra modului în care se foloseşte auditarea obiectului.

- Dacă anumite fişiere critice sunt folosite în organizaţia dumneavoastră, puteţi revedea periodic cine le accesează, folosind o tehnică exemplu:
  1. Setaţi valoarea OBJAUD pentru fiecare fişier critic la *USRPRF, folosind comanda Modificare auditare obiect:

```
                    Change Object Auditing (CHGOBJAUD)

Type choices, press Enter.

Object . . . . . . . . . . . . .   file-name
  Library  . . . . . . . . . . .     library-name
Object type  . . . . . . . . . .   *FILE
ASP device . . . . . . . . . . .   *
Object auditing value  . . . . .   *USRPRF
```

  2. Setaţi valoarea OBJAUD pentru fiecare utilizator în exemplul dumneavoastră la *CHANGE sau *ALL, folosind comanda CHGUSRAUD.
  3. Asiguraţi-vă că variabila de sistem QAUDCTL include *OBJAUD.
  4. După ce a trecut timp suficient pentru colectarea unui exemplu reprezentativ, setaţi valoarea OBJAUD din profilul utilizator la *NONE sau înlăturaţi *OBJAUD de la variabila de sistem QAUDCTL.
  5. Analizaţi intrările de jurnal de auditare folosind tehnicile descrise în “Analizarea intrărilor din jurnalul de auditare cu o interogare sau un program” la pagina 255
- Dacă sunteţi interesat de cine foloseşte un fişier particular, puteţi colecta informaţii despre toate accesările la acel fişier pentru o perioadă de timp:
  1. Setare auditare obiect pentru fişier, independent de valorile profilului utilizator:

     ```
     CHGOBJAUD OBJECT(nume-bibliotecă/nume-fişier)
               OBJTYPE(*FILE)  OBJAUD(*CHANGE sau *ALL)
     ```

  2. Asiguraţi-vă că variabila de sistem QAUDCTL include *OBJAUD.
  3. După ce a trecut timp suficient pentru colectarea unui exemplu reprezentativ, setaţi valoarea OBJAUD în obiect la *NONE.
  4. Analizaţi intrările de jurnal de auditare folosind tehnicile descrise în “Analizarea intrărilor din jurnalul de auditare cu o interogare sau un program” la pagina 255
- Pentru a audita toate accesările obiect pentru un utilizator specific, faceţi următoarele:
  1. Setaţi valoarea OBJAUD pentru toate obiectele *USRPRF folosind comanda CHGOBJAUD:

```
                    Change Object Auditing (CHGOBJAUD)

Type choices, press Enter.

Object . . . . . . . . . . . . .   *ALL
  Library . . . . . . . . . . . .  *ALLAVL
Object type  . . . . . . . . . .   *ALL
ASP device . . . . . . . . . . .   *
Object auditing value  . . . . .   *USRPRF
```

Atenţie: În funcţie de cât de multe obiecte sunt pe sistemul dumneavoastră, această comandă poate avea nevoie de multe ore pentru a rula. Setarea unei auditări de obiect pentru toate obiectele de pe sistem nu este de obicei necesară şi va degrada mult performanţa. Selectarea unui subset de tipuri obiect şi biblioteci pentru auditare este recomandată.

2. Setaţi valoarea OBJAUD pentru profilul utilizator specific la *CHANGE sau *ALL folosind comanda CHGUSRAUD.
3. Asiguraţ-vă că variabila de sistem QAUDCTL include *OBJAUD.
4. După ce aţi colectat un exemplu particular, setaţi valoarea OBJAUD pentru profilul utilizator la *NONE.

Afişarea auditării obiectului: Folosiţi comanda DSPOBJD pentru a afişa nivelul curent de auditare obiect pentru un obiect. Folosiţi comanda DSPDLOAUD pentru a afişa nivelul curent de auditare obiect pentru un obiect bibliotecă document.

Setarea auditării implicite pentru obiecte: Puteţi folosi variabila de sistem QCRTOBJAUD şi valoarea CRTOBJAUD pentru biblioteci şi directoare în scopul setării auditării obiectului pentru obiecte noi care sunt create. De exemplu, dacă doriţi toate obiectele noi din biblioteca INVLIB pentru a avea valoarea de auditare *USRPRF, folosiţi comanda următoare:

```
CHGLIB LIB(INVLIB) CRTOBJAUD(*USRPRF)
```

Această comandă afectează valoarea de auditare doar pentru noile obiecte. Nu modifică valoarea de auditare a obiectelor care există deja în bibliotecă.

Folosiţi valorile implicite de auditare cu atenţie. Folosirea necorespunzătoare poate avea drept urmare multe intrări nedorite în jurnalul de auditare a securităţii. Folosirea efectivă a capabilităţilor auditării obiectului ale sistemului cere o planificare atentă.

Împiedicarea pierderii informaţiilor de auditare

Cele două variabile de sistem controlează ceea ce face sistemul când condiţiile de eroare pot determina pierderea intrărilor de jurnal de auditare.

Nivelul de forţare a auditării: Variabila de sistem QAUDFRCLVL determină cât de des scrie sistemul intrări de jurnal de auditare din memorie în spaţiul auxiliar de stocare. Variabila de sistem QAUDFRCLVL lucrează precum nivelul de forţare pentru fişierele bazei de date. Trebuie să urmaţi indicaţii similare pentru determinarea nivelului corect de forţare în cazul instalării dumneavoastră.

Dacă permiteţi sistemului să determine când să scrie intrările pe spaţiul auxiliar de stocare, el echilibrează impactul asupra performanţei cu posibilitatea pierderii informaţiilor la întreruperea alimentării. Alegerea implicită şi recomandată este *SYS.

Dacă setaţi nivelul de forţare la un număr mic, minimizaţi posibilitatea pierderii înregistrărilor de audit, dar puteţi sesiza o înrăutăţire a performanţei. Dacă instalarea dumneavoastră cere ca nici o înregistrare de auditare să nu fie pierdută la căderea alimentării, trebuie să setaţi QAUDFRCLVL la 1.

Acţiunea la oprirea auditării: Variabila de sistem QAUDENDACN determină ce face sistemul dacă nu poate scrie o intrare în jurnalul de auditare. Valoarea implicită este *NOTIFY. Sistemul realizează ceea ce urmează, dacă nu poate să scrie intrările de jurnal de auditare şi QAUDENDACN este *NOTIFY:

1. Variabila de sistem QAUDCTL este setată la *NONE pentru a împiedica încercările suplimentare de scriere de intrări.
2. Mesajul CPI2283 este trimis cozii de mesaje QSYSOPR şi coziide mesaje QSYSMSG (dacă aceasta există) la fiecare oră până când auditarea este repornită cu succes.
3. Procesarea normală continuă.
4. Dacă este realizat un IPL pe sistem, mesajul CPI2284 este trimis cozilor de mesaje QSYSOPR şi QSYSMSG în timpul IPL-ului.

Notă: În majoritatea cazurilor, realizarea unui IPL rezolvă problema care a cauzat eşuarea auditării. După ce aţi repornit sistemul, setaţi variabila de sistem QAUDCTL la valoarea corectă. Sistemul încearcă să scrie o înregistrare jurnal audit, oricând această variabilă de sistem se schimbă.

Puteţi seta QAUDENDACN să oprească sistemul dacă eşuează auditarea (*PWRDWNSYS). Folosiţi această valoare doar dacă instalarea dumneavoastră cere ca auditarea să fie activată pentru sistemul ce rulează. Dacă sistemul nu poate să scrie o intrare în jurnalul de auditare şi variabila de sistem QAUDENDACN este *PWRDWNSYS, se produc următoarele:

1. Sistemul se opreşte imediat (echivalentul emiterii comenzii PWRDWNSYS *IMMED).
2. SRC cod B900 3D10 este afişat.

Mai departe, trebuie să faceţi următoarele:

1. Porniţi un IPL de la sistemul unitate. Asiguraţi-vă că este alimentat dispozitivul specificat în variabila de sistem pentru consolă (QCONSOLE).
2. Pentru a reliza IPL-ul, terbuie să se logeze un utilizator cu autorizarea specială *ALLOBJ şi *AUDIT, la consolă.
3. Sistemul porneşte într-o satere restricţionată cu un mesaj ce indică faptul că eroarea de auditare a cauzat oprirea sistemului.
4. Variabila de sistem QAUDCTL este setată la *NONE.
5. Pentru a restaura sistemul la normal, setaţi variabila de sistem QAUDCTL la altă valoare decât nici una. Când modificaţi variabila de sistem QAUDCTL, sistemul încearcă să scrie o intrare jurnal de auditare. Dacă are succes, sistemul se întoarce la starea normală.

   Dacă sistemul nu se întoarce cu succes la starea normală, folosiţi un istoric de job pentru a determina de ce a eşuat auditarea. Corectaţi problema şi încercaţi să resetaţi din nou valoarea QAUDCTL.

Alegerea neauditării obiectelor din QTEMP

Valoarea *NOQTEMP poate fi specificată ca valoare pentru variabila de sistem QAUDCTL. Dacă este specificată, trebuie să specificaţi, de asemenea, atât *OBJAUD cât şi *AUDLVL. Când este activă auditarea şi este specificat *NOQTEMP, următoarele acţiuni asupra obiectelor din biblioteca QTEMP NU vor fi auditate.

Modificare sau citire a obiectelor din QTEMP (tipuri de intrări jurnal ZC, ZR).

Modificare a autorizării, proprietarului sau grupului primar de obiectedin QTEMP (tipuri de intrări jurnal CA, OW, PG).

Folosirea CHGSECAUD pentru a seta auditarea securităţii

Privire generală:

Scop: Setare a sistemului pentru a colecta evenimentele de securitate în jurnalul QAUDJRN.

Cum se face:
CHGSECAUD
DSPSECAUD

Autorizare:
Utilizatorul trebuie să aibă autorizarea specială *ALLOBJ şi *AUDIT.

Intrare jurnal:
CO (creare obiect)
SV (modificare variabilă de sistem)
AD (modificare auditare obiect şi utilizator)

Note: Comanda CHGSECAUD creează jurnalul şi receptorul jurnal, dacă acesta nu există. CHGSECAUD setează apoi variabilele de sistem QAUDCTL, QAUDLVL şi QAUDLVL2.

Setarea auditării securităţii

Privire generală:

Scop: Setare a sistemului pentru a colecta evenimentele de securitate în jurnalul QAUDJRN.

Cum se face:

CRTJRNRCV
CRTJRN QSYS/QAUDJRN
WRKSYSVAL *SEC
CHGOBJAUD
CHGDLOAUD
CHGUSRAUD

Autorizare:

autorizare *ADD pentru QSYS şi pentru jurnal
bibliotecă receptor
autorizare specială *AUDIT

Intrare jurnal:

CO (creare obiect)
SV (modificare variabilă de sistem)
AD (modificare auditare obiect şi utilizator)

Notă: QSYS/QAUDJRN trebuie să existe înainte ca QAUDCTL să fie modificat.

Pentru a seta auditarea securităţii, faceţi paşii următori. Setarea auditării cere autorizare specială *AUDIT.

1. Creaţi un receptor de jurnal într-o bibliotecă, la alegerea dumneavoastră, folosind comanda CRTJRNRCV (Create Journal Receiver - Creare receptor jurnal. Acest exemplu foloseşte o bibliotecă numită JRNLIB pentru receptori de jurnal.

   ```
   CRTJRNRCV  JRNRCV(JRNLIB/AUDRCV0001) +
              THRESHOLD(100000) AUT(*EXCLUDE)   +
              TEXT('Auditare receptor jurnal')
   ```

   - Puneţi receptorul jurnal într-o bibliotecă salvată în mod regulat. **Nu** plasaţi receptorul jurnal în biblioteca QSYS, chiar dacă acolo este locul unde va fi jurnalul.
   - Alegeţi un nume de receptor jurnal care poate fi folosit pentru a crea o convenţie de denumire pentru viitorii receptori jurnale, precum AUDRCV0001. Puteţi folosi opţiunea *GEN, când modificaţi receptorii jurnal pentru a continua convenţia de denumire. Folosind acest tip de convenţie de numire, este util, de asemenea, dacă alegeţi ca sistemul dumneavoastră să gestioneze schimbarea receptorilor dumneavoastră jurnal.
   - Specificaţi un prag de receptor adecvat mărimii şi activităţii sistemului dumneavoastră. Dimensiunea pe care o alegeţi trebuie să se bazeze pe numărul de tranzacţii de pe sistemul dumneavoastră şi pe numărul de acţiuni pe care dumneavoastră le alegeţi spre a le audita. Dacă folosiţi suport de gestionare a jurnalului - modificare sistem, pragul receptorilor jurnal trebuie să fie de cel puţin 100,000KB. Pentru informaţii suplimentare despre pragul receptorului de jurnal, consultaţi Gestionarea jurnalului.
   - Specificaţi *EXCLUDE pe parametrul AUT pentru a limita accesul la informaţiile memorate în jurnal.
2. Creaţi jurnal QSYS/QAUDJRN prin folosirea comenzii CRTJRN (Create Journal - Creare jurnal):

   ```
   CRTJRN  JRN(QSYS/QAUDJRN) +
           JRNRCV(JRNLIB/AUDRCV0001) +
           MNGRCV(*SYSTEM) DLTRCV(*NO) +
           AUT(*EXCLUDE) TEXT('Auditare jurnal')
   ```

   - Trebuie folosit numele QSYS/QAUDJRN.
   - Specificaţi numele receptorului jurnal pe care l-aţi creat la pasul anterior.
   - Specificaţi *EXCLUDE pe parametrul AUT pentru a limita accesul la informaţiile memorate în jurnal. Trebuie să aveţi autorizarea de a adăuga obiecte la QSYS pentru a crea jurnalul.

- Folosiţi parametrul *Gestionare receptor* (MNGRCV) pentru ca sistemul să schimbe receptorul jurnal şi să ataşeze unul nou receptorul ataşat depăşeşte pregul speciifcat când a fost creat receptorul jurnal. Dacă alegeţi această opţiune, nu trebuie să folosiţi comanda CHGJRN pentru a detaşa receptorii şi pentru a crea şi ataşa manual receptori noi.
- Nu trebuie ca sistemul să ştearagă receptorii detaşaţi. Specificaţi DLTRCV(*NO), care este implicit. Receptorii QAUDJRN reprezintă coada dumneavoastră de auditare a securităţii. Asiguraţi-vă că aceştia sunt salvaţi adecvat înainte de ştergerea lor din sistem.

Subiectul Gestionare jurnal furnizează mai multe informaţii despre lucrul cu jurnale şi receptorii jurnal.

3. Setaţi valoarea de sistem pentru nivelul de auditare (QAUDLVL) sau valoarea de sistem pentru extensie nivel de auditare (QAUDLVL2), folosind comanda WRKSYSVAL. Variabilele de sistem QAUDLVL şi QAUDLVL2 determină ce acţiuni sunt înregistrate în jurnalul de auditare pentru toţi utilizatorii de pe sistem. Vedeţi “Planificarea auditării acţiunilor” la pagina 228.
4. Setaţi acţiunea de auditare pentru utilizatori individuali, dacă este necesar folosind comanda CHGUSRAUD. Vedeţi “Planificarea auditării acţiunilor” la pagina 228.
5. Setaţi auditarea de obiect pentru obiecte specifice, dacă este necesar, folosind comanda CHGOBJAUD şi CHGDLOAUD. Vedeţi “Planificarea auditării accesului la obiect” la pagina 246.
6. Setaţi auditarea de obiect pentru utilizatori specifici, dacă este necesar, folosind comanda CHGUSRAUD.
7. Setaţi valoarea de sistem QAUDENDACN pentru controlul a ceea ce se întâmplă dacă sistemul nu poate accesa jurnalul de auditare. Vedeţi “Acţiunea la oprirea auditării” la pagina 248.
8. Setaţi variabila de sistem QAUDFRCLVL pentru a controla cât de des sunt scrise înregistrările de auditare în spaţiul auxiliar de stocare. Vedeţi “Împiedicarea pierderii informaţiilor de auditare” la pagina 248.
9. Porniţi auditarea prin setarea valorii de sistem QAUDCTL la altă valoare decât *NONE.

Jurnalul QSYS/QAUDJRN trebuie să existe înainte ca dumneavoastră să puteţi modifica variabila de sistem QAUDCTL la altă valoare decât *NONE. Când porniţi auditarea, sistemul încearcă să scrie o înregistrare în jurnalul de auditare. Dacă încercarea nu este reuşită, dumneavoastră primiţi un mesaj şi auditarea nu porneşte.

Gestionarea jurnalului de auditare şi a receptorilor de jurnal

Jurnalul de auditare, QSYS/QAUDJRN, este destinat numai auditării securităţii. Obiectele nu trebuie să fie jurnalizate în jurnalul de auditare. Controlul obligaţiilor nu trebuie să folosească jurnalul de auditare. Intrările utilizatorului nu trebuie trimise acestui jurnal folosind comanda SNDJRNE (Send Journal Entry - Trimitere intrare jurnal) sau API-ul QJOSJRNE (Send Journal Entry - Trimitere intrare jurnal).

Protecţia specială de blocare este folosită pentru a asigura faptul că sistemul poate scrie intrări de auditare în jurnalul de auditare. Când auditarea este activă (variabila de sistem QAUDCTL nu este *NONE), jobul de arbitraj al sistemului (QSYSARB) reţine un blocaj în jurnalul QSYS/QAUDJRN. Nu puteţi realiza anumite operaţii în jurnalul de auditare când auditarea este activă, precum:

- comanda DLTJRN
- comenzile ENDJRNxxx (End Journaling - Final jurnalizare)
- comanda APYJRNCHG
- comanda RMVJRNCHG
- comanda DMPOBJ sau DMPSYSOBJ
- Mutare a jurnalului
- Restaurare a jurnalului
- Operaţii care lucrează cu autorizare, precum comanda GRTOBJAUT
- comanda WRKJRN

Informaţiile înregistrate în intrările jurnal securitate sunt descrise în Anexa F. Toate intrările de securitate din jurnalul de auditare au codul de jurnal T. Pe lângă intrările de securitate, în jurnalul QAUDJRN apar de asemenea intrările de sistem. Acestea sunt intrări cu codul de jurnal J, care se referă la IPL (initial program load) şi la operaţii generale realizate asupra receptorilor de jurnal (de exemplu, salvarea receptorului).

Dacă apare deteriorarea la jurnal sau la receptorul său curent, astfel încât intrările de auditare nu pot fi jurnalizate, variabila de sistem QAUDENDACN determină ce acţiune realizează sistemul. Recuperarea unui jurnal deteriorat sau a unui receptor jurnal este aceeaşi ca la alte jurnale.

Este posibil să doriţi ca sistemul să gestioneze modificarea receptorilor jurnal. Specifcaţi MNGRCV(*SYSTEM) când creaţi jurnalul QAUDJRN sau modificaţi jurnalul la acea valoare. Dacă specificaţi MNGRCV(*SYSTEM), sistemul dezataşează automat receptorul când atinge dimensiunea sa de prag şi creează şi ataşează un nou receptor jurnal. Aceasta se numeşte **modificare sistem-gestionare jurnal**

Dacă specificaţi MNGRCV(*USER) pentru QAUDJRN, este trimis un mesaj cozii de mesaje prag specificată pentru jurnal când receptorul jurnal atinge un prag al spaţiului de stocare. Mesajul indică faptul că receptorul a atins pragul său. Folosiţi comanda CHGJRN pentru a detaşa receptorul şi a ataşa un nou receptor jurnal. Aceasta împiedică condiţiile eroare *Intare nejurnalizată* Dacă primiţi acest mesaj, trebuie să folosiţi comanda CHGJRN pentru a continua auditarea securităţii.

Coada implicită de mesaje pentru un jurnal este QSYSOPR. Dacă instalarea dumneavoastră are un volum mare de mesaje în coada de mesaje QSYSOPR, este posibil să doriţi să asociaţi o coadă diferită de mesaje, precum AUDMSG, cu jurnalul QAUDJRN. Puteţi folosi un program de tratare a mesajelor pentru a monitoriza coada de mesaje AUDMSG. Când este primit un avertisment al pragului jurnal (CPF7099), puteţi ataşa în mod automat un nou receptor. Dacă folosiţi o modificare sistem-gestionare de jurnal, atunci mesajul CPF7020 este trimis cozii de mesaje jurnal când este completat un jurnal modificare sistem. Puteţi monitoriza acest mesaj pentru a ştii când să executaţi o salvare a receptorilor jurnal detaşaţi.

Atenţie: Funcţia de ştergere automată furnizată folosind meniurile Asistent operaţional nu şterge receptorii QAUDJRN. Trebuie să detaşaţi în mod regulat, să salvaţi şi să ştergeţi receptorii QAUDJRN pentru a evita problemele cu spaţiul pe disc.

Vedeţi subiectul Gestionarea jurnalului pentru informaţii complete despre gestionarea jurnalelor şi a receptorilor de jurnal.

Notă: Jurnalul QAUDJRN este creat în timpul unui IPL dacă nu există şi variabila de sistem QAUDCTL este setată la o altă valoare decât *NONE. Aceasta se petrece doar după o situaţie neobişnuită, precum înlocuirea unui dispozitiv disc sau ştergerea unui pool de memorie auxiliară.

Salvarea şi ştergerea receptorilor de jurnal de auditare

Privire generală:

Scop: Pentru a ataşa un receptor nou jurnal audit; pentru a salva şi şterge vechiul receptor

Cum se face:

- CHGJRN QSYS/QAUDJRN
- JRNRCV(*GEN) SAVOBJ (pentru a salva vechiul receptor)
- DLTJRNRCV (pentru a şterge vechiul receptor)

Autorizare:
Autorizare *ALL pentru autorizarea receptor jurnal *USE la jurnal

Intrare jurnal:
J (intrare sistem la QAUDJRN)

Notă: Selectare a timpului când sistemul nu este ocupat.

Trebuie să detaşaţi în mod regulat receptorul de jurnal de auditare curent şi să ataşaţi unul nou pentru două motive:

- Analizarea intrărilor jurnal este mai facilă decât dacă fiecare receptor jurnal conţine intrările pentru o perioadă de timp specifică, gestionabilă.

- Receptorii jurnal mari pot afecta performanţa sistemului, în plus faţă de ocuparea unui spaţiu folositor de pe spaţiul de stocare auxiliar.

Gestionarea receptorilor în mod automat de către sistem este abordarea recomandată. Puteţi specifica aceasta folosind parametrul *Gestionare receptor* când creaţi jurnalul.

Dacă aţi setat auditarea acţiune şi auditarea obiect pentru a înregistra multe evenimente diferite, este posibil să trebuiască să specificaţi o valoare mare de prag pentru receptorul jurnal. Dacă gestionaţi manual receptorii, este posibil să trebuiască să modificaţi zilnic receptorii jurnal. Dacă înregistraţi doar câteva evenimente, este posibil să doriţi să modificaţi receptorii pentru a corespunde programului de rezervă pentru biblioteca ce conţine receptorul jurnal.

Folosiţi comanda CHGJRN pentru a detaşa un receptor şi a ataşa un nou receptor jurnal.

Receptorii de jurnale gestionaţi de sistem: Dacă sistemul dumneavoastră gestionează receptorii, folosiţi următoarea procedură pentru a salva toţi receptorii detaşaţi QAUDJRN şi pentru a-i şterge:

1. Introduceţi WRKJRNA QAUDJRN. Ecranul vă arată receptorul curent ataşat. Nu salvaţi sau ştergeţi acest receptor.
2. Folosiţi F15 pentru a lucra cu directorul receptor. Aceasta arată toţi receptorii care au fost asociaţi cu jurnalul şi starea lor.
3. Folosiţi comanda SAVOBJ pentru a salva fiecare receptor, cu excepţia receptorului ataşat în prezent, care nu a fist deja salvat.
4. Folosiţi comanda DLTJRNRCV pentru a şterge fiecare receptor după ce este salvat.

Notă: O alternativă la procedura de mai sus ar putea fi realizată folosind coada de mesaje jurnal şi monitorizând mesajul CPF7020 ceea ce indică faptul că jurnalul modificare sistem s-a terminat cu succes. Vedeţi *Backup and Recovery* pentru informaţii suplimentare despre acest suport.

Receptorii de jurnale gestionaţi de utilizator: Dacă alegeţi să gestionaţi manual receptorii jurnal, folosiţi următoarea procedură pentru a detaşa, salva şi şterge un receptor jurnal:

1. Introduceţi CHGJRN JRN(QAUDJRN) JRNRCV(*GEN). Această comandă:
   a. Detaşează receptorul ataşat în prezent.
   b. Creează un receptor nou cu numărul secvenţial următor.
   c. Ataşează noul receptor la jurnal.

   De exemplu, dacă receptorul curent este AUDRCV0003, sistemul creează şi ataşează un nou receptor numit AUDRCV0004.

   Comanda Gestionare atribute jurnal (Work with Journal Attributes - WRKJRNA) vă spune care receptor este ataşat în prezent: WRKJRNA QAUDJRN.
2. Folosiţi comanda Salvare obiect (SAVOBJ) pentru a salva receptorul jurnal detaşat. Specificaţi tipul obiectului *JRNRCV.
3. Folosiţi comanda DLTJRNRCV (Delete Journal Receiver - Ştergere receptor jurnal) pentru a şterge receptorul. Dacă încercaţi să ştergeţi receptorul fără a-l salva, primiţi un mesaj de avertizare.

Oprirea funcţiei de auditare

Este posibil să doriţi să folosiţi funcţia de auditare în mod periodic, decât tot timpul. De exemplu, puteţi dori să o folosiţi când testaţi o aplicaţie nouă. Sau e posibil să o folosiţi pentru a realiza o auditare de securitate în mod secvenţial.

Pentru a opri funcţia de auditare, faceţi ceea ce urmează:

1. Folosiţi comanda WRKSYSVAL pentru a modifica variabila de sistem QAUDCTL la *NONE. Aceasta opreşte sistemul de la înregistrarea în continuare a altor evenimente.
2. Detaşaţi receptorul jurnal curent folosind comanda CHGJRN.
3. Salvaţi şi ştergeţi receptorul detaşat, folosind comenzile SAVOBJ şi DLTJRNRCV.

4. Puteţi şterge jurnalul QAUDJRN după ce l-aţi modificat pe QAUDCTL la *NONE. Dacă plănuiţi să continuaţi auditarea securităţii, în viitor, este posibil să doriţi părăsirea jurnalului QAUDJRN pe sistem. Însă dacă jurnalul QAUDJRN este setat cu MNGRCV(*SYSTEM), sistemul detaşează receptorul şi ataşează unul nou ori de câte ori realizaţi un IPL, chiar dacă auditarea securităţii este activă. Trebuie să ştergeţi aceşti receptori jurnal. Salvarea lor înainte de a-i şterge nu trebuie să aibă loc neapărat, deoarece ei nu conţin nici o intrare de auditare.

Analizarea intrărilor din jurnalul de auditare

O dată ce aţi setat funcţia de auditare securitate, puteţi folosi câteva metode diferite pentru a analiza evenimentele care sunt înregistrate:

- Vizualizare a intrărilor setate la staţia dumneavoastră de lucru
- Folosirea unei unelte de interogare sau a unui program pentru a analiza intrările
- Folosirea comenzii Afişare intrări jurnal auditare - Display Audit Journal Entries (DSPAUDJRNE)

Notă: IBM a oprit furnizarea îmbunătăţirilor pentru comanda DSPAUSJRNE. Comanda nu suportă toate tipurile de înregistrări de auditare a securităţii şi nu listează toate câmpurile pentru înregistrările pe care ea le suportă.

Puteţi, de asemenea, să folosiţi comanda RCVJRNE (Receive Journal Entry - Primire intrare jurnal) în jurnalul QAUDJRN pentru a primi intrările aşa cum sunt ele scrise în jurnalul QAUDJRN.

Vizualizarea intrărilor din jurnalul de auditare

Privire generală:

Scop: Vizualizare intrări QAUDJRN

Cum se face:
Comanda DSPJRN (Display Journal - Afişare jurnal)

Autorizare:
Autorizare *USE pentru autorizare QSYS/QAUDJRN *USE receptor jurnal

Comanda Afişare jurnal (DSPJRN) vă permite să vedeţi intrările jurnal selectate la staţia dumneavoastră de lucru. Pentru a vedea intrările jurnal, faceţi ceea ce urmează:

1. Introduceţi DSPJRN QAUDJRN şi apăsaţi F4. În ecranul prompt, puteţi să introduceţi informaţii pentru a selecta intervalul de intrări ce este arătat. De exemplu, puteţi selecta toate intrările într-un interval specific de date sau puteţi selecta doar un anumit tip de intrare, precum o încercare incorectă de logare (tip de intrare jurnal PW).

   Este implicită afişarea intrărilor doar din receptorul ataşat. Puteţi folosi RCVRNG(*CURCHAIN) pentru a vedea intrările din toţi receptorii ce sunt în lanţul receptor pentru jurnalul QAUDJRN, până la a include receptorul care este ataşat curent.
2. Când apăsaţi tasta Introducere, vedeţi ecranul Afişare intrări jurnal:

```
                          Display Journal Entries

Journal  . . . . . :   QAUDJRN         Library  . . . . . :   QSYS
Largest sequence number on this screen  . . . . . :00000000000000000012
Type options, press Enter.
  5=Display entire entry


Opt    Sequence  Code  Type  Object      Library     Job       Time
              1   J     PR                          SCPF      10:24:55
              2   T     CA                          SCPF      10:24:55
              3   T     CO                          SCPF      10:24:55
              4   T     CA                          SCPF      10:24:55
              5   T     CO                          SCPF      10:24:55
              6   T     CA                          SCPF      10:24:55
              7   T     CO                          SCPF      10:24:55
              8   T     CA                          SCPF      10:24:56
              9   T     CO                          SCPF      10:24:56
             10   T     CA                          SCPF      10:24:57
             11   T     CO                          SCPF      10:24:57
             12   T     CA                          SCPF      10:24:57
                                                                More...
F3=Exit   F12=Cancel
```

3. Folosiţi opţiunea 5 (Afişare întraga intrare) pentru a vedea informaţii despre o anumită intrare:

```
                            Display Journal Entry

Object . . . . . :   NEWESTAREA      Library  . . . . . :LEVERING
Member . . . . . :
Incomplete data  . . :   No              Minimized entry data :No
Sequence . . . . . :   3
Code . . . . . :   E  - Data area operation
Type . . . . . :   EG - Start journal for data area

            Entry specific data
Column      *...+....1....+....2....+....3....+....4....+....5
00001      '0'
```

4. Puteţi folosi F6 (Afişare doar a datelor specifice intrării) pentru intrări cu o mare cantitate de date specifice. Puteţi selecta de asemenea o versiune hexazecimală a afişării. Puteţi folosi F10 pentru a afişa detalii despre intrările din jurnal fără date specifice intrării.

   Anexa F conţine modelul pentru fiecare tip al intrării jurnal QAUDJRN.

Analizarea intrărilor din jurnalul de auditare cu o interogare sau un program

Privire generală:

Scop: Afişare sau printare a informaţiilor selectate din intrările jurnal.

Cum se face:
DSPJRN OUTPUT(*OUTFILE), Creare a interogării şi programului sau Rulare interogare sau program

Autorizare:
Autorizare *USE pentru autorizare QSYS/QAUDJRN, autorizare *USE pentru receptor jurnal

Puteţi folosi comanda DSPJRN (Display Journal - Afişare jurnal) pentru a scrie intrările selectate din receptorii jurnal audt într-un fişier de ieşire. Puteţi folosi programul sau interogarea pentru a vedea informaţiile din fişierul ieşire.

Pentru parametrul ieşire al comenzii DSPJRN, specificaţi *OUTFILE. Vedeţi parametrii suplimentari ce vă afişează informaţiile despre fişierul ieşire:

```
                        Display Journal (DSPJRN)

Type choices, press Enter.
  :
Output . . . . . . . . . . . . . > *OUTFILE
Outfile format . . . . . . . . .   *TYPE5
File to receive output . . . . .   dspjrnout
  Library  . . . . . . . . . . .     mylib
Output member options:
  Member to receive output . . .   *FIRST
  Replace or add records . . . .   *REPLACE
Entry data length:
  Field data format  . . . . . .   *OUTFILFMT
  Variable length field length
  Allocated length . . . . . . .
```

Toate intrările relative la securitate din jurnalul audit conţin aceleaşi informaţii antet, ca şi tipul intrării, data intrării şi jobul care a determinat intrarea. QADSPJR5 (cu formatul înregostrare QJORDJE5) este furnizat pentru a defini aceste câmpuri când specificaţi *TYPE5 ca parametru format ieşire. Vedeţi Tabela 152 la pagina 489 pentru informaţii suplimentare.

Pentru informaţii suplimentare despre alte înregistrări şi formatele lor de ieşire, vedeţi Anexa F.

Dacă doriţi să realizaţi o analiză detaliată a unui tip particular de intrare, folosiţi unul din fişierele bază de date model furnizate. De exemplu, pentru a crea un fişier ieşire numit AUDJRNAF în QGPL care include doar intrările eşec autorizare:

1. Creaţi un fişier ieşire gol cu formatul definit pentru intrările jurnal AF:

   ```
   CRTDUPOBJ OBJ(QASYAFJ5) FROMLIB(QSYS) +
     OBJTYPE(*FILE) TOLIB(QGPL) NEWOBJ(AUDJRNAF5)
   ```

2. Folosiţi comanda DSPJRN pentru a scrie intrările jurnal selectate pentru fişierul ieşire:

   ```
   DSPJRN JRN(QAUDJRN) ... +
      JRNCDE(T) ENTTYP(AF) OUTPUT(*OUTFILE) +
      OUTFILFMT(*TYPE5) OUTFILE(QGPL/AUDJRNAF5)
   ```

3. Folosiţi Interogare sau un program pentru a analiza informaţia din fişierul AUDJRNAF.

Tabela 126 la pagina 233 arată numele fişierului bază de date model pentrufiecare tip de intrare. Anexa F arată machetele fişier pentru fiecare model de fişier bază de date.

Ceea ce urmează sunt câteva exemple despre cum puteţi folosi informaţia QAUDJRN:

- Dacă suspectaţi că cineva încearcă să intre în sistemul dumneavoastră:
  1. Asiguraţi-vă că variabila de sistem QAUDLVL include *AUTFAIL.
  2. Folosiţi comanda obiect CRTDUPOBJ pentru a crea un fişier ieşire gol cu formatul QASYPWJ5.
  3. O intrare jurnal de tip PW este înregistrată când introduce cineva un ID sau o parolă utilizator incorecte în ecranul Logare. Folosiţi comanda DSPJRN pentru a scrie intrările jurnal de tip PW în fişierul ieşire.
  4. Creaţi un program interogare care afişează sau tipăreşte data, timpul şi staţia de lucru pentru fiecare intrare jurnal. Aceste informaţii vă ajută să determinaţi când şi unde apar încercările.
- Dacă doriţi să testaţi resursa de securitate pe care a-ţi definit-o pentru o aplicaţie nouă:

1. Asiguraţi-vă că variabila de sistem QAUDLVL include *AUTFAIL.
2. Rulaţi testele aplicaţie cu ID-uri utilizator diferite.
3. Folosiţi comanda obiect CRTDUPOBJ pentru a crea un fişier ieşire gol cu formatul QASYAFJ5.
4. Folosiţi comanda DSPJRN pentru a scrie intrările jurnal de tip AF în fişierul ieşire.
5. Creaţi un program interogare care afişează sau tipăreşte informaţii depre obiect, job şi utilizator. Această informaţie vă ajută să determinaţi ce utilizatori şi funcţii aplicaţie determină eşecurile de autorizare.

- Dacă planificaţi o migrare spre nivelul de securitate 40:
  1. Asiguraţi-vă că variabila de sistem QAUDLVL include *PGMFALL şi *AUTFAIL.
  2. Folosiţi comanda obiect CRTDUPOBJ pentru a crea un fişier ieşire gol cu formatul QASYAFJ5.
  3. Folosiţi comanda DSPJRN pentru a scrie intrările jurnal de tip AF în fişierul ieşire.
  4. Creaţi un program de interogare ce selectează tipul de încălcări pe care le experimentaţi în timpul testului şi tipăreşte informaţii despre jobul şi programul ce determină fiecare intrare.

     Notă: Tabela 126 la pagina 233arată care intrare jurnal este scrisă pentru fiecare mesaj de încălcare a autorizării.

Alte tehnici pentru monitorizarea securităţii

Jurnalul auditare securitate (QAUDJRN) este sursa primară de informaţii despre evenimentele în legătură cu securitatea de pe sistemul dumneavoastră. Următoarele secţiuni discută alte moduri de observare a evenimentelor legate de securitate şi a valorilor de securitate de pe sistemul dumneavoastră.

Veţi găsi informaţii suplimentare înAnexa G, “Comenzile şi meniurile pentru comenzi de securitate”, la pagina 593. Această anexă include exemple de folosire a comenzii şi informaţiilor depre meniuri pentru instrumente de securitate.

Monitorizarea mesajelor de securitate

Unele evenimente relevante de securitate, precum încercările de logare incorectă, realizează un mesaj în coada de mesaje QSYSOPR. Puteţi crea separat, de asemenea,o coadă de mesaje numită QSYSMSG în biblioteca QSYS.

Dacă realizaţi coada de mesaje QSYSMSG în biblioteca QSYS, mesajele despre evenimentele critice de sistem sunt trimise atât către acea coadă de mesaje cât şi către QSYSOPR. Coda de mesaje QSYSMSG poate fi monitorizată separat de un program sau un operator de sistem. Aceasta furnizează protecţie suplimentară pentru resursele dumneavoastră de sistem. Mesajele critice de sistem din QSYSOPR sunt uneori ratate din cauza volumului de mesaje trimis la acea coadă de mesaje.

Utilizarea istoricului sistem

Unele evenimente în relaţie cu securitatea, precum depăşirea încercărilor de logare incorectă în variabila de sistem QMAXSIGN, determină ca un mesaj să fie trimis istoricului QHST(istoric sistem-history). Mesajele de securitate sunt în intervalul 2200 - 22FF. Ele au prefixele CPI, CPF, CPC, CPD şi CPA.

Începând cu Versiunea 2 Ediţia 3 a programului licenţiat OS/400, unele mesaje privind eşecul autorizării şi violarea integrităţii nu mai sunt trimise în istoricul (istoria) QHST. Toate informaţiile care au fost disponibile în isttoricul QHST pot fi obţinute din jurnalul audit securitate. Înregistrarea informaţiei în jurnalul audit furnizează o performanţă mai bună a sistemului şi informaţii complete despre aceste evenimente legate de securitate decât o face istoricul QHST. Istoricul QHST nu trebuie considerat o sursă completă de violări de securitate. Folosiţi în schimb funcţiile de auditare securitate.

Aceste mesaje nu mai sunt scrise în istoricul QHST log:

- CPF2218. aceste evenimente ot fi capturate în jurnalul audit prin specificarea *AUTFAIL pentru variabila de sistem QAUDLVL.
- CPF2240. aceste evenimente ot fi capturate în jurnalul audit prin specificarea *AUTFAIL pentru variabila de sistem QAUDLVL.

Folosirea jurnalelor pentru monitorizarea activităţii obiectului

Dacă includeţi valoarea *AUTFAIL pentru auditarea acţiunii sistem (QAUDLVL variabilă de sistem), sistemul scrie o intrare jurnal audit pentru fiecare încercare nereuşită de accesare a resursei. Pentru obiecte critice, puteţi seta, de asemenea, o auditare obiect astfel încât sistemul scrie o intrare jurnal audit pentru fiecare acces reuşit.

Jurnalul audit înregistrează doar faptul că obiectul a fost accesat. Nu înregistrează în istoric fiecare tranzacţie către obiect. Pentru obiecte critice de pe sistemul dumneavoastră, este posibil să doriţi informaţii mai detaliate despre datele specifice care au fost accesate şi modificate. Jurnalizarea obiectului vă poate furniza aceste detalii. Jurnalizarea obiectului este folosită în mod primar pentru integritatea şi recuperarea obiectului. Vedeţi secţiuneaGestionarea jurnalului din Centrul de informare pentru o listă de tipuri de obiecte ce pot fi jurnalizate şi ceea ce este jurnalizat pentru fiecare tip de obiect. Un responsabil de securitate sau un auditor poate folosi, de asemenea, aceste intrări jurnal pentru a revedea modificările obiectului. A nu se jurnaliza orice obiecte în jurnalul QAUDJRN.

Intrările jurnal pot include:

- Identificarea jobului şi utilizatorului şi timpul de acces
- Imagini înainte şi după modificările tuturor obiectelor
- Înregistrări atunci când obiectul a fost deschis, închis, modificat, salvat etc.

O intrare jurnal nu poate fi alterată de nici un utilizator, chiar dacă acesta este responsabilul de securitate. Un jurnal complet sau un receptor jurnal poate fi şters, dar aceasta se descoperă uşor.

Dacă jurnalizaţi pagini şi doriţi să tipăriţi toate informaţiile despre un anumit fişier, tipăriţi următoarele:

```
DSPJRN JRN(bibliotecă/jurnal) +
       FILE(bibliotecă/fişier) OUTPUT(*PRINT)
```

De exemplu, dacă jurnalul JRNCUST din bilioteca CUSTLIB este folosit pentru a înregistra informaţii despre fişierul CUSTFILE (de asemenea în biblioteca CUSTLIB), comanda va fi:

```
DSPJRN JRN(CUSTLIB/JRNCUST) +
       FILE(CUSTLIB/CUSTFILE) OUTPUT(*PRINT)
```

Dacă jurnalizaţi alte tipuri de obiect şi doriţi să vedeţi informaţiile pentru un obiect particular, tipăriţi următoarele:

```
DSPJRN JRN(bibliotecă/jurnal)
       OUTPUT(*OUTFILE)
       OUTFILEFMT(*TYPE5)
       OUTFILE(bibliotecă/fişier de ieşire)
       ENTDTALEN(*CALC)
```

Puteţi atunci să faceţi o interogare sau să folosiţi SQL pentru a selecta toate înregistrările din acest fişier de ieşire pentru un anumit nume de obiect.

Dacă doriţi să aflaţi ce jurnale sunt pe sistem, folosiţi comanda WRKJRN (Work with Journals - Gestionare jurnale). Dacă doriţi să aflaţi ce obiecte sunt jurnalizate pentru un jurnal particular, folosiţi comanda WRKJRA (Work with Journal Attributes - Gestionare atribute jurnal).

Subiectul Gestionarea jurnalului furnizează informaţii complete despre jurnalizare.

Analizarea profilurilor de utilizator

Puteţi afişa sau tipări o listă completă a tuturor utilizatorilor de pe sistemul dumneavoastră folosind comanda DSPAUTUSR (Display Authorized Users - Afişare utilizatori autorizaţi). Lista poate fi aranjată pe nume de profil sau nume de profil grup. Ceea ce urmează este un exemplu al unei secvenţe profil:

```
                          Display Authorized Users

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

Tipărirea profilurilor de utilizator selectate

Puteţi folosi comanda DSPUSRPRF (Display User Profile - Afişare profil utilizator pentru a crea un fişier ieşire, pe care îl puteţi procesa folosind o unealtă de interogare.

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

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

- O listă a tuturor utilizatorilor care au atât autorizarea specială *ALLOBJ cât şi *SPLCTL.
- O listă a tuturor utilizatorilor ordonaţi secvenţial de un câmp profil utilizator, precum un program iniţial sau o clasă utilizator.

Puteţi crea programe interogare pentru a produce rapoarte diferite de la fişierul dumneavoastră de ieşire. De exemplu:

- Listare a tuturor profilurilor utilizator care au orice tip de autorizări speciale prin selectarea înregistrărilor unde câmpul UPSPAU nu este egal cu *NONE.
- Listare a tuturor utilizatorilor cărora le este permis să introducă comenzi prin selectarea înregistrărilor unde câmpul *Cpabilităţi limită* (numit UPLTCP în fişierul model bază de date) este egal cu *NO sau *PARTIAL.
- Listare a tuturor utilizatorilor care au un meniu iniţial particular sau un program iniţial.
- Listare a utilizatorilor inactivi prin cercetarea datei câmp de ultimă logare.
- Listare a tuturor utilizatorilor care nu au o parolă pentru folosire la nivelurile 0 şi 1 de parolare prin selectarea înregistrărilor unde Parola prezentă pentru câmpul nivel 0 sau 1 (numit UPENPW în modelul de fişier ieşire) este egală cu N.
- Listare a tuturor utilizatorilor care au o parolă pentru folosire la nivelurile 2 şi 3 prin selectarea înregistrărilor unde Parola prezentă pentru câmpul nivel 2 sau 3 (numit UPENPH în modelul de fişier ieşire) este egală cu Y.

Examinarea profilurilor mari de utilizatori

Profilurile de utilizator cu numere mari de autorizări, părând a fi răspândite la întâmplare în majoritatea sistemului, pot reflecta o lipsă de planificare a securităţii. Ceea ce urmează este o metodă de localizare a profilurilor mari de utilizatori şi de evaluare a lor:

1. Folosiţi comanda DSPOBJD (Display Object Description - Afişare descriere de obiect) pentru a crea un fişier de ieşire conţinând informaţii despre toate profilurile utilizator de pe sistem:

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

2. Creaare a unui program de interogare pentru a lista numele şi dimensiunea fiecărui profil utilizator, în ordine descrescătoare după dimensiune.
3. Tipăreşte informaţii detaliate despre cele mai mari profiluri de utilizator şi evaluează autorizările şi obiectele deţinute pentru a vedea dacă ele sunt corespunzătoare:

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

   Unele profiluri utilizator furnizate de IBM sunt foarte mari datorită numărului de obiecte pe care le deţin. Listarea şi analizarea acestora nu este necesară. Oricum, trebuie să verificaţi dacă există programe de adoptare a autorizării profilurilor utilizator furnizate de IBM care au autorizare specială *ALLOBJ, precum QSECOFR şi QSYS. Vedeţi “Analizarea programelor care adoptă autorizarea”.

   Anexa B furnizează informaţii despre toate profilurile utilizator furnizate de IBM şi funcţiile acestora.

Analizarea autorizărilor pentru obiect

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

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

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

2. Folosiţi comanda DSPOBJAUT (Display Object Authority - Afişare autorizare obiect) pentru a lista autorizările unei bibliotecispecifice:

   ```
   DSPOBJAUT OBJ(nume-bibliotecă) OBJTYPE(*LIB) +
            ASPDEV(asp-nume-dispozitiv) OUTPUT(*PRINT)
   ```

3. Folosiţi comanda DSPLIB (Display Library - Afişare bibliotecă) pentru a lista obiectele din bibliotecă:

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

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

Analizarea programelor care adoptă autorizarea

Programe care adoptă autorizarea unui utilizator cu autorizarea speială *ALLOBJ reprezintă o expunere de securitate. Următoarea metodă poate fi folosită pentru a găsi şi inspecta acele programe:

1. Pentru fiecare utilizator cu autorizarea specială *ALLOBJ, folosiţi comanda DSPPGMADP (Display Programs That Adopt - Afişare programe care adoptă) pentru a lista programele care adoptă acea autorizare de utilizator:

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

   Notă: Subiectul “Tipărirea profilurilor de utilizator selectate” la pagina 259 arată cum se listează utilizatori cu autorizarea *ALLOBJ.

2. Folosiţi comanda DSPOBJAUT pentru a determina cine este autorizat pentru a folosi fiecare program de adoptare şi ce este autorizarea publică pentru program:

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

3. Inspectaţi codul sursă şi descrierea de program pentru a evalua:
   - Dacă utilizatorul programului este împiedicat să folosească funcţia exces, precum folosirea unei linii de comandă, în timpul rulării sub un profil adoptat.
   - Dacă programul adoptă nivelul minim de autorizare necesar pentru funcţia dorită. Aplicaţii care folosesc eşuarea de program pot fi proiectate folosind acelaşi profil utilizator pentru obiecte şi programe. Când autorizarea proprietarului programului este adoptată, utilizatorul are autorizarea *ALL pentru obiectele autorizare. În multe cazuri, profilul proprietarului nu necesită nici o autorizare specială.

4. Verificaţi când a fost modificat programul ultima dată, folosind comnada DSPOBJD:

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

Verificarea obiectelor ce au fost modificate

Puteţi folosi comanda CHKOBJITG (Check Object Integrity - Verificare integritate a obiectului) pentru a căuta obiecte care au fost modificate. Un obiect transformat este, de obicei, un indiciu că cineva încearcă să facă modificări pe sistemul dumneavoastră. Este posibil să doriţi să rulaţi această comandă dacă cineva:

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

| Când rulaţi comanda, sistemul creează un fişier bază de date ce conţine informaţii despre orice problemă potenţială de
| integritate. Puteţi verifica obiectele deţinute de unul sau mai multe profiluri, obiectele care se potrivesc unui nume de
| cale sau toate obiectele de pe sistemul dumneavoastră. Puteţi căuta obiecte ale cărui nume de domeniu a fost
| transformat şi obiecte cu care au fost falsificate. Puteţi recalcula valorile de validare ale programului pentru a căuta
| obiecte de tipul *PGM, *SRVPGM, *MODULE şi *SQLPKG, care au fost transformate. Puteţi verifica semnătura
| obiectelor care au fost semnate digital. Puteţi verifica dacă bibliotecile şi comenzile au fost falsificate. Puteţi, de
| asemenea, porni o scanare de sistem fişier integrat sau să verificaţi dacă obiectele au eşuat unei scanări anterioare de
| sistem fişier.

Rularea programului CHKOBJITG cere autorizare specială *AUDIT. Comanda poate necesita mult timp pentru a rula, din cauza scanărilor şi calculelor pe care le realizează. Trebuie să o rulaţi într-un moment când sistemul dumneavoastră nu este ocupat. Cele mai multe dintre comenzile IBM duplicat din ediţiile apărute înainte de V5R2 vor fi înregistrate ca violări în istoric. Aceste comenzi trebuie să fie şterse şi create din nou folosind comanda CRTDUPOBJ (Create duplicate object - Creare duplicat obiect), de fiecare dată când este încărcată o nouă ediţie.

Verificarea sistemului de operare

| Puteţi folosi API-ul QYDOCHKS (Check System - Verificare sistem) pentru a vedea dacă a fost modificat un obiect
| cheie al sistemului de operare de când a fost semnat. Un obiect care nu este semnat sau a fost modificat de când a fost
| semnat, va fi raportat ca eroare. Numai semnăturile dintr-o sursă de încredere a sistemului sunt valide.

| Rularea API-ului QYDOCHKS cere autorizare specială *AUDIT. API-ul poate necesita mult timp pentru a rula, din
| cauza calculelor pe care le realizează. Trebuie să o rulaţi într-un moment când sistemul dumneavoastră nu este ocupat.

Auditarea acţiunilor responsabilului cu securitatea

Este posibil să doriţi să păstraţi o înregistrare a tuturor acţiunilor realizate de utilizatori cu autorizarea specială *ALLOBJ şi *SECADM. Puteţi folosi valoarea de auditare a acţiunii în profilul utilizator pentru a face aceasta:

1. Pentru fiecare utilizator cu autorizarea specială *ALLOBJ şi *SECADM, folosiţi comanda CHGUSRAUD pentru a seta AUDLVL să aibă toate valorile care nu sunt incluse în variabilele de sistem QAUDLVL sau QAUDLVL2 de pe sistemul dumneavoastră. De exemplu, dacă variabila de sistem QAUDLVL este setată la *AUTFAIL, *PGMFAIL, *PRTDTA şi *SECURITY, folosiţi această comandă pentru a seta AUDLVL pentru profilul utilizator responsabilul cu securitatea:

```
CHGUSRAUD USER((SECUSER)
          AUDLVL(*CMD *CREATE *DELETE +
                 *OBJMGT *OFCSRV *PGMADP +
                 *SAVRST *SERVICE, +
                 *SPLFDTA *SYSMGT)
```

   Notă: Tabela 125 la pagina 229arată toate valorile posibile pentru auditarea acţiunii.

2. Înlătură autorizarea specială *AUDIT din profilul utilizator cu autorizarea specială *ALLOBJ şi *SECADM. Aceasta îi împiedică pe aceşti utilizatori să modifice caracteristicile de auditare ale profilurilor lor.

Notă: Nu puteţi înlătura autorizările speciale din profilul QSECOFR. De aceea, nu puteţi împiedica un utilizator logat ca QSECOFR de la modificarea caracteristicilor auditării acelui profil. Oricum, dacă un utilizator logat ca QSECOFR foloseşte comanda CHGUSRAUD pentru a modifica caracteristicile de auditare, un tip de intrare AD este scris în jurnalul de auditare.

Se recomandă ca responsabilii cu securitatea (utilizatori cu autorizarea specială *ALLOBJ sau *SECADM) să folosească propriile lor profiluri pentru o auditare mai bună. Parola pentru profilul QSECOFR nu trebuie să fie dietribuită.

3. Asiguraţi-vă că variabila de sistem QAUDCTL include *AUDLVL.
4. Folosiţi comanda DSPJRN pentru a revedea intrările din jurnalul audit folosind tehnicile descrise. “Analizarea intrărilor din jurnalul de auditare cu o interogare sau un program” la pagina 255

Anexa A. Comenzile de securitate

Această anexă conţine comenzile de sistem legate de securitate. Puteţi folosi aceste comenzi în locul meniurilor de sistem, dacă doriţi, tastând aceste comenzi la o linie de comandă. Comenzile sunt împărţite în grupuri orientate pe operaţii.

Subiectul CL din Centrul de informare informaţii mai detaliate despre aceste comenzi. Vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii. Tabelele din Anexa D arată ce autorizări de obiect suntnecesare pentru a folosi aceste comenzi.

Tabela 128. Comenzi pentru lucrul cu deţinători de autorizare

Nume comandă	Nume descriptiv	Funcţie
CRTAUTHLR	Creare deţinător de autorizare	Vă permite să asiguraţi un fişier înainte ca fişierul să existe. Deţinătorii de autorizare sunt valizi doar pentru fişiere bază de date descrise de program.
DLTAUTHLR	Ştergere deţinător de autorizare	Vă permite să ştergeţi un deţinător de autorizare. Dacă fişierul asociat există, informaţiile deţinătorului de autorizare sunt copiate în fişier.
DSPAUTHLR	Afişare deţinător de autorizare	Vă permite să afişaţi toţi deţinătorii de autorizare din sistem.

Tabela 129. Comenzi pentru lucrul cu liste de autorizaţii

Nume comandă	Nume descriptiv	Funcţie
ADDAUTLE	Adăugare intrare listă de autorizaţii	Vă permite să adăugaţi un utilizator la o listă de autorizaţii. Dumneavoastră specificaţi ce autorizare are utilizatorul pentru toate obiectele din listă.
CHGAUTLE	Modificare intrare listă de autorizaţii	Vă permite să modificaţi autorizările de utilizator pentru obiectele din lista de autorizare.
CRTAUTL	Comanda Creare listă de autorizaţii	Vă permite să creaţi o listă de autorizaţii.
DLTAUTL	Ştergere listă de autorizaţii	Vă permite să ştergeţi o întreagă listă de autorizaţii.
DSPAUTL	Afişare listă de autorizaţii	Vă permite să afişaţi o listă de utilizatori şi autorizările lor pentru o listă de autorizaţii.
DSPAUTLOBJ	Afişare obiecte listă de autorizaţii	Vă permite să afişaţi o listă de obiecte asigurate de o listă de autorizaţii.
EDTAUTL	Editare listă de autorizaţii	Vă permite să adăugaţi, modificaţi şi să înlăturaţi utilizatori şi autorizările lor de la o listă de autorizaţii.
RMVAUTLE	Înlăturare intrare listă de autorizaţii	Vă permite să înlăturaţi un utilizator de la o listă de autorizaţii.
RTVAUTLE	Extragere intrare de listă de autorizaţii	Folosită într-un program în limbaj de control (CL) pentru a obţine una sau mai multe valori asociate cu un utilizator din lista de autorizaţii. Comanda poate fi folosită împreună cu comanda CHGAUTLE pentru a acorda unui utilizator noi autorizări faţă de cele pe care le are deja.
WRKAUTL	Lucru cu liste de autorizaţie	Vă permite să lucraţi cu liste de autorizaţii dintr-un ecran listă.

Tabela 130. Comenzi pentru lucru cu autorizări şi auditare de obiecte

Nume comandă	Nume descriptiv	Funcţie
CHGAUD	Modificare auditare	Vă permite să modificaţi valoarea de auditare pentru un obiect.
CHGAUT	Modificare autorizare	Vă permite să modificaţi autorizarea utilizatorilor pentru obiecte.
CHGOBJAUD	Modificare auditare obiect	Vă permite să specificaţi dacă accesul la un obiect este auditat.
CHGOBJOWN	Modificare proprietar obiect	Vă permite să modificaţi dreptul de proprietate pentru un obiect de la un utilizator la altul.
CHGOBJPGP	Modificare grup primar obiect	Vă permite să modificaţi grupul primar pentru un obiect la un alt utilizator sau la nici un grup primar.
CHGOWN	Modificare proprietar	Vă permite să modificaţi dreptul de proprietate al unui obiect de la un utilizator la altul.
CHGPGP	Modificare grup primar	Vă permite să modificaţi grupul primar pentru un obiect la un alt utilizator sau la nici un grup primar.
DSPAUT	Afişare autorizare	Vă permite să afişaţi autorizări ale utilizatorilor pentru un obiect.
DSPOBJAUT	Afişare autorizare obiect	Afişează proprietarul obiectului, autorizare publică pentru obiect, toate autorizările private pentru obiect şi numele listei de autorizaţii folosite pentru a asigura obiectul.
DSPOBJD	Afişare descriere obiect	Afişează nivelul de auditare obiect pentru obiect.
EDTOBJAUT	Editare autorizare obiect	Vă permite să adăugaţi, să modificaţi sau să înlăturaţi o autorizare a unui utilizator pentru un obiect.
GRTOBJAUT	Acordare de autorizare obiect	Vă permite să acordaţi explicit autorizare către utilizatori numiţi, tuturor utilizatorilor (*PUBLIC) sau utilizatorilor obiectului referit pentru obiectele numite în această comandă.
RVKOBJAUT	Revocare autorizare obiect	Vă permite să înlăturaţi una sau mai multe (sau toate) din din autorizările date explicit unui utilizator pentru obiectele numite.
WRKAUT	Lucru cu autorizări	Vă permite să lucraţi cu autorizări de obiect prin selectarea de opţiuni dintr-o listă afişată.
WRKOBJ	Lucru cu obiecte	Vă permite să lucraţi cu autorizări de obiect prin selectarea de opţiuni dintr-o listă afişată.
WRKOBJOWN	Lucru cu obiecte după proprietar	Vă permite să lucraţi cu obiectele deţinute de un profil utilizator.
WRKOBJPGP	Lucru cu obiecte după grup primar	Vă permite să lucraţi cu obiectele pentru care un profil este grupul primar folosind opţiuni dintr-un ecran listă.

Tabela 131. Comenzi pentru Gestionare parole

Nume comandă	Nume descriptiv	Funcţie
CHGDSTPWD	Modificare parolă Unelte de service dedicate	Vă permite să resetaţi profilul cu capabilităţi de securitate DST la parola implicită livrată cu sistemul.
CHGPWD	Modificare parolă	Permite unui utilizator să îşi modifice parola proprie.
CHGUSRPRF	Modificare profil utilizator	Vă permite să modificaţi valorile specificate într-un profil de utilizator, inclusiv parola utilizatorului.
CHKPWD	Verificare parolă	Permite verificarea parolei unui utilizator. De exemplu, dacă doriţi ca utilizatorul să introducă din nou parola pentru a rula o anumită aplicaţie, puteţi folosi CHKPWD în programul dumneavoastră CL pentru a verifica parola.
CRTUSRPRF[1]	Creare profil utilizator	Când adăugaţi un utilizatorul în sistem, asignaţi o parolă utilizatorului.

1 Când se termină CRTUSRPRF, nu puteţi specifica crearea *USRPRF într-un pool de memorie auxiliară (ASP) independent. Totuşi, când un utilizator este autorizat privat pentru un obiect de pe un ASP independent, este proprietarul unui obiect de pe un ASP independent sau este grupul primar al unui obiect de pe un ASP independent, numele profilului este stocat pe ASP-ul independent. Dacă ASP-ul independent este mutat în alt sistem, autorizarea privată, dreptul de proprietate asupra obiectului şi intrările de grup primar vor fi ataşate la profilul cu acelaşi nume din sistemul destinaţie. Dacă nu există un profil pe sistemul destinaţie, va fi creat. Utilizatorul nu va avea nici o autorizare specială şi parola va fi setată la *NONE.

Tabela 132. Comenzi pentru lucru cu profiluri utilizator

Nume comandă	Nume descriptiv	Funcţie
CHGPRF	Modificare profil	Permite unui utilizator să modifice unele din atributele profilului propriu.
CHGUSRAUD	Modificare auditare utilizator	Vă permite să specificaţi acţiunea şi auditarea de obiect pentru un profil utilizator.
CHGUSRPRF	Modificare profil utilizator	Vă permite să modificaţi valorile specificate într-un profil utilizator, cum ar fi parola utilizatorului, autorizări speciale, meniu iniţial, program iniţial, bibliotecă curentă şi limită de prioritate.
CHKOBJITG	Verificare integritate obiect	Verificaţi obiectele deţinute de unul sau mai mulţi utilizatori sau verificaţi obiectele care corespund numelui de cale, pentru a vă asigura că obiectele nu au fost modificate.
CRTUSRPRF	Creare profil utilizator	Vă permite să adăugaţi un utilizator la sistem şi să specificaţi valori cum ar fi parola utilizatorului, autorizări speciale, meniu iniţial, bibliotecă curentă şi limită de prioritate.
DLTUSRPRF	Ştergere profil utilizator	Vă permite să ştergeţi un profil utilizator din sistem. Această comandă furnizează o opţiune de a şterge sau modifica dreptul de proprietate asupra obiectelor deţinute de profilul utilizator.
DSPAUTUSR	Afişare utilizatori autorizaţi	Afişează sau tipăreşte următoarele pentru toate profilurile de utilizator de pe sistem: profilul de grup asociat (dacă există), dacă profilul de utilizator are o parolă utilizabilă la orice nivel de parolă, dacă profilul de utilizator are o parolă utilizabilă la diferitele niveluri de parolă, dacă profilul de utilizator are o parolă utilizabilă cu NetServer, data când a fost modificată parola ultima dată şi textul profilului de utilizator.
DSPUSRPRF	Afişare profil utilizator	Vă permite să afişaţi un profil utilizator în câteva formate diferite.
GRTUSRAUT	Acordare autorizare utilizator	Vă permite să copiaţi autorizări private de la un profil utilizator la alt profil utilizator.
PRTPRFINT	Tipărire valori interne profil	Vă permite să tipăriţi un raport de informaţii interne despre numărul de intrări.
PRTUSRPRF	Tipărire profil utilizator	Vă permite să analizaţi profiluri utilizator care îndeplinesc anumite criterii.
RTVUSRPRF	Extragere profil utilizator	Folosită într-un program în limbaj de control (CL) pentru a obţine şi utiliza una sau mai multe valori care sunt stocate şi asociate cu un profil utilizator.
WRKUSRPRF	Lucru cu profiluri utilizator	Vă permite să lucraţi cu profiluri utilizator prin introducere de opţiuni într-o listă afişată.

Tabela 133. Comenzi înrudite pentru profil utilizator

Nume comandă	Nume descriptiv	Funcţie
DSPPGMADP	Afişare programe care adoptă	Vă permite să afişaţi o listă de programe şi pachete SQL care adoptă un anume profil utilizator.
RSTAUT	Restaurare autorizare	Vă permite să restauraţi autorizări pentru obiecte conţinute de un profil utilizator când acesta a fost salvat. Aceste autorizări pot fi restaurate doar ce un profil utilizator este restaurat cu comanda Restaurare profil utilizator (RSTUSRPRF).
RSTUSRPRF	Restaurare profil utilizator	Vă permite să restauraţi un profil utilizator şi atributele sale. Restaurarea autorizărior specifice obiectelor se face cu comanda RSTAUT după ce este restaurat profilul. Comanda RSTUSRPRF restaurează de asemenea toate listele de autorizări şi deţinătorii de autorizări, dacă se specifică RSTUSRPRF(*ALL).
SAVSECDTA	Salvare date de securitate	Salvează toate profilurile utilizator, liste de autorizaţii şi deţinători de autorizare fără a folosi un sistem care este într-o stare restrictivă.
SAVSYS	Salvare sistem	Salvează toate profilurile utilizator, listele de autorizări şi deţinători de autorizare din sistem. Este necesar un sistem dedicat pentru a folosi această funcţie.

Tabela 134. Comenzi pentru lucru cu auditare

Nume comandă	Nume descriptiv	Funcţie
CHGAUD	Modificare auditare	Vă permite să specificaţi auditarea pentru un obiect.
CHGDLOAUD	Modificare auditare obiect de bibliotecă de documente	Vă permite să specificaţi dacă se face auditare de acces pentru un obiect de bibliotecă de documente.
CHGOBJAUD	Modificare auditare obiect	Vă permite să specificaţi auditarea pentru un obiect.
CHGUSRAUD	Modificare auditare utilizator	Vă permite să specificaţi acţiunea şi auditarea de obiect pentru un profil utilizator.

Tabela 135. Comenzi pentru lucrul cu obiecte de bibliotecă de documente.

Nume comandă	Nume descriptiv	Funcţie
ADDDLOAUT	Adăugare autorizare obiect de bibliotecă de documente	Vă permite să acordaţi acces unui utilizator la un document sau folder sau să asiguraţi un document sau folder cu o listă de autorizaţii sau un un cod de acces.
CHGDLOAUD	Modificare auditare obiect de bibliotecă de documente	Vă permite să specificaţi nivelul de auditare obiect pentru un obiect de bibliotecă de documente.
CHGDLOAUT	Modificare autorizare obiect de bibliotecă de documente	Vă permite să modificaţi autorizarea pentru un document sau un folder.
CHGDLOOWN	Modificare proprietar obiect de bibliotecă de documente	Transferă dreptul de proprietate asupra documentului sau folderului de la un utilizator la altul.
CHGDLOPGP	Modificare grup primar pentru obiect de bibliotecă de documente	Vă permite să modificaţi grupul primar pentru un obiect de bibliotecă de documente.
DSPAUTLDLO	Afişare obiecte de bibliotecă de documente pentru listă de autorizaţii	Vă permite să afişaţi documentele şi folderele care sunt asigurate prin lista de autorizaţii specificată.
DSPDLOAUD	Afişare auditare obiect de bibliotecă de documente	Afişează nivelul de auditare pentru un obiect de bibliotecă de documente.
DSPDLOAUT	Afişare autorizare obiect de bibliotecă de documente	Vă permite să afişaţi informaţii de autorizare pentru un document sau un folder.
EDTDLOAUT	Editare autorizare obiect de bibliotecă de documente	Folosită pentru a adăuga, modifica sau înlătura autorizări utilizator pentru un document sau un folder.

Tabela 135. Comenzi pentru lucrul cu obiecte de bibliotecă de documente (continuare).

Nume comandă	Nume descriptiv	Funcţie
GRTUSRPMN	Acordare permisiune utilizator	Dă permisiune unui utilizator de a manipula documente şi foldere sau de a efectua operaţii de birou în numele altui utilizator.
RMVDLOAUT	Înlăturare autorizare obiect de bibliotecă de documente	Folosită pentru a înlătura autorizarea unui utilizator de la un document sau folder.
RVKUSRPMN	Revocare permisiune utilizator	Retrage de la un utilizator (sau toţi utilizatorii) autorizarea de a accesa documente în numele unui alt utilizator.

Tabela 136. Comenzi pentru lucru cu intrări de autentificare server

Nume comandă	Nume descriptiv	Funcţie
ADDSVRAUTE	Adăugare intrare de autentificare server	Vă permite să adăugaţi informaţii de autentificare server pentru un profil utilizator.
CHGSVRAUTE	Modificare intrare de autentificare server	Vă permite să modificaţi intrări de autentificare server existente pentru un profil utilizator.
DSPSVRAUTE	Afişare intrări de autentificare server	Vă permite să afişaţi intrări de autentificare server pentru un profil utilizator.
RMVSVRAUTE	Înlăturare intrare de autentificare server	Vă permite să înlăturaţi intrări de autentificare server din profilul utilizator specificat.

Aceste comenzi permit unui utilizator să specifice un nume de utilizator, parola asociată şi numele unei maşini server la distanţă. Distributed Relational Database Access (DRDA) foloseşte aceste intrări pentru a rula cereri de acces la baza de date ca utilizatorul specificat de pe serverul la distanţă.

Tabela 137. Comenzi pentru lucru cu directorul de distribuţie sistem

Nume comandă	Nume descriptiv	Funcţie
ADDDIRE	Adăugare intrare director	Adaugă intrări noi la directorul de distribuţie sistem. Directorul conţine informaţii despre un utilizator, cum ar fi ID şi adresă utilizator, numele sistemului, nume profil utilizator, adresă de poştă şi număr de telefon.
CHGDIRE	Modificare intrare director	Modifică datele pentru o anumită intrare din directorul de distribuţie sistem. Administratorul de sistem are autorizare de a actualiza orice date conţinute într-o intrare de director, în afară de ID utilizator, adresă şi descriere utilizator. Utilizatorii îşi pot actualiza propria intrare în director, dar nu şi anumite câmpuri.
RMVDIRE	Înlăturare intrare director	Înlătură o anumită intrare din directorul de distribuţie sistem. Când un ID utilizator şi adresă este înlăturat din director, este de asemenea înlăturat din orice liste de distribuţie.
WRKDIRE	Lucru cu directoare	Furnizează un set de ecrane care permit unui utilizator să vizualizeze, adauge, modifice şi înlăture intrări din directorul de distribuţie sistem.

Tabela 138. Comenzi pentru lucru cu liste de validare

Nume comandă	Nume descriptiv	Funcţie
CRTVLDL	Creare liste de validare	Vă permite să creaţi un obiect listă de validare care conţine intrări ce constau dintr-un identificator, date care vor fi criptate de sistem când sunt memorate şi date în formă liberă.
DLTVLDL	Ştergere listă de validare	Vă permite să ştergeţi lista de validate specificată dintr-o bibliotecă.

Tabela 139. Comenzi pentru lucru cu informaţii de utilizare funcţie

Nume comandă	Nume descriptiv	Funcţie
CHGFCNUSG	Modificare utilizare funcţie	Vă permite să modificaţi informaţiile de utilizare pentru o funcţie înregistrată.
DSPFCNUSG	Afişare utilizare funcţie	Vă permite să afişaţi o listă de identificatori de funcţie şi informaţiile detaliate de utilizare pentru o anumită funcţie.
WRKFCNUSG	Gestionare utilizare funcţie	Vă permite să afişaţi o listă de identificatori de funcţie şi să modificaţi sau să afişaţi informaţiile de utilizare de funcţie.

Următoarele tabele descriu diferite tipuri de unelte de securitate. Pentru informaţii suplimentare despre uneltele de securitate, vedeţi Anexa G, “Comenzile şi meniurile pentru comenzi de securitate”.

Tabela 140. Unelte de securitate pentru Gestionare auditare

Nume comandă	Nume descriptiv	Funcţie
CHGSECAUD	Modificare auditare de securitate	Vă permite să setaţi auditarea de securitate şi să modificaţi valorile de sistem care controlează auditarea de securitate.
DSPAUDJRNE	Afişare intrări jurnal de auditare	Vă permite să afişaţi sau să tipăriţi informaţii despre intrările din jurnalul de auditare de securitate. Puteţi să selectaţi anumite tipuri de intrare, anumiţi utilizatori şi o perioadă de timp.
DSPSECAUD	Afişare valori auditare de securitate	Vă permite să afişaţi informaţii despre jurnalul de auditare de securitate şi valorile de sistem care controlează auditarea de securitate.

Tabela 141. Unelte de securitate pentru Gestionare autorizări

Nume comandă	Nume descriptiv	Funcţie
PRTJOBDAUT	Tipărire autorizare descriere de job	Vă permite să tipăriţi o listă de descrieri de job a căror autorizare publică nu este *EXCLUDE. Puteţi folosi această comandă pentru a tipări informaţii despre descrieri de job care specifică un profil utilizator care poate fi accesat de toţi utilizatorii din sistem.
PRTPUBAUT	Tipărire obiecte autorizate public	Vă permite să tipăriţi o listă de obiecte de tip specificat a căror autorizare publică nu este *EXCLUDE.
PRTPVTAUT	Tipărire autorizări private	Vă permite să tipăriţi o listă de autorizări private pentru obiecte de tipul specificat.
PRTQAUT	Tipărire autorizare coadă	Vă permite să tipăriţi setările de securitate pentru cozi de ieşire şi cozi de job din sistemul dumneavoastră. Aceste setări controlează cine poate vizualiza şi modifica intrări din coada de ieşire sau coada de joburi.
PRTSBSDAUT	Tipărire autorizare descriere subsistem	Vă permite să tipăriţi o listă de descrieri de subsistem dintr-o bibliotecă care conţine un utilizator implicit într-o intrare de subsistem.
PRTTRGPGM	Tipărire programe de declanşare	Vă permite să tipăriţi o listă de programe de declanşare care sunt asociate cu fişiere de bază de date de pe sistemul dumneavoastră.
PRTUSROBJ	Tipărire obiecte utilizator	Vă permite să tipăriţi o listă cu obiectele utilizator (obiecte care nu sunt livrate de IBM) care sunt într-o bibliotecă.

Tabela 142. Unelte de securitate pentru Gestionare securitate sistem

Nume comandă	Nume descriptiv	Funcţie
CHGSECA [1]	Modificare atribute de securitate	Vă permite să setaţi noi valori de pornire pentru generarea de numere de ID utilizator sau numere de ID de grup. Utilizatorii pot specifica un ID utilizator de pornire şi un ID grup de pornire.
CFGSYSSEC	Configurare securitate sistem	Vă permite să setaţi valori sistem importante pentru securitate la setările lor recomandate. Comanda setează de asemenea auditarea de securitate pe sistemul dumneavoastră.
CLRSVRSEC	Curăţare date de securitate server	Vă permite să curăţaţi informaţii de autentificare decriptabile care sunt asociate cu profiluri utilizator şi intrări de listă de validare (*VLDL). **Notă:** Acestea sunt aceleaşi informaţii care au fost curăţate în ediţii anteriare V5R2 când valoarea sistem QRETSVRSEC se schimba de ’1’ la ’0’.
DSPSECA	Afişare atribute de securitate	Vă permite să afişaţi valorile curente şi în aşteptare ale unor atribute de securitate sistem.
PRTCMNSEC	Tipărire securitate comunicaţii	Vă permite să tipăriţi atributele de securitate ale obiectelor *DEVD, *CTL şi *LIND din sistem.
PRTSYSSECA	Tipărire atribute de securitate sistem	Vă permite să tipăriţi o listă de valori sistem şi atribute de reţea importante pentru securitate. Raportul arată valoarea curentă şi valoarea recomandată.
RVKPUBAUT	Revocare autorizare publică	Vă permite să setaţi autorizarea publică la *EXCLUDE pentru un set de comenzi sensibile la securitate de pe sistemul dumneavoastră.

1 Pentru a folosi această comandă, trebuie să aveţi autorizare specială *SECADM.

Pentru informaţii suplimentare despre unelte şi sugestii despre cum se folosesc uneltele de securitate, vedeţi cartea *Tips for Making Your iSeries 400 Secure*, GC41-0615.

Anexa B. Profilurile de utilizator furnizate de IBM

Această anexă conţine informaţii despre profilurile utilizator care sunt livrate cu sistemul. Aceste profiluri sunt folosite ca proprietari de obiecte pentru diferite funcţii sistem. Unele funcţii sistem de asemenea rulează sub anumite profiluri utilizator furnizate de IBM.

Tabela 143 arată valorile implicite care sunt folosite pentru toate profilurile utilizator furnizate de IBM şi la comanda CRTUSRPRF (Create User Profile - Creare profil utilizator). Parametrii sunt ordonaţi în funcţie de momentul apariţiei lor în ecranul Creare profil utilizator.

Tabela 144 menţionează fiecare profil livrat de IBM, scopul lui şi orice valoare pentru profil care este diferită de valorile implicite pentru profilurile utilizator livrate de IBM.

Notă:

> Tabela 144 include acum profiluri utilizator adiţionale care sunt livrate cu produsele de programe cu licenţă. Tabela include doar **unele**, dar nu toate profilurile utilizator pentru produsele de programe cu licenţă, de aceea, lista nu este completă.

Atenţie:

- Parola pentru profilul QSECOFR

  Trebuie să modificaţi parola pentru profilul QSECOFR după ce instalaţi sistemul dumneavoastră. Această parolă este aceeaşi pentru fiecare sistem iSeries şi aduce o expunere de securitate până în momentul schimbării ei. Totuşi, **nu** modificaţi nici o valoare pentru profilurile utilizator livrate de IBM. Modificarea acestor profiluri poate face ca funcţiile sistemului să eşueze.
- Autorizările pentru profilurile livrate de IBM

  Manifestaţi **precauţie** când îndepărtaţi autorizările deţinute de profilurile livrate de IBM asupra obiectelor care sunt livrate cu sistemul de operare. Unor profiluri livrate de IBM le sunt acordate autorizări private care sunt livrate cu sistemul de operare. Îndepărtarea oricărei dintre aceste autorizări poate provoca funcţiile sistem să eşueze.

Tabela 143. Valorile implicite pentru profilurile utilizator

	Valori implicite	
Parametru profil utilizator	**Profiluri utilizator livrate de IBM**	**Ecranul Creare profil utilizator**
Parolă (PASSWORD)	*NONE	*USRPRF[4]
Setare parolă ca să expire (PWDEXP)	*NO	*NO
Stare (STATUS)	*ENABLED	*ENABLED
Clasă utilizator (USRCLS)	*USER	*USER
Nivel de ajutorare (ASTLVL)	*SYSVAL	*SYSVAL
Bibliotecă actuală (CURLIB)	*CRTDFT	*CRTDFT
Program iniţial (INLPGM)	*NONE	*NONE
Meniu iniţial (INLMNU)	MAIN	MAIN
Bibliotecă meniu iniţial	*LIBL	*LIBL
Capabilităţi limitate (LMTCPB)	*NO	*NO
Text (TEXT)	*BLANK	*BLANK
Autorizare specială (SPCAUT)	*ALLOBJ[1] *SAVSYS[1]	*USRCLS[2]
Mediu special (SPCENV)	*SYSVAL	*SYSVAL
Afişare informaţii de semnare (DSPSGNINF)	*SYSVAL	*SYSVAL
Interval de expirare parolă (PWDEXPITV)	*SYSVAL	*SYSVAL
Limitare sesiuni dispozitiv (LMTDEVSSN)	*SYSVAL	*SYSVAL

Tabela 143. Valorile implicite pentru profilurile utilizator (continuare)

	Valori implicite	
Parametru profil utilizator	**Profiluri utilizator livrate de IBM**	**Ecranul Creare profil utilizator**
Punere în buffer tastatură (KBDBUF)	*SYSVAL	*SYSVAL
Spaţiu de stocare maxim (MAXSTG)	*NOMAX	*NOMAX
Limitare prioritate (PTYLMT)	0	3
Descriere de job (JOBD)	QDFTJOBD	QDFTJOBD
Bibliotecă descriere de job	QGPL	*LIBL
Profil grup (GRPPRF)	*NONE	*NONE
Proprietar (OWNER)	*USRPRF	*USRPRF
Autorizare grup (GRPAUT)	*NONE	*NONE
Tip de autorizare grup (GRPAUTTYP)	*PRIVATE	*PRIVATE
Grupuri suplimentare (SUPGRPPRF)	*NONE	*NONE
Cod de contabilizare (ACGCDE)	*SYS	*BLANK
Parolă document (DOCPWD)	*NONE	*NONE
Coadă de mesaje (MSGQ)	*USRPRF	*USRPRF
Livrare (DLVRY)	*NOTIFY	*NOTIFY
Gravitate (SEV)	00	00
Dispozitiv imprimantă (PRTDEV)	*WRKSTN	*WRKSTN
Coadă de ieşire (OUTQ)	*WRKSTN	*WRKSTN
Programul Attention (ATNPGM)	*NONE	*SYSVAL
Secvenţă sortare (SRTSEQ)	*SYSVAL	*SYSVAL
Identificator limbă (LANGID)	*SYSVAL	*SYSVAL
Identificator regiune sau ţară (CNTRYID)	*SYSVAL	*SYSVAL
Identificator set de caractere codat (CCSID)	*SYSVAL	*SYSVAL
Setare atribute job (SETJOBATR)	*SYSVAL	*SYSVAL
Locale (LOCALE)	*NONE	*SYSVAL
Opţiune utilizator (USROPT)	*NONE	*NONE
Număr identificare utilizator (UID)	*GEN	*GEN
Număr de identificare grup (GID)	*NONE	*NONE
Director iniţial (HOMEDIR)	*USRPRF	*USRPRF
Autorizare (AUT)	*EXCLUDE	*EXCLUDE
Auditare acţiune (AUDLVL) [3]	*NONE	*NONE
Auditare obiect (OBJAUD) [3]	*NONE	*NONE

1 Când nivelul de securitate sistem este modificat de la nivelul 10 sau 20 la nivelul 30 sau mai sus, această valoare este înlăturată.

2 Când un profil utilizator este automat creat cu nivelul de securitate 10, clasa utilizator *USER dă autorizare specială *ALLOBJ şi *SAVSYS.

3 Auditarea de obiecte şi acţiuni este specificată folosind comanda CHGUSRAUD.

4 Când executaţi o comandă CRTUSRPRF, nu puteţi crea un profil de utilizator (*USRPRF) într-un pool de discuri independent. Totuşi, când un utilizator este autorizat în particular asupra unui obiect din pool-ul de disc independent, este proprietarul unui obiect dintr-un pool de disc independent sau este grupul primar al unui obiect dintr-un pool de disc independent atunci numele profilului este memorat în pool-ul de disc independent. Dacă pool-ul de disc independent este mutat în alt sistem, autorizarea particulară, dreptul de proprietate asupra obiectului şi intrările de grup primar vor fi ataşate la profilul cu acelaşi nume din sistemul destinaţie. Daca un profil nu exista pe sistemul destinatie, va fi creat un profil. Utilizatorul nu va avea nici o autorizare speciala si parola va fi setata la *NONE.

Tabela 144. Profiluri utilizator livrate de IBM

Nume profil	Nume descriptiv	Parametrii diferiţi din valorile implicite
QADSM	Profil utilizator ADSM	• USERCLS: *SYSOPR • CURLIB: QADSM • TEXT: Profil ADSM folosit de serverul ADSM • SPCAUT: *JOBCTL, *SAVSYS • JOBD: QADSM/QADSM • OUTQ: QADSM/QADSM
QAFOWN	Profil utilizator APD	• USRCLS: *PGMR • SPCAUT: *JOBCTL • JOBD: QADSM/QADSM • TEXT: Profil utilizator intern APD
QAFUSR	Profil utilizator APD	• TEXT: Profil utilizator intern APD
QAFDFTUSR	Profil utilizator APD	• INLPGM: *LIBL/QAFINLPG • LMTCPB: *YES • TEXT: Profil utilizator intern APD
QAUTPROF	Profil utilizator autorizare IBM	
QBRMS	Profil utilizator BRM	
QCLUMGT	Profil gestiune cluster	• STARE: *DISABLED • MSGQ: *NONE • ATNPGM: *NONE
QCLUSTER	Profil cluster disponibilitate înaltă	• SPCAUT: *IOSYSCFG
QCOLSRV	Profil utilizator servicii de colectare Administrare centrală	
QDBSHR	Profil partajare bază de date	• AUT: *ADD, *DELETE
QDBSHRDO	Profil partajare bază de date	• AUT: *ADD, *DELETE
QDCEADM	Profil utilizator DCE	• PASSWORD: *USRPRF • PWDEXP: *YES • STARE: *DISABLED • TEXT: *NONE • SPCAUT: *JOBCTL
QDFTOWN	Profil proprietar implicit	• PTYLMT: 3
QDIRSRV	Profil de utilizator server OS/400 Directory Server	• LMTCPB: *YES • JOBD: QGPL/QBATCH • DSPSGNINF: *NO • LMTDEVSSN: *NO • DLVRY: *HOLD • SPCENV: *NONE • ATNPGM: *NONE

Tabela 144. Profiluri utilizator livrate de IBM (continuare)

Nume profil	Nume descriptiv	Parametrii diferiţi din valorile implicite
QDLFM	Profil manager fişiere legături de date	• SRTSEQ: *HEX
QDOC	Profil document	• AUT: *CHANGE
QDSNX	Profil executiv nod sisteme distribuite	• PTYLMT: 3 • CCSID: *HEX • SRTSEQ: *HEX
QEJBSVR	Profil utilizator WebSphere Application Server	
QEJB	Profil utilizator Enterprise Java	
QFNC	Profil Finanţe	• PTYLMT: 3
QGATE	Profil punte VM/MVS*	• CCSID: *HEX • SRTSEQ: *HEX
QIPP	Profil tipărire internet	• MSGQ: QUSRSYS/QIPP
QLPAUTO	Profil instalare automată program cu licenţă	• USRCLS: *SYSOPR • INLMNU: *SIGNOFF • SPCAUT: *ALLOBJ, *JOBCTL ,*SAVSYS, *SECADM, *IOSYSCFG • INLPGM: QSYS/QLPINATO • DLVRY: *HOLD • SEV: 99
QLPINSTALL	Profil instalare program cu licenţă	• USRCLS: *SYSOPR • DLVRY: *HOLD • SPCAUT: *ALLOBJ, *JOBCTL, *SAVSYS, *SECADM, *IOSYSCFG
QMGTC	Profil Administrare centrală	• JOBD: QSYS/QYPSJOBD
QMSF	Profil cadru de lucru server de mail	• CCSID: *HEX • SRTSEQ: *HEX
QMQM	Profil utilizator MQSeries	• USRCLS: *SECADM • SPCAUT: *NONE • PRTDEV: *SYSVAL • TEXT: Utilizator MQM care deţine biblioteca QMQM
QNFSANON	Profil utilizator NFS	
QNETSPLF	Profil de spool reţea	
QNETWARE	Profil utilizator ECS	• STARE: *DISABLED • TEXT: QFPNTWE USER PROFILE
QNTP	Profil timp reţea	• JOBD: QTOTNTP • JOBD LIBRARY: QSYS

Tabela 144. Profiluri utilizator livrate de IBM (continuare)

Nume profil	Nume descriptiv	Parametrii diferiţi din valorile implicite
QOIUSER	Subsistem comunicaţii OSI	• USRCLS: *SYSOPR • SPCAUT: *JOBCTL, *SAVSYS, *IOSYSCFG • CURLIB: QOSI • MSGQ: QOSI/QOIUSER • DLVRY: *HOLD • OUTQ: *DEV • PRTDEV: *SYSVAL • ATNPGM: *NONE • CCSID: *HEX • TEXT: Profil utilizator subsistem de comunicaţii intern OSI
QOSIFS	Profil utilizator server fişiere OSI	• USRCLS: *SYSOPR • SPCAUT: *JOBCTL, *SAVSYS • OUTQ: *DEV • CURLIB: *QOSIFS • CCSID: *HEX • TEXT: Profil utilizator servicii fişiere intern OSI
QPGMR	Profil programator	• USRCLS: *PGMR • SPCAUT: *ALLOBJ [1] *SAVSYS *JOBCTL • PTYLMT: 3 • ACGCDE: *BLANK
QPEX	Profil utilizator Performance Explorer	• PTYLMT: 3 • ATNPGM: *SYSVAL • TEXT: Profil utilizator livrat de IBM
QPM400	IBM Performance Management pentru eServer iSeries (PM iSeries)	• SPCAUT: *IOSYSCFG, *JOBCTL
QPRJOWN	Profil utilizator proprietar de proiecte şi părţi	• STARE: *DISABLED • CURLIB: QADM • TEXT: Profilul utilizator al proprietarului de proiecte şi părţi
QRDARSADM	Profil utilizator R/DARS	• INLMNU: *SIGNOFF • TEXT: Profil administraţie R/DARS
QRDAR	Profil de proprietar R/DARS	• USRCLS: *PGMR • INLMNU: *SIGNOFF • OUTQ: *DEV • TEXT: Profil proprietar R/DARS-400
QRDARS4001	Profil proprietar 1 R/DARS	• INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Profil proprietar 1 R/DARS-400

Tabela 144. Profiluri utilizator livrate de IBM (continuare)

Nume profil	Nume descriptiv	Parametrii diferiţi din valorile implicite
QRDARS4002	Profil proprietar 2 R/DARS	• INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Profil proprietar 2 R/DARS-400
QRDARS4003	Profil proprietar 3 R/DARS	• INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Profil proprietar 3 R/DARS-400
QRDARS4004	Profil proprietar 4 R/DARS	• INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Profil proprietar 4 R/DARS-400
QRDARS4005	Profil proprietar 5 R/DARS	• INLMNU: *SIGNOFF • GRPPRF: QRDARS400 • OUTQ: *DEV • TEXT: Profil proprietar 5 R/DARS-400
QRMTCAL	Profil utilizator Calendar la distanţă	• TEXT: Utilizator Calendar la distanţă OfficeVision
QRJE	Profil intrare job la distanţă	• USRCLS: *PGMR • SPCAUT: *ALLOBJ [1] *SAVSYS [1] *JOBCTL
QSECOFR	Profil responsabil cu securitatea	• PWDEXP: *YES • USRCLS: *SECOFR • SPCAUT: *ALLOBJ, *SAVSYS, *JOBCTL, *SECADM, *SPLCTL, *SERVICE, *AUDIT, *IOSYSCFG • UID: 0 • PAROLĂ: QSECOFR
QSNADS	Profil servicii distribuţie SNA	• CCSID: *HEX • SRTSEQ: *HEX
QSOC	Profil utilizator OptiConnect	• USRCLS: *SYSOPR • CURLIB: *QSOC • SPCAUT: *JOBCTL • MSGQ: QUSRSYS/QSOC
QSPL	Profil spool	
QSPLJOB	Profil job spool	• AUT: *USE
QSRV	Profil service	• USRCLS: *PGMR • SPCAUT: *ALLOBJ [1], *SAVSYS [1], *JOBCTL, *SERVICE • ASTLVL: *INTERMED • ATNPGM: QSYS/QSCATTN
QSRVAGT	Profil utilizator agent service	

Tabela 144. Profiluri utilizator livrate de IBM (continuare)

Nume profil	Nume descriptiv	Parametrii diferiţi din valorile implicite
QSRVBAS	Profil service de bază	• USRCLS: *PGMR • SPCAUT: *ALLOBJ [1] *SAVSYS [1] *JOBCTL • ASTLVL: *INTERMED • ATNPGM: QSYS/QSCATTN
QSVCCS	Profil utilizator CC Server	• USRCLS: *SYSOPR • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: Profil utilizator CC Server
QSVCM	Profil utilizator Client Management Server	• TEXT: Profil utilizator Client Management Server
QSVSM	Profil utilizator ECS	• USRCLS: *SYSOPR • STATUS: *DISABLED • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: Profil utilizator Manager sistem SystemView
QSVSMSS	Profil utilizator Managed System Service	• STARE: *DISABLED • USRCLS: *SYSOPR • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: Profil utilizator Managed System Service
QSYS	Profil sistem	• USRCLS: *SECOFR • SPCAUT: *ALLOBJ, *SECADM, *SAVSYS, *JOBCTL, *AUDIT, *SPLCTL, *SERVICE, *IOSYSCFG
QSYSOPR	Profil operator sistem	• USRCLS: *SYSOPR • SPCAUT: *ALLOBJ [1], *SAVSYS, *JOBCTL • INLMNU: SYSTEM • LIBRARY: *LIBL • MSGQ: QSYSOPR • DLVRY: *BREAK • SEV: 40
QTCM	Profil TCM (Triggered Cache Manager)	• STARE: *DISABLED
QTCP	Profil TCP (Transmission control protocol)	• USRCLS: *SYSOPR • SPCAUT: *JOBCTL • CCSID: *HEX • SRTSEQ: *HEX
QTFTP	Profil TFTP (Trivial File Transfer Protocol)	
QTMPLPD	Profil suport tipărire TCP/IP	• PTYLMT: 3 • AUT: *USE
QTMPLPD	Profil utilizator LPR la distanţă	• JOBD: QGPL/QDFTJOBD • PWDEXPITV: *NOMAX • MSGQ: QTCP/QTMPLPD

Tabela 144. Profiluri utilizator livrate de IBM (continuare)

Nume profil	Nume descriptiv	Parametrii diferiţi din valorile implicite
QTMTWSG	Profil utilizator HTML Workstation Gateway	• MSGQ: QUSRSYS/QTMTWSG • TEXT: Profil HTML Workstation Gateway
QTMHHTTP	Profil utilizator HTML Workstation Gateway	• MSGQ: QUSRSYS/QTMHHTTP • TEXT: Profil server HTTP
QTMHHTP1	Profil utilizator HTML Workstation Gateway	• MSGQ: QUSRSYS/QTMHHTTP • TEXT: Profil CGI server HTTP
QTSTRQS	Profil cerere test	
QUMB	Profil utilizator Ultimedia System Facilities	
QUMVUSER	Profil utilizator Ultimedia Business Conferencing	
QUSER	Profil utilizator staţie de lucru	• PTYLMT: 3
QX400	Profil utilizator servicii fişier servicii mesaje OSI	• CURLIB: *QX400 • USRCLS: *SYSOPR • MSGQ: QX400/QX400 • DLVRY: *HOLD • OUTQ: *DEV • PRTDEV: *SYSVAL • ATNPGM: *NONE • CCSID: *HEX • TEXT: Profil utilizator servicii mesaje interne OSI
QYCMCIMOM	Profil utilizator server	
QYPSJSVR	Profil server Administrare centrală Java	
QYPUOWN	Profil utilizator intern APU	• TEXT: Profil utilizator — Internal APU

[1] Când nivelul de securitate sistem este modificat de la nivelul 10 sau 20 la nivelul 30 sau mai sus, această valoare este înlăturată.

Anexa C. Comenzile livrate cu autorizarea publică *EXCLUDE

Tabela 145 identifică acele comenzi care au autorizare restricţionată (autorizarea publică este *EXCLUDE) când sistemul dumneavoastră este livrat. Arată ce profiluri utilizator livrate de IBM sunt autorizate să folosească aceste comenzi restricţionate. Pentru mai multe detalii despre profilurile utilizator, vedeţi subiectul “Profiluri utilizator livrate de IBM” la pagina 105.

În Tabela 145, comenzile care sunt restricţionate pentru responsabilul cu securitatea şi pentru orice profil utilizator cu autorizare *ALLOBJ au un **R** în profilul QSECOFR. Comenzile care sunt autorizate special unuia sau mai multor profiluri utilizator livrate de IBM, în plus faţă de responsabilul cu securitatea, au un **S** sub numele de profil pentru care sunt autorizate).

Orice comenzi care nu sunt menţionate aici sunt publice, ceea ce înseamnă că ele pot fi folosite de către toţi utilizatorii. Oricum, unele comenzi necesită autorizare specială, precum *SERVICE sau *JOBCTL. Autorizările speciale necesare pentru o comandă sunt menţionate în Anexa D, “Autorizarea cerută pentru obiectele folosite de comenzi”, la pagina 289

Dacă alegeţi să acordaţi altor utilizatori sau autorizare publică *USE acestor comenzi, actualizaţi această tabelă pentru a indica ieşirea din starea restricţionată pe sistemul dumneavoastră. Folosirea unor comenzi poate necesita autorizarea la anumite obiecte din sistem precum şi la comenzile respective. Vedeţi Anexa D, “Autorizarea cerută pentru obiectele folosite de comenzi”, la pagina 289 pentru autorizările de obiect necesare pentru comenzi.

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricţionate

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
ADDCLUNODE	R					S
ADDCMDCRQA		S	S	S	S	
ADDCRGDEVE	R					S
ADDCRGNODE	R					S
ADDCRSDMNK	R					
ADDDEVDMNE	R					S
ADDDSTQ		S	S			
ADDDSTRTE		S	S			
ADDDSTSYSN		S	S			
ADDEXITPGM	R					
ADDIMGCLGE	R					
ADDMFS	R					
ADDNETJOBE	R					
ADDOBJCRQA		S	S	S	S	
ADDOPTCTG	R					
ADDOPTSVR	R					
ADDPEXDFN		S		S		
ADDPEXFTR		S		S		
ADDPRDCRQA		S	S	S	S	
ADDPTFCRQA		S	S	S	S	
ADDRPYLE		S				

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
ADDRSCCRQA		S	S	S	S	
ADDTRCFTR	R					
ANSQST	R					
ANZACCGRP	R					
ANZBESTMDL	R					
ANZDBF	R					
ANZDBFKEY	R					
ANZDFTPWD	R					
ANZJVM		S	S	S	S	
ANZPFRDTA	R					
ANZPGM	R					
ANZPRB		S	S	S	S	
ANZPRFACT	R					
ANZS34OCL	R					
ANZS36OCL	R					
APYJRNCHG		S		S		
APYPTF				S		
APYRMTPTF		S	S	S	S	
CFGDSTSRV		S	S			
CFGRPDS		S	S			
CFGSYSSEC	R					
CHGACTSCDE	R					
CHGCLUCFG	R					S
CHGCLUNODE	R					
CHGCLURCY	R					S
CHGCLUVER	R					S
CHGCMDCRQA		S	S	S	S	
CHGCRG	R					S
CHGCRGDEVE	R					S
CHGCRGPRI	R					S
CHGCRSDMNK	R					
CHGDSTPWD[1]	R					
CHGDSTQ		S	S			
CHGDSTRTE		S	S			
CHGEXPSCDE	R					
CHGFCNARA	R					
CHGGPHFMT	R					
CHGGPHPKG	R					
CHGIMGCLG	R					
CHGIMGCLGE	R					

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
CHGJOBTRC	R					
CHGJOBTYP	R					
CHGJRN		S	S	S		
CHGLICINF	R					
CHGMGDSYSA		S	S	S	S	
CHGMGRSRVA		S	S	S	S	
CHGMSTK	R					
CHGNETA	R					
CHGNETJOBE	R					
CHGNFSEXP	R					
CHGNWSA	R					
CHGOBJCRQA		S	S	S	S	
CHGOPTA	R					
CHGPEXDFN		S		S		
CHGPRB		S	S	S	S	
CHGPRDCRQA		S	S	S	S	
CHGPTFCRQA		S	S	S	S	
CHGPTR				S		
CHGQSTDB	R					
CHGRCYAP		S	S			
CHGRPYLE		S				
CHGRSCCRQA		S	S	S	S	
CHGSYSLIBL	R					
CHGSYSVAL		S	S	S		
CHGS34LIBM	R					
CHKASPBAL	R					
CHKCMNTRC				S		
CHKPRDOPT		S	S	S	S	
CPHDTA	R					
CPYFCNARA	R					
CPYGPHFMT	R					
CPYGPHPKG	R					
CPYPFRDTA	R					
CPYPTF		S	S	S	S	
CPYPTFGRP		S	S	S	S	
CRTAUTHLR	R					
CRTBESTMDL	R					
CRTCLS	R					
CRTCLU	R					S
CRTCRG	R					S

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
CRTFCNARA	R					
CRTGPHFMT	R					
CRTGPHPKG	R					
CRTHSTDTA	R					
CRTIMGCLG	R					
CRTJOBD	R					
CRTPFRDTA	R					
CRTLASREP		S				
CRTPEXDT		S		S		
CRTQSTDB	R					
CRTQSTLOD	R					
CRTSBSD		S	S			
CRTUDFS	R					
CRTUDFS	R					
CRTVLDL	R					
CVTBASSTR	R					
CVTBASUNF	R					
CVTBGUDTA	R					
CVTDIR	R					
CVTPFRDTA	R					
CVTPFRTHD	R					
CVTS36CFG	R					
CVTS36FCT	R					
CVTS36JOB	R					
CVTS36QRY	R					
CVTS38JOB	R					
CVTTCPCL		S	S	S	S	
DLTAPARDTA		S	S	S	S	
DLTBESTMDL	R					
DLTCLU	R					S
DLTCMNTRC				S		
DLTCRGCLU	R					S
DLTFCNARA	R					
DLTGPHFMT	R					
DLTGPHPKG	R					
DLTHSTDTA	R					
DLTIMGCLG	R					
DLTLICPGM	R					
DLTPEXDTA		S		S		
DLTPFRDTA	R					

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
DLTPRB		S	S	S	S	
DLTPTF		S	S	S	S	
DLTQST	R					
DLTQSTDB	R					
DLTRMTPTF		S	S	S	S	
DLTSMGOBJ		S	S	S	S	
DLTUDFS	R					
DLTVLDL	R					
DMPDLO		S	S	S	S	
DMPJOB		S	S	S	S	
DMPJOBINT		S	S	S	S	
DMPJVM		S	S	S	S	
DMPOBJ				S	S	
DMPSYSOBJ		S	S	S	S	
DMPTRC	R	S		S		
DSPACCGRP	R					
DSPDSTLOG	R					
DSPHSTGPH	R					
DSPMFSINF	R					
DSPMGDSYSA		S	S	S	S	
DSPPFRDTA	R					
DSPPFRGPH	R					
DSPPTF		S	S	S	S	
DSPSRVSTS		S	S	S	S	
DSPUDFS	R					
EDTCPCST			S			
EDTQST	R					
EDTRBDAP			S			
EDTRCYAP		S	S			
ENCCPHK	R					
ENCFRMMSTK	R					
ENCTOMSTK	R					
ENDCHTSVR	R					S
ENDCLUNOD	R					S
ENDCMNTRC	R			S		
ENDCRG	R					
ENDDBGSVR		S	S	S	S	
ENDHOSTSVR		S	S	S	S	
ENDIDXMON	R					
ENDIPSIFC		S	S	S	S	

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
ENDJOBABN		S	S	S		
ENDJOBTRC	R					
ENDMGDSYS		S	S	S	S	
ENDMGRSRV		S	S	S	S	
ENDMSF			S	S	S	
ENDNFSSVR	R		S	S	S	
ENDPEX		S		S		
ENDPFRTRC	R			S		
ENDSRVJOB		S	S	S	S	
ENDSYSMGR		S	S	S	S	
ENDTCP		S	S	S	S	
ENDTCPCNN		S	S	S	S	
ENDTCPIFC		S	S	S	S	
ENDTCPSVR		S	S	S	S	
GENCPHK	R					
GENCRSDMNK	R					
GENMAC	R					
GENPIN	R					
GENS36RPT	R					
GENS38RPT	R					
GRTACCAUT	R					
HLDCMNDEV		S	S	S	S	
HLDDSTQ		S	S			
INSPTF[3]				S		
INSRMTPRD		S	S	S	S	
INZDSTQ		S	S			
INZSYS	R					
LODIMGCLG	R					
LODPTF				S		
LODQSTDB	R					
MGRS36	R					
MGRS36APF	R					
MGRS36CBL	R					
MGRS36DFU	R					
MGRS36DSPF	R					
MGRS36ITM	R					
MGRS36LIB	R					
MGRS36MNU	R					
MGRS36MSGF	R					
MGRS36QRY	R					

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
MGRS36RPG	R					
MGRS36SEC	R					
MGRS38OBJ	R					
MIGRATE	R					
PKGPRDDST		S	S	S	S	
PRTACTRPT	R					
PRTCMNTRC				S		
PRTCPTRPT	R					
PRTJOBRPT	R					
PRTJOBTRC	R					
PRTLCKRPT	R					
PRTPOLRPT	R					
PRTRSCRPT	R					
PRTSYSRPT	R					
PRTTNSRPT	R					
PRTTRCRPT	R					
PRTDSKINF	R					
PRTERRLOG		S	S	S	S	
PRTINTDTA		S	S	S	S	
PRTPRFINT	R					
PWRDWNSYS	R		S			
RCLOPT	R					
RCLSPLSTG	R					
RCLSTG		S	S	S	S	
RCLTMPSTG		S	S	S	S	
RESMGRNAM	R	S	S	S	S	
RLSCMNDEV		S	S	S	S	
RLSDSTQ		S	S			
RLSIFSLCK	R					
RLSRMTPHS		S	S			
RMVACC	R					
RMVCLUNODE	R					S
RMVCRGDEVE	R					S
RMVCRGNODE	R					S
RMVCRSDMNK	R					
RMVDEVDMNE	R					S
RMVDSTQ		S	S			
RMVDSTRTE		S	S			
RMVDSTSYSN		S	S			
RMVEXITPGM	R					

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
RMVIMGCLGE	R					
RMVJRNCHG		S		S		
RMVLANADP	R					
RMVMFS	R					
RMVNETJOBE	R					
RMVOPTCTG	R					
RMVOPTSVR	R					
RMVPEXDFN		S		S		
RMVPEXFTR		S		S		
RMVPTF				S		
RMVRMTPTF		S	S	S	S	
RMVRPYLE		S				
RMVTRCFTR	R					
RSTAUT	R					
RST[4]						S
RSTCFG	R					
RSTDLO	R					
RSTLIB	R					
RSTLICPGM	R					
RSTOBJ[4]						S
RSTS36F	R					
RSTS36FLR	R					
RSTS36LIBM	R					
RSTS38AUT	R					
RSTUSFCNR[5]						S
RSTUSRPRF	R					
RTVDSKINF	R					
RTVPRD		S	S	S	S	
RTVPTF		S	S	S	S	
RTVSMGOBJ		S	S	S	S	
RUNLPDA		S	S	S	S	
RUNSMGCMD		S	S	S	S	
RUNSMGOBJ		S	S	S	S	
RVKPUBAUT	R					
SAVAPARDTA		S	S	S	S	
SAVLICPGM	R					
SAVRSTCHG	R					
SAVRSTLIB	R					
SAVRSTOBJ	R					
SBMFNCJOB	R					

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
SBMNWSCMD	R					
SETMSTK	R					
SNDDSTQ		S	S			
SNDPRD		S	S	S	S	
SNDPTF		S	S	S	S	
SNDPTFORD				S	S	
SNDSMGOBJ		S	S	S	S	
SNDSRVRQS				S	S	
STRBEST	R					
STRCHTSVR	R					S
STRCLUNOD	R					S
STRCMNTRC				S		
STRCRG	R					S
STRDBG		S		S	S	
STRDBGSVR		S	S	S	S	
STRHOSTSVR		S	S	S	S	
STRIDXMON	R					
STRIPSIFC		S	S	S	S	
STRJOBTRC	R					
STRMGDSYS		S	S	S	S	
STRMGRSRV		S	S	S	S	
STRMSF[2]			S	S	S	
STRNFSSVR	R					
STRPEX		S		S		
STRPFRG	R					
STRPFRT	R					
STRPFRTRC	R			S		
STRRGZIDX	R					
STRSRVJOB		S	S	S	S	
STRSST				S		
STRSYSMGR		S	S	S	S	
STRS36MGR	R					
STRS38MGR	R					
STRTCP		S	S	S	S	
STRTCPIFC		S	S	S	S	
STRTCPSVR		S	S	S	S	
STRUPDIDX	R					
TRCCPIC	R					
TRCICF	R					
TRCINT		S		S		

Tabela 145. Autorizările profilurilor utilizator furnizate de IBM pentru comenzile restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS	QSYS[6]
TRCJOB		S	S	S	S	
TRCTCPAPP				S	S	
TRNPIN	R					
VFYCMN		S	S	S	S	
VFYIMGCLG	R					
VFYLNKLPDA		S	S	S	S	
VFYMSTK	R					
VFYPIN	R					
VFYPRT		S	S	S	S	
VFYTAP		S	S	S	S	
WRKCNTINF				S	S	
WRKDEVTBL	R					
WRKDPCQ		S	S			
WRKDSTQ		S	S			
WRKFCNARA	R					
WRKIMGCLGE	R					
WRKJRN		S	S	S		
WRKLICINF	R					
WRKORDINF			S	S		
WRKPEXDFN		S		S		
WRKPEXFTR		S		S		
WRKPGMTBL	R					
WRKPRB		S	S	S	S	
WRKPTFGRP		S	S	S	S	
WRKSRVPVD				S	S	
WRKSYSACT	R					
WRKTXTIDX	R					
WRKUSRTBL	R					

[1] Comanda CHGDSTPWD este livrată cu autorizare publică *USE, dar trebuie să fiţi semnat ca QSECOFR pentru a folosi această comandă.

[2] Profilul utilizator QMSF este de asemenea autorizat la acesată comandă.

[3] QSRV poate să ruleze această comandă doar dacă nu se face un IPL.

[4] În plus la QSYS, profilul utilizator QRDARS400 are autorizare.

[5] În plus la QSYS, profilul utilizator QUMB are autorizare.

[6] Aceste comenzi sunt livrate cu profilul de utilizator QSYS având autorizarea *ALL.

Anexa D. Autorizarea cerută pentru obiectele folosite de comenzi

Tabelele din această anexă arată ce autorizare este necesară pentru obiectele referite de către comenzi. De exemplu, în intrarea pentru comanda CHGUSRPRF (Change User Profile - Modificare profil utilizator), tabela prezintă toate obiectele pentru care aveţi nevoie de autorizare, cum ar fi coada de mesaje a utilizatorului, descrierea de job şi programul iniţial.

Tabelele sunt organizate în ordine alfabetică după tipul obiectului. În plus, sunt incluse tabele pentru elemente care nu sunt obiecte OS/400 (joburi, fişiere spool, atribute de reţea şi valori de sistem) şi pentru unele funcţii (de emulare dispozitiv şi financiare). Consideraţiile suplimentare (dacă există) pentru comenzi sunt incluse ca note de subsol în tabel.

În continuare sunt descrise coloanele din tabele:

Obiect referit

Obiectele prezentate în coloana *Obiect referit* sunt obiectele pentru care utilizatorul are nevoie de autorizare pentru folosirea comenzii.

Autorizarea cerută pentru obiect

Autorizările specificate în tabele arată autorizările pentru obiect şi autorizările pentru date care sunt necesare pentru obiect când folosiţi comanda. Tabela următoare prezintă autorizările specificate în coloana *Autorizare necesară*. Descrierea include exemple ale modului în care este folosită autorizarea. În majoritatea cazurilor, accesarea unui obiect necesită o combinaţie de autorizări pentru obiect şi pentru date.

Autorizarea cerută pentru bibliotecă

Această coloană arată ce autorizare este necesară pentru biblioteca în care se află obiectul. Pentru majoritatea operaţiilor, este necesară autorizarea *EXECUTE pentru a localiza obiectul în bibliotecă. Pentru adăugarea unui obiect în bibliotecă sunt necesare autorizările *READ şi *ADD. Această tabelă prezintă autorizările specificate în coloana *Autorizare necesară*.

Tabela 146. Descriere a tipurilor de autorizare

Autorizare	Nume	Funcţii permise
Autorizări obiect:		
*OBJOPR	Obiect Operaţional	Cercetaţi descrierea unui obiect. Folosiţi obiectul aşa cum este determinat de către autorizările de date ale utilizatorului.
*OBJMGT	Gestionare obiect	Specificarea securităţii pentru un obiect. Mutarea sau redenumirea obiectului. Toate funcţiile definite pentru *OBJALTER şi *OBJREF.
*OBJEXIST	Object Existence - Existenţă obiect	Ştergerea obiectului. Stocarea liberă a obiectului. Realizarea operaţiilor de salvare şi restaurare pentru obiect [1]. Transferarea dreptului de propietate la obiect.
*OBJALTER	Transformare obiect	Adăugarea, curăţarea, iniţializarea şi reorganizarea membrilor fişierului bază de date. Transformarea şi adăugarea atributelor fişierelor bază de date: adăugarea şi înlăturarea de declanşatori. Modificarea atributelor pachetelor SQL. Mutarea bibliotecii sau folderului la un alt ASP.

Tabela 146. Descriere a tipurilor de autorizare (continuare)

Autorizare	Nume	Funcţii permise
*OBJREF	Referenţiere obiect	Specificarea unui fişier bază de date ca părinte în constrângerea referenţială. De exemplu, doriţi să definiţi o regulă că o înregistrare client trebuie să existe în fişierul CUSMAS, înainte ca o comandă pentru client să poată să fie adăugată în fişierul CUSORD. Aveţi nevoie de autorizare *OBJREF pentru fişierul CUSMAS ca să definiţi această regulă.
*AUTLMGT	Gestionare listă de autorizare	Adăugarea şi înlăturarea utilizatorilor şi autorizărilor acestora din lista de autorizare [2].
Autorizări date:		
*READ	Read - Citire	Afişarea conţinutului obiectului, precum vizualizarea înregistrărilor într-un fişier.
*ADD	Adăugare.	Adăugarea de intrări la un obiect, precum adăugarea mesajelor la o coadă de mesaje sau adăugarea înregistrărilor la un fişier.
*UPD	Update - Actualizare	Modificarea intrărilor într-un obiect, precum modificarea înregistrărilor într-un fişier.
*DLT	Ştergere.	Înlăturarea intrările dintr-un obiect, percum înlăturarea mesajelor dintr-o coadă de mesaje sau ştergerea înregistrărilor dintr-un fişier.
*EXECUTE	Executare	Rularea unui program, program service sau a unui pachet SQL. Localizarea unui obiect într-o bibliotecă sau director.

1 Dacă un utilizator are autorizarea specială de salvare sistem (*SAVSYS), autorizarea existenţă obiect nu este cerută pentru a realiza operaţiile de salvare şi restaurare pe obiect.

2 Pentru informaţii suplimentare, consultaţi Referinţe de securitate iSeries.

În plus faţă de aceste valori, coloanele *Autorizare necesară* ale tabelului pot arăta subseturi definite de sistem ale acestor autorizări. Tabela următoare prezintă subseturile autorizărilor pentru obiect şi autorizărilor pentru date.

Tabela 147. Autorizare definită de sistem

Autorizare	*ALL	*CHANGE	*USE	*EXCLUDE
Autorizări obiect				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
Autorizări pentru date				
*READ	X	X	X	
*ADD	X	X		
*UPD	X	X		
*DLT	X	X		
*EXECUTE	X	X	X	

Tabela următoare prezintă subseturile suplimentare de autorizare care sunt suportate de comenzile CHGAUT şi WRKAUT.

Tabela 148. Autorizare definită de sistem

Autorizare	*RWX	*RW	*RX	*R	*WX	*W	*X
Autorizări obiect							
*OBJOPR	X	X	X	X	X	X	X

Tabela 148. Autorizare definită de sistem (continuare)

Autorizare	*RWX	*RW	*RX	*R	*WX	*W	*X
*OBJMGT							
*OBJEXIST							
*OBJALTER							
*OBJREF							
Autorizări pentru date							
*READ	X	X	X	X			
*ADD	X	X			X	X	
*UPD	X	X			X	X	
*DLT	X	X			X	X	
*EXECUTE	X		X		X		X

Pentru informaţii suplimentare despre aceste autorizări şi descrierile lor, consultaţi Referinţe de securitate iSeries.

Presupuneri privind utilizarea comenzii

1. Pentru a folosi o comandă, este necesară autorizarea *USE pentru comanda respectivă. Această autorizare nu este menţionată în tabele.
2. Pentru a introduce o comandă de afişare, aveţi nevoie de autorizare de operare pentru fişierul de afişare furnizat de IBM, fişierul de ieşire pentru imprimantă sau grupul de panouri folosit de comandă. Aceste fişiere şi grupuri de panouri sunt livrate cu autorizarea publică *USE.

Reguli generale privind autorizările pentru obiecte cerute de comenzi

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
Modificare (CHG) cu F4 (Prompt)[7]	Valori curente	Valorile curente sunt afişate dacă utilizatorul are autorizare pentru aceste valori.	*EXECUTE
Comanda care accesează obiectul din director	Directoarele din prefixul cale pentru sistemul de fişiere QLANSrv	*R	
	Directoarele din prefixul cale pentru toate celelalte sisteme de fişiere	*X	
	Directorul când este specificat modelul (* sau ?) pentru sistemul de fişiere QLANSrv	nici una	
	Directorul când este specificat modelul (* sau ?) pentru toate celelalte sisteme de fişiere	*R	
Creare obiect în director	Directoarele din prefix cale	*X	
	Directorul care va conţine obiecte noi	*WX	

Reguli generale privind autorizările pentru obiecte cerute de comenzi

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
Copiere (CPY) unde fişierul în care se va copia este un fişier bază de date	Obiectul de copiat	*OBJOPR, *READ	*EXECUTE
	Comanda CRTPF, dacă se specifică CRTFILE (*YES)	*OBJOPR	*EXECUTE
	Fişier-destinaţie, dacă se specifică CRTFILE (*YES)[1]		*ADD, *EXECUTE
	Fişier-destinaţie, dacă el există şi se adaugă un nou membru	*OBJOPR, *OBJMGT, *ADD, *DLT	*ADD, *EXECUTE
	Fişier-destinaţie, dacă el şi membrul există şi se specifică opţiunea *ADD	*OBJOPR, *ADD	*EXECUTE
	Fişier-destinaţie, dacă el şi membrul există şi se specifică opţiunea *REPLACE	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	Fişier-destinaţie, dacă el există, este adăugat un nou membru şi este specificată opţiunea *UPDADD.[8]	*OBJOPR, *OBJMGT, *ADD, *UPD	*EXECUTE
	Fişier-destinaţie, dacă el şi membrul există şi se specifică opţiunea *UPDADD.[8]	*OBJOPR, *ADD, *UPD	*EXECUTE
Creare (CRT)	Obiectul care va fi creat[2]		*READ, *ADD
	Profilul utilizator care va deţine obiectul creat (fie profilul utilizator care rulează jobul, fie profilul de grup al utilizatorului)	*ADD	
Creare (CRT) dacă se specifică REPLACE(*YES) [6, 9]	Obiectul care va fi creat (şi înlocuit)[2]	*OBJMGT, *OBJEXIST, *READ[5]	*READ, *ADD
	Profilul de utilizator care va deţine obiectul creat (fie profilul de utilizator care rulează jobul, fie profilul de grup al utilizatorului)	*ADD	
Afişare (DSP) sau altă operaţie care foloseşte fişierul ieşire (OUTPUT(*OUTFILE))	Obiectul care va fi afişat	*USE	*EXECUTE
	Fişierul de ieşire, dacă fişierul nu există[3]		*ADD, *EXECUTE
	Fişierul de ieşire, dacă fişierul există şi este adăugat un membru nou şi dacă este specificată opţiunea *REPLACE şi membrul nu există	*OBJOPR, *OBJMGT sau *OBJALTER, *ADD, *DLT	*ADD, *EXECUTE
	Fişierul de ieşire, dacă fişierul există şi este adăugat un membru nou şi este dacă specificată opţiunea *ADD şi membrul nu există.	OBJOPR, *OBJMGT sau *OBJALTER, *ADD	*ADD, *EXECUTE
	Fişier-destinaţie, dacă el şi membrul există şi se specifică opţiunea *ADD	*OBJOPR, *ADD	*EXECUTE
	Fişier-destinaţie, dacă el şi membrul există şi se specifică opţiunea *REPLACE	*OBJOPR, *OBJMGT sau *OBJALTER, *ADD, *DLT	*EXECUTE
Afişare (DSP) folosind *PRINT sau Lucru (WRK) folosind *PRINT	Obiectul care va fi afişat	*USE	*EXECUTE
	Coadă de ieşire[4]	*READ	*EXECUTE
	Fişier imprimantă (QP*xxxxx* în QSYS)	*USE	*EXECUTE
Fişier format (QA*xxxxx*), dacă fişierul ieşire nu există	*OBJOPR		

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
Salvare (SAV) sau altă operaţie care foloseşte descriere dispozitiv	Descriere dispozitiv	*USE	*EXECUTE
	Fişierul dispozitiv asociat cu descrierea dispozitivului, cum ar fi QSYSTAP pentru descrierea dispozitivului TAP01	*USE	*EXECUTE

1 Profilul utilizator care rulează comanda de copiere devine proprietarul fişierului-destinaţie, doar dacă utilizatorul nu este membru al unui profil de grup şi are OWNER(*GRPPRF). Dacă profilul de utilizator specifică OWNER(*GRPPRF), profilul de grup devine proprietarul fişierului destinaţie. În acest caz, utilizatorul care rulează comanda trebuie să aibă autorizarea *ADD pentru profilul de grup şi autorizarea de a adăuga un membru şi de a scrie date în noul fişier. Fişierului destinaţie îi este dată aceeaşi autorizare publică, autorizare de grup primar, autorizările private şi listă de autorizare, ca şi fişierului sursă.

2 Profilul utilizator care rulează comanda de creare devine proprietarul noului obiect creat, doar dacă utilizatorul nu este membru al unui profil de grup şi are OWNER(*GRPPRF). Dacă profilul de utilizator specifică OWNER(*GRPPRF), profilul de grup devine proprietarul fişierului nou creat. Autorizarea publică pentru obiect este controlată de parametrul AUT.

3 Profilul utilizator care rulează comanda de afişare devine proprietarul noului fişier ieşire creat, doar dacă utilizatorul nu este membru al unui profil de grup şi are OWNER(*GRPPRF). Dacă profilul de utilizator specifică OWNER(*GRPPRF), profilul de grup devine proprietarul fişierului de ieşire. Autorizarea publică pentru fişierul ieşire este controlată de parametrul CRTAUT al bibliotecii fişierului de ieşire.

4 Dacă coada de ieşire este definită ca OPRCTL (*YES), un utilizator cu autorizarea specială *JOBCTL nu are nevoie de nici o autorizare pentru ea. Un utilizator cu autorizarea specială *SPLCTL nu are nevoie de nici o autorizare pentru coada de ieşire.

5 Pentru fişiere dispozitiv, autorizarea *OBJOPR este de asemenea necesară.

6 Parametrul REPLACE nu e disponibil în mediul S/38. REPLACE(*YES) este echivalent cu a folosi o tastă funcţională din meniul de programare pentru a şterge obiectul curent.

7 E necesară de asemenea autorizare pentru comanda corespunzătoare (DSP).

8 Opţiunea *UPDADD este disponibilă doar în parametrul MBROPT al comenzii CPYF.

9 Aceasta nu se aplică parametrului REPLACE din comanda CRTJVAPGM.

Comenzi comune pentru toate obiectele

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Tabela 149. Comenzi comune pentru toate obiectele

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ALCOBJ [1,2,11]	Obiect	*OBJOPR	*EXECUTE
ANZUSROBJ [20]			
CHGOBJAUD [18]	Dispozitiv ASP (dacă este specificat)	*USE	
CHGOBJD [3]	Obiect, dacă este un fişier	*OBJOPR, *OBJMGT	*EXECUTE
	Obiect, dacă este un fişier	*OBJMGT	*EXECUTE

Comenzi comune pentru toate obiectele

Tabela 149. Comenzi comune pentru toate obiectele (continuare)

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
CHGOBJOWN [3,4]	Obiect	*OBJEXIST	*EXECUTE
	Obiect (dacă avem fişier, bibliotecă, descriere subsistem)	*OBJOPR, *OBJEXIST	*EXECUTE
	Obiect (dacă este *AUTL)	Drept de proprietate sau *ALLOBJ	*EXECUTE
	Profil utilizator vechi	*DLT	*EXECUTE
	Profil utilizator nou	*ADD	*EXECUTE
	Dispozitiv ASP (dacă este specificat)	*USE	
CHGOBJPGP [3]	Obiect	*OBJEXIST	*EXECUTE
	Obiect (dacă avem fişier, bibliotecă, descriere subsistem)	*OBJOPR, *OBJEXIST	*EXECUTE
	Obiect (dacă este *AUTL)	Drept de propietate şi *OBJEXIST sau *ALLOBJ	*EXECUTE
	Profil utilizator vechi	*DLT	
	Profil utilizator nou	*ADD	
	Dispozitiv ASP (dacă este specificat)	*USE	
CHKOBJ [3]	Obiect	Autorizare specificată de parametrul AUT [14]	*EXECUTE
CPROBJ	Obiect	*OBJMGT	*EXECUTE
CHKOBJITG [11](Q)			
CRTDUPOBJ [3,9,11,21]	Obiect nou		*USE, *ADD
	Obiectul copiat, dacă este *AUTL	*AUTLMGT	*USE, *ADD
	Obiect ce este copiat, toate celelalte tipuri	*OBJMGT, *USE	*USE
	comanda CRTSAVF (dacă obiectul este un fişier salvare)	*OBJOPR	
	Dispozitiv ASP (dacă este specificat)	*USE	
DCPOBJ	Obiect	*USE	*EXECUTE
DLCOBJ [1,11]	Obiect	*OBJOPR	*EXECUTE
DMPOBJ (Q) [3]	Obiect	*OBJOPR, *READ	*EXECUTE
DMPSYSOBJ (Q)	Obiect	*OBJOPR, *READ	*EXECUTE
DSPOBJAUT [3]	Obiect (pentru a vedea toate imformaţiile de autorizare)	autorizare specială sau drept de proprietate *OBJMGT sau *ALLOBJ	*EXECUTE
	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
	Dispozitiv ASP (dacă este specificat)	*USE	
DSPOBJD [2, 28]	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
	Object	O autorizare alta decât *EXCLUDE	*EXECUTE
	Dispozitiv ASP (dacă este specificat)	*EXECUTE	

Tabela 149. Comenzi comune pentru toate obiectele (continuare)

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
EDTOBJAUT [3,5,6,15]	Obiect	*OBJMGT	*EXECUTE
	Obiect (dacă avem fişier)	*OBJOPR, *OBJMGT	*EXECUTE
	*AUTL, dacă s-a folosit pentru a securiza obiectul	Non *EXCLUDE	
	Dispozitiv ASP (dacă este specificat)	*USE	
GRTOBJAUT [3,5,6,15]	Obiect	*OBJMGT	*EXECUTE
	Obiect (dacă avem fişier)	*OBJOPR, *OBJMGT	*EXECUTE
	*AUTL, dacă s-a folosit pentru a securiza obiectul	Non *EXCLUDE	
	Dispozitiv ASP (dacă este specificat)	*USE	
	Dispozitiv ASP referinţă (dacă este specificat)	*EXECUTE	
	Obiect referinţă	*OBJMGT sau drept de proprietate	*EXECUTE
MOVOBJ [3,7,12]	Obiect	*OBJMGT	
	Obiect (dacă avem *FILE)	*ADD, *DLT, *EXECUTE	
	Obiect (nu *FILE),	*DLT, *EXECUTE	
	Bibliotecă sursă		*CHANGE
	Bibliotecă destinaţie		*READ, *ADD
	Dispozitiv ASP (dacă este specificat)	*USE	
PRTADPOBJ [26](Q)			
PRTPUBAUT [26]			
PRTUSROBJ [26]			
PRTPVTAUT [26]			
RCLSTG (Q)			
RCLTMPSTG (Q)	Obiect	*OBJMGT	*EXECUTE
RNMOBJ [3,11]	Obiect	*OBJMGT	*UPD, *EXECUTE
	Obiect, dacă este *AUTL	*AUTLMGT	*EXECUTE
	Obiect (dacă avem *FILE)	*OBJOPR, *OBJMGT	*UPD, *EXECUTE
	Dispozitiv ASP (dacă este specificat)	*USE	

Comenzi comune pentru toate obiectele

Tabela 149. Comenzi comune pentru toate obiectele (continuare)

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
RSTOBJ [3,13] (Q)	Obiect, dacă există deja în bibliotecă	*OBJEXIST [8]	*EXECUTE, *ADD
	Obiect, dacă este *CFGL, *CNNL, *CTLD, *DEVD, *LIND, sau *NWID	*CHANGE şi *OBJMGT	*EXECUTE
	Definiţie mediu de stocare	*USE	*EXECUTE
	Cozile de mesaje care sunt restaurate în biblioteca unde există deja	*OBJOPR, *OBJEXIST [8]	*EXECUTE, *ADD
	Profilul utilizator deţine obiectele care sunt create	*ADD [8]	
	Program care adoptă autorizare	Proprietar sau autorizare spacială *SECADM şi *ALLOBJ	*EXECUTE
	Bibliotecă destinaţie	*EXECUTE, *ADD [8]	
	Bibliotecă pentru obiect salvat dacă VOL(*SAVVOL) este specificat	*USE [8]	
	Fişer de salvare	*USE	*EXECUTE
RSTOBJ [3,13] (Q)	Unitate de bandă, unitate de dischetă sau unitate optică	*USE	*EXECUTE
	Fişier bandă (QSYSTAP) sau fişier dischetă (QSYSDKT)	*USE [8]	*EXECUTE
	Fişier optic (OPTFILE)[22]	*R	Nu se aplică
	Director părinte sau fişier optic (OPTFILE)[22]	*X	Nu se aplică
	Prefix cale OPTFILE[22]	*X	Nu se aplică
	Volume optic[24]	*USE	Nu se aplică
	Ieşire imprimantă QSYS/QPSRLDSP, dacă s-a specificat OUTPUT(*PRINT)	*USE	*EXECUTE
	Fişier sursă, dacă este specificat	Vedeţi regulile generale.	Vedeţi regulile generale.
	Fişierul referinţă de câmp QSYS/QASRRSTO pentru fişierul de ieşire, dacă un fişier de ieşire este specificat şi nu există.	*USE	*EXECUTE
	Decriere de dispozitiv ASP[25]	*USE	
RVKPUBAUT [20]	Fişier bandă (QSYSTAP) sau fişier dischetă (QSYSDKT)	*USE [8]	*EXECUTE
RTVOBJD [2, 29]	Obiect	O autorizare alta decât *EXCLUDE	*EXECUTE
RVKOBJAUT [3,5,15, 27]	Prefix cale OPTFILE[22]	*X	Nu se aplică
	Volume optic[24]	*USE	Nu se aplică
	Ieşire imprimantă QSYS/QPSRLDSP, dacă s-a specificat OUTPUT(*PRINT)	*USE	*EXECUTE
	Dispozitiv ASP (dacă este specificat)	*USE	

Tabela 149. Comenzi comune pentru toate obiectele (continuare)

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
SAVCHGOBJ [3]	Obiect (8)	*OBJEXIST	*EXECUTE
	Unitate de bandă, unitate de dischetă, unitate optică	*USE	*EXECUTE
	Fişier de salvare, dacă e gol	*USE, *ADD	*EXECUTE
	Fişier de salvare, dacă există înregistrări în el	*OBJMGT, *USE, *ADD	*EXECUTE
	Coadă de mesaje salvare active	*OBJOPR, *ADD	*EXECUTE
SAVCHGOBJ [3]	Fişier optic (OPTFILE)[22]	*RW	Nu se aplică
	Director părinte sau fişier optic (OPTFILE)[22]	*WX	Nu se aplică
	Prefix cale sau fişier optic (OPTFILE)[22]	*X	Nu se aplică
	Director rădăcină (/) al volumului optic[22, 23]	*RWX	Nu se aplică
	Volume optic[24]	*CHANGE	
	Fişier sursă, dacă este specificat	Vedeţi regulile generale.	Vedeţi regulile generale.
	Fişierul referinţă de câmp QSYS/QASAVOBJ pentru fişierul de ieşire, dacă un fişier de ieşire este specificat şi nu există.	*USE [8]	*EXECUTE
	Ieşire imprimantă QSYS/QPSAVOBJ	*USE [8]	*EXECUTE
	Decriere de dispozitiv ASP[25]	*USE	
SAVOBJ [3]	Obiect	*OBJEXIST [8]	*EXECUTE
	Definiţie mediu de stocare	*USE	*EXECUTE
	Unitate de bandă, unitate de dischetă, unitate optică	*USE	*EXECUTE
	Fişier de salvare, dacă e gol	*USE, *ADD	*EXECUTE
	Fişier de salvare, dacă există înregistrări în el	*OBJMGT, *USE, *ADD	*EXECUTE
	Coadă de mesaje salvare active	*OBJOPR, *ADD	*EXECUTE
SAVOBJ [3]	Fişier optic (OPTFILE)[22]	*RW	Nu se aplică
	Director părinte sau fişier optic (OPTFILE)[22]	*WX	Nu se aplică
	Prefix cale OPTFILE[22]	*X	Nu se aplică
	Director rădăcină (/) al volumului optic[22, 23]	*RWX	Nu se aplică
	Volume optic[24]	*CHANGE	
	Fişier sursă, dacă este specificat	Vedeţi regulile generale.	Vedeţi regulile generale.
	Fişierul referinţă de câmp QSYS/QASAVOBJ pentru fişierul de ieşire, dacă un fişier de ieşire este specificat şi nu există.	*USE [8]	*EXECUTE
	Ieşire imprimantă QSYS/QPSAVOBJ	*USE [8]	*EXECUTE
	Decriere de dispozitiv ASP[25]	*USE	
SAVSTG [10]			
SAVSYS [10]	Unitate de bandă, unitate optică	*USE	*EXECUTE
	Director rădăcină (/) al volumului optic[22]	*RWX	Nu se aplică
	Volume optic[24]	*CHANGE	Nu se aplică

Comenzi comune pentru toate obiectele

Tabela 149. Comenzi comune pentru toate obiectele (continuare)

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
SAVRSTCHG	Pe sistemul sursă, aceeaşi autorizare precum se cere prin comanda SAVCHGOBJ.		
	Pe sistemul destinaţie, aceeaşi autorizare precum se cere prin comanda RSTOBJ.		
	Decriere de dispozitiv ASP[25]	*USE	
SAVRSTLIB	Pe sistemul sursă, aceeaşi autorizare precum se cere prin comanda SAVLIB.		
	Pe sistemul destinaţie, aceeaşi autorizare precum se cere prin comanda RSTLIB.		
SAVRSTOBJ	Pe sistemul sursă, aceeaşi autorizare precum se cere prin comanda SAVOBJ.		
	Pe sistemul destinaţie, aceeaşi autorizare precum se cere prin comanda RSTOBJ.		
	Decriere de dispozitiv ASP[25]	*USE	
SETOBJACC	Obiect	*OBJOPR	*EXECUTE
WRKOBJ [19]	Obiect	Orice autorizaţie	*USE
WRKOBJLCK	Obiect		*EXECUTE
	Dispozitiv ASP	*EXECUTE	
WRKOBJOWN [17]	Ptofil utilizator	*READ	*EXECUTE
WRKOBJPGP [17]	Ptofil utilizator	*READ	*EXECUTE
WRKOBJPVT[17]	Ptofil utilizator	*READ	*EXECUTE

1 Vedeţi cuvântul cheie OBJTYPE al comenzii ALCOBJ pentru lista de tipuri de obiecte care pot fi alocate şi dezalocate.

2 Aceeaşi autorizare pentru obiectul (altul când *EXCLUDE) este cerut.

3 Această comandă nu poate fi utilizată pentru documente sau fişiere. Folosiţi comanda echivalentă DLO (Document Library Object - Obiect bibliotecă document).

4 Trebuie să aveţi autorizarea specială *ALLOBJ şi *SECADM pentru a modifica proprietarul obiect al unui program, programul service sau pachetul SQL care adoptă autorizarea.

5 Trebuie să fiţi proprietar sau să aveţi autorizarea *OBJMGT şi autorizările care sunt acordate sau revocate.

6 Trebuie să fiţi propietarul sau să aveţi autorizarea specială *ALLOBJ pentru a garanta autoriyarea *OBJMGT sau *AUTLMGT.

7 Această comandă nu poate fi utilizată pentru profiluri utilizator, descrieri de controller, descrieri de dispozitiv, descrieri linie, documente, biblioteci documente şi fişiere.

8 Dacă aveţi autorizarea specială *SAVSYS, nu aveţi nevoie de autorizarea specificată.

9 Dacă utilizatorul rulează comanda CRTDUPOBJ are profilul utilizator OWNER(*GRPPRF), propietarul unui obiect nou este profilul grup. Pentru a copia cu succes autorizările la un nou obiect deţinut de un profil grup, au loc următoarele:

- Utilizatorul ce rulează comanda trebuie să aibă autorizare pentru obiectul sursă. Autorizările pot fi obţinute prin adoptarea autorizării sau prin profilul de grup.
- Dacă apare o eroare în timpul copierii autorizăriloe pentru noul obiect, noul obiect creat este şters.

10 Trebuie să aveţi autorizarea specială *SAVSYS.

Tabela 149. Comenzi comune pentru toate obiectele (continuare)

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
[11] Această comandă nu poate fi utilizată pentru jurnale şi receptori jurnale. [12] Această comandă poate fi utilizată pentru jurnale şi receptori jurnale, doar dacă biblioteca-sursă este QRCL şi biblioteca-destinaţie este biblioteca originală pentru jurnal sau receptorii jurnal. [13] Trebuie să aveţi autorizaţia specială *ALLOBJ pentru a specifica ALWOBJDIF(*ALL). [14] Pentru a verifica o autorizare de utilizator pentru un obiect, trebuie să aveţi autorizarea pe care o verificaţi. De exemplu, pentru a verifica dacă un utilizator are autorizarea *OBJEXIST pentru FILEB, trebuie să aveţi autorizarea *OBJEXIST pentru FILEB. [15] Pentru a securiza un obiect cu o listă de autorizare sau a înlătura lista de autorizare de la un obiect, trebuie să îndepliniţi una dintre următoarele condiţii: • Să deţineţi obiectul. • Să aveţi autorizarea *ALL pentru obiect. • Să aveţi autorizarea specială *ALLOBJ.			
[16] Dacă şi fişierul original şi fişierul redenumit are un deţinător de autorizare asociată, autorizarea *ALL pentru deţinătorul de autorizare este cerută. [17] Această comandă nu suportă sistemul fişier QOPT. [18] Trebuie să aveţi autorizaţia specială *AUDIT. [19] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizarea cerută de operaţia individuală. [20] Trebuie să aveţi autorizarea specială *ALLOBJ.			
[21] Toate autorizările de la obiectul-sursă sunt duplicate pentru obiectul nou. Grupul primar al noului obiect este determinat de câmpul tip de autorizare grup(GRPAUTTYP) din profilul utilizator care rulează comanda. Dacă obiectul-sursă are un grup primar, noul obiect este posibil să nu aibă acelaşi grup primar, dar autorizarea pe care o are grupul primar asupra obiectului-sursă va fi duplicată la noul obiect. [22] Această verificare de autorizare este făcută doar când formatul mediului de stocare optic este UDF (format disc universal). [23] Această verificare de autorizare este făcută doar când dumneavoastră curăţaţi volumul optic. [24] Volumele optice nu sunt obiecte sistem reale. Legătura între volumul optic şi lista de autorizare folosită pentru a securiza volumul este menţinută de funcţia de suport optic. [25] Autorizarea este necesară doar dacă operaţia de salvare sau restaurare necesită o comutare a spaţiului de nume de bibliotecă. [26] Trebuie să aveţi autorizaţia specială *ALLOBJ sau *AUDIT pentru a folosi această comandă. [27] *** **Risc securitate** *** Revocarea specifică a tututor autorizărilor date unui utilizator pentru un obiect poate duce la o situaţie în care utilizatorul să aibă mai multe autorizări decât înainte de operaţia de revocare. Dacă utilizatorul are autorizarea *USE pentru un obiect şi *CHANGE pentru lista de autorizare care securizează obiectul, revocarea autorizării *USE face ca utilizatorul să aibă autorizarea *CHANGE pentru obiect. [28] Trebuie să aveţi autorizarea specială *ALLOBJ sau *AUDIT pentru a fi afişată valoarea curentă de auditare a obiectului. În caz contrar va fi afişată valoarea *NOTAVL, pentru a indica faptul că valoarea nu este disponibilă pentru afişare. [29] Trebuie să aveţi autorizarea specială *ALLOBJ sau *AUDIT pentru a fi extrasă valoarea curentă de auditare a obiectului. În caz contrar va fi returnată valoarea *NOTAVL, pentru a indica faptul că valorile nu sunt disponibile pentru extragere.		

Comenzile de recuperare a căii de acces: autorizările necesare

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Aceste comenzi nu necesită nici o autorizare obiect.

		Autorizări necesare	
Comanda	**Obiect referinţă**	**Pentru obiecte**	**Pentru biblioteci**
CHGRCYAP [1] (Q)	Dispozitiv ASP (dacă este specificat)	*USE	
DSPRCYAP [1]	Dispozitiv ASP (dacă este specificat)	*USE	
EDTRBDAP [2] (Q)			
EDTRCYAP [1] (Q)	Dispozitiv ASP (dacă este specificat)	*USE	

[1] Trebuie să aveţi autorizaţia specială *JOBCTL pentru a folosi această comandă.

[2] Trebuie să aveţi autorizaţia specială *ALLOBJ pentru a folosi această comandă.

Comenzile AFP*: autorizările necesare

		Autorizări necesare	
Comanda	**Obiect referinţă**	**Pentru obiecte**	**Pentru biblioteci**
ADDFNTTBLE	Tabel font DBCS	*CHANGE	*EXECUTE
CHGCDEFNT	Resursă fonturi	*CHANGE	*EXECUTE
CHGFNTTBLE	Tabel font DBCS	*CHANGE	*EXECUTE
CRTFNTRSC	Fişier sursă	*USE	*EXECUTE
	Resursă fonturi: REPLACE(*NO)		*READ, *ADD
	Resursă fonturi: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
CRTFNTTBL	Tabel font DBCS		*READ, *ADD
CRTFORMDF	Fişier sursă	*USE	*EXECUTE
	Definiţie formular: REPLACE(*NO)		*READ, *ADD
	Definiţie formular: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
CRTOVL	Fişier sursă	*USE	*EXECUTE
	Suprapunere: REPLACE(*NO)		*READ, *ADD
	Suprapunere: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
CRTPAGDFN	Fişier sursă	*USE	*EXECUTE
	Definiţie pagină: REPLACE(*NO)		*READ, *ADD
	Definiţie pagină: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
CRTPAGSEG	Fişier sursă	*USE	*EXECUTE
	Segment de pagină: REPLACE(*NO)		*READ, *ADD
	Segment de pagină: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
DLTFNTRSC	Resursă fonturi	*OBJEXIST	*EXECUTE
DLTFNTTBL	Tabel font DBCS	*CHANGE	*EXECUTE
DLTFORMDF	Definiţie formular	*OBJEXIST	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DLTOVL	Suprapunere	*OBJEXIST	*EXECUTE
DLTPAGDFN	Definiţie de pagină	*OBJEXIST	*EXECUTE
DLTPAGSEG	Segment pagină	*OBJEXIST	*EXECUTE
DSPCDEFNT	Resursă fonturi	*USE	*EXECUTE
DSPFNTRSCA	Resursă fonturi	*USE	*EXECUTE
DSPFNTTBL	Tabel font DBCS	*USE	*EXECUTE
RMVFNTTBLE	Tabel font DBCS	*CHANGE	*EXECUTE
WRKFNTRSC [1]	Resursă fonturi	*USE	*USE
WRKFORMDF [1]	Definiţie formular	*USE	*USE
WRKOVL [1]	Suprapunere	*USE	*USE
WRKPAGDFN [1]	Definiţie de pagină	Orice autorizaţie	*USE
WRKPAGSEG [1]	Segment pagină	*USE	Orice autorizaţie
[1] Pentru a folosi operaţii individuale, trebuie să aveţi autorizaţia cerută de operaţii individuale.			

Comenzile pentru socket-uri AF_INET peste SNA: autorizările necesare

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul cu securitatea poate acorda autorizare *USE altora. Aceste comenzi nu necesită vreo autorizaţie obiect:

Aceste comenzi nu necesită vreo autorizaţie obiect:			
ADDIPSIFC[1]	CHGIPSIFC[1]	CVTIPSLOC	RMVIPSLOC[1]
ADDIPSRTE[1]	CHGIPSLOC[1]	ENDIPSIFC (Q)	RMVIPSRTE[1]
ADDIPSLOC[1]	CHGIPSTOS[1]	PRTIPSCFG	STRIPSIFC (Q)
CFGIPS	CVTIPSIFC	RMVIPSIFC[1]	
[1] Trebuie să aveţi autorizaţia specială *IOSYSCFG pentru a folosi această comandă.			

Alertele: autorizările necesare

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDALRD	Tabel alertă	*USE, *ADD	*EXECUTE
CHGALRD	Tabel alertă	*USE, *UPD	*EXECUTE
CHGALRTBL (Q)	Tabel alertă	*CHANGE	*EXECUTE
CRTALRTBL (Q)	Tabel alertă		*READ, *ADD
DLTALR	Fişier fizic QAALERT	*USE, *DLT	*EXECUTE
DLTALRTBL (Q)	Tabel alertă	*OBJEXIST	*EXECUTE
RMVALRD	Tabel alertă	*USE, *DLT	*EXECUTE
WRKALR [1]	Fişier fizic QAALERT	*USE	*EXECUTE
WRKALRD [1]	Tabel alertă	*USE	*EXECUTE
WRKALRTBL [1]	Tabel alertă	*READ	*USE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
[1] Pentru a folosi operaţii individuale, trebuie să aveţi autorizaţia cerută de operaţii individuale.			

Comenzile de dezvoltare a aplicaţiei: autorizările necesare

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
FNDSTRPDM	Parte sursă	*READ	*EXECUTE
MRGFORMD	Descriere formular	*READ	*EXECUTE
STRAPF [1]	Fişier sursă	*OBJMGT, *CHANGE	*READ, *ADD
	Comenzi CRTPF, CRTLF, ADDPFM, ADDLFM şi RMVM	*USE	*EXECUTE
STRBGU [1]	Grafic	*OBJMGT, *CHANGE	*EXECUTE
STRDFU [1]	Program (dacă se creează opţiune program)		*READ, *ADD
	Program (dacă există opţiunea de modificare sau ştergere program)	*OBJEXIST	*EXECUTE
	Program (dacă se modifică sau afişează opţiune de date)	*USE	*EXECUTE
	Fişier bază de date (dacă se modifică opţiunea de date)	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	Fişier bază de date (dacă se afişează opţiunea de date)	*USE	*EXECUTE
	Fişier afişare (dacă se afişează sau modifică opţiunea de date)	*USE	*EXECUTE
	Fişier afişare (dacă se modifică opţiunea de program)	*USE	*EXECUTE
	Fişier afişare (dacă se şterge opţiunea de program)	*OBJEXIST	*EXECUTE
STRPDM [1]			
STRRLU	Fişier sursă	*READ, *ADD, *UPD, *DLT	*EXECUTE
	Editare, adăugare sau modificare a unui membru	*OBJOPR, *OBJMGT	*READ, *ADD
	Răsfoire un membru	*OBJOPR	*EXECUTE
	Tipărire raport prototip	*OBJOPR	*EXECUTE
	Înlăturare a unui membru	*OBJOPR, *OBJEXIST	*EXECUTE
	Modificare tip sau text al membrului	*OBJOPR	*EXECUTE
STRSDA	Fişier sursă	*READ, *ADD, *UPD, *DLT	*EXECUTE
	Actualizare şi adăugare a unui nou membru	*CHANGE, *OBJMGT	*READ, *ADD
	Ştergere membru	*ALL	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
STRSEU [1]	Fişier sursă	*USE	*EXECUTE
	Editare sau modificare a unui membru	*CHANGE, *OBJMGT	*EXECUTE
	Adăugare un membru	*USE, *OBJMGT	*READ, *ADD
	Răsfoire un membru	*USE	*EXECUTE
	Tipărire un membru	*USE	*EXECUTE
	Înlăturare a unui membru	*USE, *OBJEXIST	*EXECUTE
	Modificare tip sau text al membrului	*USE, *OBJMGT	*EXECUTE
WRKLIBPDM [1]			
WRKMBRPDM [1]	Fişier sursă	*USE	*EXECUTE
WRKOBJPDM [1]	Fişier	*READ sau drept de proprietate	*EXECUTE

[1] Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea cerută de operaţia individuală.

[2] Un grup corespunde bibliotecii.

[3] Un proiect se alcătuieşte din unul sau mai multe grupuri (biblioteci).

Comenzile pentru deţinător de autorizare: autorizările necesare

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTAUTHLR (Q)	Obiect asociat dacă acesta există	*ALL	*EXECUTE
DLTAUTHLR	Deţinător de autorizare	*ALL	*EXECUTE
DSPAUTHLR	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.

Comenzile pentru lista de autorizare: autorizările necesare

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă QSYS
ADDAUTLE [1]	*AUTL	*AUTLMGT sau drept de proprietate	*EXECUTE
CHGAUTLE [1]	*AUTL	*AUTLMGT sau drept de proprietate	*EXECUTE
CRTAUTL			
DLTAUTL	*AUTL	Proprietar sau *ALLOBJ	*EXECUTE
DSPAUTL	*AUTL		*EXECUTE
	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
DSPAUTLDLO	*AUTL	*USE	*EXECUTE
DSPAUTLOBJ	*AUTL	*READ	*EXECUTE
	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
EDTAUTL [1]	*AUTL	*AUTLMGT sau drept de proprietate	*EXECUTE

Comenzi listă autorizare

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă QSYS
RMVAUTLE [1]	*AUTL	*AUTLMGT sau drept de propietate	*EXECUTE
RTVAUTLE [2]	*AUTL	*AUTLMGT sau drept de propietate	*EXECUTE
WRKAUTL [3,4,5]	*AUTL		

1 Trebuie să fiţi propietarul sau să aveţi autorizarea gestionare listă şi să aveţi autorizările ce sunt date sau luate.

2 Dacă nu aveţi *OBJMGT sau *AUTLMGT, puteţi extrage autorizarea *PUBLIC şi autorizarea dumneavoastră proprie. Trebuie să aveţi autorizarea *READ pentru profilul dumneavoastră pentru a extrage propria dumneavoastră autorizare.

3 Pentru a folosi o operaţie individuală, trebuie să aveţi autorizaţia necesară de operaţie.

4 Nu trebuie să fiţi exclus (*EXCLUDE) din lista autorizare.

5 O anumită autorizare pentru lista autorizare este cerută.

Comenzile pentru director de legare: autorizările necesare

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDBNDDIRE	Director legare	*OBJOPR, *ADD	*USE
CRTBNDDIR	Director legare		*READ, *ADD
DLTBNDDIR	Director legare	*OBJEXIST	*EXECUTE
DSPBNDDIR	Director legare	*READ, *OBJOPR	*USE
RMVBNDDIRE	Director legare	*OBJOPR, *DLT	*READ, *OBJOPR
WRKBNDDIR [1]	Director legare	Orice autorizaţie	*USE
WRKBNDDIRE [1]	Director legare	*READ, *OBJOPR	*USE

1 Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea cerută de operaţie.

Comenzile descriere cerere de modificare

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDCMDCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
ADDOBJCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
ADDPRDCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
ADDPTFCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
ADDRSCCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
CHGCMDCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
CHGOBJCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
CHGPRDCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
CHGPTFCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
CHGCRQD	Descriere cerere de modificare	*CHANGE	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGRSCCRQA (Q)	Descriere cerere de modificare	*CHANGE	*EXECUTE
CRTCRQD	Descriere cerere de modificare		*READ, *ADD
DLTCRQD	Descriere cerere de modificare	*OBJEXIST	*EXECUTE
RMVCRQDA	Descriere cerere de modificare	*CHANGE	*EXECUTE
WRKCRQD [1]	Descriere cerere de modificare		*EXECUTE

[1] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizaţia necesară de operaţie.

Comenzile pentru diagramă

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DLTCHTFMT	Format diagramă	*OBJEXIST	*EXECUTE
DSPCHT	Format diagramă	*USE	*USE
	Fişier bază de date	*USE	*USE
DSPGDF	Fişier bază de date	*USE	*USE
STRBGU (Opţiunea 3) [2]	Format diagramă	*CHANGE, *OBJEXIST	*EXECUTE
WRKCHTFMT [1]	Format diagramă	Orice autorizaţie	*USE

[1] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizaţia necesară de operaţie.

[2] Opţiunea 3 din meniul BGU (afişat atunci când este rulat STRGBU) este opţiunea Modificare format diagramă.

Comenzile pentru clasă

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGCLS	Clasă	*OBJMGT, *OBJOPR	*EXECUTE
CRTCLS	Clasă		*READ, *ADD
DLTCLS	Clasă	*OBJEXIST	*EXECUTE
DSPCLS	Clasă	*USE	*EXECUTE
WRKCLS [1]	Clasă	*OBJOPR	*USE

[1] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizaţia necesară de operaţie.

Comenzile pentru clasă-de-serviciu

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGCOSD [3]	Descriere clasă-de-serviciu	*CHANGE, OBJMGT	*EXECUTE
CRTCOSD [3]	Descriere clasă-de-serviciu		
DLTCOSD	Descriere clasă-de-serviciu	*OBJEXIST	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DSPCOSD	Descriere clasă-de-serviciu	*USE	*EXECUTE
WRKCOSD [1,2]	Descriere clasă-de-serviciu	*OBJOPR	*EXECUTE

[1] Pentru a folosi operaţii individuale, trebuie să aveţi autorizaţia cerută de operaţii individuale.

[2] E necesară aceeaşi autorizare pentru obiect.

[3] Pentru a folosi această comandă, trebuie să aveţi autorizaţia specială *IOSYSCFG.

Comenzile pentru cluster

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul cu securitatea poate acorda *USE altora.

Comanda	Obiect referinţă	Autorizaţie necesară	
		Pentru obiecte	Pentru biblioteci
ADDCLUNODE (Q)[1]	Programul serviciu QCSTCTL	*USE	
ADDCRGDEVE (Q)[1]	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil utilizator pentru rulare program de ieşire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
ADDCRGNODE (Q)[1]	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil utilizator pentru rulare program de ieşire	*USE	
	Coada de mesaje preluare la defectare	*OBJOPR, *ADD	*EXECUTE
	Coadă utilizator informaţii distribuire	*OBJOPR, *ADD	*EXECUTE
ADDDEVDMNE (Q)[1]	Programul serviciu QCSTDD	*USE	
CHGCLUCFG (Q)[1]	Programul serviciu QCSTCTL2	*USE	
CHGCLUNODE (Q)[1]	Programul serviciu QCSTCTL	*USE	
CHGCLURCY	Grup resursă cluster	*USE	
		*JOBCTL	
		*SERVICE sau funcţia Urmărire service	
CHGCLUVER (Q)[1]	Programul serviciu QCSTCTL2	*USE	
CHGCRG (Q)[1]	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil utilizator pentru rulare program de ieşire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
	Coada de mesaje preluare la defectare	*OBJOPR, *ADD	*EXECUTE

Comanda	Obiect referinţă	Autorizaţie necesară	
		Pentru obiecte	**Pentru biblioteci**
CHGCRGDEVE (Q)[1]	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil utilizator pentru rulare program de ieşire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
CHGCRGPRI (Q)[1]	Programul serviciu QCSTCRG2	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil utilizator pentru rulare program de ieşire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
	Comanda VFYCFG (Vary configuration - Verificare configurare)	*USE	
CRTCLU (Q)[1]	Programul serviciu QCSTCTL	*USE	
CRTCRG (Q) [1]	Programul serviciu QCSTCRG1	*USE	
	Bibliotecă grup resursă cluster		*OBJOPR, *ADD, *READ (QUSRSYS)
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil utilizator pentru rulare program de ieşire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
	Coadă utilizator informaţii distribuire	*OBJOPR, *ADD	*EXECUTE
	Coada de mesaje preluare la defectare	*OBJOPR, *ADD	*EXECUTE
DLTCLU (Q)[1]	Programul serviciu QCSTCTL	*USE	
DLTCRG[1]	Grup resursă cluster	*OBJEXIST, *USE	*EXECUTE (QUSRSYS)
DLTCRGCLU (Q)[1]	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*OBJEXIST, *USE	*EXECUTE (QUSRSYS)
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil utilizator pentru rulare program de ieşire	*USE	
DMPCLUTRC	Grup resursă cluster	*USE	
		*SERVICE sau funcţia Urmărire service	
DSPCLUINF			
DSPCRGINF	Grup resursă cluster	*USE	*EXECUTE (QUSRSYS)
ENDCLUNOD (Q)[1]	Programul serviciu QCSTCTL	*USE	
ENDCHTSVR (Q)	Listă de autorizaţii	*CHANGE	

Comanda	Obiect referinţă	Autorizaţie necesară	
		Pentru obiecte	Pentru biblioteci
ENDCRG (Q)[1]	Programul serviciu QCSTCRG2	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil utilizator pentru rulare program de ieşire	*USE	
RMVCLUNODE (Q)[1]	Programul serviciu QCSTCTL	*USE	
RMVCRGDEVE (Q)[1]	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil utilizator pentru rulare program de ieşire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
RMVCRGNODE (Q) [1]	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*CHANGE, *OBJEXIST	*EXECUTE
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil utilizator pentru rulare program de ieşire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
RMVDEVDMNE (Q)[1]	Programul serviciu QCSTDD	*USE	
STRCHTSVR	Listă de autorizaţii	*CHANGE	
STRCLUNOD (Q)[1]	Programul serviciu QCSTCTL	*USE	
STRCRG (Q)[1]	Programul serviciu QCSTCRG2	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil utilizator pentru rulare program de ieşire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	

[1] Trebuie să aveţi autorizaţia specială *IOSYSCFG pentru a folosi această comandă.

[2] Se aplică pentru pentru profil utilizator apelator şi profil utilizator rulare program de ieşire.

Comenzile pentru comandă (*CMD)

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGCMD	Comanda	*OBJMGT	*EXECUTE
CHGCMDDFT	Comanda	*OBJMGT, *USE	*EXECUTE
CRTCMD	Fişier sursă	*USE	*EXECUTE
	Comandă: REPLACE(*NO)		*READ, *ADD
	Comandă: REPLACE(*YES)	Vedeţi regulile generale.	Vedeţi regulile generale.
DLTCMD	Comanda	*OBJEXIST	*EXECUTE
DSPCMD	Comanda	*USE	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
GENCMDDOC[3]	Comanda	*USE	*EXECUTE
	Grup de panouri (asociat)	*USE	*EXECUTE
	Fişier ieşire: REPLACE = (*YES)	*ALL	*CHANGE
SBMRMTCMD	Comanda	*OBJOPR	*EXECUTE
	Fişier DDM	*USE	*EXECUTE
SLTCMD [1]	Comanda	Orice autorizaţie	*USE
WRKCMD [2]	Comanda	Orice autorizaţie	*USE

1 Drept de proprietate sau unele autorizaţii pentru obiect sunt necesare.

2 Pentru a folosi operaţii individuale, trebuie să aveţi autorizaţia cerută de operaţii individuale.

3 Trebuie să aveţi autorizare de execuţie (*X) pentru directoarele din calea fişierului generat şi autorizări de scriere şi execuţie (*WX) pentru directorul părinte al fişierului generat.

Comenzile pentru controlul comiterii

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
COMMIT			
ENDCMTCTL	Coada de mesaje, aşa cum a fost specificată în cuvântul cheie NFYOBJ pentru comanda STRCMTCTL asociată.	*OBJOPR, *ADD	*EXECUTE
ROLLBACK			
STRCMTCTL	Coada de mesaje, când a fost specificată în cuvântul cheie NFYOBJ	*OBJOPR, *ADD	*EXECUTE
	Zona de date, aşa cum a fost specificată în cuvântul cheie NFYOBJ pentru comanda STRCMTCTL asociată.	*CHANGE	*EXECUTE
	Fişierele, aşa cum au fost specificate în cuvântul cheie NFYOBJ pentru comanda STRCMTCTL asociată.	*OBJOPR *READ	*EXECUTE
WRKCMTDFN [1]			

1 Orice utilizator poate rula această comandă pentru definiţii de comitere care aparţin unui job care rulează sub profilul de utilizator al utilizatorului respectiv. Un utilizator care are autorizarea specială de control job (*JOBCTL) poate rula această comandă pentru orice definiţie de comitere.

Comenzile CSI (informaţii parte comunicaţii)

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGCSI	Obiect CSI	*USE, *OBJMGT	*EXECUTE
	Descriere dispozitiv [1]	*CHANGE	
CRTCSI	Obiect CSI		*READ, *ADD
	Descriere dispozitiv [1]	*CHANGE	

Comenzi informaţii parte comunicaţii

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
DLTCSI	Obiect CSI	*OBJEXIST	*EXECUTE
DSPCSI	Obiect CSI	*READ	*EXECUTE
WRKCSI	Obiecte CSI	*USE	*EXECUTE

1 Autorizarea este verificată când este folosit obiectul CSI (informaţii parte comunicaţii).

Comenzile de configurare

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
PRTDEVADR	Descriere controler (CTL)	*USE	*EXECUTE
	Descriere dispozitiv	*USE	*EXECUTE
RSTCFG (Q) [5]	Fiecare obiect care este restaurat peste, de o versiune salvată	*OBJEXIST [1]	*EXECUTE
	Bibliotecă destinaţie		*ADD, *EXECUTE [1]
	Profilul utilizator care deţine obiectele care sunt create	*ADD [1]	
	Unitate bandă	*USE	*EXECUTE
	Fişier bandă (QSYSTAP)	*USE [1]	*EXECUTE
	Fişier salvare, dacă este specificat	*USE	*EXECUTE
	Ieşire imprimantă (QPSRLDSP), dacă s-a specificat output(*print)	*USE	*EXECUTE
	Fişier sursă, dacă este specificat	Vedeţi regulile generale.	Vedeţi regulile generale.
	Fişierul referinţă câmp QSYS/QASRRSTO, dacă fişierul de ieşire este specificat şi nu există	*USE	*EXECUTE
RTVCFGSTS	Obiect	*OBJOPR	*EXECUTE
RTVCFGSRC	Obiect	*USE	*EXECUTE
	Fişier sursă	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
SAVCFG [2]	Fişier de salvare, dacă e gol	*USE, *ADD	*EXECUTE
	Fişier de salvare, dacă există înregistrări în el	*USE, *ADD, *OBJMGT	*EXECUTE
SAVRSTCFG	Pe sistemul sursă, aceeaşi autorizare ca cea necesară pentru comanda SAVCFG.		
	Pe sistemul destinaţie, aceeaşi autorizare ca cea necesară pentru comanda RSTCFG.		
VRYCFG [3,6]	Obiect	*USE, *OBJMGT	*EXECUTE
WRKCFGSTS [4]	Obiect	*OBJOPR	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci

[1] Dacă aveţi autorizarea specială *SAVSYS, nu aveţi nevoie de autorizarea specificată.

[2] Trebuie să aveţi autorizarea specială *SAVSYS.

[3] Dacă un utilizator are autorizarea specială *JOBCTL, nu e necesară autorizarea pentru obiect.

[4] Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea cerută de operaţia individuală.

[5] Trebuie să aveţi autorizaţia specială *ALLOBJ pentru a specifica ALWOBJDIF(*ALL).

[6] Trebuie să aveţi autorizarea specială *IOSYSCFG pentru biblioteca mediu de stocare când starea e *ALLOCATE sau *DEALLOCATE.

Comenzile pentru listă de configurare

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDCFGLE [2]	Listă de configurare	*CHANGE, *OBJMGT	*EXECUTE
CHGCFGL [2]	Listă de configurare	*CHANGE, *OBJMGT	*EXECUTE
CHGCFGLE [2]	Listă de configurare	*CHANGE, *OBJMGT	*EXECUTE
CPYCFGL [2]	Listă de configurare	*USE, *OBJMGT	*ADD
CRTCFGL [2]	Listă de configurare		
DLTCFGL	Listă de configurare	*OBJEXIST	*EXECUTE
DSPCFGL [2]	Listă de configurare	*USE, *OBJMGT	*EXECUTE
RMVCFGLE [2]	Listă de configurare	*CHANGE, *OBJMGT	*EXECUTE
WRKCFGL [1, 2]	Listă de configurare	*OBJOPR	*EXECUTE

[1] Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea cerută de operaţia individuală.

[2] Pentru a folosi această comandă, trebuie să aveţi autorizaţia specială *IOSYSCFG.

Comenzile pentru listă de conexiuni

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DLTCNNL	Listă de conexiuni	*OBJEXIST	*EXECUTE
DSPCNNL	Listă de conexiuni	*USE	*EXECUTE
WRKCNNL [1]	Listă de conexiuni	*OBJOPR	*EXECUTE

[1] Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea cerută de operaţia individuală.

Comenzile pentru descriere de controler

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGCTLAPPC [2]	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
	Descriere linie (SWTLINLST)	*USE	*EXECUTE
	Listă de conexiuni (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLASC [2]	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
	Descriere linie (SWTLINLST)	*USE	*EXECUTE
CHGCTLBSC [2]	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
	Descriere linie (SWTLINLST)	*USE	*EXECUTE
CHGCTLFNC [2]	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
	Descriere linie (SWTLINLST)	*USE	*EXECUTE
CHGCTLHOST [2]	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
	Descriere linie (SWTLINLST)	*USE	*EXECUTE
	Listă de conexiuni (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLLWS [2]	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
	Program (INZPGM)	*USE	*EXECUTE
CHGCTLNET [2]	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
CHGCTLRTL [2]	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
	Descriere linie (SWTLINLST)	*USE	*EXECUTE
CHGCTLRWS [2]	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
	Descriere linie (SWTLINLST)	*USE	*EXECUTE
	Listă de conexiuni (CNNLSTOUT)	*USE	*EXECUTE
CHGCTLTAP [2]	Descriere controler	*CHANGE, *OBJMGT	*EXECUTE
CHGCTLVWS [2]	Controler	*CHANGE, *OBJMGT	*EXECUTE
CRTCTLAPPC [2]	Descriere de linie (LINE sau SWTLINLST)	*USE	*EXECUTE
	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Listă de conexiuni (CNNLSTOUT)	*USE	*EXECUTE
	Descriere controler		
CRTCTLASC [2]	Descriere de linie (LINE sau SWTLINLST)	*USE	*EXECUTE
	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Descriere controler		
CRTCTLBSC [2]	Descriere de linie (LINE sau SWTLINLST)	*USE	*EXECUTE
	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Descriere controler		
CRTCTLFNC [2]	Descriere de linie (LINE sau SWTLINLST)	*USE	*EXECUTE
	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Descriere controler		

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTCTLHOST [2]	Descriere de linie (LINE sau SWTLINLST)	*USE	*EXECUTE
	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Listă de conexiuni (CNNLSTOUT)	*USE	*EXECUTE
	Descriere controler		
CRTCTLLWS [2]	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Descriere controler		
	Program (INZPGM)	*USE	*EXECUTE
CRTCTLNET [2]	Descriere de linie (LINE)	*USE	*EXECUTE
	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Descriere controler		
CRTCTLRTL [2]	Descriere de linie (LINE sau SWTLINLST)	*USE	*EXECUTE
	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Descriere controler		
CRTCTLRWS [2]	Descriere de linie (LINE sau SWTLINLST)	*USE	*EXECUTE
	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Listă de conexiuni (CNNLSTOUT)	*USE	*EXECUTE
	Descriere controler		
CRTCTLTAP [2]	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Descriere controler		
CRTCTLVWS [2]	Descriere dispozitiv (DEV)	*USE	*EXECUTE
	Descriere controler		
DLTCTLD	Descriere controler	*OBJEXIST	*EXECUTE
DSPCTLD	Descriere controler	*USE	*EXECUTE
ENDCTLRCY	Descriere controler	*USE	*EXECUTE
PRTCMNSEC [3]			
RSMCTLRCY	Descriere controler	*USE	*EXECUTE
WRKCTLD [1]	Descriere controler	*OBJOPR	*EXECUTE

1 Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea cerută de operaţia individuală.

2 Pentru a folosi această comandă, trebuie să aveţi autorizaţia specială *IOSYSCFG.

3 Pentru a folosi această comandă trebuie să aveţi autorizările speciale *ALLOBJ şi *IOSYSCFG sau *AUDIT.

Comenzile pentru criptografie

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
	Coada de mesaje QHST	*OBJOPR, *ADD	*EXECUTE

Comenzi criptografie

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	Coada de mesaje QHST	*OBJOPR, *ADD	*EXECUTE
CHGMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	Coada de mesaje QHST	*OBJOPR, *ADD	*EXECUTE
CPHDTA (Q)			
ENCCPHK (Q)			
ENCFRMMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
ENCTOMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
GENCPHK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
GENCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
	QCRP/QPCRGENX *FILE	*OBJOPR, *READ	*EXECUTE
	Coada de mesaje QHST	*OBJOPR, *ADD	*EXECUTE
GENMAC (Q)			
GENPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
RMVCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *DLT	*EXECUTE
	Coada de mesaje QHST	*OBJOPR, *ADD	*EXECUTE
SETMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ, *UPD	*EXECUTE
	Coada de mesaje QHST	*OBJOPR, *ADD	*EXECUTE
TRNPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
VFYMSTK (Q)	Coada de mesaje QHST	*OBJOPR, *ADD	*EXECUTE
VFYPIN (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, READ	*EXECUTE

Comenzile pentru zonă de date

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGDTAARA [1]	Zonă de date	*CHANGE	*EXECUTE
CRTDTAARA [1]	Zonă de date		*READ, *ADD
	APPC device description[4]	*CHANGE	
DLTDTAARA	Zonă de date	*OBJEXIST	*EXECUTE
DSPDTAARA	Zonă de date	*USE	*EXECUTE
RTVDTAARA [2]	Zonă de date	*USE	*EXECUTE
WRKDTAARA [3]	Zonă de date	Orice autorizaţie	*USE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci

[1] Dacă comenzile de creare şi modificare a zonei de date sunt rulate folosind funcţii ale limbajului de nivel înalt, aceste autorizări sunt încă necesare deşi autorizarea pentru comandă nu e necesară.

[2] Autorizarea este verificată în momentul rulării, dar nu şi la momentul compilării.

[3] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizaţia necesară de operaţie.

[4] Autorizarea este verificată când este folosită zona de date.

Comenzile pentru coadă de date

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTDTAQ	Coadă de date		*READ, *ADD
	Coada de date destinaţie pentru programul QSNDDTAQ	*OBJOPR, *ADD	*EXECUTE
	Coada de date sursă pentru programul QRCVDTAQ	*OBJOPR, *READ	*EXECUTE
	Descriere dispozitiv APPC[2]	*CHANGE	
DLTDTAQ	Coadă de date	*OBJEXIST	*EXECUTE
WRKDTAQ [1]	Coadă de date	*READ	*USE

[1] Pentru a folosi operaţii individuale, trebuie să aveţi autorizaţia cerută de operaţii individuale.

[2] Autorizarea este verificată când este folosită zona de date.

Comenzile pentru descriere de dispozitiv

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CFGDEVMLB [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVAPPC [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
	Descriere mod (MODE)	*USE	*EXECUTE
CHGDEVASC [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVASP[4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVBSC [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVCRP[4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVDKT [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVDSP [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
	Imprimantă (PRINTER)	*USE	*EXECUTE
CHGDEVFNC [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVHOST [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVINTR [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVMLB [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVNET [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE

Comenzi descriere dispozitiv

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGDEVOPT [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVPRT [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
	Listă de validare (dacă e specificată)	*READ	*EXECUTE
CHGDEVRTL [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVSNPT [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVSNUF [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVTAP [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CRTDEVAPPC [4]	Descriere controler (CTL)	*USE	*EXECUTE
	Descriere dispozitiv		
	Descriere mod (MODE)	*USE	*EXECUTE
CRTDEVASC [4]	Descriere controler (CTL)	*USE	*EXECUTE
	Descriere dispozitiv		
CRTDEVASP [4]	Descriere dispozitiv		*EXECUTE
CRTDEVBSC [4]	Descriere controler (CTL)	*USE	*EXECUTE
	Descriere dispozitiv		
CRTDEVCRP[4]	Descriere dispozitiv		*EXECUTE
CRTDEVDKT [4]	Descriere dispozitiv		*EXECUTE
CRTDEVDSP [4]	Descriere imprimantă (PRINTER)	*USE	*EXECUTE
	Descriere controler (CTL)	*USE	*EXECUTE
	Descriere dispozitiv		
CRTDEVFNC [4]	Descriere controler (CTL)	*USE	*EXECUTE
	Descriere dispozitiv		
CRTDEVHOST [4]	Descriere controler (CTL)	*USE	*EXECUTE
	Descriere dispozitiv		
CRTDEVINTR [4]	Descriere dispozitiv		
CRTDEVMLB [4]	Descriere dispozitiv		*EXECUTE
CRTDEVNET [4]	Descriere controler (CTL)	*USE	*EXECUTE
	Descriere dispozitiv		
CRTDEVOPT [4]	Descriere dispozitiv		*EXECUTE
CRTDEVPRT [4]	Descriere controler (CTL)	*USE	*EXECUTE
	Descriere dispozitiv		
	Listă de validare (dacă e specificată)	*READ	*EXECUTE
CRTDEVRTL [4]	Descriere controler (CTL)	*USE	*EXECUTE
	Descriere dispozitiv		
CRTDEVSNPT [4]	Descriere controler (CTL)	*USE	*EXECUTE
	Descriere dispozitiv		
CRTDEVSNUF [4]	Descriere controler (CTL)	*USE	*EXECUTE
	Descriere dispozitiv		
CRTDEVTAP [4]	Descriere controler (CTL)	*USE	*EXECUTE
	Descriere dispozitiv		

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DLTDEVD [1]	Descriere dispozitiv	*OBJEXIST	*EXECUTE
DSPCNNSTS	Descriere dispozitiv	*OBJOPR	*EXECUTE
DSPDEVD	Descriere dispozitiv	*USE	*EXECUTE
ENDDEVRCY	Descriere dispozitiv	*USE	*EXECUTE
HLDCMNDEV [2]	Descriere dispozitiv	*OBJOPR	*EXECUTE
PRTCMNSEC [4, 5]			
RLSCMNDEV	Descriere dispozitiv	*OBJOPR	*EXECUTE
RSMDEVRCY	Descriere dispozitiv	*USE	*EXECUTE
WRKDEVD [3]	Descriere dispozitiv	*OBJOPR	*EXECUTE

1 Pentru a înlătura o coadă de ieşire asociată, sunt necesare autorizarea existenţă obiect (*OBJEXIST) pentru coada de ieşire şi autorizarea de citire pentru biblioteca QUSRSYS.

2 Trebuie să aveţi autorizările specială control job (*JOBCTL) şi cea operaţională obiect pentru descrierea dispozitivului.

3 Pentru a folosi operaţii individuale, trebuie să aveţi autorizaţia cerută de operaţii individuale.

4 Trebuie să aveţi autorizarea specială *IOSYSCFG pentru a rula această comandă.

5 Trebuie să aveţi autorizarea specială *ALLOBJ pentru a rula această comandă.

Comenzile pentru emulare dispozitiv

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDEMLCFGE	Fişier de configurare emulare	*CHANGE	*EXECUTE
CHGEMLCFGE	Fişier de configurare emulare	*CHANGE	*EXECUTE
EJTEMLOUT	Descriere dispozitiv emulare când e specificat	*OBJOPR	*EXECUTE
	Descriere dispozitiv emulare când locaţia e specificată	*OBJOPR	*EXECUTE
ENDPRTEML	Descriere dispozitiv emulare când e specificat	*OBJOPR	*EXECUTE
	Descriere dispozitiv emulare când locaţia e specificată	*OBJOPR	*EXECUTE
EMLPRTKEY	Descriere dispozitiv emulare când e specificat	*OBJOPR	*EXECUTE
	Descriere dispozitiv emulare când locaţia e specificată	*OBJOPR	*EXECUTE
EML3270	Descriere dispozitiv emulare	*OBJOPR	*EXECUTE
	Descriere controler emulare	*OBJOPR	*EXECUTE
RMVEMLCFGE	Fişier de configurare emulare	*CHANGE	*EXECUTE
STREML3270	Fişier de configurare emulare	*OBJOPR	*EXECUTE
	Dispozitiv de emulare, descriere controler de emulare, dispozitiv staţie de afişare şi descriere controler staţie de afişare	*OBJOPR	*EXECUTE
	Descriere dispozitiv imprimantă, program de ieşire utilizator şi tabele de translatare când sunt specificate	*OBJOPR	*EXECUTE

Comenzi emulare dispozitiv

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
STRPRTEML	Fişier de configurare emulare	*OBJOPR	*EXECUTE
	Descriere dispozitiv emulare şi descriere controler emulare	*OBJOPR	*EXECUTE
	Descriere dispozitiv imprimantă, ieşire imprimantă, coadă de mesaje, descriere job, coadă de joburi şi tabele de translatare când sunt specificate	*OBJOPR	*EXECUTE
SNDEMLIGC	Din-fişier	*OBJOPR	*EXECUTE
TRMPRTEML	Descriere dispozitiv emulare	*OBJOPR	*EXECUTE

Comenzile pentru director şi umbrire director

Aceste comenzi nu necesită nici o autorizaţie obiect:

ADDDIRE [2]	CHGDIRSHD [1]	ENDDIRSHD [4]	STRDIRSHD [4]
ADDDIRSHD [1]	CPYFRMDIR [1]	RMVDIRE [1]	WRKDIRE [3,5]
CHGSYSDIRA [2]	CPYTODIR [1]	RMVDIRSHD [1]	WRKDIRLOC [1,5]
CHGDIRE [3]	DSPDIRE	RNMDIRE [2]	WRKDIRSHD [1,5]

1 Trebuie să aveţi autorizarea specială *SECADM.

2 Trebuie să aveţi autorizările speciale *SECADM sau *ALLOBJ.

3 Un utilizator cu autorizarea specială *SECADM poate lucra cu toate intrările director. Utilizatorii fără autorizarea specială *SECADM pot lucra doar cu propriile lor intrări.

4 Trebuie să aveţi autorizaţia specială *JOBCTL.

5 Pentru a folosi o operaţie individuală, trebuie să aveţi autorizaţia necesară de operaţie.

Comenzile pentru disc

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Aceste comenzi nu necesită autorizarea pentru nici un obiect:

ENDDSKRGZ (Q) [1]	STRDSKRGZ (Q) [1]	WRKDSKSTS

1 Pentru a folosi această comandă, trebuie să aveţi autorizarea specială *ALLOBJ.

Comenzile pentru passthrough staţie de afişare

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ENDPASTHR			

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
STRPASTHR	Dispozitiv APPC pe sistem sursă	*CHANGE	*EXECUTE
	Dispozitiv APPC pe sistem destinaţie	*CHANGE	*EXECUTE
	Controler virtual pe sistem destinaţie [1]	*USE	*EXECUTE
	Dispozitiv virtual pe sistem destinaţie [1],[2]	*CHANGE	*EXECUTE
	Program specificat în valoarea de sistem QRMTSIGN pe sistemul destinaţie, dacă există[1]	*USE	*USE
TFRPASTHR			

1 Profilul utilizator care necesită această autorizare este cel care rulează jobul batch passthrough. Pentru un passthrough care ocoleşte ecranul de semnare, profilul de utilizator este cel specificat în parametrul de utilizator la distanţă (RMTUSER). Pentru un passtrough care foloseşte procedura normală de semnare (RMTUSER(* NONE)), utilizatorul este profilul de utilizator implicit specificat în intrarea de comunicaţii a subsistemului care tratează cererea de passthrough. În general, acesta este QUSER.

2 Dacă passthrough-ul este unul care foloseşte procedura normală de semnare, profilul de utilizator specificat în ecranul de semnare pe sistemul destinaţie trebuie să aibă autorizare pentru acest obiect.

Comenzile pentru distribuţie

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDDSTQ (Q)			
ADDDSTRTE (Q)			
ADDDSTSYSN (Q)			
CFGDSTSRV (Q)			
CFGRPDS (Q)			
CHGDSTD [1]	Document [2]	*CHANGE	*EXECUTE
CHGDSTQ (Q)			
CHGDSTRTE (Q)			
DLTDST [1]			
DSPDSTLOG (Q)	Jurnal	*USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
DSPDSTSRV (Q)			
HLDDSTQ (Q)			
INZDSTQ (Q)			
QRYDST [1]	Fişier cerut	*CHANGE	*EXECUTE
RCVDST [1]	Fişier cerut	*CHANGE	*EXECUTE
	Folder	*CHANGE	*EXECUTE
RLSDSTQ (Q)			
RMVDSTQ (Q)			

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
RMVDSTRTE (Q)			
RMVDSTSYSN (Q)			
SNDDST [1]	Fişier sau document cerut	*USE	*EXECUTE
SNDDSTQ (Q)			
WRKDSTQ (Q)			
WRKDPCQ (Q)			

[1] Dacă un utilizator cere distribuţie pentru alt utilizator, el trebuie să aibă autorizarea de a lucra în numele celuilalt.

[2] Când distribuţia este plină.

Comenzile pentru listă de distribuţie

Aceste comenzi nu necesită nici o autorizare obiect:

ADDDSTLE [1]	CRTDSTL	DSPDSTL	RNMDSTL [1]
CHGDSTL [1]	DLTDSTL [1]	RMVDSTLE [1]	WRKDSTL [2]

[1] Trebuie să aveţi autorizarea specială *SECADM sau să deţineţi lista de distribuţie.

[2] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizaţia necesară de operaţie.

Comenzile pentru obiecte din biblioteca de documente

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDDLOAUT	Obiect bibliotecă document	*ALL sau proprietar	*EXECUTE
CHGDLOAUD [1]			
CHGDLOAUT	Obiect bibliotecă document	*ALL sau proprietar	*EXECUTE
CHGDLOOWN	Obiect bibliotecă document	Proprietar sau autorizare specială *ALLOBJ	*EXECUTE
	Profil utilizator vechi	*DLT	*EXECUTE
	Profil utilizator nou	*ADD	*EXECUTE
CHGDLOPGP	Obiect bibliotecă document	Proprietar sau autorizare specială *ALLOBJ	*EXECUTE
	Profil de grup primar vechi	*DLT	*EXECUTE
	Profil de grup primar nou	*ADD	*EXECUTE
CHGDOCD [2]	Descriere document	*CHANGE	*EXECUTE
CHKDLO [2]	Obiect bibliotecă document	Cum a fost cerut de cuvântul cheie AUT	*EXECUTE
CHKDOC	Document	*CHANGE	*EXECUTE
	Dicţionar ajutător pentru corectare ortografică	*CHANGE	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CPYDOC	Document-sursă	*USE	*EXECUTE
	Document-destinaţie, dacă se înlocuieşte documentul existent	*CHANGE	*EXECUTE
	Folder-destinaţie dacă acesta e nou	*CHANGE	*EXECUTE
CRTDOC	Folder-destinaţie	*CHANGE	*EXECUTE
CRTFLR	Folder-destinaţie	*CHANGE	*EXECUTE
DLTDLO [3]	Obiect bibliotecă document	*ALL	*EXECUTE
DLTDOCL[20]	Listă documente	*ALL [4]	*EXECUTE
DMPDLO [15]			
DSPAUTLDLO	Listă de autorizaţii	*USE	*EXECUTE
	Obiect bibliotecă document	*USE	*EXECUTE
DSPDLOAUD[21]	Fişier sursă, dacă este specificat	Vedeţi regulile generale.	Vedeţi regulile generale.
DSPDLOAUT	Obiect bibliotecă document	*USE sau proprietar	*EXECUTE
DSPDLONAM[22]	Obiect bibliotecă document	*USE	*EXECUTE
DSPDOC	Document	*USE	*EXECUTE
DSPFLR	Folder	*USE	*EXECUTE
EDTDLOAUT	Obiect bibliotecă document	*ALL sau proprietar	*EXECUTE
EDTDOC	Document	*CHANGE	*EXECUTE
FILDOC [2]	Fişier cerut	*USE	*EXECUTE
	Folder	*CHANGE	*EXECUTE
MOVDOC	Folder-sursă, dacă documentul sursă este într-un folder	*CHANGE	*EXECUTE
	Document-sursă	*ALL	*EXECUTE
	În-fişier	*CHANGE	*EXECUTE
MRGDOC [5]	Document	*USE	*EXECUTE
	Folder-sursă	*USE	*EXECUTE
	Document-destinaţie dacă acesta este înlocuit	Vedeţi regulile generale.	Vedeţi regulile generale.
	Folder-destinaţie dacă acesta e nou	Vedeţi regulile generale.	Vedeţi regulile generale.
PAGDOC	Document	*CHANGE	*EXECUTE
PRTDOC	Folder	*USE	*EXECUTE
	Document	*USE	*EXECUTE
	Comenzile DLTPF, DLTF şi DLTOVR, dacă e specificată o instrucţiune *INDEX*	*USE	*EXECUTE
	Comenzile CRTPF, OVRPRTF, DLTSPLF şi DLTOVR, dacă se specifică o instrucţiune *RUN*	*USE	*EXECUTE
	Document salvare, dacă se specifică SAVOUTPUT (*YES)	*USE	*EXECUTE
	Folder salvare, dacă se specifică SAVOUTPUT (*YES)	*USE	*EXECUTE
QRYDOCLIB [2,6]	Fişier cerut	*USE	*EXECUTE
	Listă documente, dacă există	*CHANGE	*EXECUTE

Comenzi obiect bibliotecă document

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
RCLDLO	Obiect bibliotecă document		
	Documentele interne sau toate documentele şi folderele[16]		
RGZDLO	Obiect bibliotecă document	*CHANGE sau proprietar	*EXECUTE
	DLO(*ALL), DLO(*ALL) FLR(*ANY) sau DLO(*ALL) FLR(*ANY) MAIL(*YES)[16]		
RMVDLOAUT	Obiect bibliotecă document	*ALL sau proprietar	*EXECUTE
RNMDLO	Obiect bibliotecă document	*ALL	*EXECUTE
	Folder-destinaţie	*CHANGE	*EXECUTE
RPLDOC [2]	Fişier cerut	*READ	*EXECUTE
	Document	*CHANGE	*EXECUTE
RSTDLO	Obiect bibliotecă documen, dacă înlocuieşte	*ALL[10]	*EXECUTE
	Folderul părinte, dacă DLO este nou	*CHANGE[10]	*EXECUTE
	Profilul utilizator proprietar, dacă DLO este nou	*ADD[10]	*EXECUTE
	Fişier sursă, dacă este specificat	Vedeţi regulile generale.	Vedeţi regulile generale.
	Fişer de salvare	*USE	*EXECUTE
	Fişier optic (OPTFILE)[17]	*R	Nu se aplică
	Prefix cale al fişierului optic (OPTFILE)[17]	*X	Nu se aplică
	Volum optic[19]	*USE	Nu se aplică
	Bandă, dischetă şi unitate optică	*USE	*EXECUTE
RSTS36FLR [11,12,14]	Folder S/36	*USE	*EXECUTE
	În-fişier	*CHANGE	*EXECUTE
	Fişier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
RTVDLONAM[22]	Obiect bibliotecă document	*USE	*EXECUTE
RTVDOC [2]	Document dacă se verifică	*CHANGE	*EXECUTE
	Document dacă nu se verifică	*USE	*EXECUTE
	Fişier cerut	*CHANGE	*EXECUTE
SAVDLO [7,13]	Obiect bibliotecă document	*ALL[10]	*EXECUTE
	Unitate de bandă, unitate de dischetă şi unitate optică	*USE	*EXECUTE
	Fişier de salvare, dacă e gol	*USE, *ADD	*EXECUTE
	Fişier de salvare, dacă există înregistrări în el	*USE, *ADD, *OBJMGT	*EXECUTE
	Fişier sursă, dacă este specificat	Vedeţi regulile generale.	Vedeţi regulile generale.
	Fişier optic (OPTFILE)[17]	*RW	Nu se aplică
	Directorul părinte al fişierului optic (OPTFILE)[17]	*WX	Nu se aplică
	Prefixul cale al fişierului optic (OPTFILE)[17]	*X	Nu se aplică
	Directorul root (/) al volumului[17, 18]	*RWX	Nu se aplică
	Volum optic[19]	*CHANGE	Nu se aplică

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
SAVRSTDLO	Pe sistemul sursă, aceeaşi autorizare ca cea necesară pentru comanda SAVDLO.		
	Pe sistemul destinaţie, aceeaşi autorizare ca cea necesară pentru comanda RSTDLO.		
WRKDOC	Folder	*USE	
WRKFLR	Folder	*USE	

[1] Trebuie să aveţi autorizaţia specială *AUDIT.

[2] Dacă utilizatorul lucrează în numele altui utilizator, este verificată autorizarea celuilalt utilizator pentru obiect.

[3] Utilizatorul trebuie să aibă autorizarea *ALL pentru toate obiectele din folder pentru a şterge folderul şi toate obiectele din el.

[4] Dacă aveţi autorizarea specială *ALLOBJ sau *SECADM, nu aveţi nevoie de autorizarea *ALL pentru lista bibliotecă a documentului.

[5] Utilizatorul trebuie să aibă autorizare pentru obiectul care e folosit ca sursă de combinare. De exemplu, dacă se specifică MRGTYPE(*QRY), utilizatorul trebuie să aibă autorizare de utilizare pentru interogarea specificată în parametrul QRYDFN.

[6] Doar obiectele care îndeplinesc criteriile interogării şi pentru care utilizatorul are cel puţin autorizarea *USE sunt returnate în lista de documente sau fişierul de ieşire

[7] E necesară *SAVSYS, *ALLOBJ sau înrolare în directorul de distribuţie a sistemului.

[8] E necesară autorizarea specială *SAVSYS sau *ALLOBJ pentru a folosi următoarea combinaţie de parametri: RSTDLO DLO(*MAIL).

[9] E necesară *ALLOBJ pentru a specifica ALWOBJDIF(*ALL).

[10] Dacă aveţi autorizarea specială *SAVSYS, nu aveţi nevoie de autorizarea specificată.

[11] Aveţi nevoie de autorizaţia *ALL pentru document dacă îl inlocuiţi. Aveţi nevoie de autorizaţii operaţionale şi pentru toate datele pentru folder dacă restauraţi informaţii noi în aceste foldere, sau aveţi nevoie de autorizaţia specială *ALLOBJ.

[12] Dacă este folosit pentru dicţionar, este necesară doar autorizaţia pentru comandă.

[13] E necesară autorizarea specială *SAVSYS sau *ALLOBJ pentru a folosi următoarea combinaţie de parametri:

SAVDLO DLO(*ALL) FLR(*ANY)

SAVDLO DLO(*MAIL)

SAVDLO DLO(*CHG)

SAVDLO DLO(*SEARCH) OWNER(not *CURRENT)

[14] Trebuie să fiţi înscris în directorul de distribuire sistem dacă folderul sursă este un folder document.

[15] Trebuie să aveţi autorizarea specială *ALLOBJ pentru a face dump la obiectele bibliotecă document interne.

Comenzi obiect bibliotecă document

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**

[16] Trebuie să aveţi autorizările speciale *ALLOBJ sau *SECADM.

[17] Această verificare de autorizare este făcută doar când formatul mediului de stocare optic este UDF (Universal Disk Format).

[18] Această verificare de autorizare este făcută doar când ştergeţi volumul optic.

[19] Volumele optice nu sunt obiecte sistem reale. Legătura între volumul optic şi lista de autorizare folosită pentru a securiza volumul este menţinută de funcţia de suport optic.

[20] Utilizatorul trebuie să aibă autorizarea specială *ALLOBJ când s-a specificat OWNER (*ALL) sau OWNER (nume) şi Nume reprezintă alt profil de utilizator decât apelantul.

[21] Pentru a folosi această comandă, utilizatorul trebuie să aibă autorizarea specială pentru toate obiectele (*ALLOBJ) sau pentru audit (*AUDIT).

[22] Pentru a folosi această comandă când se specifică *DST pentru clasa de obiecte de localizat, utilizatorul trebuie să aibă autorizarea specială pentru toate obiectele (*ALLOBJ).

Comenzile pentru setul de caractere pe doi octeţi

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
CPYIGCTBL	Tabelă de sortare DBCS (*IN)	*ALL	*EXECUTE
	Tabelă de sortare DBCS (*OUT)	*USE	*EXECUTE
CRTIGCDCT	Dicţionar conversie DBCS		*READ, *ADD
DLTIGCDCT	Dicţionar conversie DBCS	*OBJEXIST	*EXECUTE
DLTIGCSRT	Tabelă de sortare DBCS	*OBJEXIST	*EXECUTE
DLTIGCTBL	Tabel font DBCS	*OBJEXIST	*EXECUTE
DSPIGCDCT	Dicţionar conversie DBCS	*USE	*EXECUTE
EDTIGCDCT	Dicţionar conversie DBCS	*USE, *UPD	*EXECUTE
	Dicţionar utilizator	*ADD, *DLT	*EXECUTE
STRCGU	Tabelă de sortare DBCS	*CHANGE	*EXECUTE
	Tabel font DBCS	*CHANGE	*EXECUTE
STRFMA	Tabela de font DBCS, dacă e specificată opţiunea de copiere în	*OBJOPR, *READ *ADD, *UPD	*EXECUTE
	Tabela de font DBCS, dacă e specificată opţiunea de copiere din	*OBJOPR, *READ	*EXECUTE
	Fişierul de lucru de ajutor gestionare font (QGPL/QAFSVDF)	*CHANGE	*EXECUTE

Comenzile pentru descriere editare

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
CRTEDTD	Descriere de editare		*EXECUTE, *ADD
DLTEDTD	Descriere de editare	*OBJEXIST	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DSPEDTD	Descriere de editare	*OBJOPR	*EXECUTE
WRKEDTD [1]	Descriere de editare	Orice autorizaţie	*USE
[1] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizaţia necesară de operaţie.			

Comenzile pentru variabile de mediu

Aceste comenzi nu necesită nici o autorizare obiect.			
ADDENVVAR[1]	CHGENVVAR [1]	RMVENVVAR[1]	WRKENVVAR[1]
[1] Pentru a actualiza variabile de mediu de nivel sistem, aveţi nevoie de autorizarea specială *JOBCTL.			

Comenzile pentru configuraţie LAN extinsă prin comunicaţie fără fir

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDEWCBCDE	Fişier sursă	*USE	*EXECUTE
ADDEWCM	Fişier sursă	*USE	*EXECUTE
ADDEWCPTCE	Fişier sursă	*USE	*EXECUTE
ADDEWLM	Fişier sursă	*USE	*EXECUTE
CHGEWCBCDE	Fişier sursă	*USE	*EXECUTE
CHGEWCM	Fişier sursă	*USE	*EXECUTE
CHGEWCPTCE	Fişier sursă	*USE	*EXECUTE
CHGEWLM	Fişier sursă	*USE	*EXECUTE
DSPEWCBCDE	Fişier sursă	*USE	*EXECUTE
DSPEWCM	Fişier sursă	*USE	*EXECUTE
DSPEWCPTCE	Fişier sursă	*USE	*EXECUTE
DSPEWLM	Fişier sursă	*USE	*EXECUTE
RMVEWCBCDE	Fişier sursă	*USE	*EXECUTE
RMVEWCPTCE	Fişier sursă	*USE	*EXECUTE

Comenzile pentru fişier

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDICFDEVE	Fişier ICF	*OBJOPR, *OBJMGT	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
ADDLFM	Fişier logic	*OBJOPR, *OBJMGT sau *OBJALTER	*EXECUTE, *ADD
	Fişierul la care se referă parametrul DTAMBRS, când fişierul logic este cu cheie	*OBJOPR, *OBJMGT sau *OBJALTER	*EXECUTE
	Fişierul la care se referă parametrul DTAMBRS, când fişierul logic nu este cu cheie	*OBJOPR	*EXECUTE
ADDPFCST	Fişier dependent, dacă se specifică TYPE(*REFCST)	*OBJMGT sau *OBJALTER	*EXECUTE
	Fişierul părinte, dacă se specifică TYPE(*REFCST)	*OBJMGT sau *OBJREF	*EXECUTE
	Fişierul, dacă se specifică TYPE(*UNQCST) sau TYPE(*PRIKEY)	*OBJMGT	*EXECUTE
ADDPFM	Fişier fizic	*OBJOPR, *OBJMGT sau *OBJALTER	*EXECUTE, *ADD
ADDPFTRG	Fişier fizic, pentru a insera declanşator	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Fişier fizic, pentru a şterge declanşator	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Fişier fizic, pentru a actualiza declanşator	*OBJALTER, *OBJMGT, *READ, *OBJOPR	*EXECUTE
	Program declanşator	*EXECUTE	*EXECUTE
CHGDDMF	Fişier DDM	*OBJOPR, *OBJMGT	*EXECUTE
	Descriere dispozitiv [7]	*CHANGE	
CHGDKTF	Fişier dischetă	*OBJOPR, *OBJMGT	*EXECUTE
	Dispozitivul dacă numele dispozitivului e specificat în comandă	*OBJOPR	*EXECUTE
CHGDSPF	Fişier afişare	*OBJOPR, *OBJMGT	*EXECUTE
	Dispozitivul dacă numele dispozitivului e specificat	*OBJOPR	*EXECUTE
CHGDTA	Fişier date	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	Program	*USE	*EXECUTE
	Fişier afişare	*USE	*EXECUTE
CHGICFDEVE	Fişier ICF	*OBJOPR, *OBJMGT	*EXECUTE
CHGICFF	Fişier ICF	*OBJOPR, *OBJMGT	*EXECUTE
CHGLF	Fişier logic	*OBJMGT sau *OBJALTER	*EXECUTE
CHGLFM	Fişier logic	*OBJMGT sau *OBJALTER	*EXECUTE
CHGPF	Fişier fizic	*OBJMGT sau *OBJALTER	*EXECUTE
CHGPFCST	Fişier dependent	*OBJMGT sau *OBJALTER	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGPFM	Fişier fizic	*OBJMGT sau *OBJALTER	*EXECUTE
CHGPFTRG	Fişier fizic	*OBJMGT sau *OBJALTER	*EXECUTE
CHGPRTF	Ieşire imprimantă	*OBJOPR, *OBJMGT	*EXECUTE
	Dispozitivul dacă numele dispozitivului e specificat	*OBJOPR	*EXECUTE
CHGSAVF	Fişer de salvare	*OBJOPR, *OBJMGT	*EXECUTE
CHGSRCPF	Fişier fizic sursă	*OBJMGT sau *OBJALTER	*EXECUTE
CHGTAPF	Fişier bandă	*OBJOPR, *OBJMGT	*EXECUTE
	Dispozitivul dacă numele dispozitivului e specificat	*OBJOPR	*EXECUTE
CLRPFM	Fişier fizic	*OBJOPR, *OBJMGT sau *OBJALTER, *DLT	*EXECUTE
CLRSAVF	Fişer de salvare	*OBJOPR, *OBJMGT	*EXECUTE
CPYF	Din-fişier	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier dispozitiv)	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier fizic)	Vedeţi regulile generale.	Vedeţi regulile generale.
	Pe baza fişierului dacă fişier-sursă este unul logic	*READ	*EXECUTE
CPYFRMDKT	Din-fişier	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier dispozitiv)	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier fizic)	Vedeţi regulile generale.	Vedeţi regulile generale.
CPYFRMIMPF	Din-fişier	*OBJOPR, *READ	*USE
	Fişier-destinaţie (fişier dispozitiv)	*OBJOPR, *READ	*USE
	Fişier-destinaţie (fişier fizic)	Vedeţi regulile generale.	Vedeţi regulile generale.
	Pe baza fişierului dacă fişier-sursă este unul logic	*READ	*USE
CPYFRMQRYF [1]	Din-fişier	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier dispozitiv)	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier fizic)	Vedeţi regulile generale.	Vedeţi regulile generale.
CPYFRMSTMF	Fişier flux	*R	
	Directoarele din prefix nume cale al fişierului flux	*X	
	Fişierul bază de date destinaţie, dacă se specifică MBROPT(*ADD)	*X, *ADD	*X
	Fişierul bază de date destinaţie, dacă se specifică MBROPT(*REPLACE)	*X, *ADD, *DLT, *OBJMGT	*X
	Fişierul bază de date destinaţie, dacă este creat un nou membru)	*X, *OBJMGT, *ADD	*X, *ADD
	Tabela de conversie *TBL folosită pentru a translata datele	*OBJOPR	*X
	Fişierul de salvare destinaţie există	*RX, *ADD, *OBJMGT	*X
	Fişierul de salvare destinaţie este creat		*RX, *ADD

Comenzi fişier

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
CPYFRMTAP	Din-fişier	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier dispozitiv)	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier fizic)	Vedeţi regulile generale.	Vedeţi regulile generale.
CPYSRCF	Din-fişier	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier dispozitiv)	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier fizic)	Vedeţi regulile generale.	Vedeţi regulile generale.
CPYTODKT	Fişier-destinaţie şi din fişier	*OBJOPR, *READ	*EXECUTE
	Dispozitivul dacă numele dispozitivului e specificat în comandă	*OBJOPR, *READ	*EXECUTE
	Pe baza fişierului fizic dacă fişier-sursă este unul logic	*READ	*EXECUTE
CPYTOIMPF	Din-fişier	*OBJOPR, *READ	*USE
	Fişier-destinaţie (fişier dispozitiv)	*OBJOPR, *READ	*USE
	Fişier-destinaţie (fişier fizic)	Vedeţi regulile generale.	Vedeţi regulile generale.
	Pe baza fişierului dacă fişier-sursă este unul logic	*READ	*USE
CPYTOSTMF	Fişier bază de date sau fişier de salvare	*RX	*X
	Fişier flux, dacă există deja	*W	
	Directorul părinte al fişierului flux, dacă fişierul flux nu există	*WX,	
	Prefixul numelui căii fişierului flux	*X	
	Tabela de conversie *TBL folosită pentru a translata datele	*OBJOPR	*X
CPYTOTAP	Fişier-destinaţie şi din fişier	*OBJOPR, *READ	*EXECUTE
	Dispozitivul dacă numele dispozitivului e specificat	*OBJOPR, *READ	*EXECUTE
	Pe baza fişierului fizic dacă fişier-sursă este unul logic	*READ	*EXECUTE
CRTDDMF	Fişier DDM: REPLACE(*NO)		*READ, *ADD
	Fişier DDM: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Descriere dispozitiv [7]	*CHANGE	
CRTDKTF	Dispozitivul dacă numele dispozitivului e specificat	*OBJOPR	*EXECUTE
	Fişier dischetă: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Fişier dischetă: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD, *EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTDSPF	Fişier sursă	*USE	*EXECUTE
	Dispozitivul dacă numele dispozitivului e specificat	*OBJOPR	*EXECUTE
	Fişierul specificat în cuvintele cheie REF şi REFFLD	*OBJOPR	*EXECUTE
	Fişier de afişare: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Fişier de afişare: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD, *EXECUTE
CRTICFF	Fişier sursă	*USE	*EXECUTE
	Fişierul specificat în cuvintele cheie REF şi REFFLD	*OBJOPR	*EXECUTE
	Fişier ICF: REPLACE(*NO)		*READ, *ADD
	Fişier ICF: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
CRTLF	Fişier sursă	*USE	*EXECUTE
	Fişierul specificat în cuvântul cheie PFILE sau JFILE, când fişierul logic este cu cheie	*OBJOPR, *OBJMGT sau *OBJALTER	*EXECUTE
	Fişierul specificat în cuvântul cheie PFILE sau JFILE, când fişierul logic nu este cu cheie	*OBJOPR	*EXECUTE
	Fişierele specificate în cuvintele cheie FORMAT şi REFACCPTH	*OBJOPR	*EXECUTE
	Tabele specificate în cuvântul cheie ALTSEQ	*OBJOPR	*EXECUTE
	Fişier logic		*EXECUTE, *ADD
	Fişierul la care se referă parametrul DTAMBRS, când fişierul logic este cu cheie	*OBJOPR, *OBJMGT sau *OBJALTER	*EXECUTE
	Fişierul la care se referă parametrul DTAMBRS, când fişierul logic nu este cu cheie	*OBJOPR	*EXECUTE
CRTPF	Fişier sursă	*USE	*EXECUTE
	Fişierele specificate în cuvintele cheie FORMAT şi REFFLD şi tabelele specificate în cuvântul cheie ALTSEQ	*OBJOPR	*EXECUTE
	Fişier fizic		*EXECUTE, *ADD
CRTPRTF	Fişier sursă	*USE	*EXECUTE
	Dispozitivul dacă numele dispozitivului e specificat	*OBJOPR	*EXECUTE
	Fişierele specificate în cuvintele cheie REF şi REFFLD	*OBJOPR	*EXECUTE
	Ieşire imprimantă: Replace(*NO)		*READ, *ADD, *EXECUTE
	Ieşire imprimantă: Replace(*YES)	Vedeţi regulile generale.	*READ, *ADD, *EXECUTE
CRTSAVF	Fişer de salvare		*READ, *ADD, *EXECUTE
CRTSRCPF	Fişier fizic sursă		*READ, *ADD, *EXECUTE

Comenzi fişier

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
CRTS36DSPF	Fişier-destinaţie sursă când TOMBR nu e *NONE	*ALL	*CHANGE
	Fişier sursă QS36SRC	*USE	*EXECUTE
	Fişier de afişare: REPLACE(*NO)		*READ, *ADD
	Fişier de afişare: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Comanda Creare fişier de afişare (CRTDSPF)	*OBJOPR	*EXECUTE
CRTTAPF	Fişier bandă: REPLACE(*NO)		*READ, *ADD
	Fişier bandă: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Dispozitivul dacă numele dispozitivului e specificat	*OBJOPR	*EXECUTE
DLTF	Fişier	*OBJOPR, *OBJEXIST	*EXECUTE
DSPCPCST	Fişierul bază de date care are contrângere în aşteptare	*OBJOPR, *READ	*EXECUTE
DSPDBR	Fişier bază de date	*OBJOPR	*EXECUTE
	Fişier sursă, dacă este specificat	Vedeţi regulile generale.	Vedeţi regulile generale.
DSPDDMF	Fişier DDM	*OBJOPR	
DSPDTA	Fişier date	*USE	*EXECUTE
	Program	*USE	*EXECUTE
	Fişier afişare	*USE	*EXECUTE
DSPFD [2]	Fişier	*OBJOPR	*EXECUTE
	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
	Fişierul este unul fizic şi se specifică TYPE(*ALL, *MBR, SAU *MBRLST)	O autorizare alta decât *EXECUTE	*EXECUTE
DSPFFD	Fişier	*OBJOPR	*EXECUTE
	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
DSPPFM	Fişier fizic	*USE	*EXECUTE
DSPSAVF	Fişer de salvare	*USE	*EXECUTE
EDTCPCST	Zona de date, aşa cum a fost specificată în cuvântul cheie NFYOBJ pentru comanda STRCMTCTL asociată.	*CHANGE	*EXECUTE
	Fişierele, aşa cum au fost specificate în cuvântul cheie NFYOBJ pentru comanda STRCMTCTL asociată.	*OBJOPR, *ADD	*EXECUTE
GENCAT	Fişier bază de date	*OBJOPR şi o autorizare pentru date alta decât *EXECUTE	*EXECUTE
INZPFM	Fişierul fizic, când se specifică RECORD(*DFT)	*OBJOPR, *OBJMGT sau *OBJALTER, *ADD	*EXECUTE
	Fişierul fizic, când se specifică RECORD(*DLT)	*OBJOPR, *OBJMGT sau *OBJALTER, *ADD, *DLT	*EXECUTE
MRGSRC	Fişier destinaţie	*CHANGE, *OBJMGT	*CHANGE
	Fişier întreţinere	*USE	*EXECUTE
	Fişier rădăcină (root)	*USE	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
OPNDBF	Fişier bază de date	*OBJOPR şi o autorizare pentru date alta decât *EXECUTE	*EXECUTE
OPNQRYF	Fişier bază de date	*OBJOPR şi o autorizare pentru date alta decât *EXECUTE	*EXECUTE
PRTTRGPGM [11]			
RGZPFM	Fişierul conţinând membrul	*OBJOPR, *OBJMGT sau *OBJALTER, *READ, *ADD, *UPD, *DLT, *EXECUTE	*EXECUTE
RMVICFDEVE	Fişier ICF	*OBJOPR, *OBJMGT	*EXECUTE
RMVM	Fişierul conţinând membrul	*OBJEXIST, *OBJOPR	*EXECUTE
RMVPFCST	Fişier	*OBJMGT sau *OBJALTER	*EXECUTE
RMVPFTRG	Fişier fizic	*OBJALTER, *OBJMGT	*EXECUTE
RNMM	Fişierul conţinând membrul	*OBJOPR, *OBJMGT	*EXECUTE, *UPD
RSTS36F [4] (Q)	În-fişier	*ALL	Vedeţi regulile generale.
	Fişier de-la	*USE	*EXECUTE
	Pe baza fişierului fizic, dacă fişierul care este restaurat este unul logic (alternativ)	*CHANGE	*EXECUTE
	Descrierea dispozitiv pentru dischetă sau bandă	*USE	*EXECUTE
RTVMBRD	Fişier	*USE	*EXECUTE
SAVSAVFDTA	Descriere bandă, dischetă sau unitate optică	*USE	*EXECUTE
	Fişer de salvare	*USE	*EXECUTE
	Fişier Salvare/Restaurare optic[8] (dacă cel anterior există)	*RW	Nu se aplică
	Directorul părinte al OPTFILE[8]	*WX	Nu se aplică
	Prefixul căii lui OPTFILE[8]	*X	Nu se aplică
	Director rădăcină (/) volum optic [8,9]	*RWX	Nu se aplică
	Volum optic[10]	*CHANGE	Nu se aplică
SAVS36F	Din-fişier	*USE	*EXECUTE
	În-fişier, atunci când este fişier fizic	*ALL	Vedeţi regulile generale.
	Fişier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
SAVS36LIBM	În-fişier, atunci când este fişier fizic	*ALL	Vedeţi regulile generale.
	Din-fişier	*USE	*EXECUTE
	Fişier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
STRAPF [3]	Fişier sursă	*OBJMGT, *CHANGE	*READ, *ADD
	Comenzi CRTPF, CRTLF, ADDPFM, ADDLFM şi RMVM	*USE	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
STRDFU [3]	Program (dacă se creează opţiune program)		*READ, *ADD
	Program (dacă există opţiunea de modificare sau ştergere program)	*OBJEXIST	*READ, *ADD
	File (dacă există opţiunea de modificare sau afişare date)	*OBJOPR, *ADD, *UPD, *DLT	*EXECUTE
	File (dacă există opţiunea de afişare date)	*READ	*EXECUTE
UPDDTA	Fişier	*CHANGE	*EXECUTE
WRKCMTDFN [1]			
WRKDDMF [3]	Fişier DDM	*OBJOPR, *OBJMGT, *OBJEXIST	*READ, *ADD
WRKF [3,5]	Fişiere	*OBJOPR	*USE
WRKPFCST[3]			*EXECUTE

1 Comanda CPYFRMQRYF foloseşte un parametru FROMOPNID, nu FROMFILE. Un utilizator trebuie să aibă suficientă autorizare pentru a executa comanda OPNQRYF înainte de a rula comanda CPYFRMQRYF. Dacă se specifică CRTFILE(*YES) în comanda CPYFRMQRYF, primul fişier specificat în parametrul corespondent OPNQRYF FILE este considerat a fi fişierul-sursă când se determină autorizările pentru noul fişier-destinaţie.

2 Este necesar drept de proprietate sau autorizare operaţională pentru fişier.

3 Pentru a folosi operaţii individuale, trebuie să aveţi autorizaţia cerută de operaţii individuale.

4 Dacă se creează un nou fişier şi există un deţinător de autorizare pentru el, atunci utilizatorul trebuie să aibă autorizarea toate (*ALL) pentru deţinătorul de autorizare sau să fie posesorul acestuia. Dacă nu există un deţinător de autorizare, proprietarul fişierului este utilizatorul care a introdus comanda RSTS36F şi autorizarea publică este *ALL.

5 E necesară aceeaşi autorizare pentru obiect.

6 Trebuie să aveţi autorizarea specială *ALLOBJ.

7 Autorizarea este verificată când este folosit fişierul DDM.

8 Această verificare de autorizare este făcută doar când formatul mediului de stocare optic este UDF (Universal Disk Format).

9 Această verificare de autorizare este făcută doar când ştergeţi volumul optic.

10 Volumele optice nu sunt obiecte sistem reale. Legătura între volumul optic şi lista de autorizare folosită pentru a securiza volumul este menţinută de funcţia de suport optic.

11 Trebuie să aveţi autorizaţia specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.

Comenzile pentru filtrare

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDALRACNE	Filtru	*USE, *ADD	*EXECUTE
ADDALRSLTE	Filtru	*USE, *ADD	*EXECUTE
ADDPRBACNE	Filtru	*USE, *ADD	*EXECUTE
ADDPRBSLTE	Filtru	*USE, *ADD	*EXECUTE
CHGALRACNE	Filtru	*USE, *UPD	*EXECUTE
CHGALRSLTE	Filtru	*USE, *UPD	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGFTR	Filtru	*OBJMGT	*EXECUTE
CHGPRBACNE	Filtru	*USE, *UPD	*EXECUTE
CHGPRBSLTE	Filtru	*USE, *UPD	*EXECUTE
CRTFTR	Filtru		*READ, *ADD
DLTFTR	Filtru	*OBJEXIST	*EXECUTE
RMVFTRACNE	Filtru	*USE, *DLT	*EXECUTE
RMVFTRSLTE	Filtru	*USE, *DLT	*EXECUTE
WRKFTR [1]	Filtru	Orice autorizaţie	*EXECUTE
WRKFTRACNE [1]	Filtru	*USE	*EXECUTE
WRKFTRSLTE [1]	Filtru	*USE	*EXECUTE
1 Pentru a folosi o operaţie individuală, trebuie să aveţi autorizaţia necesară de operaţie.			

Comenzile financiare

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
SBMFNCJOB (Q)	Descriere job şi coadă de mesaje [1]	*OBJOPR	*EXECUTE
SNDFNCIMG (Q)	Descriere job şi coadă de mesaje [1]	*OBJOPR	*EXECUTE
WRKDEVTBL (Q)	Descriere dispozitiv [1]	Cel puţin o autorizare pentru date	*EXECUTE
WRKPGMTBL (Q)			
WRKUSRTBL (Q)			
1 Profilul utilizator QFNC trebuie să aibă această autorizare.			

Operaţii grafice OS/400

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGFCNUSG[5]			
DSPFCNUSG			
EDTWSOAUT	Obiect staţie de lucru [1]	*OBJMGT [2,3,4]	*EXECUTE
GRTWSOAUT	Obiect staţie de lucru [1]	*OBJMGT [2,3,4]	*EXECUTE
RVKWSOAUT	Obiect staţie de lucru [1]	*OBJMGT [2,3,4]	*EXECUTE
SETCSTDTA	Profilul utilizator sursă copiere	*CHANGE	*EXECUTE
	Profilul utilizator destinaţie copiere	*CHANGE	*EXECUTE
WRKFCNUSG			

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci

[1] Obiectul staţie de lucru este un obiect intern care e creat când instalaţi opţiunea OS/400 Operaţii grafice. Este livrat cu autorizarea publică *USE.

[2] Trebuie să fiţi proprietar sau să aveţi autorizarea *OBJMGT şi autorizările care sunt acordate sau revocate.

[3] Trebuie să fiţi proprietar sau să aveţi autorizarea *ALLOBJ pentru a acorda autorizarea *OBJMGT sau *AUTLMGT.

[4] Pentru a securiza obiectul staţie de lucru cu o listă de autorizare sau pentru a o înlătura, trebuie să aveţi una din următoarele:

Să deţineţi obiectul staţie de lucru.

Să aveţi autorizare *ALL pentru obiectul staţie de lucru.

Să aveţi autorizarea specială *ALLOBJ.

[5] Trebuie să aveţi autorizarea specială administrator de securitate (*SECADM) pentru a modifica utilizarea acestei funcţii.

Comenzile pentru setul de simboluri grafice

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTGSS	Fişier sursă	*USE	*EXECUTE
	Set de simboluri grafice		*READ, *ADD
DLTGSS	Set de simboluri grafice	*OBJEXIST	*EXECUTE
WRKGSS [1]	Set de simboluri grafice	*OBJOPR	*USE

[1] Drept de proprietate sau unele autorizaţii pentru obiect sunt necesare.

Comenzile pentru server gazdă

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Aceste comenzi nu necesită nici o autorizare obiect.	
ENDHOSTSVR (Q)	STRHOSTSVR (Q)

Comenzile pentru imagine

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizaţie necesară pentru obiect
ADDIMGCLGE (Q)[1]				
CHGIMGCLG (Q)[1]				
CHGIMGCLGE (Q)[1]				
CRTIMGCLG (Q)[1]				

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizaţie necesară pentru obiect
DLTIMGCLG (Q)[1]				
LODIMGCLG (Q)[1]				
RMVIMGCLGE (Q)[1]				
VFYIMGCLG (Q)[1]				
WRKIMGCLGE (Q)[1]				
[1] Trebuie să aveţi autorizarea specială *ALLOBJ şi *SECADM pentru a folosi această comandă.				

Comenzile pentru sistem de fişiere integrat

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect[1]
ADDLNK	Obiect	*STMF	QOpenSys, ’root,’ UDFS	*OBJEXIST
	Părinte al noii legături	*DIR	QOpenSys, ’root,’ UDFS	*WX
	Prefix cale	Vedeţi regulile generale.		
CHGATR	Obiectul la setarea unui atribut, altul decât *USECOUNT, *ALWCKPWRT, *DISKSTGOPT,*MAINSTGOPT, *ALWSAV, *SCAN, *CRTOBJSCAN, *SETUID, *SETGID, *RSTRDRNMUNL	Orice	Toate exceptând QSYS.LIB	*W
	Obiectul la setarea *USECOUNT, *DISKSTGOPT, *MAINSTGOPT, *ALWSAV	Orice	Toate exceptând QSYS.LIB	*OBJMGT
		*FILE	QSYS.LIB	*OBJOPR, *OBJMGT
		*MBR	QSYS.LIB	*X, *OBJMGT (autorizare moştenită de la *FILE părinte)
		alt	QSYS.LIB	*OBJMGT
	Obiect la setarea *ALWCKPWRT	Orice	Toate	*OBJMGT
	Directorul care conţine obiecte când se specifică SUBTREE(*ALL)	Orice director	Toate	*RX
	Obiect la setarea următoarelor atribute: *CRTOBJSCAN sau *SCAN	*DIR şi *STMF	QOpenSys, ’root,’ UDFS	Vedeţi nota[26]
	Obiect la setarea următoarelor atribute: *SETUID, *SETGID, *RSTDRNMUNL	Orice	Toate exceptând QSYS.LIB şi QLDS	Drept de proprietate [15]
	Prefix cale	Vedeţi regulile generale.		
CHGAUD [4]				

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect[1]
CHGAUT	Obiect	Toate	QOpenSys, 'root,' UDFS	Drept de proprietate [15]
			QSYS.LIB, QOPT[11]	Drept de proprietate sau *ALLOBJ
			QDLS	Drept de proprietate, *ALL sau *ALLOBJ
				*OBJMGT
	Volum optic	*DDIR	QOPT[8]	*CHANGE
CHGCURDIR	Obiect	Orice director		*R
	Volum optic	*DDIR	QOPT[8]	*X
	Prefix cale	Vedeţi regulile generale.		
CHGOWN	Obiect	Toate	QSYS.LIB	*OBJEXIST
		*FILE, *LIB, *SBSD	QSYS.LIB	*OBJEXIST, *OBJOPR
		Toate	QOpenSys, 'root,' UDFS	Drept de proprietate şi *OBJEXIST[15]
		Toate	QDLS	Drept de proprietate sau *ALLOBJ
			QOPT[11]	Drept de proprietate sau *ALLOBJ
CHGOWN[24]	Profilul utilizator al vechiului proprietar—toate mai puţin QOPT, QDLS	*USRPRF	Toate	*DLT
	Profilul utilizator al noului proprietar—toate mai puţin QOPT, QDLS	*USRPRF	Toate	*ADD
	Volum optic	*DDIR	QOPT[8]	*CHANGE
CHGPGP	Obiect	Toate	QSYS.LIB	*OBJEXIST
		*FILE, *LIB, *SBSD	QSYS.LIB	*OBJEXIST, *OBJOPR
		Toate	QOpenSys, 'root,' UDFS	Drept de proprietate [5, 15]
		Toate	QDLS	Drept de proprietate sau *ALLOBJ
			QOPT[11]	Drept de proprietate sau *ALLOBJ

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect[1]
CHGPGP	Profilul utilizator al vechiului grup primar—toate exceptând QOPT, QDLS	*USRPRF	Toate	*DLT
	Profilul utilizator al noului grup primar—toate exceptând QOPT, QDLS	*USRPRF	Toate	*ADD
	Volum optic	*DDIR	QOPT[8]	*CHANGE
CHKIN	Obiect, dacă utilizatorul i-a anulat înregistrarea (check out).	*STMF	QOpenSys, ’root,’ UDFS	*W
		*DOC	QDLS	*W
	Obiect, dacă nu utilizatorul i-a anulat înregistrarea (check out).	*STMF	QOpenSys, ’root,’ UDFS	*ALL sau *ALLOBJ sau Drept de proprietate
		*DOC	QDLS	*ALL sau *ALLOBJ sau Drept de proprietate
	Cale, dacă nu e utilizatorul care l-a verificat.	*DIR	QOpenSys, ’root,’ UDFS	*X
	Prefix cale	Vedeţi regulile generale.		
CHKOUT	Obiect	*STMF	QOpenSys, ’root,’ UDFS	*W
		*DOC	QDLS	*W
	Prefix cale	Vedeţi regulile generale.		

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect[1]
CPY[25]	Obiectul care e copiat, obiectul origine	Orice	QOpenSys, 'root,' UDFS	*R şi *OBJMGT sau drept de proprietate
		*DOC	QDLS	*RWX şi *ALL sau drept de proprietate
		*MBR	QSYS.LIB	nici una
		alte	QSYS.LIB	*RX, *OBJMGT
		*DSTMF	QOPT[11]	*R
	Obiect destinaţie când e specificat REPLACE(*YES) (dacă obiectul destinaţie există deja)	Orice	Toate[10]	*W, *OBJEXIST, *OBJMGT
		*DSTMF	QOPT[11]	*W
		*LIB	QSYS.LIB	*RW, *OBJMGT, *OBJEXIST
		*FILE (PF sau LF)	QSYS.LIB	*RW, *OBJMGT, *OBJEXIST
		*DOC	QDLS	*RWX, *ALL
	Directorul copiat care conţine obiecte când e specificat SUBTREE(*ALL), ce duce la copierea conţinutul său	*DIR	QOpenSys, 'root,' UDFS	*RX, *OBJMGT
CPY[25]	Cale (destinaţie), directorul părinte al obiectului destinaţie	*FILE	QSYS.LIB	*RX, *OBJMGT
		*LIB	QSYS.LIB	*RX, *ADD
		*DIR	QOpenSys, 'root,' UDFS	*WX
		*FLR	QDLS	*RWX
		*DDIR	QOPT[11]	*WX
	Volum optic sursă	*DDIR	QOPT[8]	*USE
	Volum optic destionaţie	*DDIR	QOPT[8]	*CHANGE
CPY[25]	Director părinte al obiectului origine	*DIR	QOpenSys, 'root,' UDFS	*X
		*FLR	QDLS	*X
		Alte	QSYS.LIB	*RX
		*DDIR	QOPT[11]	*X
	Prefix cale (destinaţie destinaţie)	*LIB	QSYS.LIB	*WX
		*DIR	QOpenSys, 'root,' UDFS	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
	Prefix cale (obiect origine)	*DDIR	QOPT[11]	*X

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect[1]
CRTDIR[21, 22]	Director părinte	*DIR	QOpenSys, ’root,’ UDFS	*WX
		*FLR	QDLS	*CHANGE
		*FILE	QSYS.LIB	*RX, *ADD
		Orice		*ADD
		*DDIR	QOPT[11]	*WX
CRTDIR	Prefix cale	Vedeţi regulile generale.		
	Volum optic	*DDIR	QOPT[8]	*CHANGE
CVTDIR (Q)[16]				
DSPAUT	Obiect	Toate	QDLS	*ALL
		Toate	Toate celelalte	*OBJMGT sau drept de proprietate
		ALL	QOPT[11]	nici una
	Volum optic	*DDIR	QOPT[8]	*USE
	Prefix cale	Vedeţi regulile generale.		
DSPCURDIR	Prefix cale	*DIR	QOpenSys, ’root,’ UDFS	*RX
		*FLR	QDLS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*DIR		*R
		*DDIR	QOPT[11]	*RX
DSPCURDIR	Director curent	*DIR	QOpenSys, ’root,’ UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DIR		*R
		*DDIR	QOPT[11]	*X
	Volum optic	*DDIR*	QOPT[8]	*USE
DSPLNK	Orice	Orice	’root,’ QOpenSys, UDFS QSYS.LIB, QDLS, QOPT[11]	nici una
	Fişier, opţiunea 12 (Afişare legături)	*STMF, *SYMLNK, *DIR, *BLKSF, *SOCKET	’root,’ QOpenSys, UDFS	*R

Comenzi sistem de fişiere integrate

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect[1]
DSPLNK	Obiect legătură simbolic	*SYMLNK	'root,' QOpenSys, UDFS	nici una
	Volum optic	*DDIR	QOPT[8]	*USE
	Directorul părinte al obiectului referinţă - fără model [13]	*DIR	'root,' QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Directorul părinte al obiectului referinţă - model specificat[13]	*DIR	'root,' QOpenSys, UDFS	*R
		*LIB, *FILE	QSYS.LIB	*R
		*FLR	QDLS	*R
		*DDIR	QOPT[11]	*R
		*DDIR		*R
	Directorul părinte al obiectului referinţă-opţiunea 8 (Afişare atribute)	*DIR	'root,' QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Directorul părinte al obiectului referinţă-opţiunea 12 (Afişare legături)	*DIR	'root,' QOpenSys, UDFS	*RX
		*SYMLNK	'root,' QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Directorul părinte al obiectului referinţă - fără model [13]	*DIR	'root,' QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect[1]
DSPLNK	Prefixul obiectului referinţă părinte - model specificat[13]	*DIR	’root,’ QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Prefixul obiectului referinţă părinte - opţiunea 8 (Afişare atribute)	*DIR	’root,’ QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Prefixul obiectului referinţă părinte - opţiunea 12 (Afişare legături)	*DIR	’root,’ QOpenSys, UDFS	*RX
		*SYMLNK	’root,’ QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Nume cale relativă [14] : Directorul curent de lucru care conţine obiectul -Fără model[13]	*DIR	’root,’ QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Nume cale relativă [14] : Directorul curent de lucru care conţine obiectul -Model specificat[13]	*DIR	’root,’ QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R

Comenzi sistem de fişiere integrate

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect[1]
DSPLNK	Nume cale relativă [14] : Prefixul directorul curent de lucru care conţine obiectul -Fără model[13]	*DIR	'root,' QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
DSPLNK	Nume cale relativă [14] : Prefixul directorul curent de lucru care conţine obiectul -Model specificat[13]	*DIR	'root,' QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
DSPMFSINF	Obiect	Orice	Orice	nici una
	Prefix cale	Vedeţi regulile generale.		
ENDJRN	Obiect	*DIR dacă subarborele (*ALL)	QOpenSys, 'root,' UDFS	*R, *X, *OBJMGT
		*DIR dacă subarborele (*NONE), *SYMLNK, *STMF	QOpenSys, 'root,' UDFS	*R, *OBJMGT
		*DTAARA, *DTAQ	QSYS.LIB	*OBJOPR, *READ, *OBJMGT
	Director părinte	*DIR	QOpenSys, 'root,' UDFS	*X
		*LIB	QSYS.LIB	*X
	Prefix cale	Vedeţi regulile generale.		
	Jurnal			*OBJMGT, *OBJOPR
MOV[19]	Obiect mutat în interiorul aceluiaşi sistem de fişiere	*DIR	QOpenSys, 'root'	*OBJMGT, *W
		non *DIR	QOpenSys, 'root'	*OBJMGT
		*DOC	QDLS	*ALL
		*FILE	QSYS.LIB	*OBJOPR, *OBJMGT
		*MBR	QSYS.LIB	nici una
		alt	QSYS.LIB	nici una
		*STMF	QOPT[11]	*W

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect[1]
MOV	Cale (sursă), director părinte	*DIR	QOpenSys, 'root,' UDFS	*WX
		*FLR	QDLS	*RWX
		*FILE	QSYS.LIB, 'root'	*RX, *OBJEXIST
		alte	QOpenSys, 'root'	*RWX
	Cale (destinaţie), director părinte	*DIR	QSYS.LIB	*WX
		*FLR	QDLS	*CHANGE (*RWX)
		*FILE	QSYS.LIB	*X, *ADD, *DLT, *OBJMGT
		*LIB	QSYS.LIB	*RWX
		*DDIR	QOPT[11]	*WX
MOV	Prefix cale (destinaţie)	*LIB	QSYS.LIB	*X, *ADD
		*FLR	QDLS	*X
		*DIR	alte	*X
		*DDIR	QOPT[11]	*X
	Obiect mutat între sistemele de fişiere în QOpenSys, root sau QDLS (fişier flux *STMF şi *DOC, numai *MBR) .	*STMF	QOpenSys, 'root,' UDFS	*R, *OBJEXIST, *OBJMGT
		*DOC	QDLS	*ALL
		*MBR	QSYS.LIB	Nu se aplică
		*DSTMF	QOPT[11]	*RW
MOV	Mutat în QSYS *MBR	*STMF	QOpenSys, 'root,' UDFS	*R, *OBJMGT, *OBJEXIST
		*DOC	QDLS	*ALL
		*DSTMF	QOPT[11]	*RW
MOV	Cale (sursă) mutat prin sistemele de fişiere, director părinte	*DIR	QOpenSys, 'root,' UDFS	*WX
		*FLR	QDLS	*X
		*FILE	QSYS. LIB	drept de proprietate, *RX, *OBJEXIST
		*DDIR	QOPT[11]	*WX
	Prefix cale	Vedeţi regulile generale.		
	Volum optic (sursă şi destinaţie)	*DDIR	QOPT[8]	*CHANGE
RLSIFSLCK [18]	*some_stmf*	*STMF	″root″, QOpenSys, UDFS	*R
	Prefix cale	Vedeţi regulile generale.		

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect[1]
RMVDIR[19,20]	Director	*DIR	QOpenSys, 'root,' UDFS	*OBJEXIST
		*LIB	QSYS.LIB	*RX, *OBJEXIST
		*FILE	QSYS.LIB	*OBJOPR, *OBJEXIST
		*FLR	QDLS	*ALL
		*DDIR	QOPT[11]	*W
RMVDIR	Director părinte	*DIR	QOpenSys, 'root,' UDFS	*WX
		*FLR	QDLS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*DDIR	QOPT[11]	*WX
	Prefix cale	Vedeţi regulile generale.		
	Volum optic	*DDIR	QOPT[8]	*CHANGE
RMVLNK[19]	Obiect	*DOC	QDLS	*ALL
		*MBR	QSYS.LIB	
		*FILE	QSYS.LIB	*OBJOPR, *OBJEXIST
		*JRNRCV	QSYS.LIB	*OBJEXIST, *R
		alt	QSYS.LIB	*OBJEXIST
		*DSTMF	QOPT[11]	*W
		orice	QOpenSys, 'root,' UDFS	*OBJEXIST
RMVLNK	Director părinte	*FLR	QDLS	*X
		*FILE	QSYS.LIB	*X, *OBJEXIST
		*LIB	QSYS.LIB	*X
		*DIR	QOpenSys, 'root,' UDFS	*WX
		*DDIR	QOPT[11]	*WX
	Prefix cale	Vedeţi regulile generale.		
	Volum optic	*DDIR	QOPT[8]	*CHANGE

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect[1]
RNM[19]	Obiect	*DIR	QOpenSys, 'root,' UDFS	*OBJMGT, *W
		Non *DIR	QOpenSys, 'root,' UDFS	*OBJMGT
		*DOC, *FLR	QDLS	*ALL
		*MBR	QSYS.LIB	Nu se aplică
		*FILE	QSYS.LIB	*OBJMGT, *OBJOPR
		alte	QSYS.LIB	*OBJMGT
		*DSTMF	QOPT[11]	*W
	Volum optic (sursă şi destinaţie)	*DDIR	QOPT[8]	*CHANGE
RNM	Director părinte	*DIR	QOpenSys, 'root,' UDFS	*WX
		*FLR	QDLS	*CHANGE (*RWX)
		*FILE	QSYS.LIB	*X, *OBJMGT
		*LIB	QSYS.LIB	*X, *UPD
		*DDIR	QOPT[11]	*WX
	Prefix cale	*LIB	QSYS.LIB	*X, *UPD
		Orice	QOpenSys, 'root,' UDFS, QDLS	*X
RST (Q) [23]	Obiectul, dacă există[2]	Orice	QOpenSys, 'root,' UDFS	*W, *OBJEXIST
			QSYS.LIB	Variază [10]
			QDLS	*ALL
	Prefix cale	Vedeţi regulile generale.		
RST (Q)	Directorul părinte al obiectului care e restaurat[2]	*DIR	QOpenSys, 'root,' UDFS	*WX
	Directorul părinte al obiectului care e restaurat, dacă obiectul nu există[2]	*FLR	QDLS	*CHANGE
		*DIR		*OBJMGT, *OBJALTER, *READ, *ADD, *UPD
	Profilul utilizator care deţine obiectul nou restaurat[2]	*USRPRF	QSYS.LIB	*ADD
	Unitate de bandă, unitate de dischetă, unitate optică sau fişier de salvare	*DEVD, *FILE	QSYS.LIB	*RX

Comenzi sistem de fişiere integrate

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect[1]
RST (Q)	Bibliotecă pentru descrierea dispozitivului sau fişierul de salvare	*LIB	QSYS.LIB	*EXECUTE
	Fişier sursă, dacă este specificat	*STMF	QOpenSys, 'root,' UDFS	*W
		*USRSPC	QSYS.LIB	*RWX
	Prefix cale al fişierului ieşire	*DIR	QOpenSys, 'root,' UDFS	*X
		*LIB	QSYS.LIB	*RX
RST (Q)	Volumul optic dacă se restaurează de pe un dispozitiv optic	*DDIR	QOPT[8]	*USE
	Prefix cale optic şi părinte dacă se restaurează de pe un dispozitiv optic	*DDIR	QOPT[11]	*X
	Fişierul optic dacă se restaurează de pe un dispozitiv optic	*DSTMF	QOPT[11]	*R
RTVCURDIR	Prefix cale	*DIR	QOpenSys, 'root,' UDFS,QDLS, QOPT[11]	*RX
		*DDIR	QOPT[11]	*RX
		*FLR	QDLS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		Orice		*R
RTVCURDIR	Director curent	*DIR	QOpenSys, 'root,' UDFS,QOPT [11]	*X
		*DDIR	QOPT[11]	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		Orice		*R
SAV	Obiect[2]	Orice	QOpenSys, 'root,' UDFS	*R, *OBJEXIST
			QSYS.LIB	Variază [10]
			QDLS	*ALL
	Prefix cale	Vedeţi regulile generale.		
	Unitate de bandă, unitate de dischetă sau unitate optică	*DEVD	QSYS.LIB	*RX
SAV	Fişier de salvare, dacă e gol	*FILE	QSYS.LIB	*USE, *ADD
	Fişier de salvare, dacă nu e gol	*FILE	QSYS.LIB	*OBJMGT, *USE, *ADD
	Coadă de mesaje salvare-când-este-activ	*MSGQ	QSYS.LIB	*OBJOPR, *ADD
	Biblioteci pentru descrierea dispozitivului, fişierul ieşire, coadă de mesaje salvare-când-este-activ	*LIB	QSYS.LIB	*EXECUTE

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect[1]
SAV	Fişier sursă, dacă este specificat	*STMF	QOpenSys, 'root,' UDFS	*W
		*USRSPC	QSYS.LIB	*RWX
	Prefix cale al fişierului ieşire	*DIR	QOpenSys, 'root,' UDFS	*X
		*LIB	QSYS.LIB	*RX
SAV	Volumul optic, dacă se salvează pe dispozitiv optic	*DDIR	QOPT[8]	*CHANGE
	Prefix cale optic dacă se salvează pe dispozitiv optic	*DDIR	QOPT[11]	*X
	Director părinte optic, dacă se salvează pe dispozitiv optic	*DDIR	QOPT[11]	*WX
	Fişier optic (Dacă există deja)	*DSTMF	QOPT[11]	*RW
SAVRST	Pe sistemul sursă, aceeaşi autorizare ca cea necesară pentru comanda SAV.			
	Pe sistemul destinaţie, aceeaşi autorizare ca cea necesară pentru comanda RST.			
STATFS	Obiect	Orice	Orice	nici una
	Prefix cale	Vedeţi regulile generale.		
STRJRN	Obiect	*DIR dacă subarborele (*ALL)	QOpenSys, 'root,' UDFS	*R, *X, *OBJMGT
		*DIR dacă subarborele (*NONE), *SYMLNK, *STMF	QOpenSys, 'root,' UDFS	*R, *OBJMGT
		*DTAARA, *DTAQ	QSYS.LIB	*OBJOPR, *READ, *OBJMGT
	Director părinte	*DIR	QOpenSys, 'root,' UDFS	*X
		*LIB	QSYS.LIB	*X
	Prefix cale	Vedeţi regulile generale.		
	Jurnal	*JRN		*OBJMGT, *OBJOPR
WRKAUT[6, 7]	Obiect	*DOC sau *FLR	QDLS	*ALL
		Toate	not QDLS	*OBJMGT sau drept de proprietate
		*DDIR şi *DSTMF	QOPT[11]	*NONE
	Prefix cale	Vedeţi regulile generale.		
	Volum optic	*DDIR	QOPT[8]	*USE

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect[1]
WRKLNK	Orice	Orice	'root,' QOpenSys, UDFS, QSYS.LIB, QDLS, QOPT[11]	nici una
	Fişier, opţiunea 12 (Afişare legături)	*STMF, *SYMLNK, *DIR, *BLKSF, *SOCKET	'root,' QOpenSys, UDFS	*R
	Obiect legătură simbolic	*SYMLNK	'root,' QOpenSys, UDFS	nici una
	Volum optic	*DDIR	QOPT[8]	*USE
WRKLNK	Directorul părinte al obiectului referinţă - fără model [13]	*DIR	'root,' QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Directorul părinte al obiectului referinţă - Model specificat	*DIR	'root,' QOpenSys, UDFS	*R
		*LIB *FILE	QSYS.LIB	*R
		*FLR	QDLS	*R
		*DDIR	QOPT[11]	*R
		*DDIR		*R
WRKLNK	Directorul părinte al obiectului referinţă-opţiunea 8 (Afişare atribute)	*DIR	'root,' QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Directorul părinte al obiectului referinţă-opţiunea 12 (Afişare legături)	*DIR	'root,' QOpenSys, UDFS	*RX
		*SYMLNK	'root,' QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect[1]
WRKLNK	Directorul părinte al obiectului referinţă - fără model [13]	*DIR	'root,' QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Prefixul obiectului referinţă părinte - model specificat[13]	*DIR	'root,' QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Prefixul obiectului referinţă părinte - opţiunea 8 (Afişare atribute)	*DIR	'root,' QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Prefixul obiectului referinţă părinte - opţiunea 12 (Afişare legături)	*DIR	'root,' QOpenSys, UDFS	*RX
		*SYMLNK	'root,' QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Comenzi sistem de fişiere integrate

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect[1]
WRKLNK	Nume cale relativă [14] : Directorul curent de lucru care conţine obiectul -Fără model[13]	*DIR	'root,' QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Nume cale relativă [14] : Directorul curent de lucru care conţine obiectul -Model specificat[13]	*DIR	'root,' QOpenSys, UDFS	*RX
		*LIB *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
WRKLNK	Nume cale relativă [14] : Prefixul directorul curent de lucru care conţine obiectul -Fără model[13]	*DIR	'root,' QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
	Nume cale relativă [14] Prefixul directorul curent de lucru care conţine obiectul -Model specificat[13]	*DIR	'root,' QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R

1 Autoritatea adoptată nu este folosită pentru comenzile sistemului de fişiere integrat.

2 Dacă aveţi autorizarea specială *SAVSYS, nu aveţi nevoie de autorizarea specificată pentru sistemele de fişiere QSYS.LIB, QDLS, QOpenSys şi ″root″.

3 Autorizarea necesară variază în funcţie de tipul obiectului. Vedeţi descrierea API-ului QLIRNMO în Centrul de informare. Dacă obiectul este un membru bază de date, vedeţi autorizările pentru comanda RNMM (Rename Member - Redenumire membru).

4 Trebuie să aveţi autorizarea specială *AUDIT pentru a modifica un volum de auditare.

5 Dacă utilizatorul care lansează comanda nu are autorizare *ALLOBJ, el trebuie să fie un membru a noului grup primar.

6 Această comandă nu este suportată pentru sistemul de fişiere QLANSrv.

7 Aceste comenzi necesită ca autorizarea afişată plus autorizările necesare pentru comanda DSPCURDIR.

8 Volumele optice nu sunt obiecte sistem reale. Legătura între volumul optic şi lista de autorizare folosită pentru a securiza volumul este menţinută de funcţia de suport optic.

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizare necesară pentru obiect[1]

[9] Pentru informaţii despre restricţii privind această comandă, vedeţi Capitolul 7 din cartea Suportul optic iSeries.

[10] Autorizarea necesară variază după comanda nativă folosită. Vedeţi comanda respectivă SAVOBJ sau RSTOBJ pentru autorizarea necesară.

[11] Autorizarea cerută de QOPT pentru mediul de stocare formatat în UDF (Universal Disk Format).

[12] *ADD este necesară doar când obiectul mutat este un *MRB.

[13] Model: În unele comenzi, poate fi folosit un asterisc (*) sau un semn de întrebare (?) în ultima parte a numelui căii, pentru a căuta nume care se potrivesc unui model.

[14] Nume cale relativă: Dacă un nume cale nu începe cu un slash, predecesorul primei componente a numelui căii este luat ca fiind directorul curent de lucru al procesului. De exemplu, dacă un nume cale de 'a/b' este specificată şi directorul curent de lucru este '/home/john', atunci obiectul accesat este '/home/john/a/b'.

[15] Dacă aveţi autorizarea specială *ALLOBJ, nu aveţi nevoie de autorizarea menţionată.

[16] Trebuie să aveţi autorizaţia specială *ALLOBJ pentru a folosi această comandă.

[17] În tabelul de mai sus, QSYS.LIB se referă la sistemul de fişiere QSYS.LIB al ASP-ului independent, precum şi la sistemul de fişiere QSYS.LIB.

[18] Pentru a folosi această comandă, trebuie să aveţi autorizaţia specială *IOSYSCFG.

[19] Dacă atributul redenumiri şi dezlegări restricţionate (cunoscut de asemenea ca bit S_ISVTX) este activat pentru un director, va restricţiona dezlegarea cobiectelor de la acel director, numai dacă una din aceste autorizări nu e îndeplinită: *ALLOBJ; utilizatorul este deţinătorul obiectului dezlegat; sau utilizatorul este proprietarul directorului.

[20] Dacă se specifică RMVLNK (*YES), utilizatorul trebuie să aibă autorizarea *OBJEXIST pentru toate obiectele din directorul specificat.

[21] Pentru QSYS.LIB, 'root', QOpenSys şi sisteme de fişiere definite de utilizator, este necesară autorizarea specială (*AUDIT) dacă este specificată o altă valoare decât *SYSVAL pentru parametrul CRTOBJAUD.

[22] Utilizatorul trebuie să aibă autorizările speciale *ALLOBJ (toate obiectele) şi *SECADM (administrator securitate) pentru a specifica o valoare pentru parametrul CRTOBJSCAN (opţiunea Scanare pentru obiecte) alta decât *PARENT.

[23] Trebuie să aveţi autorizarea specială *ALLOBJ pentru a specifica altă valoare decât *NONE pentru parametrul ALWOBJDIF.

[24] Utilizatorul trebuie să aibă autorizarea specială *ALLOBJ şi *SECADM când schimbă proprietarul unui fişier flux (*STMF) cu un program Java ataşat a cărui verificare de autoritate în timpul rulării include utilizatorul şi proprietarul.

[25] Utilizatorul trebuie să aibă autorizarea specială *ALLOBJ şi *SECADM când copiază un fişier flux (*STMF) cu un program Java ataşat a cărui verificare de autoritate în timpul rulării include utilizatorul şi proprietarul.

[26] Utilizatorul trebuie să aibă autorizarea specială *ALLOBJ şi *SECADM pentru a specifica atributele *CRTOBJSCAN şi *SCAN.

Comenzile pentru definirea interactivă a datelor

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDDTADFN	Dicţionar de date	*CHANGE	*EXECUTE
	Fişier	*OBJOPR, *OBJMGT	*EXECUTE
CRTDTADCT	Dicţionar de date		*READ, *ADD
DLTDTADCT [3]	Dicţionar de date	OBJEXIST, *USE	
DSPDTADCT	Dicţionar de date	*USE	*EXECUTE

Comenzi de definire interactivă a datelor

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
LNKDTADFN [1]	Dicţionar de date	*USE	*EXECUTE
	Fişier	*OBJOPR, *OBJMGT	*EXECUTE
STRIDD			
WRKDTADCT [2]	Dicţionar de date	*OBJOPR	*EXECUTE
WRKDBFIDD [2]	Dicţionar de date	*USE [4]	*EXECUTE
	Fişier bază de date	*OBJOPR	*EXECUTE
WRKDTADFN [1]	Dicţionar de date	*USE, *CHANGE	*EXECUTE

1 Nu e necesară autorizare pentru dicţionarul de date pentru a dezlega un fişier.

2 Pentru a folosi operaţii individuale, trebuie să aveţi autorizaţia cerută de operaţii individuale.

3 Înainte ca dicţionarul să fie şters, toate fişierele legate sunt dezlegate. Consultaţi comanda LNKDTADFN pentru autorizarea necesară pentru a dezlega un fişier.

4 Aveţi nevoie de autorizarea de utilizare pentru dicţionarul de date pentru a crea un nou fişier. Nu e necesară nici o autorizare pentru dicţionarul de date pentru a introduce date într-un fişier existent.

Comenzile IPX (Internetwork packet exchange)

Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DLTIPXD	Descriere IPX	*OBJEXIST	*EXECUTE
DSPIPXD	Descriere IPX	*USE	*EXECUTE
WRKIPXD	Descriere IPX	*OBJOPR	*EXECUTE

Comenzile pentru index de căutare informaţii

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDSCHIDXE	Index de căutare	*CHANGE	*USE
	Grup de panouri	*USE	*EXECUTE
CHGSCHIDX	Index de căutare	*CHANGE	*USE
CRTSCHIDX	Index de căutare		*READ, *ADD
DLTSCHIDX	Index de căutare	*OBJEXIST	*EXECUTE
RMVSCHIDXE	Index de căutare	*CHANGE	*USE
STRSCHIDX	Index de căutare	*USE	*EXECUTE
WRKSCHIDX [1]	Index de căutare	*ANY	*USE
WRKSCHIDXE	Index de căutare	*USE	*USE

1 Această comandă nu este suportată pentru sistemul de fişiere QLANSrv.

Comenzile pentru atribute IPL

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Aceste comenzi nu necesită autorizare pentru nici un obiect:
CHGIPLA (Q) [1] DSPIPLA
[1] Pentru a folosi această comandă trebuie să aveţi autorizările speciale *SECADM şi *ALLOBJ.

Comenzile pentru Java

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ANZJVM	Comandă QSYS/STRSRVJOB	*USE	
	Comandă QSYS/STRDBG	*USE	

Comenzile pentru job

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
BCHJOB	Descriere job [9,11]	*USE	*EXECUTE
	Bibliotecile din lista de biblioteci (sistem, curent şi utilizator)[7]	*USE	
	Profil utilizator din descrierea jobului [10]	*USE	
	Tabelă secvenţă de sortare[7]	*USE	*EXECUTE
	Coadă de mesaje [10]	*USE, *ADD	*EXECUTE
	Coadă de joburi [10,11]	*USE	*EXECUTE
	Coadă de ieşire [7]	*READ	*EXECUTE
CHGACGCDE [1]			
CHGGRPA [4]	Coada de mesaje dacă se asociază o coadă de mesaje cu un grup	*OBJOPR	*EXECUTE
CHGJOB [1,2,3]	Coadă nouă de mesaje, dacă se modifică coada de mesaje[10,11]	*USE	*EXECUTE
	Coadă nouă de ieşire, dacă se modifică coada de ieşire[7]	*READ	*EXECUTE
	Coada de ieşire curentă, dacă se modifică[7]	*READ	*EXECUTE
	Tabelă secvenţă de sortare[7]	*USE	*EXECUTE
CHGPJ	Profil utilizator pentru pornire program necesită specificarea *PGMSTRRQS	*USE	*EXECUTE
	Profil utilizator şi descriere job	*USE	*EXECUTE

Comenzi job

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
CHGSYSJOB(Q) [13]			
CHGUSRTRC[14]	Buffer-ul urmărire utilizator când e folosit CLEAR (*YES).[15]	*OBJOPR	*EXECUTE
	Buffer-ul urmărire utilizator când e folosit MAXSTG[15]	*CHANGE, *OBJMGT	*USE
	Buffer-ul urmărire utilizator când e folosit FULL. [15]	*OBJOPR	*EXECUTE
DLTUSRTRC	Buffer urmărire utilizator [15]	*OBJOPR, *OBJEXIST	*EXECUTE
DLYJOB [4]			
DMPUSRTRC	Buffer urmărire utilizator [15]	*OBJOPR	*EXECUTE
DSCJOB [1]			
DSPACTPJ			
DSPJOB [1]			
DSPJOBTBL			
DSPJOBLOG [1,5]	Fişierul de ieşire şi membrul există	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	Membrul nu există	*OBJOPR, *OBJMGT, *ADD	*EXECUTE, *ADD
	Fişierul de ieşire nu există	*OBJOPR	*EXECUTE, *ADD
ENDGRPJOB			
ENDJOB [1]			
ENDJOBABN [1]			
ENDPJ [6]			
HLDJOB [1]			
RLSJOB [1]			
RRTJOB			
RTVJOBA			
SBMDBJOB	Fişier bază de date	*USE	*EXECUTE
	Coadă joburi	*READ	*EXECUTE
SBMDKTJOB	Coadă de ieşire	*USE, *ADD	*EXECUTE
	Coadă de joburi şi descriere dispozitiv	*READ	*EXECUTE
SBMJOB [2, 12]	Descriere job [9,11]	*USE	*EXECUTE
	Bibliotecile din lista de biblioteci (sistem, curent şi utilizator)[7]	*USE	
	Coadă de mesaje [10]	*USE, *ADD	*EXECUTE
	Profilul utilizator [10,11]	*USE	
	Profil utilizator din descrierea jobului [10]	*USE (la nivel 40)	
	Coadă de joburi [10,11]	*USE	*EXECUTE
	Coadă de ieşire [7]	*READ	*EXECUTE
	Tabelă secvenţă de sortare[7]	*USE	*EXECUTE
	Dispozitive ASP din grupul ASP iniţial	*USE	

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
SBMNETJOB	Fişier bază de date	*USE	*EXECUTE
STRPJ [6]	Descriere subsistem	*USE	
	Program		*EXECUTE
TFRBCHJOB	Coadă joburi	*READ	*EXECUTE
TFRGRPJOB	Program primul grup	*USE	*EXECUTE
TFRJOB [8]	Coadă joburi	*USE	*EXECUTE
	Descrierea subsistemului la care e alocată coada de joburi	*USE	
TFRSECJOB			
WRKACTJOB			
WRKJOB [1]			
WRKSBMJOB			
WRKSBSJOB			
WRKUSRJOB			

1 Orice utilizator poate rula aceste comenzi pentru joburi care rulează sub propriul său profil utilizator. Un utilizator cu autorizarea specială control job (*JOBCTL) poate rula aceste comenzi pentru orice job. Dacă aveţi autorizarea specială *SPLCTL, nu aveţi nevoie de nici o autorizare pentru coada de joburi. Totuşi, aveţi nevoie de autorizare pentru biblioteca care conţine coada de joburi.

2 Trebuie să aveţi autorizare (specificată în profilul dumneavostră utilizator) pentru prioritatea de planificare şi prioritatea de ieşire specificate.

3 Pentru a modifica anumite atribute de joburi, chiar în propriul job al utilizatorului, e necesară autorizarea specială control job (*JOBCTL). Aceste atribute sunt RUNPTY, TIMESLICE, PURGE, DFTWAIT şi TSEPOOL.

4 Această comandă afişează doar jobul în care a fost specificată.

5 Pentru a afişa un istoric de job pentru un job care are autorizarea specială toate obiectele (*ALLOBJ), trebuie să aveţi autorizarea specială *ALLOBJ sau să fiţi autorizat pentru funcţia Istoric job pentru toate obiectele OS/400 prin suportul de Administrare aplicaţie al Navigatorului iSeries. Se poate folosi comanda CHGFCNUSG (Change Function Usage), cu un ID funcţie de QIBM_ACCESS_ALLOBJ_JOBLOG, pentru a modifica lista de utilizatori cărora le este permis să afişeze un istoric de job pentru un job cu autorizarea specială *ALLOBJ.

6 Pentru a folosi această comandă, e necesară autorizarea specială control job *JOBCTL.

7 Profilul utilizator sub care rulează jobul lansat este verificat pentru autorizare pentru obiectul referinţă. Autorizarea adoptată a utilizatorului care lansează sau modifică jobul nu e folosită.

8 Dacă jobul transferat este unul interactiv, se aplică următoarele restricţii:

- Coada de joburi în care e plasat jobul trebuie să fie asociată cu un subsistem activ.
- Staţia de lucru asociată cu jobul trebuie să aibă o intrare de staţie de lucru corespondentă în descrierea de subsistem asociată cu noul subsistem.
- Staţia de lucru asociată cu jobul nu trebuie să aibă alt job asociat cu ea care să fi fost suspendat prin intermediul tastei SysReq (cerere sistem). Jobul suspendat trebuie să fie anulat înainte de a putea rula comanda Transferare job.
- Jobul nu trebuie să fie un job de grup.

9 Atât utilizatorul care lansează jobul cât şi profilul utilizator sub care rulează jobul sunt verificate pentru autorizare pentru obiectul referinţă.

10 Utilizatorul care lansează jobul este verificat pentru autorizare pentru obiectul referinţă.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
[11] E folosită autorizarea adoptată a utilizatorului care lansează comanda CHGJOB sau SBMJOB.			
[12] Trebuie să fiţi autorizat pentru profilul utilizator şi descrierea jobului; profilul utilizator trebuie să fie de asemenea autorizat pentru descrierea jobului.			
[13] Pentru a modifica anumite atribute ale jobului, chiar în propriul job al utilizatorului, sunt necesare autorizările speciale de control job (*JOBCTL) şi toate obiectele (*ALLOBJ).			
[14] Orice utilizator poate rula aceste comenzi pentru joburi care rulează sub propriul său profil utilizator. Un utilizator cu autorizarea specială control job (*JOBCTL) poate rula aceste comenzi pentru orice job.			
[15] Un buffer de urmărire utilizator este un obiect spaţiu utilizator (*USRSPC) din biblioteca QUSRSYS, cu numele QPOZ*nnnnnn*, unde '*nnnnnn*' este numărul jobului care foloseşte facilitatea de urmărire utilizator.			

Comenzile pentru descriere de job

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGJOBD	Descriere job	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Profil utilizator (USER)	*USE	*EXECUTE
CPYAUDJRNE[8]	Fişierul de ieşire deja există	*OBJOPR *OBJMGT *ADD *DLT	*EXECUTE
	Fişierul de ieşire nu există		*EXECUTE *ADD
CRTJOBD (Q)	Descriere job		*READ, *ADD
	Profil utilizator (USER)	*USE	*EXECUTE
DLTJOBD	Descriere job	*OBJEXIST	*EXECUTE
DSPJOBD	Descriere job	*OBJOPR, *READ	*EXECUTE
PRTJOBDAUT [1]			
WRKJOBD	Descriere job	Orice	*USE
[1] Trebuie să aveţi autorizaţia specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.			

Comenzile pentru coadă de joburi

Comanda	Obiect referinţă	Parametri coadă de joburi [4]		Autorizaţie specială	Autorizaţie necesară	
		AUTCHK	OPRCTL		Pentru obiect	Pentru biblioteci
CLRJOBQ [1]	Coadă joburi	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CRTJOBQ [1]	Coadă joburi					*READ, *ADD
DLTJOBQ	Coadă joburi				*OBJEXIST	*EXECUTE

Comanda	Obiect referinţă	Parametri coadă de joburi [4]		Autorizaţie specială	Autorizaţie necesară	
		AUTCHK	OPRCTL		Pentru obiect	Pentru biblioteci
HLDJOBQ [1]	Coadă joburi	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
PRTQAUT [5]						
RLSJOBQ [1]	Coadă joburi	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKJOBQ [1,3]	Coadă joburi	*DTAAUT			*READ	*EXECUTE
		*OWNER			Proprietar [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE

1 Dacă aveţi autorizarea specială *SPLCTL, nu aveţi nevoie de nici una pentru coada de joburi, dar aveţi nevoie de autorizare pentru biblioteca care conţine coada de joburi.

2 Trebuie să fiţi proprietarul cozii de joburi.

3 Dacă cereţi să lucraţi cu toate cozile de joburi, ecranul listă include toate cozile de joburi din biblioteci pentru care aveţi autorizare *EXECUTE.

4 Pentru a afişa parametrii cozii de joburi, folosiţi API-ul QSPRJOBQ.

5 Trebuie să aveţi autorizaţia specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.

Comenzile pentru planificarea joburilor

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDJOBSCDE	Planificare job	*CHANGE	*EXECUTE
	Descriere job [1]	*USE	*EXECUTE
	Coadă de joburi [1,2]	*READ	*EXECUTE
	Ptofil utilizator	*USE	*EXECUTE
	Coadă de mesaje [1]	*USE, *ADD	*EXECUTE
CHGJOBSCDE [3]	Planificare job	*CHANGE	*EXECUTE
	Descriere job [1]	*USE	*EXECUTE
	Coadă de joburi [1,2]	*READ	*EXECUTE
	Ptofil utilizator	*USE	*EXECUTE
	Coadă de mesaje [1]	*USE, *ADD	*EXECUTE
HLDJOBSCDE [3]	Planificare job	*CHANGE	*EXECUTE
RLSJOBSCDE [3]	Planificare job	*CHANGE	*EXECUTE
RMVJOBSCDE [3]	Planificare job	*CHANGE	*EXECUTE
WRKJOBSCDE [4]	Planificare job	*USE	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci

[1] Atât profilul utilizat care adaugă intrarea, cât şi cel sub care rulează jobul sunt verificate pentru autorizare pentru obiectul referinţă.

[2] Autorizarea pentru coada de joburi nu poate veni din autorizare adoptată.

[3] Trebuie să aveţi autorizarea specială *JOBCTL sau să fi adăugat intrarea.

[4] Pentru a afişa detaliile unei intrări (opţiunea 5 sau formatul de tipărire *FULL), trebuie să aveţi autorizarea specială *JOBCTL sau să fi adăugat intrarea.

Comenzile pentru jurnal

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă sau director
ADDRMTJRN	Jurnal sursă	*CHANGE, *OBJMGT	*EXECUTE
	Jurnal destinaţie		*EXEC, *ADD
APYJRNCHG (Q)	Jurnal	*USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
	Obiecte non-IFS ale căror modificări jurnalizate sunt aplicate	*OBJMGT, *CHANGE, *OBJEXIST	*EXECUTE, *ADD
	Obiecte IFS ale căror modificări jurnalizate sunt aplicate	*RW, *OBJMGT	*RX dacă subarborele (*ALL)
APYJRNCHGX	Jurnal	*USE	
	Receptor jurnal	*USE	
	Fişier	*OBJMGT, *CHANGE, *OBJEXIST’	*EXECUTE, *ADD
CHGJRN (Q)	Receptor jurnal, dacă se specifică	*OBJMGT, *USE	*EXECUTE
	Receptor jurnal ataşat	*OBJMGT, *USE	*EXECUTE
	Jurnal	*OBJOPR, *OBJMGT, *UPD	*EXECUTE
	Jurnal dacă se specifică RCVSIZOPT(*MINFIXLEN).	*OBJOPR, *OBJMGT, *UPD, *OBJALTER	*EXECUTE
CHGJRNOBJ [9]		*OBJOPR, *OBJMGT	
	Obiecte non-IFS	*READ, *OBJMGT	
	Obiecte IFS *R	*OBJMGT	
	Cale obiect SUBTREE(*ALL) *RX	*OBJMGT	
	Cale obiect SUBTREE(*NONE) *R	*OBJMGT	
	Director părinte *X		
CHGRMTJRN	Jurnal sursă	*CHANGE, *OBJMGT	*EXECUTE
	Jurnal sursă	*USE, *OBJMGT	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru bibliotecă sau director**
CMPJRNIMG	Jurnal	*USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
	Fişier	*USE	*EXECUTE
CRTJRN	Jurnal		*READ, *ADD
	Receptor jurnal	*OBJOPR, *OBJMGT, *READ	*EXECUTE
DLTJRN	Jurnal	*OBJOPR, *OBJEXIST	*EXECUTE
DSPAUDJRNE[8]			
DSPJRN [6]	Jurnal	*USE	*EXECUTE
	Jurnal dacă se specifică FILE(*ALLFILE), fişierul specificat a fost şters din sistem sau se specifică *IGNFILSLT pentru orice coduri de jurnal selectate sau jurnalul este unul la distanţă.	*OBJEXIST, *USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
	Fişier, dacă se specifică	*USE	*EXECUTE
	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
DSPJRNMNU[1]			
ENDJRN	Vedeţi “Comenzile pentru sistem de fişiere integrat” la pagina 335.		
ENDJRNAP	Jurnal	*OBJOPR, *OBJMGT	*EXECUTE
	Fişier	*OBJOPR, *OBJMGT	*EXECUTE
ENDJRNOBJ	Jurnal	*OBJOPR, *OBJMGT	*EXECUTE
	Obiect	*OBJOPR, *READ, *OBJMGT	*EXECUTE
ENDJRNPF	Jurnal	*OBJOPR, *OBJMGT	*EXECUTE
	Fişier	*OBJOPR, *OBJMGT, *READ	*EXECUTE
JRNAP [2]			
JRNPF [3]			
RCVJRNE	Jurnal	*USE	*EXECUTE
	Jurnal dacă se specifică FILE(*ALLFILE), fişierul specificat a fost şters din sistem sau se specifică *IGNFILSLT pentru orice coduri de jurnal selectate sau jurnalul este unul la distanţă.	*OBJEXIST, *USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
	Fişier	*USE	*EXECUTE
	Program ieşire	*EXECUTE	*EXECUTE
RMVJRNCHG (Q)	Jurnal	*USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
	Obiecte non-IFS ale căror modificări jurnalizate sunt înlăturate	*OBJMGT, *CHANGE	*EXECUTE

Comenzi jurnal

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru bibliotecă sau director**
RTVJRNE	Jurnal	*USE	*EXECUTE
	Jurnal dacă se specifică FILE(*ALLFILE), fişierul specificat a fost şters din sistem sau se specifică *IGNFILSLT pentru orice coduri de jurnal selectate sau jurnalul este unul la distanţă.	*OBJEXIST, *USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
	Fişier	*USE	*EXECUTE
RMVRMTJRN	Jurnal sursă	*CHG, *OBJMGT	
SNDJRNE	Jurnal	*OBJOPR, *ADD	*EXECUTE
	Obiect non-IFS dacă se specifică	*OBJOPR	*EXECUTE
	Obiect IFS dacă se specifică	*R	*X
STRJRN	Vedeţi “Comenzile pentru sistem de fişiere integrat” la pagina 335.		
STRJRNAP	Jurnal	*OBJOPR, *OBJMGT	*EXECUTE
	Fişier	*OBJOPR, *OBJMGT	*EXECUTE
STRJRNPF	Jurnal	*OBJOPR, *OBJMGT	*EXECUTE
	Fişier	*OBJOPR, *OBJMGT	*EXECUTE
STRJRNOBJ	Jurnal	*OBJOPR, *OBJMGT	*EXECUTE
	Obiect	*OBJOPR, *READ, *OBJMGT	*EXECUTE
WRKJRN [4] (Q)	Jurnal	*USE	*READ[7]
	Receptor jurnal dacă e cerută informaţia receptorului	*USE	*EXECUTE
	Fişierul dacă e cerută recuperarea înainte sau înapoi	*OBJMGT, *CHANGE	*EXECUTE
	Obiecte care sunt şterse în timpul recuperării	*OBJEXIST	*EXECUTE
WRKJRNA [6]	Jurnal	*OBJOPR şi o autorizare pentru date alta decât *EXECUTE	*EXECUTE
	Receptor jurnal [5]	*OBJOPR şi o autorizare pentru date alta decât *EXECUTE	*EXECUTE

1 Vedeţi comanda WRKJRN (această comandă are aceeaşi funcţie)

2 Vedeţi comanda STRJRNAP.

3 Vedeţi comanda STRJRNPF.

4 E necesară autorizare suplimentară pentru funcţii specifice apelate în timpul operaţiei selectate. De exemplu, pentru a restaura un obiect trebuie să aveţi autorizarea necesară pentru comanda RSTOBJ.

5 Sune necesare autorizările *OBJOPR şi *OBJEXIST pentru receptori jurnal dacă opţiunea este aleasă pentru a şterge receptori.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă sau director

[6] Pentru a specifica JRN(*INTSYSJRN), trebuie să aveţi autorizarea specială *ALLOBJ.

[7] E necesară autorizarea *READ pentru biblioteca jurnalului pentru a afişa meniul WRKJRN. E necesară autorizarea *EXECUTE pentru bibliotecă pentru a folosi o opţiune din meniu.

[8] Trebuie să aveţi autorizaţia specială *AUDIT pentru a folosi această comandă.

[9] Pentru a specifica PTLTNS(*ALWUSE), trebuie să aveţi autorizarea specială *ALLOBJ.

Comenzile pentru receptor de jurnal

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTJRNRCV	Receptor jurnal		*READ, *ADD
DLTJRNRCV	Receptor jurnal	*OBJOPR, *OBJEXIST şi o autorizare pentru date alta decât *EXECUTE	*EXECUTE
	Jurnal	*OBJOPR	*EXECUTE
DSPJRNRCVA	Receptor jurnal	*OBJOPR şi o autorizare pentru date alta decât *EXECUTE	*EXECUTE
	Jurnal, dacă e ataşat	*OBJOPR	*EXECUTE
WRKJRNRCV [1], [2], [3]	Receptor jurnal	Orice autorizaţie	*USE

[1] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizaţia necesară de operaţie.

[2] Sune necesare autorizările *OBJOPR şi *OBJEXIST pentru receptori jurnal dacă opţiunea este aleasă pentru a şterge receptori.

[3] Sunt necesare *OBJOPR şi altă autorizare de date decât *EXECUTE pentru receptorii de jurnal dacă este aleasă opţiunea de afişare descriere.

Comenzile pentru limbaj

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTBNDC	Fişier sursă	*USE	*EXECUTE
	Fişiere dispozitiv descrise extern şi fişiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Directorul specificat în parametrii OUTPUT, PPSRCSTMF sau MAKEDEP	*USE	*EXECUTE
	Fişierul specificat în parametrii OUTPUT, PPSRCSTMF sau MAKEDEP	Vedeţi regulile generale.	*READ, *ADD

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
CRTBNDCBL	Fişier sursă	*USE	*EXECUTE
	Fişiere dispozitiv descrise extern şi fişiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Director legare	*USE	*EXECUTE
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTBNDCL	Fişier sursă	*USE	*EXECUTE
	Fişiere dispozitiv descrise extern şi fişiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	Vedeţi regulile generale.
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTBNDCPP	Fişier sursă	*USE	*EXECUTE
	Fişiere dispozitiv descrise extern şi fişiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Directorul specificat în parametrii OUTPUT, PPSRCSTMF, TEMPLATE sau MAKEDEP	*USE	*EXECUTE
	Fişierul specificat în parametrii OUTPUT, PPSRCSTMF, TEMPLATE sau MAKEDEP	Vedeţi regulile generale.	*READ, *ADD
	Anteturi generate de parametrul TEMPLATE	*USE	*EXECUTE
CRTBNDRPG	Fişier sursă	*USE	*EXECUTE
	Fişiere dispozitiv descrise extern şi fişiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Director legare	*USE	*EXECUTE
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTCBLMOD	Fişier sursă	*USE	*EXECUTE
	Fişiere dispozitiv descrise extern şi fişiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Module: REPLACE(*NO)		*READ, *ADD
	Module: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTCLD	Fişier sursă	*USE	*EXECUTE
	Obiect Locale - REPLACE(*NO)		*READ, *ADD
	Obiect Locale - REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTCLMOD	Fişier sursă	*USE	*EXECUTE
	Fişiere dispozitiv descrise extern şi fişiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	Vedeţi regulile generale.
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTCLPGM	Fişier sursă	*USE	*EXECUTE
	Fişiere dispozitiv descrise extern şi fişiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	Vedeţi regulile generale.
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTCBLPGM (COBOL/400* program licenţiat sau mediu S/38)	Fişier sursă	*USE	*EXECUTE
	Fişiere dispozitiv descrise extern şi fişiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTCMOD	Fişier sursă	*USE	*EXECUTE
	Fişiere dispozitiv descrise extern şi fişiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Module: REPLACE(*NO)		*READ, *ADD
	Module: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Fişierul specificat în parametrii OUTPUT, PPSRCSTMF sau MAKEDEP	*USE	*EXECUTE
	Fişierul specificat în parametrii OUTPUT, PPSRCSTMF sau MAKEDEP	Vedeţi regulile generale.	*READ, *ADD
CRTCPPMOD	Fişier sursă	*USE	*EXECUTE
	Fişiere dispozitiv descrise extern şi fişiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Module: REPLACE(*NO)		*READ, *ADD
	Module: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Directorul specificat în parametrii OUTPUT, PPSRCSTMF, TEMPLATE sau MAKEDEP	*USE	*EXECUTE
	Fişierul specificat în parametrii OUTPUT, PPSRCSTMF, TEMPLATE sau MAKEDEP	Vedeţi regulile generale.	*READ, *ADD
	Anteturi generate de parametrul TEMPLATE	*USE	*EXECUTE
CRTRPGMOD	Fişier sursă	*USE	*EXECUTE
	Fişiere dispozitiv descrise extern şi fişiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Module: REPLACE(*NO)		*READ, *ADD
	Module: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
CRTRPGPGM (RPG/400* program licenţiat sau mediu S/38)	Fişier sursă	*USE	*EXECUTE
	Fişiere dispozitiv descrise extern şi fişiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTRPTPGM (RPG/400 program licenţiat şi mediu S/38)	Fişier sursă	*USE	*EXECUTE
	Program - REPLACE(*NO)		*READ, *ADD
	Program - REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Fişier sursă pentru program RPG generat	Vedeţi regulile generale.	Vedeţi regulile generale.
	Fişiere dispozitiv descrise extern şi fişiere bază de date la care se face referire în programul sursă	*OBJOPR	*EXECUTE
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTS36CBL (mediu S/36)	Fişier sursă	*USE	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
CRTS36RPG	Fişier sursă	*USE	*READ, *ADD
	Program: REPLACE(*NO)		*READ, *ADD
	Program - REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
CRTS36RPGR	Fişier sursă	*USE	*READ, *ADD
	Fişier de afişare: REPLACE(*NO)		*READ, *ADD
	Fişier de afişare: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
CRTS36RPT	Fişier sursă	*USE	*EXECUTE
	Fişier sursă pentru program RPG generat	Vedeţi regulile generale.	Vedeţi regulile generale.
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
CRTSQLC OS/400’ (DB2 Query Manager şi SQL Development pentru programul licenţiat OS/400) [1]	Fişier sursă	*OBJOPR, *READ	*EXECUTE
	Fişier sursă destinaţie	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificaţii descriere date	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
CRTSQLCI OS/400' (DB2 Query Manager şi SQL Development pentru programul licenţiat OS/400) [1]	Fişier sursă	*OBJOPR, *READ	*EXECUTE
	Fişier sursă destinaţie	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificaţii descriere date	*OBJOPR	*EXECUTE
	Obiect: REPLACE(*NO)		*READ, *ADD
	Obiect: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTSQLCBL (DB2 Query Manager şi SQL Development pentru programul licenţiat OS/400) [1]	Fişier sursă	*OBJOPR, *READ	*EXECUTE
	Fişier sursă destinaţie	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificaţii descriere date	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTSQLCBLI (DB2 Query Manager şi SQL Development pentru programul licenţiat OS/400) [1]	Fişier sursă	*OBJOPR, *READ	*EXECUTE
	Fişier sursă destinaţie	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificaţii descriere date	*OBJOPR	*EXECUTE
	Obiect: REPLACE(*NO)		*READ, *ADD
	Obiect: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTSQLCPPI (DB2 Query Manager şi SQL Development pentru programul licenţiat OS/400) [1]	Fişier sursă	*OBJOPR, *READ	*EXECUTE
	Fişier sursă destinaţie	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificaţii descriere date	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
CRTSQLFTN (DB2 Query Manager şi SQL Development pentru programul licenţiat OS/400) [1]	Fişier sursă	*OBJOPR, *READ	*EXECUTE
	Fişier sursă destinaţie	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificaţii descriere date	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTSQLPLI (DB2 Query Manager şi SQL Development pentru programul licenţiat OS/400) [1]	Fişier sursă	*OBJOPR, *READ	*EXECUTE
	Fişier sursă destinaţie	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificaţii descriere date	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTSQLRPG (DB2 Query Manager şi SQL Development pentru programul licenţiat OS/400) [1]	Fişier sursă	*OBJOPR, *READ	*EXECUTE
	Fişier sursă destinaţie	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificaţii descriere date	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CRTSQLRPGI (DB2 Query Manager şi SQL Development pentru programul licenţiat OS/400) [1]	Fişier sursă	*OBJOPR, *READ	*EXECUTE
	Fişier sursă destinaţie	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificaţii descriere date	*OBJOPR	*EXECUTE
	Obiect: REPLACE(*NO)		*READ, *ADD
	Obiect: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
CVTRPGSRC	Fişier sursă	*USE	*EXECUTE
	Fişier ieşire	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	Fişier istoric	*OBJOPR, *OBJMGT, *ADD	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CVTSQLCPP [1]	Fişier sursă	*OBJOPR, *READ	*EXECUTE
	Fişier sursă destinaţie	*OBJOPR, *OBJMGT, *EXIST, *READ, *ADD, *UPDATE, *DELETE, *EXECUTE	*ADD, *EXECUTE
	Specificaţii descriere date	*OBJOPR	*EXECUTE
	Program: REPLACE(*NO)		*READ, *ADD
	Program: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Tabela specificată în parametrul SRTSEQ	*USE	*EXECUTE
ENDCBLDBG (COBOL/400 programul licenţiat sau mediul S/38)	Program	*CHANGE	*EXECUTE
ENTCBLDBG (mediu S/38)	Program	*CHANGE	*EXECUTE
DLTCLD	Obiect Locale	*OBJEXIST, *OBJMGT	*EXECUTE
RTVCLDSRC	Obiect Locale	*USE	*EXECUTE
	În-fişier	Vedeţi regulile generale.	Vedeţi regulile generale.
RUNSQLSTM (program licenţiat SQL/400) [1]	Fişier sursă	*OBJOPR, *READ	*EXECUTE
STRCBLDBG	Program	*CHANGE	*EXECUTE
STRREXPRC	Fişier sursă	*USE	*EXECUTE
	Program ieşire	*USE	*EXECUTE
STRSQL (DB2 Query Manager şi SQL Development pentru programul licenţiat OS/400) [1]	Tabelă secvenţă de sortare	*USE	*EXECUTE
	Descriere dispozitiv imprimantă	*USE	*EXECUTE
	Coadă de ieşire imprimantă	*USE	*EXECUTE
	Fişier imprimantă	*USE	*EXECUTE

1 Vedeţi informaţiile **Autorizarea, privilegiile şi proprietatea obiectului** din Referinţe SQL **DB2 for iSeries** (în Centrul de informare iSeries) pentru informaţii suplimentare despre cerinţele de securitate pentru instrucţiunile SQL.

Comenzile pentru bibliotecă

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteca asupra căreia se acţionează
ADDLIBLE	Bibliotecă		*USE
CHGCURLIB	Bibliotecă curentă nouă		*USE
CHGLIB [8]	Bibliotecă		*OBJMGT
CHGLIBL	Fiecare bibliotecă care e pusă în lista de biblioteci		*USE

Comenzi bibliotecă

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteca asupra căreia se acţionează
CHGSYSLIBL (Q)	Bibliotecile din noua listă		*USE
CLRLIB [3]	Fiecare obiect care e şters din bibliotecă	*OBJEXIST	*USE
	Tipurile de obiecte *DTADCT[14], *JRN[14],*JRNRCV[14], *MSGQ[14], *SBSD[14]	Vedeţi autorizarea cerută de comanda DLT*xxx* pentru tipul de obiect	
	Dispozitiv ASP (dacă e specificat)	*USE	
CPYLIB [4]	Bibliotecă sursă		*USE
	Bibliotecă destinaţie, dacă ea există		*USE, *ADD
	Comenzile CHKOBJ, CRTDUPOBJ	*USE	
	Comanda CRTLIB, dacă biblioteca destinaţie este creată	*USE	
	Obiectul care e copiat	Autorizarea care e cerută când folosiţi comanda CRTDUPOBJ pentru a copia tipul obiectului.	
CRTLIB [9]	Dispozitiv ASP (dacă e specificat)	*USE	
DLTLIB [3]	Fiecare obiect care e şters din bibliotecă	*OBJEXIST	*USE, *OBJEXIST
	Tipurile de obiecte *DTADCT[14], *JRN[14],*JRNRCV[14], *MSGQ, *SBSD[14]	Vedeţi autorizarea cerută de comanda DLT*xxx* pentru tipul de obiect	
	Dispozitiv ASP (dacă e specificat)	*USE	
DSPLIB	Bibliotecă		*READ
	Obiectele din biblioteca [5]	O autorizare alta decât *EXCLUDE	
	Dispozitiv ASP (dacă e specificat)	*EXECUTE	
DSPLIBD	Bibliotecă		O autorizare alta decât *EXCLUDE
EDTLIBL	Biblioteca de adăugat la listă		*USE
RCLLIB	Bibliotecă		*USE, *OBJEXIST

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteca asupra căreia se acţionează**
RSTLIB [7] (Q)	Definiţie mediu de stocare	*USE	*EXECUTE
	Biblioteca, dacă există		*READ, *ADD
	Cozile de mesaje care sunt restaurate în biblioteca unde există deja	*OBJOPR, *OBJEXIST [7]	*EXECUTE. *READ, *ADD
	Programe care adoptă autorizarea	Proprietar sau *ALLOBJ şi *SECADM	*EXECUTE
	Bibliotecă salvată dacă se specifică VOL(*SAVVOL)		*USE [6]
	Fiecare obiect care e restaurat peste în bibliotecă	*OBJEXIST [3]	*EXECUTE, *READ, *ADD
	Profilul utilizator care deţine obiectele care sunt create	*ADD [6]	
	Unitate de bandă, unitate de dischetă, unitate optică	*USE	*EXECUTE
	Fişier sursă, dacă este specificat	Vedeţi regulile generale	Vedeţi regulile generale
	Fişierul referinţă de câmp QSYS/QASAVOBJ pentru fişierul de ieşire, dacă un fişier de ieşire este specificat şi nu există.	*USE	*EXECUTE
RSTLIB [7] (Q)	Fişier bandă (QSYSTAP) sau dischetă (QSYSDKT)	*USE [6]	*EXECUTE
	Ieşire imprimantă QSYS/QPSRLDSP, dacă s-a specificat OUTPUT(*PRINT)	*USE	*EXECUTE
	Fişer de salvare	*USE	*EXECUTE
	Fişier optic (OPTFILE)[12]	*R	Nu se aplică
	Prefix cale al fişierului optic (OPTFILE)[12]	*X	Nu se aplică
	Volum optic[11]	*USE	
	Descriere dispozitiv ASP[15]	*USE	
RSTS36LIBM	Din-fişier	*USE	*EXECUTE
	În-fişier	*CHANGE	*EXECUTE
	Bibliotecă destinaţie	*CHANGE	*EXECUTE
	Fişier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
RTVLIBD	Bibliotecă		O autorizare alta decât *EXCLUDE

Comenzi bibliotecă

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteca asupra căreia se acţionează
SAVLIB	Fiecare obiect din bibliotecă	*OBJEXIST [6]	*READ, *EXECUTE
	Definiţie mediu de stocare	*USE	*EXECUTE
	Fişier de salvare, dacă e gol	*USE, *ADD	*EXECUTE
	Fişier de salvare, dacă există înregistrări în el	*USE, *ADD, *OBJMGT	*EXECUTE
	Coadă de mesaje salvare active	*OBJOPR, *ADD	*EXECUTE
	Unitate de bandă, unitate de dischetă, unitate optică	*USE	*EXECUTE
	Fişier sursă, dacă este specificat	Vedeţi regulile generale.	Vedeţi regulile generale.
	Fişierul referinţă câmp QSYS/QASAVOBJ, dacă fişierul de ieşire este specificat şi nu există	*USE [6]	*EXECUTE
	Ieşire imprimantă QSYS/QPSAVOBJ	*USE [6]	*EXECUTE
SAVLIB	Fişier optic[12]	*RW	Nu se aplică
	Directorul părinte al fişierului optic (OPTFILE)[12]	*WX	Nu se aplică
	Prefix cale al fişierului optic (OPTFILE)[12]	*X	Nu se aplică
	Director rădăcină (/) volum optic[12, 13]	*RWX	Nu se aplică
	Volum optic[11]	*CHANGE	
	Descriere dispozitiv ASP[15]	*USE	
SAVRSTLIB	Descriere dispozitiv ASP[15]	*USE	
SAVS36LIBM	Salvare într-un fişier fizic	*OBJOPR, *OBJMGT	*EXECUTE
	Fie QSYSDKT pentru dischetă fie QSYSTAP pentru bandă şi toate comenzile au nevoie de autorizare pentru dispozitiv	*OBJOPR	*EXECUTE
	Salvare într-un fişier dacă e specificat MBROPT(*ADD)	*ADD	*READ, *ADD
	Salvare într-un fişier fizic dacă e specificat MBROPT(*REPLACE)	*ADD, *DLT	*EXECUTE
	Bibliotecă sursă		*USE
WRKLIB [10]	Bibliotecă		*USE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteca asupra căreia se acţionează
[1] Autorizarea necesară pentru biblioteca asupra căreia se lucrează este indicată în această coloană. De exemplu, pentru a adăuga biblioteca CUSTLIB la o listă de biblioteci folosind comanda ADDLIBLE este necesară autorizare *USE (Utilizare) pentru ea.			
[2] Autorizarea necesară pentru biblioteca QSYS e indicată în această coloană, deoarece toate bibliotecile sunt în QSYS.			
[3] Dacă nu sunt găsite unele obiecte în bibliotecă, acele obiecte nu sunt şterse şi biblioteca nu e complet golită şi ştearsă. Doar obiectele autorizate sunt şterse.			
[4] Toate restricţiile care se aplică pentru comanda CRTDUPOBJ, se aplică de asemenea şi la aceasta.			
[5] Dacă nu aveţi autorizare pentru un obiect din bibliotecă, textul pentru obiect spune *NOT AUTHORIZED.			
[6] Dacă aveţi autorizarea specială *SAVSYS, nu aveţi nevoie de autorizarea specificată.			
[7] Trebuie să aveţi autorizaţia specială *ALLOBJ pentru a specifica ALWOBJDIF(*ALL).			
[8] Trebuie să aveţi autorizarea specială *AUDIT pentru a modifica valoarea CRTOBJAUD pentru o bibliotecă. *OBJMGT **nu** e necesară dacă modificaţi doar valoarea CRTOBJAUD. *OBJMGT **este** necesară dacă modificaţi valoarea CRTOBJAUD şi alte valori.			
[9] Trebuie să aveţi autorizarea specială *AUDIT pentru a specifica o valoare CRTOBJAUD alta decât *SYSVAL.			
[10] Trebuie să aveţi autorizarea cerută de operaţie pentru a folosi o operaţie individuală.			
[11] Volumele optice nu sunt obiecte sistem reale. Legătura între volumul optic şi lista de autorizare folosită pentru a securiza volumul este menţinută de funcţia de suport optic.			
[12] Această verificare de autorizare este făcută doar când formatul mediului de stocare optic este UDF (format disc universal).			
[13] Această verificare de autorizare este făcută doar când ştergeţi volumul optic.			
[14] Acest obiect este permis pe ASP independent.			
[15] Autorizarea este necesară doar dacă operaţia de salvare sau restaurare necesită o comutare a spaţiului de nume de bibliotecă.			

Comenzile pentru cheie de licenţă

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDLICKEY (Q)	Fişier ieşire	*USE	*EXECUTE
DSPLICKEY (Q)	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
RMVLICKEY (Q)	Fişier ieşire	*CHANGE	*EXECUTE

Comenzile pentru program cu licenţă

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comenzi program cu licenţă

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGLICINF (Q)	Comanda WRKLICINF	*USE	*EXECUTE
DLTLICPGM [1,2] (Q)			
DSPTM			
INZSYS (Q)			
RSTLICPGM [1,2] (Q)			
SAVLICPGM [1,2] (Q)			
WRKLICINF (Q)			

1 Unele programe cu licenţă pot fi şterse, salvate sau restaurate doar dacă sunteţi înscris în directorul de distribuţie al sistemului.

2 La ştergerea, restaurarea sau salvarea unui program cu licenţă care conţine foldere, toate restricţiile care se aplică comenzii DLTDLO se aplică de asemenea şi acesteia.

3 Pentru a folosi operaţii individuale, trebuie să aveţi autorizaţia cerută de operaţii individuale.

Comenzile pentru descriere de linie

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGLINASC [2]	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
	Descriere controler (SWTCTLLST)	*USE	*EXECUTE
CHGLINBSC [2]	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
	Descriere controler (SWTCTLLST)	*USE	*EXECUTE
CHGLINDDI [2]	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
CHGLINETH [2]	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
CHGLINFAX [2]	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
CHGLINFR [2]	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
CHGLINPPP[2]	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
CHGLINSDLC [2]	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
CHGLINTDLC [2]	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
CHGLINTRN [2]	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
CHGLINX25 [2]	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
	Descriere controler (SWTCTLLST)	*USE	*EXECUTE
	Listă de conexiuni (CNNLSTIN sau CNNLSTOUT)	*USE	*EXECUTE
	Descriere interfaţă de reţea (SWTNWILST)	*USE	*EXECUTE
CHGLINWLS [2]	Descriere de linie	*CHANGE, *OBJMGT	*EXECUTE
	Program (INZPGM)	*USE	*EXECUTE
CRTLINASC [2]	Descriere controler (CTL şi SWTCTLLST)	*USE	*EXECUTE
	Descriere de linie		*READ, *ADD
CRTLINBSC [2]	Descriere controler (SWTCTLLST şi CTL)	*USE	*EXECUTE
	Descriere de linie		*READ, *ADD

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTLINDDI [2]	Descriere de linie		*READ, *ADD
	Descriere interfaţă de reţea (NWI)	*USE	*EXECUTE
	Descriere controler (NETCTL)	*USE	*EXECUTE
CRTLINETH [2]	Descriere controler (NETCTL)	*USE	*EXECUTE
	Descriere de linie		*READ, *ADD
	Descriere interfaţă de reţea (NWI)	*USE	*EXECUTE
	Descriere server de reţea (NWS)	*USE	*EXECUTE
CRTLINFAX [2]	Descriere de linie		*READ, *ADD
	Descriere controler	*USE	*EXECUTE
CRTLINFR [2]	Descriere de linie		*READ, *ADD
	Descriere interfaţă de reţea (NWI)	*USE	*EXECUTE
	Descriere controler (NETCTL)	*USE	*EXECUTE
CRTLINPPP[2]	Descriere controler (NETCTL)	*USE	*EXECUTE
	Descriere de linie		*READ, *ADD
CRTLINSDLC [2]	Descriere controler (CTL)	*USE	*EXECUTE
	Descriere de linie		*READ, *ADD
CRTLINTDLC [2]	Descriere controler (WSC şi CTL)	*USE	*EXECUTE
	Descriere de linie		*READ, *ADD
CRTLINTRN [2]	Descriere controler (NETCTL)	*USE	*EXECUTE
	Descriere de linie		*READ, *ADD
	Descriere interfaţă de reţea (NWI)	*USE	*EXECUTE
	Descriere server de reţea (NWS)	*USE	*EXECUTE
CRTLINX25 [2]	Descriere controler (SWTCTLLST)	*USE	*EXECUTE
	Descriere controler (LGLCHLE) circuit virtual permanent (PVC)	*USE	*EXECUTE
	Descriere de linie		*READ, *ADD
	Listă de conexiuni (CNNLSTIN sau CNNLSTOUT)	*USE	*EXECUTE
	Descriere interfaţă de reţea (NWI sau SWTNWILST)	*USE	*EXECUTE
CRTLINWLS [2]	Descriere de linie		*READ, *ADD
	Descriere controler (NETCTL)	*USE	*EXECUTE
	Program (INZPGM)	*USE	*EXECUTE
DLTLIND	Descriere de linie	*OBJEXIST	*EXECUTE
DSPLIND	Descriere de linie	*USE	*EXECUTE
ENDLINRCY	Descriere de linie	*OBJOPR	*EXECUTE
PRTCMNSEC [2, 3]			
RSMLINRCY	Descriere de linie	*OBJOPR	*EXECUTE
WRKLIND [1]	Descriere de linie	*OBJOPR	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci

[1] Pentru a folosi operaţii individuale, trebuie să aveţi autorizaţia cerută de operaţii individuale.

[2] Pentru a folosi această comandă, trebuie să aveţi autorizaţia specială *IOSYSCFG.

[3] Pentru a folosi această comandă, trebuie să aveţi autorizarea specială *ALLOBJ.

Comenzile pentru reţea locală (LAN)

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Aceste comenzi nu necesită nici o autorizaţie obiect:			
ADDLANADPI	DSPLANADPP	RMVLANADPT (Q)	WRKLANADPT
CHGLANADPI	DSPLANSTS	RMVLANADPI	

Comenzile pentru Locale

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTLOCALE	Fişier sursă	*USE	*USE, *ADD
DLTLOCALE	Locale	*OBJEXIST	*USE

Comenzile pentru cadru de lucru server de poştă

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Această comandă nu necesită nici o autorizare pentru obiect:	
ENDMSF (Q)	STRMSF (Q)

Comenzile pentru mediu de stocare

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDTAPCTG	Descriere bibliotecă bandă	*USE	*EXECUTE
CFGDEVMLB[1]	Descriere bibliotecă bandă	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVMLB (Q)	Descriere bibliotecă bandă	*USE	*EXECUTE
CHGJOBMLBA[4]	Descriere bibliotecă bandă	*CHANGE	*EXECUTE
CHGTAPCTG	Descriere bibliotecă bandă	*USE	*EXECUTE
CHKDKT	Descriere unitate de dischetă	*USE	*EXECUTE
CHKTAP	Descriere dispozitiv bandă	*USE	*EXECUTE
CLRDKT	Descriere unitate de dischetă	*USE	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTTAPCGY	Descriere bibliotecă bandă		
DLTDKTLBL	Descriere unitate de dischetă	*USE	*EXECUTE
DLTMEDDFN	Definiţie mediu de stocare	*OBJEXIST	*EXECUTE
DLTTAPCGY	Descriere bibliotecă bandă		
DMPTAP (Q)	Descriere dispozitiv bandă	*USE	*EXECUTE
DSPDKT	Descriere unitate de dischetă	*USE	*EXECUTE
DSPTAP	Descriere dispozitiv bandă	*USE	*EXECUTE
DSPTAPCGY	Descriere bibliotecă bandă		
DSPTAPCTG	Descriere bibliotecă bandă	*USE	*EXECUTE
DSPTAPSTS	Descriere bibliotecă bandă	*USE	*EXECUTE
DUPDKT	Descriere unitate de dischetă	*USE	*EXECUTE
DUPTAP	Descriere dispozitiv bandă	*USE	*EXECUTE
INZDKT	Descriere unitate de dischetă	*USE	*EXECUTE
INZTAP	Descriere dispozitiv bandă	*USE	*EXECUTE
RMVTAPCTG	Descriere bibliotecă bandă	*USE	*EXECUTE
RNMDKT	Descriere unitate de dischetă	*USE	*EXECUTE
SETTAPCGY	Descriere bibliotecă bandă	*USE	*EXECUTE
WRKMLBRSCQ [3]	Descriere bibliotecă bandă	*USE	*EXECUTE
WRKMLBSTS [2] (Q)	Descriere bibliotecă bandă	*USE	*EXECUTE
WRKTAPCTG	Descriere bibliotecă bandă	*USE	*EXECUTE

1 Pentru a folosi această comandă, trebuie să aveţi autorizaţia specială *IOSYSCFG.

2 Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea cerută de operaţie.

3 Pentru a modifica atributele bibliotecii mediului de stocare sesiune trebuie să aveţi autorizarea *CHANGE pentru descrierea bibliotecă bandă. Pentru a schimba prioritatea sau pentru a lucra cu alt job de utilizator, trebuie să aveţi autorizarea specială *JOBCTL.

4 Pentru a schimba prioritatea sau pentru a lucra cu alt job de utilizator, trebuie să aveţi autorizarea specială *JOBCTL.

Comenzile pentru meniu şi grup de panouri

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGMNU	Meniu	*CHANGE	*USE
CRTMNU	Fişier sursă	*USE	*EXECUTE
	Meniu: REPLACE(*NO)		*READ, *ADD
	Meniu: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
CRTPNLGRP	Grup de panouri: Replace(*NO)		*READ, *ADD
	Grup de panouri: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Fişier sursă	*USE	*EXECUTE
	Fişier includere	*USE	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTS36MNU	Meniu: REPLACE(*NO)		*READ, *ADD
	Meniu: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Fişier sursă	*USE	*EXECUTE
	Fişiere de mesaje numite în sursă	*OBJOPR, *OBJEXIST	*EXECUTE
	Fişier-destinaţie sursă când TOMBR nu e *NONE	*OBJOPR, *OBJMGT, *OBJEXIST, *ADD	*READ, *ADD
	Fişier de afişare meniu când se specifică REPLACE(*YES)	*OBJOPR, *OBJEXIST	*EXECUTE
	Fişier mesaj text comandă	*OBJOPR, *OBJEXIST	*EXECUTE
	Comanda CRTMSGF (Create Message File - Creare fişier mesaj)	*OBJOPR	*EXECUTE
	Comanda ADDMSGD (Add Message Description - Adăugare descriere mesaj)	*OBJOPR	*EXECUTE
	Comanda Creare fişier de afişare (CRTDSPF)	*OBJOPR	*EXECUTE
DLTMNU	Meniu	*OBJOPR, *OBJEXIST	*EXECUTE
DLTPNLGRP	Grup de panouri	*OBJEXIST	*EXECUTE
DSPMNUA	Meniu	*USE	*USE
GO	Meniu	*USE	*USE
	Fişierul de afişare şi fişierele mesaj cu *DSPF specificat	*USE	*EXECUTE
	Biblioteci curente şi de produse	*USE	
	Program cu *PGM specificat	*USE	*EXECUTE
WRKMNU [1]	Meniu	Orice	*USE
WRKPNLGRP [1]	Grup de panouri	Orice	*EXECUTE

1 Pentru a folosi o operaţie individuală, trebuie să aveţi autorizaţia necesară de operaţie.

Comenzile pentru mesaj

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DSPMSG	Coadă de ieşire	*USE	*USE
	Coada de mesaje care primeşte replica la un mesaj de interogare	*USE, *ADD	*USE
	Înlăturare mesaje din coada de mesaje	*USE, *DLT	*USE
RCVMSG	Coadă de ieşire	*USE	*EXECUTE
	Înlăturare mesaje din coada de mesaje	*USE, *DLT	*EXECUTE
RMVMSG	Coadă de ieşire	*OBJOPR, *DLT	*EXECUTE
RTVMSG	Fişier de mesaje	*USE	*EXECUTE
SNDBRKMSG	Coada de mesaje care primeşte replica la mesajele de interogare	*OBJOPR, *ADD	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
SNDMSG	Coadă de ieşire	*OBOPR, *ADD	*EXECUTE
	Coada de mesaje care primeşte replica la mesajul de interogare	*OBJOPR, *ADD	*EXECUTE
SNDPGMMSG	Coadă de ieşire	*OBJOPR, *ADD	*EXECUTE
	Fişierul mesaj, când se trimite mesaj predefinit	*USE	*EXECUTE
	Coada de mesaje care primeşte replica la mesajul de interogare	*OBJOPR, *ADD	*EXECUTE
SNDRPY	Coadă de ieşire	*USE, *ADD	*EXECUTE
	Înlăturare mesaje din coada de mesaje	*USE, *ADD, *DLT	*EXECUTE
SNDUSRMSG	Coadă de ieşire	*OBJOPR, *ADD	*EXECUTE
	Fişierul mesaj, când se trimite mesaj predefinit	*USE	*EXECUTE
WRKMSG	Coadă de ieşire	*USE	*USE
	Coada de mesaje care primeşte replica la mesajul de interogare	*USE, *ADD	*USE
	Înlăturare mesaje din coada de mesaje	*USE, *DLT	*USE

Comenzile pentru descriere de mesaj

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDMSGD	Fişier de mesaje	*USE, *ADD	*EXECUTE
CHGMSGD	Fişier de mesaje	*USE, *UPD	*EXECUTE
DSPMSGD	Fişier de mesaje	*USE	*EXECUTE
RMVMSGD	Fişier de mesaje	*OBJOPR, *DLT	*EXECUTE
WRKMSGD [1]	Fişier de mesaje	*USE	*EXECUTE

1 Pentru a folosi operaţii individuale, trebuie să aveţi autorizaţia cerută de operaţii individuale.

Comenzile pentru fişier de mesaj

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGMSGF	Fişier de mesaje	*USE, *DLT	*EXECUTE
CRTMSGF	Fişier de mesaje		*READ, *ADD
DLTMSGF	Fişier de mesaje	*OBJEXIST	*EXECUTE
DSPMSGF	Fişier de mesaje	*USE	*EXECUTE
MRGMSGF	Fişier-sursă mesaj	*USE	*EXECUTE
	Fişier mesaje destinaţie	*USE, *ADD, *DLT	*EXECUTE
	Fişier mesaj înlocuire	*USE, *ADD	*EXECUTE
WRKMSGF [1.]	Fişier de mesaje	Orice autorizaţie	*USE

1 Pentru a folosi operaţii individuale, trebuie să aveţi autorizaţia cerută de operaţii individuale.

Comenzile pentru coadă de mesaje

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGMSGQ	Coadă de ieşire	*USE, *DLT	*EXECUTE
CLRMSGQ	Coadă de ieşire	*OBJOPR, *DLT	*EXECUTE
CRTMSGQ	Coadă de ieşire		*READ, *ADD
DLTMSGQ	Coadă de ieşire	*OBJEXIST, *USE, *DLT	*EXECUTE
DSPLOG			*EXECUTE
WRKMSGQ [1]	Coadă de ieşire	Orice autorizaţie	*USE
[1] Pentru a folosi operaţii individuale, trebuie să aveţi autorizaţia cerută de operaţii individuale.			

Comenzile pentru migrare

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
RCVMGRDTA	Fişier	*ALL	*READ, *ADD
	Dispozitiv	*CHANGE	*EXECUTE
SNDMGRDTA	Fişier	*ALL	*READ, *ADD
	Dispozitiv	*CHANGE	*EXECUTE
Aceste comenzi nu necesită nici o autorizare obiect. Ele sunt livrate cu autorizarea publică *EXCLUDE. Trebuie să aveţi autorizarea specială *ALLOBJ pentru a folosi aceste comenzi.			
ANZS34OCL	CVTS36JOB	MGRS36DSPF	MIGRATE
ANZS36OCL	CVTS36QRY	MGRS36ITM	QMUS36
CHGS34LIBM	CVTS38JOB	MGRS36LIB	RESMGRNAM
CHKS36SRCA	GENS36RPT	MGRS36MNU	RSTS38AUT
CVTBASSTR	GENS38RPT	MGRS36MSGF	STRS36MGR
CVTBASUNF	MGRS36	MGRS36QRY [1]	STRS38MGR
CVTBGUDTA	MGRS36APF [1]	MGRS36RPG	
CVTS36CFG	MGRS36CBL	MGRS36SEC	
CVTS36FCT	MGRS36DFU [1]	MGRS38OBJ	
[1] Trebuie să aveţi autorizarea specială *ALLOBJ şi să aveţi opţiunea 4 OS/400 instalată.			

Comenzile pentru descriere de mod

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGMODD [2]	Descriere mod	*CHANGE, *OBJMGT	*EXECUTE
CRTMODD [2]	Descriere mod		*READ, *ADD
CHGSSNMAX	Descriere dispozitiv	*OBJOPR	*EXECUTE
DLTMODD	Descriere mod	*OBJEXIST	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DSPMODD	Descriere mod	*USE	*EXECUTE
DSPMODSTS	Dispozitiv	*OBJOPR	*EXECUTE
	Descriere mod	*OBJOPR	*EXECUTE
ENDMOD	Descriere dispozitiv	*OBJOPR	*EXECUTE
STRMOD	Descriere dispozitiv	*OBJOPR	*EXECUTE
WRKMODD [1]	Descriere mod	*OBJOPR	*EXECUTE

[1] Pentru a folosi operaţii individuale, trebuie să aveţi autorizaţia cerută de operaţii individuale.

[2] Pentru a folosi această comandă, trebuie să aveţi autorizaţia specială *IOSYSCFG.

Comenzile pentru modul

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGMOD	Modul	*OBJMGT, *USE	*USE
	Modul, dacă se specifică OPTIMIZE	*OBJMGT, *USE	*USE, *ADD, *DLT
	Modul, dacă se specifică FRCCRT(*YES)	*OBJMGT, *USE	*USE, *ADD, *DLT
	Modul, dacă se specifică ENBPRFCOL	*OBJMGT, *USE	*USE, *ADD, *DELETE
DLTMOD	Modul	*OBJEXIST	*EXECUTE
DSPMOD	Modul	*USE	*EXECUTE
RTVBNDSRC [1]	Modul	*USE	*EXECUTE
	*SRVPGMs şi module specificate cu *SRVPGMs	*USE	*EXECUTE
	Fişierul bază de date sursă dacă el şi membrul există şi se specifică MBROPT(*REPLACE).	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	Fişierul bază de date sursă dacă el şi membrul există şi se specifică MBROPT(*ADD).	*OBJOPR, *ADD	*EXECUTE
	Fişierul bază de date sursă dacă el există şi membrul trebuie să fie creat.	*OBJOPR, *OBJMGT, *ADD	*EXECUTE, *READ, *ADD
	Fişierul bază de date sursă dacă el există şi membrul trebuie să fie creat.		*EXECUTE, *READ, *ADD
	Comanda CRTSCRPF dacă fişierul nu există		*EXECUTE
	Comanda ADDPFM dacă fişierul nu există		*EXECUTE
	Comanda RGZPFM pentru a reorganiza membrul fişier sursă	*OBJMGT	*EXECUTE
WRKMOD [2]	Modul	Orice autorizaţie	*USE

[1] Aveţi nevoie de autorizare *USE pentru:

- Comanda CRTSRCPF dacă fişierul nu există.
- Comanda ADDPFM dacă membrul nu există.
- Comanda RGZPFM astfel ca membrul fişier sursă să fie reorganizat. Sunt necesare fie autorizările *CHANGE şi *OBJALTER sau *OBJMGT pentru a reorganiza membrul fişier sursă. Funcţiile comenzii RTVBNDSRC se efectuează apoi cu membrul fişier sursă reorganizat cu numărul de ordine zero.

[2] Pentru a folosi operaţii individuale, trebuie să aveţi autorizaţia cerută de operaţii individuale.

Comenzile pentru descriere NetBIOS

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGNTBD [2]	Descriere NetBIOS	*CHANGE, *OBJMGT	*EXECUTE
CRTNTBD [2]	Descriere NetBIOS		*EXECUTE
DLTNTBD	Descriere NetBIOS	*OBJEXIST	*EXECUTE
DSPNTBD	Descriere NetBIOS	*USE	*EXECUTE
WKRNTBD[1]	Descriere NetBIOS	*OBJOPR	*EXECUTE

1 Pentru a folosi operaţii individuale, trebuie să aveţi autorizaţia cerută de operaţii individuale.

2 Pentru a folosi această comandă, trebuie să aveţi autorizaţia specială *IOSYSCFG.

Comenzile pentru reţea

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDNETJOBE (Q)	Profil utilizator în intrarea job reţea	*USE	
APING	Descriere dispozitiv	*CHANGE	
AREXEC	Descriere dispozitiv	*CHANGE	
CHGNETA (Q) [4]			
CHGNETJOBE (Q)	Profil utilizator în intrarea job reţea	*USE	
DLTNETF [2]	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
DSPNETA			
RCVNETF [2]	Fişierul destinaţie nu există, MBROPT(*ADD) specificat	*OBJMGT, *USE	*EXECUTE, *ADD
	Fişierul destinaţie nu există, MBROPT(*REPLACE) specificat	*OBJMGT, *CHANGE	*EXECUTE, *ADD
	Fişierul destinaţie există, MBROPT(*ADD) specificat	*USE	*EXECUTE
	Fişierul destinaţie există, MBROPT(*REPLACE) specificat	*OBJMGT, *CHANGE	*EXECUTE
RMVNETJOBE (Q)	Profil utilizator în intrarea job reţea	*USE	
RTVNETA			
RUNRMTCMD	Descriere dispozitiv	*CHANGE	
SNDNETF	Fişier fizic sau fişier de salvare	*USE	*EXECUTE
SNDNETMSG pentru un utilizator local	Coadă de ieşire	*OBJOPR, *ADD	*EXECUTE
VFYAPPCCNN	Descriere dispozitiv	*CHANGE	
WRKNETF [2,3]			

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
WRKNETJOBE [3]	QUSRSYS/QANFNJE	*USE	*EXECUTE

[1] Trebuie să aveţi autorizarea specială *ALLOBJ.

[2] Un utilizator poate rula aceste comenzi pe propriile sale fişiere reţea sau pe fişierele reţea deţinute de profilul său de grup. E necesară autorizarea specială *ALLOBJ pentru a procesa fişiere reţea pentru alt utilizator.

[3] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizarea cerută de acea operaţie.

[4] Pentru a modifica unele atribute reţea, trebuie să aveţi autorizarea specială *IOSYSCFG sau *ALLOBJ şi *IOSYSCFG.

Comenzile pentru NFS

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizaţie necesară pentru obiect
ADDMFS [1,3]	dir_peste_care_ se_montează	*DIR	″root″	*W
CHGNFSEXP [1,2]	Prefix cale	Vedeţi regulile generale.		
DSPMFSINF	unele_directoare	*DIR	″root″	*RX
	Prefix cale	Vedeţi regulile generale.		
ENDNFSSVR [1,4]	nimic			
EXPORTFS [1,2]	Prefix cale	Vedeţi regulile generale.		
MOUNT [1,3]	dir_peste_care_ se_montează	*DIR	″root″	*W
RLSIFSLCK [1]	obiect	*STMF	″root″, QOpenSys, UDFS	*R
	Prefix cale	Vedeţi regulile generale.		
RMVMFS [1]				
STATFS	unele_directoare	*DIR	″root″	*RX
	Prefix cale	Vedeţi regulile generale.		
STRNFSSVR [1]	nimic			
UNMOUNT [1]				

[1] Pentru a folosi această comandă, trebuie să aveţi autorizaţia specială *IOSYSCFG.

[2] Când e specificat steguleţul -F şi fişierul /etc/exports nu există, trebuie să aveţi autorizarea de scriere, executare (*WX) pentru directorul /etc. Când e specificat steguleţul -F şi fişierul /etc/exports există, trebuie să aveţi autorizare de citire, scriere (*RW) pentru fişierul /etc/exports şi autorizare *X pentru directorul /etc.

[3] Directorul peste care se montează este orice director IFS peste care se poate monta.

[4] Pentru a opri orice joburi demon pornite de altcineva, trebuie să aveţi autorizarea specială *JOBCTL.

Comenzile pentru descriere de interfaţă de reţea

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGNWIFR [2]	Descriere interfaţă de reţea	*CHANGE, *OBJMGT	*EXECUTE

Comenzi descriere interfaţă de reţea

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTNWIFR [2]	Descriere interfaţă de reţea		*READ, *ADD
	Descriere de linie (DLCI)	*USE	*EXECUTE
DLTNWID	Descriere interfaţă de reţea	*OBJEXIST	*EXECUTE
DSPNWID	Descriere interfaţă de reţea	*USE	*EXECUTE
WRKNWID [1]	Descriere interfaţă de reţea	*OBJOPR	*EXECUTE

1 Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea cerută de operaţia individuală.

2 Pentru a folosi această comandă, trebuie să aveţi autorizaţia specială *IOSYSCFG.

Comenzile pentru server de reţea

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizaţie necesară pentru obiect
ADDNWSSTGL [2]	Cale (/QFPNWSSTG)	*DIR	″root″	*X
	Director părinte (numele spaţiului de stocare)	*DIR	″root″	*WX
	Fişierele care compun spaţiul de stocare)	*FILE	″root″	*RW
	Descriere server de reţea	*NWSD	QSYS.LIB	*CHANGE, *OBJMGT
CHGNWSUSRA [4]	Profil utilizator	*USRPRF		*OBJMGT, *USE
CRTNWSSTG [2]	Cale (root şi /QFPNWSSTG)	*DIR	″root″	*WX
DLTNWSSTG [2]	Cale (/QFPNWSSTG)	*DIR	″root″	*WX
	Director părinte (numele spaţiului de stocare)	*DIR	″root″	*RWX, *OBJEXIST
	Fişierele care compun spaţiul de stocare)	*FILE	″root″	*OBJEXIST
DSPNWSSTG	Cale la spaţiul de stocare	*DIR	″root″	*X
	Fişierele care compun spaţiul de stocare)	*FILE	″root″	*R
RMVNWSSTGL [2]	Cale (/QFPNWSSTG)	*DIR	″root″	*X
	Director părinte (numele spaţiului de stocare)	*DIR	″root″	*WX
	Fişierele care compun spaţiul de stocare)	*FILE	″root″	*RW
	Descriere server de reţea	*NWSD	QSYS.LIB	*CHANGE, *OBJMGT
WRKNWSSTG	Cale la spaţiul de stocare	*DIR	″root″	*X
	Fişierele care compun spaţiul de stocare)	*FILE	″root″	*R

Aceste comenzi nu necesită nici o autorizaţie obiect:

ADDRMTSVR	DSPNWSALS	SNDNWSMSG
CHGNWSA [4](Q)	DSPNWSSSN	WRKNWSALS
CHGNWSALS	DSPNWSSTC	WRKNWSENR
CRTNWSALS	DSPNWSUSR	WRKNWSSSN
DLTNWSALS	DSPNWSUSRA	WRKNWSSTS
DSPNWSA	SBMNWSCMD (Q) [3]	

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizaţie necesară pentru obiect

[1] Autorizarea necesară nu e folosită pentru comenzi ale serverului de reţea.

[2] Pentru a folosi această comandă, trebuie să aveţi autorizaţia specială *IOSYSCFG.

[3] Pentru a folosi această comandă, trebuie să aveţi autorizarea specială *JOBCTL.

[4] Trebuie să aveţi autorizarea specială *SECADM pentru a specifica altă valoare decât *NONE pentru parametrii NDSTREELST şi NTW3SVRLST.

Comenzi pentru descriere de server de reţea

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru bibliotecă QSYS
CHGNWSD [2]	Descriere server de reţea	*CHANGE, *OBJMGT	*EXECUTE
	Descriere NetBIOS (NTB)	*USE	*EXECUTE
CRTNWSD [2]	Descriere NetBIOS (NTB)	*USE	*EXECUTE
	Descriere de linie (PORTS)	*USE	*EXECUTE
DLTNWSD	Descriere server de reţea	*OBJEXIST	*EXECUTE
DSPNWSD	Descriere server de reţea	*USE	*EXECUTE
WRKNWSD[1]	Descriere server de reţea	*OBJOPR	*EXECUTE

[1] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizaţia necesară de operaţie.

[2] Pentru a folosi această comandă, trebuie să aveţi autorizaţia specială *IOSYSCFG.

Comenzile pentru listă de noduri

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDNODLE	Listă de noduri	*OBJOPR, *ADD	*EXECUTE
CRTNODL	Listă de noduri		*READ, *ADD
DLTNODL	Listă de noduri	*OBJEXIST	*EXECUTE
RMVNODLE	Listă de noduri	*OBJOPR, *READ, *DLT	*EXECUTE
WRKNODL [1]	Listă de noduri	*USE	*USE
WRKNODLE	Listă de noduri	*USE	*EXECUTE

[1] Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea cerută de operaţia individuală.

Comenzile pentru servicii de birou

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Aceste comenzi nu necesită nici o autorizare obiect.		
ADDACC (Q)	GRTACCAUT [2,3,6] (Q)	RVKUSRPMN [1,2]
DSPACC	GRTUSRPMN [1,2]	WRKDOCLIB [4]
DSPACCAUT	RMVACC [1] (Q)	WRKDOCPRTQ [5]
DSPUSRPMN	RVKACCAUT [1]	

1 Trebuie să aveţi autorizarea specială *ALLOBJ pentru a acorda sau revoca autorizarea cod de acces sau autorizarea document pentru alţi utilizatori.

2 Accesul e restricţionat la documente, foldere şi poştă care nu sunt personale.

3 Codul de acces trebuie să fie definit pentru sistem (folosind comanda ADDACC (Add Access Code - Adăugare cod de acces)) înainte să puteţi acorda autorizare cod de acces. Utilizatorului căruia i se acordă autorizare cod de acces trebuie să fie înregistrat în directorul distribuţie al sistemului.

4 Trebuie să aveţi autorizarea specială *SECADM.

5 Sunt necesare autorizări suplimentare pentru funcţii specifice apelate de operaţiile selectată. Utilizatorul are de asemenea nevoie de autorizări speciale pentru orice comenzi apelate în timpul unei funcţii specifice.

6 Trebuie să aveţi autorizarea specială *ALLOBJ sau *SECADM pentru a acorda autorizarea de acces la cod.

Comenzile pentru educaţie online

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

		Autorizări necesare	
Comanda	**Obiect referinţă**	**Pentru obiecte**	**Pentru biblioteci**
CVTEDU			
STREDU			

Comenzile pentru Asistent operaţional

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

		Autorizări necesare	
Comanda	**Obiect referinţă**	**Pentru obiecte**	**Pentru biblioteci**
CHGBCKUP [1]	QUSRSYS/QEZBACKUPL *USRIDX	*CHANGE	*EXECUTE
CHGCLNUP[2]			
CHGPWRSCD [3]		*USE	*EXECUTE
CHGPWRSCDE [3]		*USE	*EXECUTE
DSPBCKSTS	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
DSPBCKUP	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
DSPBCKUPL	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*USE	*EXECUTE
DSPPWRSCD			
EDTBCKUPL [1]	QUSRSYS/QEZBACKUPL *USRIDX	*CHANGE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*CHANGE	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ENDCLNUP [4]	ENDJOB *CMD	*USE	*EXECUTE
PRTDSKINF (Q)	QUSRSYS/QAEZDISK *FILE, membru QCURRENT	*USE	*EXECUTE
	Dispozitiv ASP (dacă e specificat)	*USE	
RTVBCKUP	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
RTVCLNUP			
RTVDSKINF (Q) [5]	Dispozitiv ASP (dacă e specificat)	*USE	
RTVPWRSCDE	Comanda DSPPWRSCD	*USE	
RUNBCKUP [1]	QUSRSYS/QEZBACKUPL *USRIDX	*USE	*EXECUTE
	QUSRSYS/QEZBACKUPF *USRIDX	*USE	*EXECUTE
	Comenzi: SAVLIB, SAVCHGOBJ, SAVDLO, SAVSECDTA, SAVCFG, SAVCAL, SAV	*USE	*EXECUTE
STRCLNUP[4]	Profil utilizator QPGMR	*USE	
	Coadă joburi	*USE	*EXECUTE

1 Trebuie să aveţi autorizările speciale *ALLOBJ sau *SAVSYS.

2 Trebuie să aveţi autorizările speciale *ALLOBJ, *SECADM şi *JOBCTL.

3 Trebuie să aveţi autorizările speciale *ALLOBJ şi *SECADM.

4 Trebuie să aveţi autorizaţia specială *JOBCTL.

5 Trebuie să aveţi autorizarea specială *ALLOBJ.

Comenzile pentru disc optic

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Tabela 150.

Comanda	Obiect referinţă	Autorizări necesare		
		Obiect	Bibliotecă	Volum optic [1]
ADDOPTCTG (Q)	Dispozitiv optic	*USE	*EXECUTE	
ADDOPTSVR (Q)	CSI server	*USE	*EXECUTE	
CHGDEVOPT[4]	Dispozitiv optic	*CHANGE, *OBJMGT	*EXECUTE	
CHGOPTA (Q)				
CHGOPTVOL	Directorul root (/) al volumului când se modifică descrierea text[5]	*W	Nu se aplică	Nu se aplică
	Dispozitiv optic	*USE	*EXECUTE	*CHANGE[3]
	CSI server	*USE	*EXECUTE	Nu se aplică

Tabela 150. (continuare)

Comanda	Obiect referinţă	Autorizări necesare		
		Obiect	**Bibliotecă**	**Volum optic [1]**
CPYOPT	Dispozitiv optic	*USE	*EXECUTE	*USE - Volum sursă
				*ALL - Volum destinaţie
	Fiecare director precedent în calea fişierului sursă	*X	Nu se aplică	Nu se aplică
	Fiecare director precedent în calea fişierului destinaţie	*X	Nu se aplică	Nu se aplică
	Fişier sursă (*DSTMF)[5]	*R	Nu se aplică	Nu se aplică
	Director părinte al fişierului destinaţie	*WX	Nu se aplică	Nu se aplică
	Părintele directorului părinte dacă se creează director	*WX	Nu se aplică	Nu se aplică
CPYOPT	Fişierul destinaţie dacă e înlocuit datorită SLTFILE(*ALL)	*W	Nu se aplică	Nu se aplică
	Fişierul destinaţie dacă e înlocuit datorită SLTFILE(*CHANGED)	*RW	Nu se aplică	Nu se aplică
	Fiecare director din cale care precede directorul sursă	*X	Nu se aplică	Nu se aplică
	Fiecare director din cale care precede directorul destinaţie	*X	Nu se aplică	Nu se aplică
CPYOPT	Directorul care e copiat [5]	*R	Nu se aplică	Nu se aplică
	Directorul care e copiat dacă el conţine intrări	*RX	Nu se aplică	Nu se aplică
	Părintele directorului destinaţie	*WX	Nu se aplică	Nu se aplică
	Directorul destinaţie dacă e înlocuit datorită SLTFILE(*ALL)	*W	Nu se aplică	Nu se aplică
	Directorul destinaţie dacă e înlocuit datorită SLTFILE(*CHANGED)	*RW	Nu se aplică	Nu se aplică
	Directorul destinaţie dacă intrările urmează să fie create	*WX	Nu se aplică	Nu se aplică
CPYOPT	Fişiere sursă	*R	Nu se aplică	Nu se aplică
	Fişierul destinaţie dacă e înlocuit datorită SLTFILE(*ALL)	*W	Nu se aplică	Nu se aplică
	Fişierul destinaţie dacă e înlocuit datorită SLTFILE(*CHANGED)	*RW	Nu se aplică	Nu se aplică
CRTDEVOPT[4]	Dispozitiv optic		*EXECUTE	

Tabela 150. (continuare)

Comanda	Obiect referinţă	Autorizări necesare		
		Obiect	**Bibliotecă**	**Volum optic [1]**
CVTOPTBKU	Dispozitiv optic	*USE	*EXECUTE	*ALL
DSPOPT	Prefix cale când DATA (*SAVRST)[5]	*X	Nu se aplică	Nu se aplică
	Prefix fişier când (*SAVRST)[2]	*R	Nu se aplică	Nu se aplică
	Dispozitiv optic	*EXECUTE	*USE	
	CSI server	*USE	*EXECUTE	
DSPOPTLCK				
DSPOPTSVR	CSI server	*USE	*EXECUTE	
DUPOPT	Dispozitiv optic	*USE	*EXECUTE	*USE - Volum sursă
				*ALL - Volum destinaţie
INZOPT	Directorul root (/) al volumului	*RWX	Nu se aplică	Nu se aplică
	Dispozitiv optic	*USE	*EXECUTE	*ALL
RCLOPT (Q)	Dispozitiv optic	*USE	*EXECUTE	
RMVOPTCTG (Q)	Dispozitiv optic	*USE	*EXECUTE	
RMVOPTSVR (Q)	CSI server	*USE	*EXECUTE	
WRKHLDOPTF[2]	Dispozitiv optic	*USE	*EXECUTE	*USE
	CSI server	*USE	*EXECUTE	
WRKOPTDIR[2]	Dispozitiv optic	*USE	*EXECUTE	*USE
	CSI server	*USE	*EXECUTE	
WRKOPTF[2]	Dispozitiv optic	*USE	*EXECUTE	*USE
	CSI server	*USE	*EXECUTE	
WRKOPTVOL[2]	Dispozitiv optic	*USE	*EXECUTE	

1 Volumele optice nu sunt obiecte sistem reale. Legătura între volumul optic şi lista de autorizare folosită pentru a securiza volumul este menţinută de funcţia de suport optic.

2 Sunt şapte opţiuni care pot fi invocate din utilităţile optice care nu sunt ele înseşi comenzi. Aceste opţiuni şi autorizările lor cerute pentru volumul optic sunt arătate mai jos.

Ştergere fişier: *CHANGE

Redenumire fişier: *CHANGE

Ştergere director: *CHANGE

Creare director: *CHANGE

Redenumire volum: *ALL

Eliberare fişier optic reţinut: *CHANGE

Salvare fişier optic reţinut: *USE - Volum sursă, *Change - Volum destinaţie

3 E necesară autorizare de gestionare listă de autorizaţii pentru lista care securizează curent volumul optic pentru a o modifica.

4 Pentru a folosi această comandă, trebuie să aveţi autorizaţia specială *IOSYSCFG.

5 Această verificare de autorizare este făcută doar când formatul mediului de stocare optic este UDF (Universal Disk Format).

Comenzile pentru coadă de ieşire

Comanda	Obiect referinţă	Parametri coadă de ieşire		Autorizaţie specială	Autorizaţie necesară	
		AUTCHK	OPRCTL		Pentru obiecte	Pentru biblioteci
CHGOUTQ [1]	Coadă de date				*READ	*EXECUTE
	Coadă de ieşire	*DTAAUT			*OBJMGT, *READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CLROUTQ [1]	Coadă de ieşire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CRTOUTQ	Coadă de date				*READ	*EXECUTE
	Coadă de ieşire					*READ, *ADD
DLTOUTQ	Coadă de ieşire				*OBJEXIST	*EXECUTE
HLDOUTQ [1]	Coadă de ieşire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
PRTQAUT [4]						
RLSOUTQ [1]	Coadă de ieşire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKOUTQ [1,3]	Coadă de ieşire				*READ	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKOUTQD [1,3]	Coadă de ieşire				*READ	*EXECUTE
			*YES	*JOBCTL		*EXECUTE

1 Dacă aveţi autorizarea specială *SPLCTL, nu aveţi nevoie de nici o autorizare pentru coada de ieşire. Aveţi nevoie de autorizarea specială *EXECUTE, totuşi, pentru biblioteca pentru coadă.

2 Trebuie să fiţi proprietarul cozii de ieşire.

3 Dacă cereţi să lucraţi cu toate cozile de ieşire, ecranul listă include toate cozile de ieşire din biblioteci pentru care aveţi autorizare *EXECUTE.

4 Trebuie să aveţi autorizaţia specială *ALLOBJ pentru a folosi această comandă.

Comenzile pentru pachet

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTSQLPKG	Program	*OBJOPR, *READ	*EXECUTE
	Pachet SQL: REPLACE(*NO)		*OBJOPR, *READ, *ADD, *EXECUTE
	Pachet SQL: REPLACE(*YES)	*OBJOPR, *OBJMGT, *OBJEXIST, *READ	*OBJOPR, *READ, *ADD, *EXECUTE
DLTSQLPKG	Pachet	*OBJEXIST	*EXECUTE
PRTSQLINF	Pachet	*OBJOPR, *READ	*EXECUTE
	Program	*OBJOPR, *READ	*EXECUTE
	Program service	*OBJOPR, *READ	*EXECUTE
STRSQL			

Comenzile pentru performanţă

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul cu securitatea poate acorda *USE altora.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDPEXDFN (Q) [5]	Bibliotecă PGM		*EXECUTE
ADDPEXFTR (Q)[5]	Bibliotecă PGMTRG		*EXECUTE
	Bibliotecă PGMFTR		*EXECUTE
	Cale JVAFTR	*X pentru director	
	Cale PATHFTR	*X pentru director	
ANZACCGRP (Q) [4]	QPFR/QPTPAGA0 *PGM	*USE	*EXECUTE
	Bibliotecă model		*EXECUTE, *ADD
	Descriere job	*USE	*EXECUTE
	QPFR/QCYRBCPP *PGM	*USE	*EXECUTE
	QPFR/QCYMBREX *PGM	*USE	*EXECUTE
ANZBESTMDL (Q)[4]	QPFR/QCYRBMN *PGM	*USE	*EXECUTE
	Bibliotecile aplicaţie care conţin fişierele bază de date care vor fi analizate		*EXECUTE
	Descriere de job	*USE	*EXECUTE
ANZDBF (Q)[4]	QPFR/QCYRBMN *PGM	*USE	*EXECUTE
	Descriere job	*USE	*EXECUTE
ANZDBFKEY (Q)	QPFR/QPTANZKC *PGM	*USE	*EXECUTE
	Bibliotecile aplicaţie care conţin programele care vor fi analizate		*EXECUTE
	Descriere job	*USE	*EXECUTE
ANZPGM (Q)	QPFR/QPTANZPC *PGM	*USE	*EXECUTE
	Date de performanţă[2]		*ADD, *READ

Comenzi performanţă

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
ANZPFRDTA (Q)[4]	QPFR/QACVPP *PGM	*USE	*EXECUTE
	Date de performanţă[2]		*ADD, *READ
ANZPFRDT2 (Q)[4]	QPFR/QAVCPP *PGM	*USE	*EXECUTE
	QAPTAPGP *FILE	*CHANGE	*EXECUTE
	Comanda DLTFCNARA (Q)	*USE	*EXECUTE
	QPFR/QPTAGRP *PGM	*USE	*EXECUTE
CFGPFRCOL (Q)	Bibliotecă colecţie		*EXECUTE
CHGFCNARA (Q)	QPFR/QPTAGRPD *PGM	*USE	*EXECUTE
	QAPGGPHF *FILE	*CHANGE	*EXECUTE
CHGGPHFMT (Q)	QPFR/QPGCRTFM *PGM	*USE	*EXECUTE
	QAPGPKGF *FILE	*CHANGE	*EXECUTE
	QAPGGPHF *FILE	*USE	*EXECUTE
CHGGPHPKG (Q)	QPFR/QPGCRTPK *PGM	*USE	*EXECUTE
	QAPMDMPT *FILE	*CHANGE	*EXECUTE
CHGJOBTYP (Q)	QPFR/QPTCHGJT *PGM	*USE	*EXECUTE
CHGPEXDFN (Q)[5]	Bibliotecă PGM		*EXECUTE
CHKPFRCOL (Q)			
CPYFCNARA (Q)[4]	QPFR/QPTAGRPR *PGM	*USE	*EXECUTE
	QAPGGPHF *FILE din biblioteca ″sursă″	*USE	*EXECUTE
	Biblioteca ″destinaţie″ (dacă QAPGGPHF *FILE nu există)		*EXECUTE, *ADD
	QAPGGPHF *FILE din biblioteca ″destinaţie″ (dacă se adaugă un nou format de grafic sau se înlocuieşte unul existent)	*CHANGE	*EXECUTE
CPYGPHFMT (Q)[4]	QPFR/QPGCPYGP *PGM	*USE	*EXECUTE
	QAPGPKGF *FILE din biblioteca ″sursă″	*USE	*EXECUTE
	Biblioteca ″În″ (dacă QAPGPKGF *FILE nu există)		*EXECUTE, *ADD
	QAPGPKGF *FILE din biblioteca ″destinaţie″ (dacă se adaugă un nou pachet grafic sau se înlocuieşte unul existent)	*CHANGE	*EXECUTE
	QAPGGPHF *FILE din biblioteca ″destinaţie″ (dacă se adaugă un nou pachet grafic sau se înlocuieşte unul existent)	*USE	*EXECUTE
CPYGPHPKG (Q)	QPFR/QPGCPYGP *PGM	*USE	*EXECUTE
	Bibliotecă sursă		*EXECUTE
	Bibliotecă destinaţie		*EXECUTE, *ADD
	Descriere de job	*USE	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CPYPFRDTA (Q)	QPFR/QITCPYCP *PGM	*USE	*EXECUTE
	Date de performanţă (toate fişierele QAPM*)	*USE	*EXECUTE
	Bibliotecă model		*EXECUTE, *ADD
	Descriere job	*USE	*EXECUTE
	QPFR/QCYCBMCP *PGM	*USE	*EXECUTE
	QPFR/QCYCBMDL *PGM	*USE	*EXECUTE
	QPFR/QCYOPDBS *PGM	*USE	*EXECUTE
	QPFR/QCYCLIDS *PGM	*USE	*EXECUTE
CRTBESTMDL (Q)	QPFR/QCYCAPT *PGM	*USE	*EXECUTE
	Biblioteca în care Zona funcţională este creată		*EXECUTE, *ADD
	QAPTAPGP *FILE din biblioteca destinaţie (dacă se adaugă o nouă zonă funcţională)	*CHANGE	*EXECUTE
CRTFCNARA (Q)	QPFR/QPTAGRP *PGM	*USE	*EXECUTE
	Biblioteca în care Formatul grafic este creat		*EXECUTE, *ADD
	QAPGGPHF *FILE din biblioteca destinaţie (dacă se adaugă o nou format de grafic)	*CHANGE	*EXECUTE
CRTGPHFMT (Q)	QPFR/QPGCRTFM *PGM	*USE	*EXECUTE
	Biblioteca în care este creat Pachetul grafic		*EXECUTE, *ADD
	QAPGGPHF *FILE	*CHANGE	*EXECUTE
	QAPGPKGF *FILE din biblioteca destinaţie (dacă se adaugă un nou pachet grafic)	*USE	*EXECUTE
CRTGPHPKG (Q)	QPFR/QPGCRTPK *PGM	*USE	*EXECUTE
	Biblioteca în care sunt create datele istorice		*ADD, *READ
	Descriere de job	*USE	*EXECUTE
CRTHSTDTA (Q)	QPFR/QPGCRTHS *PGM	*USE	*EXECUTE
	Bibliotecă destinaţie		*ADD, *READ
CRTPEXDTA (Q)[5]	Biblioteca *MGTCOL		*EXECUTE
	Biblioteca de date[1]		*READ, *ADD [2]
CRTPFRDTA (Q)	Bibliotecă sursă		*EXECUTE
	Bibliotecă destinaţie		*ADD, *READ
	Bibliotecă sursă		*USE
CVTPFRDTA (Q)	Descriere job	*USE	*EXECUTE
CVTPFRTHD (Q)	Date de performanţă[2]		*ADD, *READ
	Bibliotecă model		*EXECUTE, *ADD
	QPFR/QCYDBMDL *PGM	*USE	*EXECUTE
	QPFR/QCYCVTBD *CMD	*USE	*EXECUTE
DLTBESTMDL (Q)[4]	QPFR/QCYCBTOD *PGM	*USE	*EXECUTE
	QAPTAPGP *FILE din biblioteca zonei funcţionale	*CHANGE	*EXECUTE

Comenzi performanţă

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
DLTFCNARA (Q)[4]	QPFR/QPTAGRPD *PGM	*USE	*EXECUTE
	QAPGGPHF *FILE din biblioteca formatului grafic	*CHANGE	*EXECUTE
DLTGPHFMT (Q)[4]	QPFR/QPGDLTGP *PGM	*USE	*EXECUTE
	QAPGPKGF *FILE din biblioteca pachetul grafic	*CHANGE	*EXECUTE
DLTGPHPKG (Q)[4]	QPFR/QPGDLTGP *PGM	*USE	*EXECUTE
	QAPGHSTD *FILE din biblioteca datelor istorice	*CHANGE	*EXECUTE
	QAPGHSTI *FILE din biblioteca datelor istorice	*CHANGE	*EXECUTE
	QAPGSUMD *FILE din biblioteca datelor istorice	*CHANGE	*EXECUTE
DLTHSTDTA (Q)[4]	QPFR/QPGDLTHS *PGM	*USE	*EXECUTE
DLTPEXDTA (Q)[5]	Biblioteca de date[1]		*EXECUTE, *DELETE [2]
DLTPFRDTA (Q)[4]	QPFR/QPTDLTCP *PGM	*USE	*EXECUTE
DMPTRC (Q)[5]	Biblioteca în care vor fi memorate datele de urmărire		*EXECUTE, *ADD
	Fişier de ieşire (QAPTPAGD)	*CHANGE	*EXECUTE, *ADD
DSPACCGRP (Q)[4]	QPFR/QPTPAGD0 *PGM	*USE	*EXECUTE
	Biblioteca format sau pachet		*EXECUTE
	Biblioteca date istorice		*EXECUTE
	Biblioteca fişierului de ieşire		*EXECUTE, *ADD
	Coadă de ieşire	*USE	*EXECUTE
	Descriere de job	*USE	*EXECUTE
DSPHSTGPH (Q)[4]	QPFR/QPGCTRL *PGM	*USE	*EXECUTE
	Biblioteca date istorice		*EXECUTE
DSPPFRDTA (Q) [4]	QPFR/QAVCPP *PGM	*USE	*EXECUTE
	Biblioteca format sau pachet		*EXECUTE
	Date de performanţă[2]		*EXECUTE
	Biblioteca fişierului de ieşire		*EXECUTE, *ADD
	Coadă de ieşire	*USE	*EXECUTE
	Descriere job	*USE	*EXECUTE
DSPPFRGPH (Q)[4]	QPFR/QPGCTRL *PGM	*USE	*EXECUTE
	Biblioteca fişierului de ieşire		*EXECUTE
	Descriere job	*USE	*EXECUTE
ENDJOBTRC (Q)[4]	QPFR/QPTTRCJ0 *PGM	*USE	*EXECUTE
ENDPEX (Q)[5]	Biblioteca de date[1]		*READ, *ADD [2]
ENDPFRCOL (Q)			
PRTACTRPT (Q)[4]	QPFR/QITPRTAC *PGM	*USE	*EXECUTE
	Date de performanţă[2]	*USE	*ADD, *READ
	Descriere job	*USE	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
PRTCPTRPT (Q)[4]	QPFR/QPTCPTRP *PGM	*USE	*EXECUTE
	Date de performanţă[2]		*ADD, *READ
	Descriere job	*USE	*EXECUTE
PRTJOBRPT (Q)[4]	QPFR/QPTITVXC *PGM	*USE	*EXECUTE
	Date de performanţă[2]		*ADD, *READ
	Descriere job	*USE	*EXECUTE
PRTJOBTRC (Q)[4]	QPFR/QPTTRCRP *PGM	*USE	*EXECUTE
	Biblioteca fişier de urmărire job (QAPTTRCJ)		*EXECUTE
	Descriere job	*USE	*EXECUTE
PRTLCKRPT (Q)[4]	QPFR/QPTLCKQ *PGM	*USE	*EXECUTE
PRTPEXRPT[5]	Biblioteca de date[1]		*EXECUTE[2]
	Outfile	*USE	*EXECUTE, *ADD
	QPFR/QVPEPRTC *PGM	*USE	*EXECUTE
	QPFR/QVPESVGN *SRVPGM	*USE	*EXECUTE
	QPFR/QYPESVGN *SRVPGM	*USE	*EXECUTE
PRTPOLRPT (Q)[4]	QPFR/QPTITVXC *PGM	*USE	*EXECUTE
	Date de performanţă[2]		*ADD, *READ
	Descriere job	*USE	*EXECUTE
PRTRSCRPT (Q)[4]	QPFR/QPTITVXC *PGM	*USE	*EXECUTE
	Date de performanţă[2]		*ADD, *READ
	Descriere job	*USE	*EXECUTE
PRTSYSRPT (Q)[4]	QPFR/QPTTNSRP *PGM	*USE	*EXECUTE
	QAPMDMPT *FILE		*EXECUTE
	Descriere de job	*USE	*EXECUTE
PRTTNSRPT (Q)[4]	QPFR/QPTTNSRP *PGM	*USE	*EXECUTE
	Biblioteca fişier de urmărire (QTRJOBT)		*EXECUTE
	Descriere job	*USE	*EXECUTE
PRTTRCRPT (Q)[4]	QPFR/QPTTRCCP *PGM	*USE	*EXECUTE
RMVPEXDFN (Q)[5]			
RMVPEXFTR (Q)[5]			
STRBEST (Q)[4]	QPFR/QCYBMAIN *PGM	*USE	*EXECUTE
STRDBMON[3, 4]	Fişier ieşire	*OBJOPR, *ADD	*EXECUTE
STRJOBTRC (Q)	QPFR/QPTTRCJ1 *PGM	*USE	*EXECUTE
STRPEX (Q)[5]			
STRPFRCOL (Q)			
STRPFRG (Q)[4]	QPFR/QPGSTART *PGM	*USE	*EXECUTE

Comenzi performanţă

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
STRPFRT (Q)[4]	QPFR/QMNMAIN0 *PGM	*USE	*EXECUTE
	QAPTAPGP *FILE din biblioteca zonei funcţionale	*CHANGE	*EXECUTE
	Comanda CHGFCNARA (Q)	*USE	*EXECUTE
	Comanda CPYFCNARA (Q)	*USE	*EXECUTE
	Comanda CRTFCNARA (Q)	*USE	*EXECUTE
	Comanda DLTFCNARA (Q)	*USE	*EXECUTE
	QPFR/QPTAGRP *PGM	*USE	*EXECUTE
	QPFR/QPTAGRPD *PGM	*USE	*EXECUTE
	QPFR/QPTAGRPR *PGM	*USE	*EXECUTE
WRKFCNARA (Q)[4]	QPFR/QPTAGRPC *PGM	*USE	*EXECUTE
	Fişier de ieşire (QAITMON)	*CHANGE, *ALTER	*EXECUTE, *ADD
WRKPEXDFN (Q)[5]			
WRKPEXFTR (Q)[5]			
WRKSYSACT (Q)[3, 4]	QPFR/QITMONCP *PGM	*USE	*EXECUTE
Aceste comenzi nu necesită nici o autorizaţie obiect: • ENDDBMON[3] • ENDPFRTRC (Q) • STRPFRTRC (Q)			

1 Dacă se specifică biblioteca implicită (QPEXDATA), nu e verificată autorizarea pentru ea.

2 E necesară autorizare pentru biblioteca care conţine setul de fişiere bază de date. Nu e verificată autorizarea pentru setul individual de fişiere bază de date.

3 Pentru a folosi această comandă, trebuie să aveţi autorizarea specială *JOBCTL.

4 Pentru a folosi această comandă, trebuie să aveţi autorizarea specială *SERVICE.

5 Pentru a folosi această comandă, trebuie să aveţi autorizarea specială *SERVICE sau trebuie să fiţi autorizat pentru funcţia Urmărire serviciu din Operating System/400 prin suportul Administrare aplicaţie a Navigatorului iSeries. De asemenea, poate fi folosită comanda CHGFCNUSG (Change Function Usage - Modificare utilizare funcţie) cu ID-ul de funcţie QIBM_ACCESS_SERVICE_TRACE pentru a modifica lista de utilizatori cărora le este permis să realizeze operaţii de urmărire.

Comenzile pentru grup de descriptori de tipărire

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
CHGPDGPRF	Ptofil utilizator	*OBJMGT	
CRTPDG	Grup descriptor tipărire		*READ, *ADD
DLTPDG	Grup descriptor tipărire	*OBJEXIST	*EXECUTE
DSPPDGPRF	Ptofil utilizator	*OBJMGT	
RTVPDGPRF	Ptofil utilizator	*READ	

Comenzile de configurare Print Services Facility

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGPSFCFG [1, 2]			
CRTGPSFCFG [1, 2]			*READ, *ADD
DLTPSFCFG [1, 2]	Configurare PSF	*OBJEXIST	*EXECUTE
DSPPSFCFG [1]	Configurare PSF	*USE	*EXECUTE
WRKPSFCFG [1]	Configurare PSF	*READ	*EXECUTE

1 Opţiunea PSF/400 este necesară pentru a folosi această comandă.

2 Este necesară autorizarea specială *IOSYSCFG pentru a folosi această comandă.

Comenzile pentru problemă

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDPRBACNE (Q)	Filtru	*USE, *ADD	*EXECUTE
ADDPRBSLTE (Q)	Filtru	*USE, *ADD	*EXECUTE
ANZPRB (Q)	Comanda SNDSRVRQS	*USE	*EXECUTE
CHGPRB (Q)			*EXECUTE
CHGPRBACNE (Q)	Filtru	*USE, *UPD	*EXECUTE
CHGPRBSLTE (Q)	Filtru	*USE, *UPD	*EXECUTE
DLTPRB (Q) [3]	Comandă: DLTAPARDTA	*USE	*EXECUTE
DSPPRB	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
PTRINTDTA (Q)			
QRYPRBSTS (Q)			
VFYCMN (Q)	Descriere de linie [1]	*USE	*EXECUTE
	Descriere controler [1]	*USE	*EXECUTE
	ID reţea [1]	*USE	*EXECUTE
VFYOPT (Q)	Descriere dispozitiv	*USE	*EXECUTE
VFYTAP[4] (Q)	Descriere dispozitiv	*USE, *OBJMGT	*EXECUTE
VFYPRT (Q)	Descriere dispozitiv	*USE	*EXECUTE
WRKPRB (Q) [2]	Linie, controler, NWID (ID reţea) şi dispozitiv bazat pe acţiunea de analiză problemă	*USE	*EXECUTE

Comenzi problemă

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
[1] Aveţi nevoie de autorizare *USE pentru obiectul de comunicaţii pe care îl verificaţi [2] Trebuie să aveţi autorizare *USE pentru comanda SNDSRVRQS pentru a fi capabil să raportaţi o problemă. [3] Trebuie să aveţi autorizare pentru DLTAPARDTA dacă vreţi ca datele APAR asociate cu problema să fie de asemenea şterse. Vedeţi DLTAPARDTA din tabela de autorizări necesare pentru Comenzi service pentru a determina autorizările suplimentare necesare. [4] Trebuie să aveţi autorizarea specială *IOSYSCFG când descrierea de dispozitiv este alocată de un dispozitiv bibliotecă de medii de stocare.			

Comenzile pentru program

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
Autorizările pentru obiect necesare pentru comenzile CRT*xxx*PGM sunt afişate în tabela Limbaje din "Comenzile pentru limbaj" la pagina 361.			
ADDBKP [1]	Program manipulare punct de întrerupere	*USE	*EXECUTE
ADDPGM [1,2]	Program	*CHANGE	*EXECUTE
ADDTRC [1]	Program tratare urmărire	*USE	*EXECUTE
CALL	Program	*OBJOPR, *EXECUTE	*EXECUTE
	Program service [4]	*EXECUTE	*EXECUTE
CHGDBG	Operaţia de depanare	*USE, *ADD, *DLT	*EXECUTE
CHGHLLPTR [1]			
CHGPGM	Program	*OBJMGT, *USE	*USE
	Programul, dacă opţiunea de recreare este specificată, nivelul de optimizare este modificat sau colectarea datelor de performanţă s-a modificat	*OBJMGT, *USE	*USE, *ADD, *DLT
	Programul, dacă parametrul USRPRF sau USEADPAUT este modificat	Proprietarul [7]	*USE, *ADD, *DLT
CHGPGMVAR [1]			
CHGPTR [1]			
CHGSRVPGM	Program service	*OBJMGT, *USE	*USE
	Programul service, dacă opţiunea de recreare este specificată, nivelul de optimizare este modificat sau colectarea datelor de performanţă s-a modificat	*OBJMGT, *USE	*USE, *ADD, *DLT
	Program service, dacă parametrul USRPRF sau USEADPAUT este modificat.	Deţinătorul [7], *USE, *OBJMGT	*USE, *ADD, *DLT
CLRTRCDTA [1]			

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
CRTPGM	Program, Înlocuire(*NO)	Vedeţi regulile generale.	*READ, *ADD
	Program, Înlocuire(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Programul service specificat în parametrul BNDSRVPGM.	*USE	*EXECUTE
	Modul	*USE	*EXECUTE
	Director legare	*USE	*EXECUTE
CRTSRVPGM	Program service, Înlocuire(*NO)	Vedeţi regulile generale.	*READ, *ADD
	Program service, Înlocuire(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Modul	*USE	*EXECUTE
	Programul service specificat în parametrul BNDSRVPGM	*USE	*EXECUTE
	Exportar sursă fişier	*OBJOPR *READ	*EXECUTE
	Director legare	*USE	*EXECUTE
CVTCLSRC	Din-fişier	*USE	*EXECUTE
	În-fişier	*OBJOPR, *OBJMGT, *USE, *ADD, *DLT	*READ, *ADD
DLTDFUPGM	Program	*OBJEXIST	*EXECUTE
	Fişier afişare	*OBJEXIST	*EXECUTE
DLTPGM	Program	*OBJEXIST	*EXECUTE
DLTSRVPGM	Program service	*OBJEXIST	*EXECUTE
DMPCLPGM	Program CL	*USE	Nici unul[3]
DSPBKP [1]			
DSPDBG [1]			
DSPDBGWCH			
DSPMODSRC[2, 4]	Fişier sursă	*USE	*USE
	Orice fişier inclus	*USE	*USE
	Program	*CHANGE	*EXECUTE
DSPPGM	Program	*READ	*EXECUTE
	Program, dacă este specificat DETAIL(*MODULE)	*USE	*EXECUTE
DSPPGMREF	Program	*OBJOPR	*EXECUTE
	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
DSPPGMVAR [1]			
DSPSRVPGM	Program service	*READ	*EXECUTE
	Program service, dacă este specificat DETAIL(*MODULE)	*USE	*EXECUTE
DSPTRC [1]			
DSPTRCDTA [1]			
ENDCBLDBG (COBOL/400 programul licenţiat sau mediul S/38)	Program	*CHANGE	*EXECUTE

Comenzi program

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
ENDDBG [1]	Program depanare sursă	*USE	*USE
ENDRQS [1]			*EXECUTE
ENTCBLDBG (mediu S/38)	Program	*CHANGE	*EXECUTE
EXTPGMINF	Sursă fişier şi fişierele bazei de date	*OBJOPR	*EXECUTE
	Informaţii program		*READ, *ADD
PRTCMDUSG	Program	*USE	*EXECUTE
RMVBKP [1]			
RMVPGM [1]			
RMVTRC [1]			
RSMBKP [1]			
RTVCLSRC	Program	*OBJMGT, *USE	*EXECUTE
	Fişier sursă bază de date	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
SETATNPGM	Program manevrare cheie de atenţionare	*EXECUTE	*EXECUTE
SETPGMINF	Fişiere bază de date	*OBJOPR	*EXECUTE
	Fişier sursă	*USE	*EXECUTE
	Program root	*CHANGE	*READ, *ADD
	Subprogram	*USE	*EXECUTE
STRCBLDBG	Program	*CHANGE	*EXECUTE
STRDBG	Program [2]	*CHANGE	*EXECUTE
	Sursă fişier [4]	*USE	*EXECUTE
	Orice fişiere incluse [4]	*USE	*EXECUTE
	Program depanare sursă	*USE	*EXECUTE
	Program de mesaje nemonitorizate	*USE	*EXECUTE
TFRCTL [4]	Program	*USE sau o autorizare de date alta decât *EXECUTE	*EXECUTE
	Unele funcţii ale limbajului când se folosesc limbaje de nivel înalt	*READ	*EXECUTE
UPDPGM	Program	*OBJMGT, *OBJEXIST, *USE	*USE, *ADD
	Programul service specificat în parametrul BNDSRVPGM.	*USE	*EXECUTE
	Modul	*USE	*EXECUTE
	Director legare	*USE	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
UPDSRVPGM	Program service	*OBJMGT, *OBJEXIST, *USE	*USE, *ADD
	Programul service specificat în parametrul BNDSRVPGM	*USE	*EXECUTE
	Modul	*USE	*EXECUTE
	Director legare	*USE	*EXECUTE
	Exportar sursă fişier	*OBJOPR *READ	*EXECUTE
WRKPGM [6]	Program	Orice autorizaţie	*USE
WRKSRVPGM [6]	Program service	Orice autorizaţie	*USE

[1] Când un program este într-o operaţie de depanare, nici o autorizare nu mai este necesară pentru comenzile de depanare.

[2] Dacă aveţi autorizarea specială *SERVICE, vă trebuie doar autorizarea *USE pentru program.

[3] Comanda DMPCLPGM este cerută dintr-un program CL care rulează deja. Pentru că autorizarea la biblioteca care conţine programul este verificată la momentul când programul este apelat, autorizarea pentru bibliotecă nu este verificată din nou când comanda DMPCLPGM este rulată.

[4] Se aplică doar pentru programele ILE.

[5] Pentru informaţii suplimentare despre cerinţele de securitate pentru instrucţiunile SQL, vedeţi subiectul Autorizarea, privilegiile şi proprietatea obiectului din Referinţe SQL (în Centrul de informare iSeries).

[6] Pentru a folosi operaţiile individuale, vă trebuie autorizarea necesară de către operaţiile individuale.

[7] Trebuie să deţineţi programul sau să aveţi autorizările speciale *ALLOBJ şi *SECADM.

Comenzile pentru interogare

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ANZQRY	Definiţie interogare	*USE	*EXECUTE
CHGQRYA[4]			
CRTQMFORM	Formular Query Management: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Formular Query Management: REPLACE(*YES)	*ALL	*READ, *ADD, *EXECUTE
	Fişier sursă	*USE	*EXECUTE
CRTQMQRY	Interogare Query Management: REPLACE(*NO)		*READ, *ADD, *EXECUTE
	Interogare Query Management: REPLACE(*YES)	*ALL	*READ, *ADD, *EXECUTE
	Fişier sursă	*USE	*EXECUTE
	Comandă OVRDBF	*USE	*EXECUTE
DLTQMFORM	Formular Query Management	OBJEXIST	*EXECUTE
DLTQMQRY	Interogare Query Management	*OBJEXIST	*EXECUTE
DLTQRY	Definiţie interogare	*OBJEXIST	*EXECUTE

Comenzi de interogare

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
RTVQMFORM	Formular Query Manager	*OBJEXIST	*EXECUTE
	Fişier sursă destinaţie	*ALL	*READ, *ADD, *EXECUTE
	Comenzi ADDPFM, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, OVRDBF, RMVM	*USE	*EXECUTE
RTVQMQRY	Interogare Query Manager	*USE	*EXECUTE
	Fişier sursă destinaţie	*ALL	*READ, *ADD
	Comenzi ADDPFM, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, OVRDBF, RMVM	*USE	*EXECUTE
RUNQRY	Definiţie interogare	*USE	*USE
	Fişiere intrare	*USE	*EXECUTE
	Fişiere ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
STRQMQRY [1]	Interogare Query Management	*USE	*EXECUTE
	Formular Query Management, dacă este specificat.	*USE	*EXECUTE
	Definiţie interogare, dacă este specificat	*USE	*EXECUTE
	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
	Comenzi ADDPFM, CHGOBJD, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, GRTOBJAUT OVRDBF, OVRPRTF RMVM (dacă OUTPUT(*OUTFILE) este specificat)	*USE	*EXECUTE
STRQMPRC [1]	Fişier sursă care conţine procedura managerului de interogări	*USE	*EXECUTE
	Fişier sursă care conţine fişier sursă de comenzi, dacă este specificat	*USE	*EXECUTE
	Comandă OVRPRTF, dacă declaraţiile rezulztă în raport tipărit sau obiect interogare.	*USE	*EXECUTE
STRQRY			*EXECUTE
WRKQMFORM [3]	Formular Query Management	Orice autorizaţie	*USE
WRKQMQRY [3]	Interogare Query Management	Orice autorizaţie	*USE
WRKQRY [3]			

1 Pentru a rula STRQM, trebuie să aveţi autorizaţia cerută de declaraţiile din interogare. De exemplu, pentru a insera o linie într-o tabelă este necesară autorizaţia *OBJOPR, *ADD şi *EXECUTE pentru tabel.

2 Drept de proprietate sau unele autorizaţii pentru obiect sunt necesare.

3 Pentru a folosi operaţii individuale, trebuie să aveţi autorizaţia cerută de operaţii individuale.

4 Pentru a folosi comandă individuală, trebuie să aveţi autorizaţia specială *JOBCTL.

Comenzile pentru interpretorul shell QSH

Aceste comenzi nu necesită vreo autorizaţie pentru obiecte:

STRQSH [1] [2] QSH[1] [2]	
[1]	QSH este un alias pentru comanda CL STRQSH.
[2]	Utilizatorul are nevoie de autorizarea *X pentru toate scripturile şi toate directoarele din calea scriptului.

Comenzile pentru înrebare şi răspuns

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
ANSQST (Q)	Fişier bază de date QAQA*xx*BQPY [1]	*READ	*READ
ASKQST	Fişier bază de date QAQA*xx*BBPY [1] or QAQA*xx*BQPY [1]	*READ	*READ
CHGQSTDB (Q)	Fişier bază de date QAQA*xx*BQPY [1]	*READ	*READ
CRTQSTDB [2] (Q)	Fişiere bază de date		*READ, *ADD, *EXECUTE
CRTQSTLOD (Q)	Fişier bază de date QAQA*xx*BQPY [1]	*READ	*READ
DLTQST (Q)	Fişier bază de date QAQA*xx*BQPY [1]	*READ	*READ
DLTQSTDB (Q)	Fişier bază de date QAQA*xx*BQPY [1]	*READ	*READ
EDTQST (Q)	Fişier bază de date QAQA*xx*BQPY [1]	*READ	*READ
LODQSTDB [2] (Q)	Fişier bază de date QAQA*xx*BQPY [1,3]	*READ	*READ, *ADD, *EXECUTE
STRQST [4]	Fişier bază de date QAQA*xx*BBPY [1] or QAQA*xx*BQPY [1]	*READ	*READ
WRKQST	Fişier bază de date QAQA*xx*BBPY [1] QAQA*xx*BQPY [1]	*READ	*USE
WRKCNTINF			*EXECUTE

[1] Porţiunea “xx” a numelui fişierului este indexul bazei de date Întrebări şi răspunsuri care este operată de către comandă. Indexul este un număr de două cifre de la 00 la 99. Pentru a obţine indexul pentru o bază de date Întrebări şi răspunsuri, folosiţi comanda WRKCNTINF.

[2] Profilul de utilizator care rulează comanda devine proprietarul fişierelor nou create, cu excepţia cazului în care parametrul OWNER al profilului de utilizator este *GRPPRF. Autorizarea publică a noilor fişiere, cu excepţia QAQA*xx*BBPY, este setată la *EXCLUDE. Autorizarea publică pentru QAQA*xx*BBPY este setată la *READ.

[3] Este necesară autorizaţia pentru fişier numai dacă se încarcă o bază de date Întrebări şi Răspuns existentă.

[4] Comanda afişează meniul Întrebări şi răspunsuri. Pentru a folosi opţiuni individuale, trebuie să aveţi autorizaţia necesară pentru aceste opţiuni.

Comenzile pentru cititor

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
STRDBRDR	Coadă de ieşire	*OBJOPR, *ADD	*EXECUTE
	Fişier bază de date	*OBJOPR, *USE	*EXECUTE
	Coadă joburi	*READ	*EXECUTE
STRDKTRDR	Coadă de ieşire	*OBJOPR, *ADD	*EXECUTE
	Coadă joburi	*READ	*EXECUTE
	Descriere dispozitiv	*OBJOPR, *READ	*EXECUTE
Aceste comenzi nu necesită vreo autorizaţie obiect:			
ENDRDR [1]	HLDRDR [1]	RLSRDR [1]	

1 Trebuie să fiţi utilizatorul care a pornit cititorul, sau trebuie să aveţi autorizaţia specială (*ALLOBJ) sau control job (*JOBCTL).

Comenzile pentru facilitatea de înregistrare

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
ADDEXITPGM (Q)			
RMVEXITPGM (Q)			
WRKREGINF			

Comenzile pentru baze de date relaţionale

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
ADDRDBDIRE	Fişier sursă, dacă este specificat	*EXECUTE	*EXECUTE
CHGRDBDIRE	Fişier sursă, dacă este specificat	*EXECUTE	*EXECUTE
	Descriere dispozitiv locaţie la distanţă[7]	*CHANGE	
DSPRDBDIRE	Fişier sursă, dacă este specificat	Vedeţi regulile generale.	Vedeţi regulile generale.
Aceste comenzi nu necesită vreo autorizaţie obiect:			
RMVRDBDIRE WRKRDBDIRE			

1 Autorizaţie verificată atunci când este folosită intrarea director RDB.

Comenzile pentru resurse

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DSPHDWRSC			
DSPSFWRSC	Fişier sursă, dacă este specificat	Vedeţi regulile generale.	Vedeţi regulile generale.
EDTDEVRSC			
WRKHDWRSC [1]			

[1] Dacă folosiţi opţiunea de a crea un obiect de configuraţie, trebuie să aveţi autorizaţia de a folosi comanda CRT corespunzătoare.

Comenzile RJE (Intrare job la distanţă)

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDFCTE	Tabel de control formulare	*DELETE, *USE, *ADD	*READ, *EXECUTE
	Fişier dispozitiv [1,2]	*USE	*READ, *EXECUTE
	Fişier fizic [1,2] (RJE generates members)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Fişier fizic [1,2] (membru specificat)	*USE, *ADD	*READ, *EXECUTE
	Program [1,2]	*USE	*READ, *EXECUTE
	Coadă de mesaje [1,2]	*USE, *ADD	*READ, *EXECUTE
	Profil utilizator QUSER	*USE	*READ, *EXECUTE
ADDRJECMNE	Descriere sesiune	*USE, *ADD, *DLT	*READ, *EXECUTE
	Fişier BSC/CMN [1,2]	*USE	*READ, *EXECUTE
	Descriere dispozitiv [2]	*USE	*READ, *EXECUTE
	Profil utilizator QUSER	*USE	*READ, *EXECUTE
ADDRJERDRE	Descriere sesiune	*READ, *ADD, *DLT	*READ, *EXECUTE
	Coadă de joburi [2]	*READ	*READ, *EXECUTE
	Coadă de mesaje [2]	*READ, *ADD	*READ, *EXECUTE
ADDRJEWTRE	Descriere sesiune	*READ, *ADD, *DLT	*READ, *EXECUTE
	Fişier dispozitiv [1,2]	*USE	*READ, *EXECUTE
	Fişier fizic [1,2] (RJE generates members)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Fişier fizic [1,2] (membru specificat)	*OBJOPR, *ADD	*READ, *EXECUTE
	Program [1,2]	*USE	*READ, *EXECUTE
	Coadă de mesaje [1,2]	*USE, *ADD	*READ, *EXECUTE
	Profil utilizator QUSER	*USE	*READ, *EXECUTE
CHGFCT	Tabel de control formulare	*OBJOPR, *OBJMGT	*READ, *EXECUTE

Comenzi RJE (Intrare job la distanţă)

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
CHGFCTE	Tabel de control formulare	*USE	*READ, *EXECUTE
	Fişier dispozitiv [1,2]	*USE	*READ, *EXECUTE
	Fişier fizic [1,2] (RJE generates members)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Fişier fizic [1,2] (membru specificat)	*USE, *ADD	*READ, *EXECUTE
	Program [1,2]	*USE	*READ, *EXECUTE
	Coadă de mesaje [1,2]	*USE, *ADD	*READ, *EXECUTE
	Profil utilizator QUSER	*USE	*READ, *EXECUTE
CHGRJECMNE	Descriere sesiune	*USE	*READ, *EXECUTE
	Fişier BSC/CMN [1,2]	*USE	*READ, *EXECUTE
	Descriere dispozitiv [2]	*USE	*READ, *EXECUTE
	Profil utilizator QUSER	*USE	*READ, *EXECUTE
CHGRJERDRE	Descriere sesiune	*USE, *ADD, *DLT	*READ, *EXECUTE
	Coadă de joburi [2]	*USE	*READ, *EXECUTE
	Coadă de mesaje [2]	*USE, *ADD	*READ, *EXECUTE
CHGRJEWTRE	Descriere sesiune	*USE	*READ, *EXECUTE
	Fişier dispozitiv [1,2]	*USE	*READ, *EXECUTE
	Fişier fizic [1,2] (RJE generates members)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Fişier fizic [1,2] (membru specificat)	*OBJOPR, *ADD	*READ, *EXECUTE
	Program [1,2]	*USE	*READ, *EXECUTE
	Coadă de mesaje [1,2]	*USE, *ADD	*READ, *EXECUTE
	Profil utilizator QUSER	*USE	*READ, *EXECUTE
CHGSSND	Descriere sesiune	*OBJMGT, *READ, *UPD, *OBJOPR	*EXECUTE, *READ
	Coadă de joburi [1,2]	*USE	*EXECUTE
	Coadă de mesaje [1,2]	*USE, *ADD	*EXECUTE
	Tabel de control formulare [1,2]	*USE	*EXECUTE
	Profil utilizator QUSER	*USE	*EXECUTE
CNLRJERDR	Descriere sesiune	*USE	*EXECUTE
	Coadă de ieşire	*USE, *ADD	*EXECUTE
CNLRJEWTR	Descriere sesiune	*USE	*EXECUTE
	Coadă de ieşire	*USE, *ADD	*EXECUTE
CRTFCT	Tabel de control formulare		*READ, *ADD
CRTRJEBSCF	Fişier BSC		*READ, *EXECUTE, *ADD
	Fişier fizic sursă(DDS)	*READ	*EXECUTE
	Descriere dispozitiv	*READ	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTRJECFG	Descriere sesiune		*READ, *ADD, *UPD, *OBJOPR
	Coadă joburi		*READ, *ADD
	Descriere job		*READ, *OBJOPR, *ADD
	Descriere subsistem		*READ, *OBJOPR, *ADD
	Coadă de ieşire		*READ, *ADD
	Fişier CMN		*READ, *EXECUTE, *ADD
	Fişier BSC		*READ, *EXECUTE, *ADD
	Fişier imprimantă		*USE, *ADD
CRTRJECFG	Fişier fizic		*EXECUTE, *ADD
	Profil utilizator QUSER [3]	*USE	*EXECUTE
	Coadă de ieşire	*READ	*EXECUTE
	Tabel de control formulare	*READ	*READ
	Descriere dispozitiv		*EXECUTE
	Descriere controler		*EXECUTE
	Descriere de linie		*EXECUTE
CRTRJECMNF	Fişier de comunicaţie		*READ, *EXECUTE, *ADD
	Fişier fizic sursă(DDS)	*READ	*EXECUTE
	Descriere dispozitiv	*READ	*EXECUTE
CRTSSND	Descriere sesiune		*READ, *ADD, *UPD, *OBJOPR
	Coadă de joburi [1,2]	*USE	*EXECUTE
	Coadă de mesaje [1,2]	*USE, *ADD	*EXECUTE
	Tabel de control formulare [1,2]	*USE	*EXECUTE
	Profil utilizator QUSER	*USE	*EXECUTE
CVTRJEDTA	Tabel de control formulare	*USE	*EXECUTE
	Fişier de intrare	*USE, *UPD	*EXECUTE
	Fişier de ieşire (RJE generează membru)	*OBJMGT, *USE, *ADD	*READ, *EXECUTE, *ADD
	Fişier ieşire (membru specificat)	*USE, *ADD	*EXECUTE
DLTFCT	Tabel de control formulare	*OBJEXIST	*EXECUTE

Comenzi RJE (Intrare job la distanţă)

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
DLTRJECFG	Descriere sesiune	*OBJEXIST	*EXECUTE
	Coadă joburi	*OBJEXIST	*EXECUTE
	Fişier BSC/CMN	*OBJEXIST, *OBJOPR	*EXECUTE
	Fişier fizic	*OBJEXIST, *OBJOPR	*EXECUTE
	Fişier imprimantă	*OBJEXIST, OBJOPR	*EXECUTE
	Coadă de ieşire	*OBJEXIST, *USE, *DLT	*EXECUTE
	Descriere job	*OBJEXIST	*EXECUTE
	Descriere subsistem	*OBJEXIST, *USE	*EXECUTE
	Descriere dispozitiv [4]	*OBJEXIST	*EXECUTE
	Descriere controler [4]	*OBJEXIST	*EXECUTE
	Descriere de linie [4]	*OBJEXIST	*EXECUTE
DLTSSND	Descriere sesiune	*OBJEXIST	*EXECUTE
DSPRJECFG	Descriere sesiune	*READ	*EXECUTE
ENDRJESSN [5]	Descriere sesiune	*USE	*EXECUTE
RMVFCTE	Tabel de control formulare	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJECMNE	Descriere sesiune	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJERDRE	Descriere sesiune	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
RMVRJEWTRE	Descriere sesiune	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE
SNDRJECMD	Descriere sesiune	*USE	*EXECUTE
SBMRJEJOB	Descriere sesiune	*USE	*EXECUTE
	Fişier intrare [6]	*USE	*EXECUTE
	Coadă de ieşire	*USE, *ADD	*EXECUTE
	Obiecte legate de job [7]		
SNDRJECMD	Descriere sesiune	*USE	*EXECUTE
STRRJECSL	Descriere sesiune	*USE	*EXECUTE
	Coadă de ieşire	*USE	*EXECUTE
STRRJERDR	Descriere sesiune	*USE	*USE
STRRJESSN [5]	Descriere sesiune	*USE	*USE, *ADD
	Program	*USE	*EXECUTE
	Profil utilizator QUSER	*USE	*EXECUTE
	Obiecte legate de job [7]		*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
STRRJEWTR	Descriere sesiune	*USE	*USE
	Program [1]	*USE	*READ, *EXECUTE
	Fişier dispozitiv [1]	*USE, *ADD	*READ, *EXECUTE
	Fişier fizic [1] (RJE generează membri)	*OBJMGT, *USE, *ADD	*OBJOPR, *ADD
	Fişier fizic [1] (membru specificat)	*READ, *ADD	*READ, *EXECUTE
	Coadă de mesaje [1]	*USE, *ADD	*READ, *EXECUTE
	Profil utilizator QUSER	*USE	*READ, *EXECUTE
WRKFCT [8]	Tabel de control formulare	*USE	*EXECUTE
WRKRJESSN [8]	Descriere sesiune	*USE	*EXECUTE
WRKSSND [8]	Descriere sesiune	*CHANGE	*EXECUTE

1 Profil utilizator QUSER necesită autorizaţie pentru acest obiect.

2 Dacă obiectul nu este găsit sau nu este deţinută autorizaţia necesară, un mesaj informaţional este trimis şi funcţia comenzii este încă realizată.

3 Această autorizaţie este necesară pentru a crea descrierea jobului QRJESSN.

4 Această autorizaţie este necesară doar când DLTCMN(*YES) este specificat.

5 Trebuie să aveţi autorizaţia specială *JOBCTL.

6 Fişierele de intrare au include acestea folosind declaraţia de control.. READFILE.

7 Examinaţi autorizările necesare pentru comanda SBMJOB.

8 Pentru a folosi o operaţie individuală, trebuie să aveţi autorizaţia necesară de operaţie.

Comenzile pentru atribute de securitate

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CHGSECA [1]			
CHGSECAUD [2,3]			
CFGSYSSEC [1,2,3]			
DSPSECA			
DSPSECAUD [3]			
PRTSYSSECA [4]			

1 Trebuie să aveţi autorizaţia specială *SECADM pentru a folosi această comandă.

2 Trebuie să aveţi autorizaţia specială *ALLOBJ pentru a folosi această comandă.

3 Trebuie să aveţi autorizaţia specială *AUDIT pentru a folosi această comandă.

4 Trebuie să aveţi autorizaţia specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.

Comenzile pentru intrare autentificare server

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDSVRAUTE[1]			
CHGSVRAUTE[1]			
DSPSVRAUTE	Ptofil utilizator	*READ	*EXECUTE
RMVSVRAUTE[1]			

[1] Dacă profilul utilizator pentru această operaţie nu este *CURRENT sau utilizatorul curent pentru job, trebuie să aveţi autorizaţia specială *SECADM şi autorizaţia *USE pentru profil.

Comenzile pentru service

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDTRCFTR[11]			
APYPTF (Q)	Bibliotecă produs	*OBJMGT	
CHGSRVA [3] (Q)			
CHKCMNTRC [3] (Q)			*EXECUTE
CHKPRDOPT (Q)	Toate obiectele din opţiunea produs [4]		
CPYPTF[2](Q)	Fişier-sursă	*USE	*EXECUTE
	Fişier-destinaţie[8]	Aceleaşi cerinţe ca şi comanda SAVOBJ	Aceleaşi cerinţe ca şi comanda SAVOBJ
	Descriere dispozitiv	*USE	*EXECUTE
	Program licenţiat		*USE
	Comenzi: CHKTAP, CPYFRMTAP, CPYTOTAP, CRTLIB, CRTSAVF, CRTTAPF şi OVRTAPF	*USE	*EXECUTE
	Biblioteca QSRV	*USE	*EXECUTE
CPYPTFGRP [2] (Q)	Descriere dispozitiv	*USE	*EXECUTE
	În-fişier	*Aceleaşi cerinţe ca şi comanda SAVOBJ	*Aceleaşi cerinţe ca şi comanda SAVOBJ
	Din-fişier	*USE	*EXECUTE
	Comenzi: CHKTAP, CRTLIB, CRTSAVF	*USE	*EXECUTE
DLTAPARDTA (Q)			
DLTCMNTRC [3] (Q)	NWID (ID reţea) sau descriere de linie	*USE	*EXECUTE
DLTPTF (Q)	Fişier scrisoare de copertă [4]		*EXECUTE
	Fişier de salvare PTF [4]		*EXECUTE
DLTTRC (Q)	Comanda RMVM	*USE	
	Bibliotecă	*EXECUTE	
	Fişier bază de date	*OBJEXIST, *OBJOPR	

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
DMPJOB (Q)			*EXECUTE
DMPJOBINT (Q)			
DSPPTF (Q)	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
DSPSRVA (Q)			
DSPSRVSTS (Q)			
ENDCMNTRC [3] (Q)	NWID sau descriere de linie	*USE	*EXECUTE
ENDCPYSCN (Q)	Descriere dispozitiv	*USE	*EXECUTE
ENDSRVJOB (Q)			
ENDTRC (Q)	Bibliotecă	*ADD, *EXECUTE	
	Fişiere bază de date	*OBJOPR, *OBJMGMT, *ADD, *DLT	
	Comenzi: PTRTRC, DLTTRC	*USE	
INSPTF[9] (Q)			
LODPTF (Q)	Descriere dispozitiv	*USE	*EXECUTE
LODRUN [2]	Comanda RSTOBJ	*USE	*EXECUTE
PRTCMNTRC [3] (Q)	NWID (ID reţea) sau descriere de linie	*USE	*EXECUTE
	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
PRTERRLOG (Q)	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
PRTINTDTA[12,13] (Q)			
PRTTRC (Q)	Bibliotecă	*EXECUTE	
	Fişier bază de date	*USE	
	Comanda DLTTRC	*USE	
RMVPTF (Q)	Bibliotecă produs	*OBJMGT	
RMVTRCFTR[11]			
RUNLPDA (Q)	Descriere de linie	*READ	*EXECUTE
SAVAPARDTA [6] (Q)	Comenzi: CRTDUPOBJ, CRTLIB, CRTOUTQ, CRTSAVF, DLTF, DMPOBJ, DMPSYSOBJ, DSPCTLD, DSPDEVD, DSPHDWRSC, DSPJOB, DSPLIND, DSPLOG, DSPNWID, DSPPTF, DSPSFWRSC, OVRPRTF, PRTERRLOG, PRTINTDTA, SAV, SAVDLO, SAVLIB, SAVOJB, WRKACTJOB şi WRKSYSVAL	*USE	*EXECUTE
	Problemă existentă [7]	*CHANGE	*EXECUTE
SNDPTFORD [10] (Q)			
SNDSRVRQS (Q)			
STRCMNTRC [3] (Q)	NWID (ID reţea) sau descriere de linie	*USE	*EXECUTE
STRCPYSCN	Coadă joburi	*USE	*EXECUTE
	Descriere dispozitiv	*USE	*EXECUTE
	Fişier sursă, dacă este specificat	Vedeţi regulile generale.	Vedeţi regulile generale.
STRSRVJOB (Q)	Profil utilizator al jobului	*USE	*EXECUTE

Comenzi service

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
STRSST [3] (Q)			
STRTRC (Q)		*READ, *WRITE	
TRCCNN[11]			
TRCCPIC (Q)			
TRCICF (Q)			
TRCINT[11] (Q)			
TRCJOB (Q)	Fişier sursă, dacă este specificat	Vedeţi regulile generale.	Vedeţi regulile generale.
	Program de ieşire, dacă există	*USE	*EXECUTE
TRCTCPAPP[11] (Q)	Program ieşire utilizator	*USE	*EXECUTE
	Descriere de linie	*USE	
	Interfaţă reţea	*USE	
	Server de reţea	*USE	
VFYCMN (Q)	Descriere de linie [5]	*USE	*EXECUTE
	Descriere controler [5]	*USE	*EXECUTE
	ID reţea [5]	*USE	*EXECUTE
VFYLNKLPDA (Q)	Descriere de linie	*READ	*EXECUTE
VFYPRT (Q)	Descriere dispozitiv	*USE	*EXECUTE
VFYOPT (Q)	Descriere dispozitiv	*USE	*EXECUTE
VFYTAP[14] (Q)	Descriere dispozitiv	*USE, *OBJMGT	*EXECUTE
WRKCNTINF (Q)			
WRKFSTAF (Q)	QUSRSYS/QPVINDEX *USRIDX	*CHANGE	*USE
WRKFSTPCT (Q)	QUSRSYS/QPVPCTABLE *USRIDX	*CHANGE	*USE
WRKPRB [1, 10] (Q)	Linie, controler, NWID (ID reţea) şi dispozitiv bazat pe acţiunea de analiză problemă	*USE, *ADD	*EXECUTE
WRKPTFGRP (Q)			
WRKSRVPVD (Q)			

1 Aveţi nevoie de autorizaţie pentru comanda PRTERRLOG pentru unele proceduri de analiză dacă înregistrările din istoricul de erori sunt salvate.

2 Se aplică deasemenea toate restricţiile pentru comanda RSTOBJ.

3 Autorizaţia specială Service (*SERVICE) este necesară pentru a rula această comandă.

4 Obiectele listate sunt folosite de comandă, dar autorizaţia pentru obiecte nu este verificată. Autorizaţia pentru a folosi comanda este suficientă pentru a folosi obiectele.

5 Aveţi nevoie de autorizaţia *USE pentru obiectele de comunicaţii pe care le verificaţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
[6] Trebuie să aveţi autorizaţia specială *SPLCTL pentru a salva un fişier de spool.			
[7] Atunci când SAVAPARDTA este rulată pentru o problemă nouă, o bibiliotecă unică APAR este creată pentru acea problemă. Dacă rulaţi din nou SAVAPARDTA pentru aceeaşi problemă pentru a colecta mai multe informaţii, trebuie să aveţi autorizaţia Use pentru biblioteca APAR pentru acea problemă.			
[8] Opţiunea de a adăuga un membru nou la un fişier de ieşire existent nu este validă pentru această comandă.			
[9] Această comandă are aceleaşi autorizaţii şi restricţii ca şi comenzile APYPTF şi LODPTF.			
[10] Pentru a accesa opţiunile 1 şi 3 din ecranule ″Selectare opţiune de raport″ trebuie să aveţi autorizaţia *USE pentru comanda SNDSRVRQS.			
[11] Pentru a folosi această comandă, trebuie să aveţi autorizaţia specială *SERVICE sau să fiţi autorizaţi pentru funcţia Urmărire service din OS/400 prin suportul de Administrare aplicaţie al Navigatorului iSeries. Comanda Modificare informaţii de folosire funcţie (CHGFCNUSG), cu un ID funcţie QIBM_SERVICE_TRACE, poate fi folosită deasemnea pentru a modifica lista de utilizatori care au permisunea de a realiza operaţii de urmărire.			
[12] Pentru a folosi această comandă, trebuie să aveţi autorizaţia specială *SERVICE sau să fiţi autorizaţi pentru funcţia Dump service din OS/400 prin suportul de Administrare aplicaţie al Navigatorului iSeries. Se poate folosi de asemenea comanda Modificare informaţii de folosire funcţie (CHGFCNUSG), cu un ID funcţie de QIBM_SERVICE_DUMP, pentru a modifica lista utilizatorilor care au permisiunea de a rula operaţii de dump.			
[13] Această comandă trebuie să fie lansată din job cu datele interne fiind tipărite,sau emiţătorul comenzii trebuie să ruleze sub un profil utilizator care este acelaşi ca şi identitate userului jobului cu datele interne fiind tipărite, sau emiţătorul comenzii trebuie să ruleze sub un profil utilizator care are autorizaţia specială de control job (*JOBCTL).			
[14] Trebuie să aveţi autorizarea specială *IOSYSCFG când descrierea de dispozitiv este alocată de un dispozitiv bibliotecă de medii de stocare.			

Comenzile pentru dicţionar de ajutor la corectare ortografică

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTSPADCT	Dicţionar ajutător pentru corectare ortografică	*OBJEXIST	*EXECUTE
	Dicţionar - REPLACE(*NO)		*READ, *ADD
	Dicţionar - REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
DLTSPADCT	Dicţionar ajutător pentru corectare ortografică	*OBJEXIST	*EXECUTE
WRKSPADCT [1]	Dicţionar ajutător pentru corectare ortografică	Orice autorizaţie	*USE
[1] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizaţia necesară de operaţie.			

Comenzile pentru sferă de control

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDSOCE	Sferă de control[1]	*USE, *ADD	*EXECUTE
DSPSOCSTS			
RMVSOCE	Sferă de control[1]	*USE, *DLT	*EXECUTE
WRKSOC	Sferă de control[1]	*USE	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
[1] Sfera de control este fişier fizic QUSRSYS/QAALSOC.			

Comenzile pentru fişier spool

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Parametri coadă de ieşire			Autorizaţie specială	Autorizaţie necesară	
		DSPDTA	AUTCHK	OPRCTL		Pentru obiecte	Pentru biblioteci
CHGSPLFA [1,2]	Coadă de ieşire[3]		*DTAAUT			*READ, *DLT, *ADD	
			*OWNER			Proprietar [4]	
				*YES	*JOBCTL		
CHGSPLFA [1], dacă se mută fişierul de spool	Coadă de ieşire originală [3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Proprietar [4]	
				*YES	*JOBCTL		
	Fişier spoll	*OWNER				Proprietar [6]	
	Coadă de ieşire destinaţie[7]					*READ	*EXECUTE
				*YES	*JOBCTL		*EXECUTE
	Dispozitiv destinaţie					*USE	
CPYSPLF [1]	Fişier bază de date					Vedeţi regulile generale.	Vedeţi regulile generale.
	Fişier spoll	*OWNER				Proprietar [6]	
	Coadă de ieşire[3]	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Proprietar [4]	
		*YES sau *NO		*YES	*JOBCTL		
DLTSPLF [1]	Coadă de ieşire[3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Proprietar [4]	
				*YES	*JOBCTL		

Comanda	Obiect referinţă	Parametri coadă de ieşire			Autorizaţie specială	Autorizaţie necesară	
		DSPDTA	AUTCHK	OPRCTL		Pentru obiecte	Pentru biblioteci
DSPSPLF [1]	Coadă de ieşire[3]	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Proprietar [4]	
		*YES sau *NO		*YES	*JOBCTL		
	Fişier spoll	*OWNER				Proprietar [6]	
HLDSPLF [1]	Coadă de ieşire[3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Proprietar [4]	
				*YES	*JOBCTL		
RCLSPLSTG (Q)							
RLSSPLF [1, 8]	Coadă de ieşire[3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Proprietar [4]	
				*YES	*JOBCTL		
SNDNETSPLF [1,5]	Coadă de ieşire[3]	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Proprietar [4]	
		*YES sau *NO		*YES	*JOBCTL		
	Fişier spoll	*OWNER				Proprietar [6]	
WRKSPLF							

1 Utilizatorii sunt întodeauna autorizaţi pentru a-şi controla propriile fişier de spool.

2 Pentru a muta un fişier spool în faţa unei cozi de ieşire (PRTSEQ(*NEXT)) sau pentru a-i modifica prioritatea la o valoare mai mare decât limita specificată în profilul utilizator, trebuie să aveţi una din autorizările arătate în coada de ieşire sau să aveţi autorizaţia specială *SPLCTL.

3 Dacă aveţi autorizarea specială *SPLCTL, nu aveţi nevoie de nici o autorizare pentru coada de ieşire.

4 Trebuie să fiţi proprietarul cozii de ieşire.

5 Trebuie să aveţi autorizaţia *USE pentru coada de ieşire a primitorului pentru biblioteca cozii de ieşire atunci când trimiteţi un fişier unui utilizator de pe acelaşi subsistem.

6 Trebuie să fiţi proprietarul fişierului spool.

7 Dacă aveţi autorizaţia specială *SPLCTL, nu aveţi nevoie de autorizaţie pentru coada de ieşire destinaţie dar trebuie să aveţi autorizaţia *EXECUTE pentru bibliotecă.

8 Când fişierul spool a fost reţinut cu HLDJOB SPLFILE(*YES) şi fişierul spool a fost deasemenea decuplat de la job, utilizatorul trebuie să aibă autorizaţia *USE pentru comanda RLSJOB fie autorizaţia specială *JOBCTL sau să fie proprietarul fişierului spool.

Comenzile pentru descriere subsistem

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
ADDAJE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job	*OBJOPR, *READ	*EXECUTE
ADDCMNE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job	*OBJOPR, *READ	*EXECUTE
	Ptofil utilizator	*USE	
ADDJOBQE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
ADDPJE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Ptofil utilizator	*USE	
	Descriere job	*OBJOPR, *READ	*EXECUTE
ADDRTGE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
ADDWSE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job	*OBJOPR, *READ	*EXECUTE
CHGAJE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job	*OBJOPR, *READ	*EXECUTE
CHGCMNE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job	*OBJOPR, *READ	*EXECUTE
	Ptofil utilizator	*USE	
CHGJOBQE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
CHGPJE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Ptofil utilizator	*USE	
	Descriere job	*OBJOPR, *READ	*EXECUTE
CHGRTGE	Descriere subsistem	*OJBOPR, *OBJMGT, *READ	*EXECUTE
CHGSBSD [5]	Descriere subsistem	*OJBOPR, *OBJMGT, *READ	*EXECUTE
	fişier afişare semnare[4]	*USE	*EXECUTE
CHGWSE	Descriere subsistem	*OJBOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job	*OBJOPR, *READ	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTSBSD [5] (Q)	Descriere subsistem		*READ, *ADD
	fişier afişare semnare[4]	*USE	*EXECUTE
DLTSBSD	Descriere subsistem	*OBJEXIST, *USE	*EXECUTE
DSPSBSD	Descriere subsistem	*OBJOPR, *READ	*EXECUTE
ENDSBS [1]			
PRTSBSDAUT [6]			
RMVAJE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVCMNE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVJOBQE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVPJE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVRTGE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
RMVWSE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
STRSBS [1]	Descriere subsistem	*USE	*EXECUTE
WRKSBS [2, 3]	Descriere subsistem	Orice autorizaţie	*USE
WRKSBSD [3]	Descriere subsistem	Orice autorizaţie	*USE

1 Trebuie să aveţi autorizarea specială de control de joburi (*JOBCTL) pentru a folosi această comandă.

2 Necesită unele autorizaţii (orice înafară de *EXCLUDE)

3 Pentru a folosi o operaţie individuală, trebuie să aveţi autorizaţia necesară de operaţie.

4 Autorizaţia este necesară pentru a realiza verificările de forma ale fişierului de afişare. Acest ajutor prezice că afişare va merge coret atunci când subsistemul este pornit. Atunci când nu sunteţi autorizat pentru fişierul de afişare sau biblioteca lui, aceste verificări de format nu vor fi realizate.

5 Trebuie să aveţi autorizaţia specială *SECADM sau *ALLOBJ pentru a specifica o anumită bibliotecă pentru bibloteca subsistem.

6 Trebuie să aveţi autorizaţia specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.

Comenzile pentru sistem

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
PWRDWNSYS[1]	Catalog de imagini (dacă este specificat)	*USE	
Aceste comenzi nu necesită nici o autorizaţie obiect:			
CHGSHRPOOL DSPSYSSTS ENDSYS[1] RCLACTGRP[1]	RCLRSC RETURN RTVGRPA	SIGNOFF WRKSHRPOOL	WRKSYSSTS

1 Trebuie să aveţi autorizarea specială de control de joburi (*JOBCTL) pentru a folosi această comandă.

Comenzile pentru listă de replici sistem

Aceste comenzi nu necesită autorizaţii obiect:			
ADDRPYLE (Q)	CHGRPYLE (Q)	RMVRPYLE (Q)	WRKRPYLE

Comenzile pentru valori de sistem

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Aceste comenzi nu necesită vreo autorizaţie obiect:			
CHGSYSVAL (Q) [1,2]	DSPSYSVAL[3]	RTVSYSVAL[3]	WRKSYSVAL [1,2, 3]

[1] Pentru a modifica unele valori sistem, trebuie să aveţi autorizările speciale *ALLOBJ, *ALLOBJ şi *SECADM, *AUDIT, *IOSYSCFG sau *JOBCTL.

[2] Pentru a folosi această comandă cum a fost livrată de IBM, trebuie să fiţi semnat ca QPGMR, QSYSOPR sau QSRV sau să aveţi autorizarea specială *ALLOBJ.

[3] Pentru a afişa sau extrage valori de sistem referitoare la auditare, trebuie să aveţi autorizarea specială *AUDIT sau *ALLOBJ.

Comenzile pentru mediul System/36

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

		Autorizări necesare	
Comanda	**Obiect referinţă**	**Pentru obiecte**	**Pentru biblioteci**
CHGS36	Obiect de configurare S/36 QS36ENV	*UPD	*EXECUTE
CHGS36A	Obiect de configurare S/36 QS36ENV	*UPD	*EXECUTE
CHGS36PGMA	Program	*OBJMGT, *USE	*EXECUTE
CHGS36PRCA	Fişier QS36PRC	*OBJMGT, *USE	*EXECUTE
CHGS36SRCA	Sursă	*OBJMGT, *USE	*EXECUTE
CRTMSGFMNU	Meniu: REPLACE(*NO)		*READ, *ADD
	Meniu: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD
	Fişier de afişare dacă există	*ALL	*EXECUTE
	Fişier de mesaje	*USE	*CHANGE
	Fişier sursă QS36SRC	*ALL	*EXECUTE
CRTS36DSPF	Fişier de afişare: REPLACE(*NO)		*READ, *ADD
	Fişier de afişare: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD, *CHANGE
	Fişier-destinaţie sursă când TOMBR nu e *NONE	*ALL	*CHANGE
	Fişier sursă QS36SRC	*USE	*EXECUTE
	Comanda Creare fişier de afişare (CRTDSPF)	*OBJOPR	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTS36MNU	Meniu: REPLACE(*NO)		*READ, *ADD, *CHANGE
	Meniu: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD, *CHANGE
	Fişier-destinaţie sursă când TOMBR nu e *NONE	*ALL	*CHANGE
	Fişier sursă QS36SRC	*USE	*EXECUTE
	Fişier de afişare când REPLACE(*YES) este specificat	*ALL	*EXECUTE
	Fişiere de mesaje numite în sursă	*ALL	*EXECUTE
	Fişier afişare		*CHANGE
	Comanda CRTMSGF	*OBJOPR, *OBJEXIST	*EXECUTE
	Comanda ADDMSGD	*OBJOPR	*EXECUTE
	Comanda CRTDSPF	*OBJOPR	*EXECUTE
CRTS36MSGF	Fişier de mesaje: REPLACE(*NO)		*READ, *ADD, *CHANGE
	Fişier de mesaje: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD, *CHANGE
	Fişier-destinaţie sursă când TOMBR nu e *NONE	*ALL	*CHANGE
	Fişier sursă QS36SRC	*USE	*EXECUTE
	Fişier de afişare când REPLACE(*YES) este specificat	*ALL	*EXECUTE
	Fişier de afişare numite în sursă	*ALL	*EXECUTE
	Fişier de mesaje numite în sursă când OPTION este *ADD sau *CHANGE	*CHANGE	*EXECUTE
	Fişiere de mesaje numite în sursă când OPTION(*CREATE) este specificat	*ALL	*EXECUTE
	Comanda CRTMSGF	*OBJOPR, *OBJEXIST	*EXECUTE
	Comanda ADDMSGD	*OBJOPR	*EXECUTE
	Comanda CHGMSGD când OPTION(*CHANGE) este specificat	*OBJOPR	*EXECUTE
DSPS36	Obiect de configurare S/36 QS36ENV	*READ	*EXECUTE
EDTS36PGMA	Program, pentru a modifica atribute	*OBJMGT, *USE	*EXECUTE
	Program, pentru a vedea atribute	*USE	*EXECUTE
EDTS36PRCA	Fişier QS36PRC, pentru a modifica atribute	*OBJMGT, *USE	*EXECUTE
	Fişier QS36PRC, pentru a vedea atribute	*USE	*EXECUTE
EDTS36SRCA	Fişier sursă QS36SRC, pentru a modifica atribute	*OBJMGT, *USE	*EXECUTE
	Fişier sursă QS36SRC, pentru a vedea atribute	*USE	*EXECUTE
RSTS36F (Q)	Din-fişier	*USE	*EXECUTE
	În-fişier	*ALL	Vedeţi regulile generale.
	Bazat pe fişier fizic, dacă fişierul care este restaurat este fişier (alternativ) logic	*CHANGE	*EXECUTE
	Fişier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE

Comenzi mediu System/36

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
RSTS36FLR [1,2,3] (Q)	Folder S/36	*USE	*EXECUTE
	În-fişier	*CHANGE	*EXECUTE
	Fişier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
RSTS36LIBM (Q)	Din-fişier	*USE	*EXECUTE
	În-fişier	*ALL	Vedeţi regulile generale.
	Fişier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
RTVS36A	Obiect de configurare S/36 QS36ENV	*UPD	*EXECUTE
SAVS36F	Din-fişier	*USE	*EXECUTE
	În-fişier, atunci când este fişier fizic	*ALL	Vedeţi regulile generale.
	Fişier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
SAVS36LIBM	Din-fişier	*USE	*EXECUTE
	În-fişier, atunci când este fişier fizic	*ALL	Vedeţi regulile generale.
	Fişier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
WRKS36	Obiect de configurare S/36 QS36ENV	*READ	*EXECUTE
WRKS36PGMA	Program, pentru a modifica atribute	*OBJMGT, *USE	*EXECUTE
	Program, pentru a vedea atribute	*USE	*EXECUTE
WRKS36PRCA	Fişier QS36PRC, pentru a modifica atribute	*OBJMGT, *USE	*EXECUTE
	Fişier QS36PRC, pentru a vedea atribute	*USE	*EXECUTE
WRKS36SRCA	Fişier sursă QS36SRC, pentru a modifica atribute	*OBJMGT, *USE	*EXECUTE
	Fişier sursă QS36SRC, pentru a vedea atribute	*USE	*EXECUTE

1 Aveţi nevoie de autorizaţia *ALL pentru document dacă îl inlocuiţi. Aveţi nevoie de autorizaţii operaţionale şi pentru toate datele pentru folder dacă restauraţi informaţii noi în aceste foldere, sau aveţi nevoie de autorizaţia specială *ALLOBJ.

2 Dacă este folosit pentru dicţionar, este necesară doar autorizaţia pentru comandă.

3 Trebuie să fiţi înscris în directorul de distribuire sistem dacă folderul sursă este un folder document.

Comenzile pentru tabelă

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
CRTTBL	Tabelă		*READ, *ADD, *EXECUTE
	Fişier sursă	*USE	*EXECUTE
DLTTBL	Tabelă	*OBJEXIST	*EXECUTE
WRKTBL [1]	Tabelă	Orice autorizaţie	*USE

1 Pentru a folosi o operaţie individuală, trebuie să aveţi autorizaţia necesară de operaţie.

Comenzile pentru TCP/IP

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ADDTCPSVR[1]	Program de apelat	*EXECUTE	*EXECUTE
CHGTCPSVR[1]	Program de apelat	*EXECUTE	*EXECUTE
CVTTCPCL (Q)	Obiecte fişier	*USE	*EXECUTE
ENDTCP (Q)	Descriere de linie[4]	*USE	*EXECUTE
	Descriere controler[4]	*USE	*EXECUTE
	Descriere de dispozitiv[4]	*USE	*EXECUTE
	Obiecte fişier	*USE	*EXECUTE
ENDTCPIFC (Q)	Obiecte fişier	*USE	*EXECUTE
	Descriere de linie[4]	*USE	*EXECUTE
	Descriere controler[4]	*USE	*EXECUTE
	Descriere de dispozitiv[4]	*USE	*EXECUTE
ENDTCPPTP	Descriere de linie[4]	*USE	*EXECUTE
	Descriere controler[4]	*USE	*EXECUTE
	Descriere de dispozitiv[4]	*USE	*EXECUTE
	Obiecte fişier	*USE	*EXECUTE
ENDTCPSRV (Q)	Obiecte fişier	*USE	*EXECUTE
FTP	Obiecte fişier	*USE	*EXECUTE
	Obiecte tabel	*USE	*EXECUTE
LPR [2]	Obiecte de personalizare staţie de lucru	*USE	*EXECUTE
SETVTTBL	Obiecte tabel	*USE	*EXECUTE
SNDTCPSPLF [2]	Obiecte de personalizare staţie de lucru	*USE	*EXECUTE
STRTCP (Q)	Obiecte fişier	*USE	*EXECUTE
	Descriere de linie[4]	*USE	*EXECUTE
	Descriere controler[4]	*USE	*EXECUTE
	Descriere de dispozitiv[4]	*USE	*EXECUTE
STRTCPFTP	Obiecte tabel	*USE	*EXECUTE
	Obiecte fişier	*USE	*EXECUTE
STRTCPIFC (Q)	Obiecte fişier	*USE	*EXECUTE
	Descriere de linie[4]	*USE	*EXECUTE
	Descriere controler[4]	*USE	*EXECUTE
	Descriere de dispozitiv[4]	*USE	*EXECUTE
STRTCPPTP	Descriere de linie[4]	*USE	*EXECUTE
	Descriere controler[4]	*USE	*EXECUTE
	Descriere de dispozitiv[4]	*USE	*EXECUTE
	Obiecte fişier	*USE	*EXECUTE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
STRTCPSVR (Q)	Obiecte tabel	*USE	*EXECUTE
	Obiecte fişier	*USE	*EXECUTE
STRTCPTELN	Obiecte tabel	*USE	*EXECUTE
	Obiecte fişier	*USE	*EXECUTE
	Dispozitiv virtual staţie de lucru[5]	*USE	*EXECUTE
TELNET	Obiecte tabel	*USE	*EXECUTE
	Obiecte fişier	*USE	*EXECUTE
	Dispozitiv virtual staţie de lucru[5]	*USE	*EXECUTE

Aceste comenzi nu necesită nici o autorizaţie obiect:

ADDCOMSNMP [1]	CFGTCPSMTP	CHGVTMAP	RMVTCPRSI [1]
ADDNETTBLE [1]	CFGTCPSNMP	DSPVTMAP	RMVTCPRTE [1]
ADDPCLTBLE [1]	CFGTCPTELN	ENDTCPCNN	RMVTCPSVR [1]
ADDSRVTBLE [1]	CHGCOMSNMP [1]	MGRTCPHT [1]	RNMTCPHTE [1]
ADDTCPHTE [1]	CHGFTPA [1]	NETSTAT	SETVTMAP
ADDTCPIFC [1]	CHGLPDA [1]	PING	VFYTCPCNN
ADDTCPPORT [1]	CHGSMTPA [1]	RMVCOMSNMP [1]	WRKNAMSMTP [3]
ADDTCPRSI [1]	CHGSNMPA [1]	RMVNETTBLE [1]	WRKNETTBLE[1]
ADDTCPRTE [1]	CHGTCPA [1]	RMVPCLTBLE [1]	WRKPCLTBLE[1]
CFGTCP	CHGTCPHTE[1]	RMVSRVTBLE [1]	WRKSRVTBLE[1]
CFGTCPAPP	CHGTCPIFC[1]	RMVTCPHTE[1]	WRKTCPSTS
CFGTCPFTP [1]	CHGTCPRTE [1]	RMVTCPIFC[1]	
CFGTCPLPD [1]	CHGTELNA [1]	RMVTCPPORT [1]	

1 Trebuie să aveţi autorizaţia specială *IOSYSCFG pentru a folosi această comandă.

2 Comanda SNDTCPSPLF şi comanda LPR folosesc aceleaşi combinaţii de autorizaţii obiect referenţiat ca şi comanda SNDNETSPLF.

3 Trebuie să aveţi autorizaţia specială *SECADM pentru a modifica tabelul sistem alias sau alt tabel alias al unui profil utililizator.

4 Dacă aveţi autorizaţia specială *JOBCTL, nu aveţi nevoie de autorizaţia specificată pentru obiect.

5 Dacă aveţi autorizaţia specială *JOBCTL, nu aveţi nevoie de autorizaţia specificată pentru obiectul de pe sistemul la distanţă.

Comenzile pentru descriere fus orar

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
CHGTIMZON	Descriere fus orar	*CHANGE	*EXECUTE
CRTTIMZON	Descriere fus orar		*READ, *ADD
DLTTIMZON[1]	Descriere fus orar	*OBJEXIST	*EXECUTE
WRKTIMZON[2]	Descriere fus orar	*USE	*USE

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci

[1] Descrierea fus orar specificată în valoare sistem QTIMZON nu poate fi ştearsă.

[2] Dacă un mesaj este folosit pentru a specifica numele abreviate şi complete ale descrierii de fus orar, trebuie să aveţi autorizaţia *USE pentru fişierul de mesaje şi autorizaţia *EXECUTE pentru biblioteca fişierului de mesaje pentru a vedea numele complete şi abreviate.

Comenzile pentru datele comenzii de modernizare

Aceste comenzi sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
WRKORDINF	Fişier QGPL/QMAHFILE	*CHANGE, *OBJALTER	*EXECUTE

Comenzile pentru index utilizator, coadă utilizator şi spaţiu utilizator

Tabela 151.

Comanda	Obiect referenţiat	Autorizaţie necesară	
		Pentru obiect	Pentru bibliotecă
DLTUSRIDX	Index utilizator	*OBJEXIST	*EXECUTE
DLTUSRQ	Coadă utilizator	*OBJEXIST	*EXECUTE
DLTUSRSPC	Spaţiu utilizator	*OBJEXIST	*EXECUTE

Comenzile pentru profil de utilizator

Comenzi identificate de(Q) sunt livrate cu autorizaţia publică *EXCLUDE. Anexa C arată care dintre profilurile de utilizator furnizate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
ANZDFTPWD [3, 14, 15](Q)			
ANZPRFACT [3, 14, 15](Q)			
CHGACTPRFL [14](Q)			
CHGACTSCDE [3, 14, 15](Q)			
CHGDSTPWD [1]			
CHGEXPSCDE [3, 14, 15](Q)			

Comenzi profil utilizator

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
CHGPRF	Ptofil utilizator	*OBJMGT, *USE	
	Program iniţial[2]	*USE	*EXECUTE
	Meniu iniţial[2]	*USE	*EXECUTE
	Descriere job[2]	*USE	*EXECUTE
	Coadă de mesaje [2]	*USE	*EXECUTE
	Coadă de mesaje[2]	*USE	*EXECUTE
	Program de tratare tastă Attn[2]	*USE	*EXECUTE
	Bibliotecă curentă [2]	*USE	*EXECUTE
CHGPWD			
CHGUSRAUD [11](Q)			
CHGUSRPRF [3]	Ptofil utilizator	*OBJMGT, *USE	*EXECUTE
	Program iniţial[2]	*USE	*EXECUTE
	Meniu iniţial[2]	*USE	*EXECUTE
	Descriere job[2]	*USE	*EXECUTE
	Coadă de mesaje [2]	*USE	*EXECUTE
	Coadă de mesaje[2]	*USE	*EXECUTE
	Program de tratare tastă Attn[2]	*USE	*EXECUTE
	Bibliotecă curentă [2]	*USE	*EXECUTE
	Profil grup (GRPPRF sau SUPGRPPRF)[2,4]	*OBJMGT, *OBJOPR, *READ, *ADD, *UPD, *DLT	*EXECUTE
CHGUSRPRTI	Ptofil utilizator	*CHANGE	
CHKPWD			
CRTUSRPRF [3, 12, 17]	Program iniţial	*USE	*EXECUTE
	Meniu iniţial	*USE	*EXECUTE
	Descriere job	*USE	*EXECUTE
	Coadă de ieşire	*USE	*EXECUTE
	Coadă de ieşire	*USE	*EXECUTE
	Program de tratare tastă Attn	*USE	*EXECUTE
	Bibliotecă curentă	*USE	*EXECUTE
	Profil grup (GRPPRF sauSUPGRPPRF)[4]	*OBJMGT, *OBJOPR, *READ, *ADD, *UPD, *DLT	*EXECUTE
CVTUSRCERT[3, 14]			
DLTUSRPRF [3,9]	Ptofil utilizator	*OBJEXIST, *USE	*EXECUTE
	Coadă de mesaje[5]	*OBJEXIST, *USE, *DLT	*EXECUTE
DSPACTPRFL [14](Q)			
DSPACTSCD [14](Q)			
DSPAUTUSR [6]	Ptofil utilizator	*READ	
DSPEXPSCD [14](Q)			

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	**Pentru biblioteci**
DSPPGMADP	Ptofil utilizator	*OBJMGT	
	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
DSPUSRPRF[19]	Ptofil utilizator	*READ	*EXECUTE
	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
DSPUSRPRTI	Ptofil utilizator	*USE	
GRTUSRAUT [7]	Profil utilizator referenţiat	*READ	
	Obiecte pentru care acordaţi autorizaţie	*OBJMGT	*EXECUTE
PRTPRFINT [14](Q)			
PRTUSRPRF [18]			
RSTAUT (Q) [8]			
RSTUSRPRF (Q) [8,10, 16]			
RTVUSRPRF[20]	Ptofil utilizator	*READ	
RTVUSRPRTI	Ptofil utilizator	*USE	
SAVSECDTA [8]	Fişier de salvare, dacă e gol	*USE, *ADD	*EXECUTE
	Fişier de salvare, dacă există înregistrări	*OBJMGT, *USE, *ADD	*EXECUTE
WRKUSRPRF [13]	Ptofil utilizator	Orice autorizaţie	

1 Această comandă poate rula doar dacă sunteţi înregistrat ca QSECOFR.

2 Aveţi nevoie de autorizaţie obiect doar pentru câmpurile pe care le modificaţi în profilul utilizator.

3 Autorizaţia specială *SECADM este necesară.

4 Autorizaţia *OBJMGT pentru profilul utilizator nu poate veni de la autorizaţia adoptată.

5 Coada de mesaje asociată cu profilul utilizator este ştearsă dacă este deţinută de acel profil utilizator. Pentru a şterge coada de mesaje, utilizatorul care rulează DLTUSRPRF trebuie să aibă autorizaţiile specificate.

6 Afişare include doar profilurile utilizator pe care utilizatorul care rulează comanda are autorizaţia specificată.

7 Vedeţi autorizările necesare pentru comanda GRTOBJAUT.

8 Autorizaţia specială *SAVSYS este necesară.

9 Dacă selectaţi opţiunea de a şterge obiectele deţinute de profilul utilizator, trebuie să aveţi autorizaţia necesară operaţiei de ştergere. Dacă selectaţi opţiunea de transfer proprietate către alt profil utilizator, trebuie să aveţi autorizaţia necesară pentru obiecte şi pentru profilul de utilizator destinaţie. Vedeţi informaţiile pentru comanda CHGOBJOWN.

10 Trebuie să aveţi autorizaţia specială *ALLOBJ pentru a specifica ALWOBJDIF(*ALL).

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci

[11] Trebuie să aveţi autorizaţia specială *AUDIT.

[12] Utilizatorului al cărui profil este creat îi sunt date aceste autorizaţii: *OBJMGT, *OBJOPR, *READ, *ADD, *DLT, *UPD, *EXECUTE.

[13] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizaţia necesară de operaţie.

[14] Trebuie să aveţi autorizaţia specială *ALLOBJ pentru a folosi această comandă.

[15] Trebuie să aveţi autorizaţia specială *JOBCTL pentru a folosi această comandă.

[16] Trebuie să aveţi autorizaţiile speicale *ALLOBJ şi *SECADM pentru a specifica SECDTA(*PWDGRP), USRPRF(*ALL) sauOMITUSRPRF.

[17] Când executaţi o comandă CRTUSRPRF, nu puteţi crea un profil de utilizator (*USRPRF) într-un pool de discuri independent. Însă când un utilizator este autorizat în particular asupra unui obiect din pool-ul de discuri independent, când este proprietarul unui obiect dintr-un pool de discuri independent sau când este grupul primar al unui obiect dintr-un pool de discuri independent, numele profilului este memorat în pool-ul de discuri independent. Dacă pool-ul disc independent este mutat în alt sistem, autorizaţia privată, proprietatea asupra obiectului şi întrările din grupul primar vor fi ataşate profilului cu acelaşi nume de pe sistemul destinaţie. Dacă un profil nu există pe sistemul destinaţie, un profil va fi creat. Utilizatoru nu va avea nici o autorizaţie specială şi parola va fi setată la *NONE.

[18] Trebuie să aveţi autorizaţia specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.

[19] Trebuie să aveţi autorizarea specială *ALLOBJ sau *AUDIT pentru a fi afişată valoarea curentă de auditare a obiectului şi a acţiunii. În caz contrar va fi afişată valoarea *NOTAVL, pentru a indica faptul că valorile nu sunt disponibile pentru afişare.

[20] Trebuie să aveţi autorizarea specială *ALLOBJ sau *AUDIT pentru a extrage valorile curente OBJAUD şi AUDLVL. În caz contrar va fi returnată valoarea *NOTAVL, pentru a indica faptul că valorile nu sunt disponibile pentru extragere.

Comenzile pentru sistem de fişiere definit de utilizator

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizaţie necesară pentru obiect
ADDMFS [1,2,3]	dir_peste_care_se_montează	*DIR	″root″	*W
	Prefix cale	Vedeţi regulile generale.		
CRTUDFS [1,2,6,7] (Q)	/dev/QASP*xx*	*DIR	″root″	*RWX
DLTUDFS [1,2,4,5] (Q)	/dev/QASP*xx*	*DIR	″root″	*RWX
	orice_obiect_epfs		″root″	*RWX, *OBJEXIST
DSPUDFS	unele_dirxx	*DIR	″root″	*RX
MOUNT [1,2,3]	dir_peste_care_ se_montează	*DIR	″root″	*W
	Prefix cale	Vedeţi regulile generale.		
RMVMFS [1]				
UNMOUNT [1]				

Comanda	Obiect referinţă	Tip obiect	Sistem fişier	Autorizaţie necesară pentru obiect

[1] Pentru a folosi această comandă, trebuie să aveţi autorizaţia specială *IOSYSCFG.

[2] QASP*xx* este 01 (ASP de sistem) sau 02-16, în funcţie de ce ASP de utilizator este necesar. Acesta este directorul care conţine *BLKSF care este montat.

[3] Directorul peste care se montează este orice director IFS peste care se poate monta.

[4] A UDFS poate conţine un întreg subarbore de obiecte, astfel atunnci când ştergeţi un UDFS, ştergeţi obiecte de toate tipurile care pot fi stocate în sistemul de fişiere definit de utilizator.

[5] Atunci când folosiţi comenzi DLTUDFS, trebuie să aveţi autorizaţia *OBJEXIST pentru fiecare obiect din UDFS altfel nici un obiect nu este şters.

[6] Utilizatorul trebuie să aibă toate autorizările speciale pentru toate obiectele (*ALLOBJ) şi administrator securitate(*SECADM) pentru a specifica o valoare pentru opţiunea de Scanare pentru parametrul de obiecte (CRTOBJSCAN) altul decât *PARENT.

[7] Autorizaţia specială (*AUDIT) este necesară atunci când secificaţi o valoare alta decât *SYSVAL pentru valoare Auditare pentru parametrul (CRTOBJAUD) al obiectelor.

Comenzile pentru listă de validare

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTVLDL	Listă de validare		*ADD, *READ
DLTVLDL	Listă de validare	*OBJEXIST	*EXECUTE

Comenzile pentru personalizarea staţiei de lucru

Comanda	Obiect referinţă	Autorizări necesare	
		Pentru obiecte	Pentru biblioteci
CRTWSCST	Fişier sursă	*USE	*EXECUTE
	Obiect de personalizare staţie de lucru, dacă REPLACE(*NO)		*READ, *ADD
	Obiect personalizare staţie de lucru, dacă REPLACE(*YES)	*OBJMGT, *OBJEXIST	*READ, *ADD
DLTWSCST	Obiecte de personalizare staţie de lucru	*OBJEXIST	*EXECUTE
RTVWSCST	Fişier-destinaţie, dacă el există şi se adaugă un nou membru	*OBJOPR, *OBJMGT, *ADD	*EXECUTE
	Fişier-destinaţie, dacă fişierul şi membru există	*OBJOPR, *ADD, *DLT	*EXECUTE
	Fişier-destinaţie, dacă fişierul nu există		*READ, *ADD

Comenzile pentru scriitor

Comanda	Obiect referinţă	Parametri coadă de ieşire		Autorizaţie specială	Autorizări necesare	
		AUTCHK	OPRCTL		Pentru obiecte	Pentru biblioteci
CHGWTR [2, 4]	Coadă de ieşire curentă[1]	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar[3]	*EXECUTE
			*YES	*JOBCTL		
ENDWTR [1]	Coadă de ieşire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar[3]	*EXECUTE
			*YES	*JOBCTL		
HLDWTR [1]	Coadă de ieşire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar[3]	*EXECUTE
			*YES	*JOBCTL		
RLSWTR [1]	Coadă de ieşire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar[3]	*EXECUTE
			*YES	*JOBCTL		
STRDKTWTR [1]	Coadă de ieşire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar[3]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Coadă de ieşire				*OBJOPR, *ADD	*EXECUTE
	Descriere dispozitiv				*OBJOPR, *READ	
STRPRTWTR [1]	Coadă de ieşire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar[3]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Coadă de ieşire				*OBJOPR, *ADD	*EXECUTE
	Program driver dispozitiv definit de utilizator				*READ	*EXECUTE
	Program transfomare date				*READ	*EXECUTE
	Separator program				*READ	*EXECUTE
	Descriere dispozitiv				*OBJOPR, *READ	

Comanda	Obiect referinţă	Parametri coadă de ieşire		Autorizaţie specială	Autorizări necesare	
		AUTCHK	OPRCTL		Pentru obiecte	Pentru biblioteci
STRRMTWTR [1]	Coadă de ieşire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
	Coadă de ieşire	*OWNER			Proprietar[3]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
					*OBJOPR, *ADD	*EXECUTE
	Program driver dispozitiv utilizator				*READ	*EXECUTE
	Transformare date utilizator				*READ	*EXECUTE
WRKWTR						

[1] Dacă aveţi autorizarea specială *SPLCTL, nu aveţi nevoie de nici o autorizare pentru coada de ieşire.

[2] Pentru a modifica coada de ieşiri pentru scriitor, aveţi nevoie de autorizările specificate pentru noua coadă de ieşire.

[3] Trebuie să fiţi proprietarul cozii de ieşire.

[4] Trebuie să aveţi autorizaţia *EXECUTE pentru biblioteca noii cozi de ieşire chiar dacă utilizatorul are autorizaţia speicală *SPLCTL.

Anexa E. Operaţiile şi auditarea obiectelor

Această anexă listează operaţiile care pot fi executate asupra obiectelor din sistem şi dacă aceste operaţii sunt auditate. Listele sunt organizate după tipul de obiect. Operaţiile sunt grupate în funcţie de faptul că ele sunt auditate când este specificat *ALL sau *CHANGE pentru valoarea OBJAUD a comenzii CHGOBJAUD sau CHGDLOAUD.

Dacă o înregistrare de auditare este scrisă pentru o acţiune depinde de o combinaţie de valori sistem, o valoare din profilul utilizator al utilizatorului care execută acţiunea şi o valoare definită pentru obiect. “Planificarea auditării accesului la obiect” la pagina 246 descrie modul în care se setează auditarea pentru obiecte.

Operaţiile arătate în tabele cu litere mari, precum CPYF, se referă la comenzi CL, aceasta dacă nu sunt etichetate ca API (interfaţă de programare aplicaţie).

Operaţii obişnuite tututor tipurilor de obiecte:

- Operaţia citire

  CRTDUPOBJ
  Creare obiect duplicat (dacă este specificat *ALL pentru *"from-object"*).

  DMPOBJ
  Abandon obiect

  DMPSYSOBJ
  Abandon obiect sistem

  SAV Salvare obiect în director

  SAVCHGOBJ
  Salvare obiect modificat

  SAVLIB
  Salvare bibliotecă

  SAVOBJ
  Salvare obiect

  SAVSAVFDTA
  Salvare date fişier de salvare

  SAVDLO
  Salvare obiect DLO

  SAVLICPGM
  Salvare program licenţiat

  SAVSHF
  Salvare raft de cărţi

  Notă: Înregistrarea de auditare pentru operaţia de salvare va identifica dacă salvarea a fost făcută cu STG(*FREE).

- Operaţie de modificare

  APYJRNCHG
  Aplicare modificări jurnalizate

  CHGJRNOBJ
  Modificare obiect jurnalizat

Auditare obiect

CHGOBJD
Modificare descriere obiect

CHGOBJOWN
Modificare proprietar obiect

CRTxxxxxx
Creare obiect

Note:

1. Dacă este specificat *ALL sau *CHANGE pentru biblioteca destinaţie, este scrisă o intrare ZC când este creat un obiect.
2. Dacă este activ *CREATE pentru auditarea de acţiune, este scrisă o intrare CO când este creat un obiect.

DLTxxxxxx
Ştergere obiect

Note:

1. Dacă este specificat *ALL sau *CHANGE pentru biblioteca ce conţine obiectul, este scrisă o intrare ZC când este şters un obiect.
2. Dacă este specificat *ALL sau *CHANGE pentru obiect, este scrisă o intrare ZC când este şters.
3. Dacă este activ *DELETE pentru auditarea de acţiune, este scrisă o intrare DO când este şters un obiect.

ENDJRNxxx
Terminare jurnalizare

GRTOBJAUT
Acordare autorizare obiect

Notă: Dacă este acordată o autorizare pe baza unui obiect referenţiat, nu este scrisă o înregistrare de auditare pentru obiectul referenţiat.

MOVOBJ
Mutare obiect

QjoEndJournal
Terminare jurnalizare

QjoStartJournal
Pornire jurnalizare

RCLSTG
Revendicare spaţiu de stocare:

- Dacă un obiect este securizat printr-un *AUTL deteriorat, este scrisă o înregistrare de auditare când obiectul este securizat de lista de autorizaţii QRCLAUTL.
- O înregistrare de auditare este scrisă dacă un obiect este mutat într-o bibliotecă QRCL.

RMVJRNCHG
Înlăturare schimbări jurnalizate

RNMOBJ
Redenumire obiect

RST Restaurare obiect în director

RSTCFG
Restaurare obiecte de configuraţie

RSTLIB
Restaurare bibliotecă

RSTLICPGM
Restaurare program licenţiat

RSTOBJ
Restaurare obiect

RVKOBJAUT
Revocare autorizare obiect

STRJRNxxx
Pornire jurnalizare

- Operaţiile care nu sunt auditate

Prompt [2]
Program înlocuire prompt pentru o comandă de modificare (dacă există una)

CHKOBJ
Verificare obiect

ALCOBJ
Alocare obiect

CPROBJ
Comprimare obiect

DCPOBJ
Decomprimare obiect

DLCOBJ
Dealocare obiect

DSPOBJD
Afişare descriere obiect

DSPOBJAUT
Afişare autorizare obiect

EDTOBJAUT
Editare autorizare obiect

Notă: Dacă autorizarea de obiect este modificată şi auditarea acţiunii include *SECURITY sau dacă obiectul este auditat, este scrisă o înregistrare de auditare.

QSYCUSRA
Verificare autorizare utilizator pentru un API obiect

QSYLUSRA
Listează utilizatorii autorizaţi pentru un API obiect. O înregistrare de auditare nu este scrisă pentru obiectul a cărui autorizare este listată. O înregistrare de auditare este scrisă pentru spaţiul utilizator folosit pentru a conţine informaţii.

QSYRUSRA
Extragere autorizare utilizator pentru un API obiect

RCLTMPSTG
Revendicare spaţiu de stocare temporar

RTVOBJD
Extragere descriere obiect

---

2. Apare un prompt care afişează valorile curente când este cerută avertizarea pentru o comandă. De exemplu, dacă introduceţi CHGURSPRF USERA şi apăsaţi F4 (prompt), ecranul Modificare profil utilizator arată valorile curente pentru profilul utilizator USERA.

SAVSTG
Salvare spaţiu de stocare (auditare doar pentru comanda SAVSTG)

WRKOBJLCK
Gestionare blocare obiect

WRKOBJOWN
Gestionare obiecte după proprietar

WRKxxx
Gestionare comenzi de obiecte

Operaţiile pentru Timpii de recuperare cale de acces:

Notă: Modificările timpilor de recuperare cale de acces sunt auditate dacă valoarea de sistem acţiune de auditare (QAUDLVL) sau parametrul de auditare acţiune (AUDLVL) din profilul utilizator include *SYSMGT.

- Operaţiile care sunt auditate

  CHGRCYAP
  Recuperare modificări pentru căile de acces

  EDTRCYAP
  Editare modificări pentru căile de acces
- Operaţiile care nu sunt auditate

  DSPRCYAP
  Afişare modificări pentru căile de acces

Operaţiile pentru tabela de alertă (*ALRTBL):

- Citire operaţie

  Nimic
- Operaţie de modificare

  ADDALRD
  Adăugare descriere alertă

  CHGALRD
  Modificare descriere alertă

  CHGALRTBL
  Modificare tabelă alertă

  RMVALRD
  Înlăturare descriere alertă
- Operaţiile care nu sunt auditate

  Tipărire
  Tipărire descriere alertă

  WRKALRD
  Gestionare descriere alertă

  WRKALRTBL
  Gestionare tabelă alertă

Operaţiile pentru lista de autorizaţii (*AUTL):

- Citire operaţie

  Nimic
- Operaţie de modificare

ADDAUTLE
Adăugare intrare listă de autorizaţii

CHGAUTLE
Modificare intrare listă de autorizaţii

EDTAUTL
Editare listă de autorizaţii

RMVAUTLE
Înlăturare intrare listă de autorizaţii

- Operaţiile care nu sunt auditate

DSPAUTL
Afişare listă de autorizaţii

DSPAUTLOBJ
Afişare obiecte din lista de autorizaţii

DSPAUTLDLO
Afişare DLO listă de autorizaţii

RTVAUTLE
Extragere intrare listă de autorizaţii

QSYLATLO
Obiecte listă securizate de API-ul *AUTL

WRKAUTL
Gestionare listă de autorizaţii

Operaţiile pentru deţinător de autorizare (*AUTHLR):

- Citire operaţie

Nimic

- Operaţie de modificare

Asociat
Când este folosit pentru a securiza un obiect.

- Operaţiile care nu sunt auditate

DSPAUTHLR
Afişare deţinător de autorizare

Operaţiile pentru directorul de legături (*BNDDIR):

- Citire operaţie

CRTPGM
Creare program

CRTSRVPGM
Creare program service

RTVBNDSRC
Extragere sursă binder

UPDPGM
Actualizare program

UPDSRVPGM
Actualizare program service

- Operaţie de modificare

ADDBNDDIRE
Adăugare intrare director de legături

RMVBNDDIRE
Înlăturare intrare director de legături

- Operaţiile care nu sunt auditate

DSPBNDDIR
Afişare conţinut pentru un director de legături

WRKBNDDIR
Gestionare director de legături

WRKBNDDIRE
Gestionare intrare director de legături

Operaţii pentru lista de configuraţie (*CFGL):

- Citire operaţie

CPYCFGL
Copiere listă de configuraţie. O intrare este scrisă pentru *din-lista-configuraţie*

- Operaţie de modificare

ADDCFGLE
Adăugare intrări listă de configuraţie

CHGCFGL
Modificare listă de configuraţie

CHGCFGLE
Modificare intrare listă de configuraţie

RMVCFGLE
Înlăturare intrare listă de configuraţie

- Operaţiile care nu sunt auditate

DSPCFGL
Afişare listă de configuraţie

WRKCFGL
Gestionare listă de configuraţie

Operaţii pentru fişiere speciale (*CHRSF):

Vedeţi Operaţii pentru fişierul flux (*STMF) pentru auditare *CHRSF.

Operaţii pentru format diagramă (*CHTFMT):

- Citire operaţie

Afişare
comanda DSPCHT sau opţiunea F10 din meniul BGU

Tipărire/Plotare
comanda DSPCHT sau opţiunea F15 din meniul BGU

Salvare/Creare
Salvarea sau crearea fişierelor de date grafice (GDF) folosind comanda CRTGDF sau opţiunea F13 din meniul BGU

- Operaţie de modificare

Nimic

- Operaţiile care nu sunt auditate

Nimic

Operaţii pentru Modificare descriere cerere (*CRQD):

- Citire operaţie

  QFVLSTA
  API-ul Listare activităţi de modificare descriere cerere

  QFVRTVCD
  API-ul Extragere modificare descriere cerere

  SBMCRQ
  Lansare modificare cerere
- Operaţie de modificare

  ADDCMDCRQA
  Adăugare activitate cerere de modificare comandă

  ADDOBJCRQA
  Adăugare activitate cerere modificare obiect

  ADDPRDCRQA
  Adăugare activitate cerere de modificare produs

  ADDPTFCRQA
  Adăugare activitate cerere modificare PTF

  ADDRSCCRQA
  Adăugare activitate cerere de modificare resursă

  CHGCMDCRQA
  Modificare activitate cerere de modificare comandă

  CHGCRQD
  Modificare descriere cerere

  CHGOBJCRQA
  Modificare activitate cerere de modificare obiect

  CHGPRDCRQA
  Modificare activitate cerere de modificare produs

  CHGPTFCRQA
  Modificare activitate cerere de modificare PTF

  CHGRSCCRQA
  Modificare activitate cerere de modificare resursă

  QFVADDA
  API-ul Adăugare activitate de modificare descriere cerere

  QFVRMVA
  API-ul Înlăturare activitate de modificare descriere cerere

  RMVCRQDA
  Înlăturare activitate de modificare descriere cerere
- Operaţiile care nu sunt auditate

  WRKCRQD
  Gestionare descrieri cerere modificare

Operaţiile pentru descrierile C Locale (*CLD):

- Citire operaţie

RTVCLDSRC
Extragere sursă C Locale

Setlocale
Folosiţi obiectul C locale în timpul rulării programului C folosind funcţia Setare locale.

- Operaţie de modificare

  Nimic

- Operaţiile care nu sunt auditate

  Nimic

Operaţiile pentru clasă (*CLS):

- Citire operaţie

  Nimic

- Operaţie de modificare

  CHGCLS
  Modificare clasă

- Operaţiile care nu sunt auditate

  Pornire job
  Când este folosit de gestiunea de lucru pentru a porni un job

  DSPCLS
  Afişare clasă

  WRKCLS
  Gestionare clasă

Operaţii pentru comandă (*CMD):

- Citire operaţie

  Rulare Când comanda rulează

- Operaţie de modificare

  CHGCMD
  Modificare comandă

  CHGCMDDFT
  Modificare valoare implicită comandă

- Operaţiile care nu sunt auditate

  DSPCMD
  Afişare comandă

  PRTCMDUSG
  Tipărire folosire comandă

  QCDRCMDI
  API-ul Extragere informaţii comandă

  WRKCMD
  Gestionare comandă

  Următoarele comenzi sunt folosite în programele CL pentru a controla procesarea şi pentru a manipula date în interiorul programului. Folosirea lor nu este auditată.

CALL [1]
CALLPRC
CHGVAR
COPYRIGHT
DCL
DCLF
DO
ELSE
ENDDO
ENDPGM
ENDRCV
GOTO
IF
MONMSG
PGM
RCVF
RETURN
SNDF
SNDRCVF
TFRCTL
WAIT

1 CALL este auditată dacă este rulată interactiv. Nu este auditată dacă este rulată într-un program CL.

Operaţiile pentru lista de conexiuni (*CNNL):

- Citire operaţie

  Nimic

- Operaţie de modificare

  ADDCNNLE
  Adăugare intrare listă de conexiuni

  CHGCNNL
  Modificare listă de conexiuni

  CHGCNNLE
  Modificare intrare listă de conexiuni

  RMVCNNLE
  Înlăturare intrare listă de conexiuni

  RNMCNNLE
  Redenumire intrare listă de conexiuni

- Operaţiile care nu sunt auditate

  Copiere
  Opţiunea 3 din WRKCNNL

  DSPCNNL
  Afişare listă conexiuni

  RTVCFGSRC
  Extragere sursă a listei de conexiuni

  WRKCNNL
  Gestionare listă de conexiuni

  WRKCNNLE
  Gestionare intrări listă de conexiuni

Operaţiile pentru descrierea clasă de serviciu (*COSD):

- Citire operaţie

  Nimic

- Operaţie de modificare

  CHGCOSD
  Modificare descriere clasă de serviciu

- Operaţiile care nu sunt auditate

  DSPCOSD
  Afişare descriere clasă de serviciu

RTVCFGSRC
Extragere sursă a descrierii clasă de serviciu

WRKCOSD
Copiere descriere clasă-de-serviciu

WRKCOSD
Gestionare descriere clasă-de-serviciu

Operaţiile pentru Informaţiile parte comunicaţii (*CSI):

- Citire operaţie

  DSPCSI
  Afişare informaţii parte comunicaţii

  Iniţializare
  Iniţializare conversaţie
- Operaţie de modificare

  CHGCSI
  Modificare informaţii parte comunicaţii
- Operaţiile care nu sunt auditate

  WRKCSI
  Gestionare informaţii parte comunicaţii

Operaţiile pentru harta de produse sistem încrucişate (*CSPMAP):

- Citire operaţie

  Referinţă
  Când este referit într-o aplicaţie CSP
- Operaţie de modificare

  Nimic
- Operaţiile care nu sunt auditate

  DSPCSPOBJ
  Afişare obiect CSP

  WRKOBJCSP
  Gestionare obiecte pentru CSP

Operaţii pentru tabela de produse sistem încrucişate (*CSPTBL):

- Citire operaţie

  Referinţă
  Când este referit într-o aplicaţie CSP
- Operaţie de modificare

  Nimic
- Operaţiile care nu sunt auditate

  DSPCSPOBJ
  Afişare obiect CSP

  WRKOBJCSP
  Gestionare obiecte pentru CSP

Operaţii pentru Descrierea controler (*CTLD):

- Citire operaţie

SAVCFG
Salvare configuraţie

VFYCMN
Test legătură

- Operaţie de modificare

CHGCTLxxx
Modificare descriere controler

VRYCFG
Activare sau dezactivare descriere controler

- Operaţiile care nu sunt auditate

DSPCTLD
Afişare descriere controler

ENDCTLRCY
Terminare recuperare controler

PRTDEVADR
Tipărire adrese dispozitiv

RSMCTLRCY
Continuare recuperare controler

RTVCFGSRC
Extragere sursă descriere controler

RTVCFGSTS
Extragere stare descriere controler

WRKCTLD
Copiere descriere controler

WRKCTLD
Gestionare descriere controler

Operaţiile pentru descrierea dispozitiv (*DEVD):

- Citire operaţie

Achiziţie
Prima achiziţie a dispozitivului în timpul operaţiei de deschidere sau cea de achiziţie explicită

Alocare
Alocare conversaţie

SAVCFG
Salvare configuraţie

STRPASTHR
Pornire sesiune Pass-Through

Pornirea celei de-a doua sesiuni pentru pass-through intermediar

VFYCMN
Test legătură

- Operaţie de modificare

CHGDEVxxx
Modificare descriere dispozitiv

HLDDEVxxx
Reţinere descriere dispozitiv

RLSDEVxxx
Eliberare descriere dispozitiv

QWSSETWS
Modificare setare type-ahead (tastare-înainte) pentru un dispozitiv

VRYCFG
Activare sau dezactivare descriere dispozitiv

- Operaţiile care nu sunt auditate

DSPDEVD
Afişare descriere dispozitiv

DSPMODSTS
Afişare stare mod

ENDDEVRCY
Terminare recuperare dispozitiv

HLDCMNDEV
Reţinere dispozitiv comunicaţii

RLSCMNDEV
Eliberare dispozitiv comunicaţii

RSMDEVRCY
Reluare recuperare dispozitiv

RTVCFGSRC
Extragere sursă a descrierii dispozitiv

RTVCFGSTS
Extragere stare descriere dispozitiv

WRKCFGSTS
Gestionare stare configuraţie

WRKDEVD
Copiere descriere dispozitiv

WRKDEVD
Gestionare descriere dispozitiv

Operaţiile pentru director (*DIR):

- Operaţii citire/căutare

access, accessx, QlgAccess, QlgAccessx
Determinare accesabilitate fişier

CHGATR
Modificare atribut

CPY Copiere obiect

DSPCURDIR
Afişare director curent

DSPLNK
Afişare legături

faccessx
Determinare accesibilitate fişier pentru o clasă de utilizatori după descriptor

getcwd, qlgGetcwd
API-ul de obţinere nume cale pentru directorul curent

givedescriptor
API-ul de acordare acces fişier

Qp0lGetAttr, QlgGetAttr
API-uri de obţinere atribute

Qp0lGetPathFromFileID, QlgGetPathFromFileID
API-uri de obţinere cale din identificatorul de fişier

Qp0lProcessSubtree, QlgProcessSubtree
API-uri de procesare nume cale

open, open64, QlgOpen, QlgOpen64, Qp0lOpen
API-uri de deschidere fişier

Qp0lSetAttr, QlgSetAttr
API-uri de setare atribute

opendir, QlgOpendir
API-uri de deschidere director

RTVCURDIR
Extragere director curent

SAV Save

WRKLNK
Gestionare legături

- Operaţie de modificare

CHGATR
Modificare atribute

CHGAUD
Modificare auditare

CHGAUT
Modificare autorizare

CHGOWN
Modificare proprietar

CHGPGP
Modificare grup primar

chmod, QlgChmod
API-ul de modificare autorizaţii fişier

chown, QlgChown
API-ul de modificare proprietar şi grup

CPY Copy

CRTDIR
Creare director

fchmod
API-ul de modificare autorizaţii fişier după descriptor

fchown
API-ul de modificare proprietar şi grup după descriptor

givedescriptor
API-ul de acordare acces fişier

mkdir, QlgMkdir
API-ul de creare director

MOV Mutare

Qp0lRenameKeep, QlgRenameKeep
API-uri de redenumire fişier sau director, păstrare nou

Qp0lRenameUnlink, QlgRenameUnlink
API-uri de redenumire fişier sau director, dezlegare nou

Qp0lSetAttr, QlgSetAttr
API-uri de setare atribut

rmdir, QlgRmdir
API-ul de înlăturare director

RMVDIR
Înlăturare director

RNM Redenumire

RST Restaurare

utime, QlgUtime
API-ul de setare acces fişier şi timpi de modificare

WRKAUT
Gestionare autorizare

WRKLNK
Gestionare legături

- Operaţiile care nu sunt auditate
-

chdir, QlgChdir
API-ul de modificare director

CHGCURDIR
Modificare director curent

close API-ul de închidere descriptor fişier

closedir
API-ul de închidere director

DSPAUT
Afişare autorizare

dup API-ul de deschidere duplicată descriptor fişier

dup2 API-ul de deschidere duplicată de descriptor fişier la un alt descriptor

faccessx
Determinare accesabilitate fişier pentru o clasă de utilizatori după descriptor

fchdir Modificare director curent după descriptor

fcntl API-ul de executare comandă de control fişier

fpathconf
API-ul de obţinere variabile de nume cale configurabile după descriptor

fstat, fstat64
API-uri de obţinere informaţii fişier după descriptor

givedescriptor
API-ul de acordare acces fişier

ioctl API-ul de executare cereri de control I/O

lseek, lseek64
API-uri de setare offset citire/scriere fişier

lstat, lstat64, QlgLstat, QlgLstat64
API-uri de obţinere informaţii de legătură sau fişier

pathconf, QlgPathconf
API-ul de obţinere variabile de nume cale configurabile

readdir
API-ul de citire intrare director

rewinddir
API-ul de resetare flux director

select API-ul de verificare stare I/O ale descriptorilor de fişier multipli

stat, QlgStat
API-ul de oţinere informaţii fişier

takedescriptor
API-ul de preluare acces fişier

Operaţiunile pentru Directory Server:

Notă: Acţiunile Directory Server sunt auditate dacă valoarea de sistem pentru auditare acţiune (QAUDLVL) sau parametrul de auditare acţiune (AUDLVL) din profilul de utilizator conţine *OFCSRV.

- Operaţiile care sunt auditate

  Adăugare
  Adăugarea unor noi intrări director

  Modificare
  Modificarea detaliilor intrare director

  Ştergere
  Ştergerea de intrări director

  redenumire
  Redenumirea de intrări director

  Tipărire
  Afişarea sau tipărirea detaliilor intrare director

  Afişarea sau tipărirea detaliilor departament

  Afişarea sau tipărirea intrărilor director ca rezultat al unei căutări

  RTVDIRE
  Extragere intrare director

  Colectare
  Colectarea datelor de intrare director folosind umbrirea de director

  Furnizare
  Furnizarea datelor de intrare director folosind umbrirea de director

- Operaţiile care nu sunt auditate

  comenzi CL
  Comenzile CL care lucrează în director pot fi auditate separat folosind funcţia de auditare obiect.

  Notă: Unele comenzi de director CL provoacă o înregistrare de auditare pentru că ele execută o funcţie care este auditată de auditarea de acţiune *OFCSRV, precum adăugarea unei intrări director.

CHGSYSDIRA
Modificare atribute director sistem

Departamente
Adăugarea, modificarea, ştergerea sau afişarea datelor departament director

Descrieri
Asignarea unei descrieri unei intrări de director diferite folosind opţiunea 8 din panoul WRKDIR.

Adăugarea, modificarea sau ştergerea descrierilor departament director

Liste de distribuţie
Adăugarea, modificarea, redenumirea sau ştergerea listelor de distribuţie

ENDDIRSHD
Terminare umbrire director

Listă Afişarea sau tipărirea unei liste de intrări director care nu include detalii de intrare director, precum folosirea comenzii WRKDIRE sau folosirea F4 pentru a selecta intrări pentru trimiterea unei note.

Locaţii Adăugarea, modificarea, ştergerea sau afişarea datelor de locaţie director

Poreclă
Adăugarea, modificarea, redenumirea sau ştergerea poreclelor

Căutare
Căutarea intrărilor director

STRDIRSHD
Pornire umbrire director

Operaţii pentru obiectul de bibliotecă documente (*DOC sau *FLR):

- Citire operaţie

CHKDOC
Verificare scriere document

CPYDOC
Copiere document

DMPDLO
Abandon DLO

DSPDLOAUD
Afişare auditare DLO

Notă: Dacă informaţii de auditare sunt afişate pentru toate documentele dintr-un folder şi auditare de obiect este specificată pentru folder, este scrisă o înregistrare de auditare. Afişarea auditării de obiect pentru documente individuale nu provoacă o înregistrare de auditare.

DSPDLOAUT
Afişare autorizare DLO

DSPDOC
Afişare document

DSPHLPDOC
Afişare document ajutor

EDTDLOAUT
Editare autorizare DLO

MRGDOC
Combinare document

PRTDOC
Tipărire document

QHFCPYSF
API-ul de copiere fişier flux

QHFGETSZ
API-ul de oţinere dimensiune fişier flux

QHFRDDR
API-ul de citire intrare director

QHFRDSF
API-ul de citire fişier flux

RTVDOC
Extragere document

SAVDLO
Salvare DLO

SAVSHF
Salvare raft de cărţi

SNDDOC
Trimitere document

SNDDST
Trimitere distribuţie

WRKDOC
Gestionare documente

Notă: O intrare de citire este scrisă pentru folderul care conţine documentele.

- Operaţie de modificare

ADDDLOAUT
Adăugare autorizare DLO

ADDOFCENR
Adăugare înrolare birou

CHGDLOAUD
Modificare auditare DLO

CHGDLOAUT
Modificare autorizare DLO

CHGDLOOWN
Modificare drept de proprietate DLO

CHGDLOPGP
Modificare grup primar DLO

CHGDOCD
Modificare descriere document

CHGDSTD
Modificare descriere distribuţie

CPYDOC [3]
Copiere document

Notă: O intrare de modificare este scrisă dacă documentul destinaţie există deja.

CRTFLR
Creare folder

CVTTOFLR [3]
Convertire la folder

DLTDLO [3]
Ştergere DLO

DLTSHF
Ştergere raft de cărţi

DTLDOCL [3]
Ştergere listă de documente

DLTDST [3]
Ştergere distribuţie

EDTDLOAUT
Editare autorizare DLO

EDTDOC
Editare document

FILDOC [3]
Document fişier

GRTACCAUT
Acordare autorizare cod acces

GRTUSRPMN
Acordare permisiune utilizator

MOVDOC [3]
Mutare document

MRGDOC [3]
Combinare document

PAGDOC
Paginare document

QHFCHGAT
API-ul de modificare atribute intrare director

QHFSETSZ
API-ul de setare dimensiune fişier flux

QHFWRTSF
API-ul de scriere fişier flux

QRYDOCLIB [3]
Cerere bibliotecă documente

Notă: O intrare de modificare este scrisă dacă un document existent rezultat dintr-o căutare este înlocuit.

RCVDST [3]
Primire distribuţie

RGZDLO
Reorganizare DLO

---

3. O intrare de modificare este scrisă pentru document şi pentru folder dacă destinaţia operaţiei este într-un folder.

RMVACC
Înlăturare cod acces pentru orice DLO la care este ataşat codul de acces

RMVDLOAUT
Înlăturare autorizare DLO

RNMDLO [3]
Redenumire DLO

RPLDOC
Înlocuire document

RSTDLO [3]
Restaurare DLO

RSTSHF
Restaurare raft de cărţi

RTVDOC
Extragere document (verificare)

RVKACCAUT
Revocare autorizare cod acces

RVKUSRPMN
Revocare permisiune utilizator

SAVDLO [3]
Salvare DLO

- Operaţiile care nu sunt auditate

ADDACC
Adăugare cod acces

DSPACC
Afişare cod acces

DSPUSRPMN
Afişare permisiune utilizator

QHFCHGFP
API-ul de modificare cursor fişier

QHFCLODR
API-ul de închidere director

QHFCLOSF
API-ul de închidere fişier flux

QHFFRCSF
API-ul de forţare date din buffer

QHFLULSF
API-ul de blocare/deblocare interval fişier flux

QHFRTVAT
API-ul de extragere atribute intrare director

RCLDLO
Revendicare DLO (*ALL sau *INT)

WRKDOCLIB
Gestionare biblioteci de documente

WRKDOCPRTQ
Gestionare coadă de tipărire documente

Operaţiile pentru zona de date (*DTAARA):

- Citire operaţie

  DSPDTAARA
  Afişare zonă de date

  RCVDTAARA
  Primire zonă de date (comanda S/38)

  RTVDTAARA
  Extragere zonă de date

  QWCRDTAA
  API-ul de extragere zonă de date
- Operaţie de modificare

  CHGDTAARA
  Modificare zonă de date

  SNDDTAARA
  Trimitere zonă de date
- Operaţiile care nu sunt auditate

  Zone de date
  Zonă de date locală, Zonă de date grup, Zonă de date PIP (Parametrul de iniţializare program)

  WRKDTAARA
  Gestionare zonă de date

Operaţiile pentru utilizatorul Interactive Data Definition (*DTADCT):

- Citire operaţie

  Nimic
- Operaţie de modificare

  Creare Dicţionar de date şi definiţii de date

  Modificare
  Dicţionar de date şi definiţii de date

  Copiere
  Definiţii de date (înregistrate cu creare)

  Ştergere
  Dicţionar de date şi definiţii de date

  Redenumire
  Definiţii de date
- Operaţiile care nu sunt auditate

  Afişare
  Dicţionar de date şi definiţii de date

  LNKDTADFN
  Legarea şi dezlegarea definiţiilor de fişier

  Tipărire
  Dicţionar de date, definiţii de date şi informaţii loc-folosire pentru definiţiile de date

Operaţiile pentru coada de date (*DTAQ):

- Citire operaţie

QMHRDQM
API-ul de extragere mesaje din coada de date

- Operaţie de modificare

  QRCVDTAQ
  API-ul de primire coadă de date

  QSNDDTAQ
  API-ul de trimitere coadă de date

  QCLRDTAQ
  API-ul de curăţare coadă de date

- Operaţiile care nu sunt auditate

  WRKDTAQ
  Gestionare coadă de date

  QMHQRDQD
  API-ul de extragere descrieri din coada de date

Operaţii pentru descrieri editare (*EDTD):

- Citire operaţie

  DSPEDTD
  Afişare descriere editare

  QECCVTEC
  API-ul de editare expansiune cod (prin rutina QECEDITU)

- Operaţie de modificare

  Nimic

- Operaţiile care nu sunt auditate

  WRKEDTD
  Gestionare descrieri editare

  QECEDT
  API-ul de editare

  QECCVTEW
  API pentru translatarea Lucru editare în Mască editare

Operaţii pentru înregistrare ieşire (*EXITRG):

- Citire operaţie

  QUSRTVEI
  API-ul Extragere informaţii ieşire

  QusRetrieveExitInformation
  API-ul Extragere informaţii ieşire

- Operaţie de modificare

  ADDEXITPGM
  Adăugare program ieşire

  QUSADDEP
  API-ul de adăugare program ieşire

  QusAddExitProgram
  API-ul de adăugare program ieşire

  QUSDRGPT
  API-ul de anulare înregistrare punct de ieşire

QusDeregisterExitPoint
API-ul de anulare înregistrare punct de ieşire

QUSRGPT
API-ul de înregistrare punct de ieşire

QusRegisterExitPoint
API-ul de înregistrare punct de ieşire

QUSRMVEP
API-ul de înlăturare program ieşire

QusRemoveExitProgram
API-ul de înlăturare program ieşire

RMVEXITPGM
Înlăturare program ieşire

WRKREGINF
Gestionare informaţii de înregistrare

- Operaţiile care nu sunt auditate

  Nimic

Operaţii pentru tabela de control formulare (*FCT):

- Nici o operaţie de citire sau modificare nu este auditată pentru tipul de obiect *FCT.

Operaţii pentru fişier (*FILE):

- Citire operaţie

  CPYF Copiere fişier (foloseşte operaţia deschidere)

  Deschidere
  Deschide un fişier pentru citire

  DSPPFM
  Afişare membru fişier fizic (foloseşte operaţia deschidere)

  Deschidere
  Deschidere MRT-uri după deschiderea iniţială

  CRTBSCF
  Creare fişier BSC (foloseşte operaţia deschidere)

  CRTCMNF
  Creare fişier comunicaţii (foloseşte operaţia deschidere)

  CRTDSPF
  Creare fişier de afişare (foloseşte operaţia deschidere)

  CRTICFF
  Creare fişier ICF (foloseşte operaţia deschidere)

  CRTMXDF
  Creare fişier MXD (foloseşte operaţia deschidere)

  CRTPRTF
  Creare fişier imprimantă (foloseşte operaţia deschidere)

  CRTPF
  Creare fişier fizic (foloseşte operaţia deschidere)

  CRTLF
  Creare fişier logic (foloseşte operaţia deschidere)

DSPMODSRC
Afişare sursă modul (foloseşte operaţia deschidere)

STRDBG
Pornire depanare (foloseşte operaţia deschidere)

QTEDBGS
API-ul de extragere text de vizualizare

- Operaţie de modificare

Deschidere
Deschide un fişier pentru modificare

ADDBSCDEVE
(S/38E) Adăugare intrare dispozitiv Bisync unui fişier dispozitiv mixt

ADDCMNDEVE
(S/38E) Adăugare intrare dispozitiv de comunicaţii unui fişier dispozitiv mixt

ADDDSPDEVE
(S/38E) Adăugare intrare dispozitiv de afişare unui fişier dispozitiv mixt

ADDICFDEVE
(S/38E) Adăugare intrare dispozitiv ICF unui fişier dispozitiv mixt

ADDLFM
Adăugare membru fişier logic

ADDPFCST
Adăugare constrângere fişier fizic

ADDPFM
Adăugare membru fişier fizic

ADDPFTRG
Adăugare declanşator fişier fizic

ADDPFVLM
Adăugare membru de lungime variabilă fişier fizic

APYJRNCHGX
Aplicare extindere modificări jurnal

CHGBSCF
Funcţia de modificare Bisync

CHGCMNF
(S/38E) Modificare fişier de comunicaţii

CHGDDMF
Modificare fişier DDM

CHGDKTF
Modificare fişier dischetă

CHGDSPF
Modificare fişier de afişare

CHGICFDEVE
Modificare intrare fişier dispozitiv ICF

CHGICFF
Modificare fişier ICF

CHGMXDF
(S/38E) Modificare fişier dispozitiv mixt

CHGLF
Modificare fişier logic

CHGLFM
Modificare membru fişier logic

CHGPF
Modificare fişier fizic

CHGPFCST
Modificare contrângere fişier fizic

CHGPFM
Modificare membru fişier fizic

CHGPRTF
Modificare fişier imprimantă GQle

CHGSAVF
Modificare fişier salvare

CHGS36PRCA
Modificare atribute procedură S/36

CHGS36SRCA
Modificare atribute sursă S/36

CHGTAPF
Modificare fişier bandă

CLRPFM
Curăţare membru fişier fizic

CPYF Copiere fişier (deschidere fişier pentru modificare, precum adăugare de înregistrări, curăţare membru sau salvare membru

EDTS36PRCA
Editare atribute procedură S/36

EDTS36SRCA
Editare atribute sursă S/36

INZPFM
Iniţializare membru fişier fizic

JRNAP
(S/38E) Pornire cale de acces jurnal (intrare per fişier)

JRNPF
(S/38E) Pornire fişier fizic jurnal (intrare per fişier)

RGZPFM
Reorganizare membru fişier fizic

RMVBSCDEVE
(S/38E) Înlăturare intrare dispozitiv BSC dintr-un fişier dev mixt

RMVCMNDEVE
(S/38E) Înlăturare intrare dispozitiv CMN dintr-un fişier dev mixt

RMVDSPDEVE
(S/38E) Înlăturare intrare dispozitiv DSP dintr-un fişier dev mixt

RMVICFDEVE
(S/38E) Înlăturare intrare dispozitiv ICF dintr-un fişier dev ICM

RMVM
Înlăturare membru

RMVPFCST
Înlăturare constrângere fişier fizic

RMVPFTGR
Înlăturare declanşator fişier fizic

RNMM
Redenumire membru

WRKS36PRCA
Gestionare atribute procedură System/36

WRKS36SRCA
Gestionare atribute sursă System/36

- Operaţiile care nu sunt auditate

DSPCPCST
Afişare constrângeri de verificare în aşteptare

DSPFD
Afişare descriere fişier

DSPFFD
Afişare descriere câmp fişier

DSPDBR
Afişare relaţii bază de date

DSPPGMREF
Afişare referinţe program fişier

EDTCPCST
Editare constrângeri de verificare în aşteptare

OVRxxx
Înlocuire fişier

RTVMBRD
Extragere descriere membru

WRKPFCST
Gestionare constrângeri fişier fizic

WRKF
Gestionare fişier

Operaţii pentru fişierele primul intrat primul ieşit (*FIFO):

- Vedeţi Operaţii pentru fişier flux (*STMF) pentru auditare *FIFO.

Operaţii pentru folder (*FLR):

- Vedeţi operaţii pentru obiect bibliotecă documente (*DOC sau *FLR)

Operaţii pentru Resursă font (*FNTRSC):

- Citire operaţie

Tipărire
Tipărirea unui fişier spool care referă la o resursă font

- Operaţie de modificare

Nimic

- Operaţiile care nu sunt auditate

  WRKFNTRSC
  Gestionare resurse font

  Tipărire
  Referirea la resursa font la crearea unui fişier spool

Operaţii pentru definiţia de formular (*FORMDF):

- Citire operaţie

  Tipărire
  Tipărirea unui fişier spool care referă la o definiţie de formular

- Operaţie de modificare

  Nimic

- Operaţiile care nu sunt auditate

  WRKFORMDF
  Gestionare definiţii de formular

  Tipărire
  Referirea la definiţia de formular la crearea unui fişier spool

Operaţiile pentru obiectul filtrare (*FTR):

- Citire operaţie

  Nimic

- Operaţie de modificare

  ADDALRACNE
  Adăugare intrare acţiune alertă

  ADDALRSLTE
  Adăugare intrare selecţie alertă

  ADDPRBACNE
  Adăugare intrare acţiune problemă

  ADDPRBSLTE
  Adăugare intrare selecţie problemă

  CHGALRACNE
  Modificare intrare acţiune alertă

  CHGALRSLTE
  Modificare intrare selecţie alertă

  CHGPRBACNE
  Modificare intrare acţiune problemă

  CHGPRBSLTE
  Modificare intrare selecţie problemă

  CHGFTR
  Modificare filtru

  RMVFTRACNE
  Înlăturare intrare acţiune filtru

  RMVFTRSLTE
  Înlăturare intrare selecţie alertă

WRKFTRACNE
Gestionare intrări acţiune filtru

WRKFTRSLTE
Gestionare intrări selecţie filtru

- Operaţiile care nu sunt auditate

WRKFTR
Gestionare filtre

WRKFTRACNE
Gestionare intrări acţiune filtru

WRKFTRSLTE
Gestionare intrări selecţie filtru

Operaţiile cu setul de simboluri grafice (*GSS):

- Citire operaţie

Încărcat
Când este încărcat

Font Când este folosit ca font dintr-o imprimantă descrisă extern

- Operaţie de modificare

Nimic.

- Operaţiile care nu sunt auditate

WRKGSS
Gestionare setul de simboluri grafice

Operaţii pentru dicţionarul set de caractere pe doi octeţi (*IGCDCT):

- Citire operaţie

DSPIGCDCT
Afişare dicţionar IGC

- Operaţie de modificare

EDTIGCDCT
Editare dicţionar IGC

Operaţii pentru sortare set de caractere pe doi octeţi (*IGCSRT):

- Citire operaţie

CPYIGCSRT
Copiere sortare IGC (*din-obiectul-*ICGSRT*)

Conversie
Conversia la formatul V3R1, dacă este necesar

Tipărire
Tipărire caracter pentru înregistrarea în tabela de sortare (opţiunea 1 din meniul CGU)

Tipăriţi înainte de a şterge caracterul din tabela de sortare (opţiunea 2 din meniul CGU)

- Operaţie de modificare

CPYIGCSRT
Copiere sortare IGC (*la-obiectul-*ICGSRT*)

Conversie
Conversia la formatul V3R1, dacă este necesar

Creare Crearea unui caracter definit de utilizator (opţiune 1 din meniul CGU)

Ştergere
Ştergerea unui caracter definit de utilizator (opţiune 2 din meniul CGU)

Actualizare
Actualizare tabelă de sortare activă (opţiunea 5 din meniul CGU)

- Operaţiile care nu sunt auditate

FMTDTA
Sortare înregistrări sau câmpuri dintr-un fişier

Operaţii pentru tabela set de caractere pe doi octeţi (*IGCTBL):

- Citire operaţie

CPYIGCTBL
Copiere tabelă IGC

STRFMA
Pornire ajutor gestiune fonturi

- Operaţie de modificare

STRFMA
Pornire ajutor gestiune fonturi

- Operaţiile care nu sunt auditate

CHKIGCTBL
Verificare tabelă IGC

Operaţii pentru descriere job (*JOBD):

- Operaţie de citire

Nimic

- Operaţie de modificare

CHGJOBD
Modificare descriere job

- Operaţiile care nu sunt auditate

DSPJOBD
Afişare descriere job

WRKJOBD
Gestionare descrieri de job

QWDRJOBD
API-ul de extragere descriere job

Job batch
Când este folosit pentru a stabili un job

Operaţii pentru coada de joburi (*JOBQ):

- Operaţie de citire

Nimic

- Operaţie de modificare

Intrare
Când o intrare este plasată sau îndepărtată din coadă

CLRJOBQ
Curăţare coadă joburi

HLDJOBQ
Blocare coadă joburi

RLSJOBQ
Eliberare coadă joburi

- Operaţiile care nu sunt auditate

ADDJOBQE “Descrierile de subsistem” la pagina 175
Adăugare intrare coadă joburi

CHGJOB
Modificare job dintr-un JOBQ în alt JOBQ

CHGJOBQE “Descrierile de subsistem” la pagina 175
Modificare intrare coadă joburi

QSPRJOBQ
Extragere informaţii coadă joburi

RMVJOBQE “Descrierile de subsistem” la pagina 175
Înlăturare intrare coadă joburi

TFRJOB
Transfer job

TFRBCHJOB
Transfer job batch

WRKJOBQ
Gestionare coadă joburi pentru o coadă de joburi specifică

WRKJOBQ
Gestionare coadă de joburi pentru toate cozile de joburi

Operaţiile pentru obiectul de planificare job (*JOBSCD):

- Operaţie de citire

Nimic

- Operaţie de modificare

ADDJOBSCDE
Adăugare intrare planificare job

CHGJOBSCDE
Modificare intrare planificare job

RMVJOBSCDE
Înlăturare intrare planificare job

HLDJOBSCDE
Blocare intrare planificare job

RLSJOBSCDE
Eliberare intrare planificare job

- Operaţiile care nu sunt auditate

Afişare
Afişare detalii intrare job planificat

WRKJOBSCDE
Gestionare intrări planificare job

---

4. O înregistrare de auditare este scrisă dacă este specificată o auditare de obiect pentru descrierea subsistem (*SBSD).

Gestionare ...
Gestionare joburi lansate anterior din intrarea de planificare job

QWCLSCDE
API-ul de listare intrare planificare job

Operaţii pentru jurnal (*JRN):

- Operaţie de citire

  CMPJRNIMG
  Comparaţie imagini jurnal

  DSPJRN
  Afişare intrare jurnal pentru jurnale utilizator

  QJORJIDI
  Extragere informaţii de identificator jurnal (JID)

  QjoRetrieveJournalEntries
  Extragere intrări jurnal

  RCVJRNE
  Primire intrare jurnal

  RTVJRNE
  Extragere intrare jurnal

- Operaţie de modificare

  ADDRMTJRN
  Adăugare jurnal la distanţă

  APYJRNCHG
  Aplicare modificări jurnalizate

  APYJRNCHGX
  Aplicare extindere modificări jurnal

  CHGJRN
  Modificare jurnal

  CHGRMTJRN
  Modificare jurnal la distanţă

  ENDJRNxxx
  Terminare jurnalizare

  JRNAP
  (S/38E) Pornire cale acces jurnal

  JRNPF
  (S/38E) Pornire fişier fizic jurnal

  QjoAddRemoteJournal
  API-ul de adăugare jurnal la distanţă

  QjoChangeJournalState
  API-ul de modificare stare jurnal

  QjoEndJournal
  API-ul de terminare jurnalizare

  QjoRemoveRemoteJournal
  API-ul de înlăturare jurnal la distanţă

QJOSJRNE
API-ul trimitere intrare jurnal (intrări utilizator doar prin API-ul QJOSJRNE)

QjoStartJournal
API-ul Pornire jurnalizare

RMVJRNCHG
Înlăturare schimbări jurnalizate

RMVRMTJRN
Înlătuarare jurnal la distanţă

SNDJRNE
Trimitere intrare jurnal (intrări utilizator doar prin comanda SNDJRNE)

STRJRNxxx
Pornire jurnalizare

- Operaţiile care nu sunt auditate

DSPJRN
Afişare intrare jurnal pentru jurnalele sistem interne, JRN(*INTSYSJRN)

DSPJRNA
(S/38E) Gestionare atribute jurnal

DSPJRNMNU
(S/38E) Gestionare jurnal

QjoRetrieveJournalInformation
API-ul de extragere informaţii jurnal

WRKJRN
Gestionare jurnal (DSPJRNMNU în mediu S/38)

WRKJRNA
Gestionare atribute jurnal (DSPJRNA în mediu S/38)

Operaţii pentru Receptorul jurnal (*JRNRCV):

- Operaţie de citire

Nimic

- Operaţie de modificare

CHGJRN
Modificare jurnal (când se ataşează noi receptoare)

- Operaţiile care nu sunt auditate

DSPJRNRCVA
Afişare atribute receptor jurnal

QjoRtvJrnReceiverInformation
API-ul de extragere informaţii receptor jurnal

WRKJRNRCV
Gestionare receptor jurnal

Operaţii pentru bibliotecă (*LIB):

- Operaţie de citire

DSPLIB
Afişare bibliotecă (când nu este goală. Dacă biblioteca este goală, nu este executată nici o auditare.)

Localizare
Când un dispozitiv este adăugat la o tabelă de configuraţie

Note:

1. Câteva intrări de auditare pot să fi fost scrise pentru o bibliotecă pentru o singură comandă. De exemplu, când deschideţi un fişier, este scrisă o intrare jurnal de auditare ZR pentru bibliotecă atunci când sistemul localizează fişierul şi fiecare membru din fişier.
2. Nu este scrisă nici o intrare de auditare dacă funcţia de localizare nu are succes. De exemplu, rulaţi o comandă folosind un parametru generic precum:

   ```
   DSPOBJD
   OBJECT(AR*/WRK*) +
   OBJTYPE(*FILE)
   ```

   Dacă o bibliotecă al cărei nume începe cu “AR” nu are vreun nume de fişier care începe cu “WRK”, nu este scrisă nici o înregistrare de auditare pentru acea bibliotecă.

- Operaţie de modificare

  Listă de biblioteci
  Adăugare bibliotecă la lista de biblioteci

  CHGLIB
  Modificare bibliotecă

  CLRLIB
  Curăţare bibliotecă

  MOVOBJ
  Mutare obiect

  RNMOBJ
  Redenumire obiect

  Adăugare
  Adăugare obiect la bibliotecă

  Ştergere
  Ştergere obiect din bibliotecă
- Operaţiile care nu sunt auditate

  Nimic

Operaţii pentru descrierea de linie (*LIND):

- Operaţie de citire

  SAVCFG
  Salvare configuraţie

  RUNLPDA
  Rulare comenzi operaţionale LPDA-2

  VFYCMN
  Test legătură

  VFYLNKLPDA
  Test legătură LPDA-2
- Operaţie de modificare

  CHGLINxxx
  Modificare descriere linie

  VRYCFG
  Activare/dezactivare descriere de linie
- Operaţiile care nu sunt auditate

  ANSLIN
  Linie răspuns

Copiere
Opţiunea 3 din WRKLIND

DSPLIND
Afişare descriere de linie

ENDLINRCY
Terminare recuperare linie

RLSCMNDEV
Eliberare dispozitiv comunicaţii

RSMLINRCY
Reluare recuperare linie

RTVCFGSRC
Extragere sursă de descriere linie

RTVCFGSTS
Extragere stare descriere linie

WRKLIND
Gestionare descriere de linie

WRKCFGSTS
Gestionare stare descriere linie

Operaţiile pentru serviciile de mail:

Notă: Acţiunile servicii mail sunt auditate dacă valoarea de sistem acţiune de auditare (QAUDLVL) sau parametrul de auditare acţiune (AUDLVL) din profilul utilizator include *OFCSRV.

- Operaţiile care sunt auditate

  Modificare
  Modificările aduse directorului de distribuţie sistem

  În numele
  Lucrul în numele altui utilizator

  Notă: Lucrul în numele altui utilizator este auditat dacă AUDLVL din profilul utilizator sau valoarea sistem QAUDLVL include *SECURITY.

  Deschidere
  Este scrisă o înregistrare de auditare când istoricul de mail este deschis

- Operaţiile care nu sunt auditate

  Modificare
  Modificare detalii pentru un element de mail

  Ştergere
  Ştergere element de mail

  Dispunere
  Dispunere element mail într-un document sau folder

  Notă: Când un element de mail este depus, el devine obiect de bibliotecă document (DLO). Auditare de obiecte poate fi specificată pentru un DLO.

  Înaintare
  Înaintarea unui element mail

  Tipărire
  Tipărirea unui element mail

Notă: Tipărirea de elemente mail poate fi auditată folosind nivelul de auditare *SPLFDTA sau *PRTDTA.

Primire
Primire element mail

Răspuns
Răspuns unui element mail

Trimitere
Trimitere element mail

Vizualizare
Vizualizare element mail

Operaţii pentru meniu (*MENU):

- Operaţie de citire

  Afişare
  Afişarea unui meniu cu comanda GO MENU sau cu comanda din caseta de dialog UIM
- Operaţie de modificare

  CHGMNU
  Modificare meniu
- Operaţiile care nu sunt auditate

  Întoarcerea
  Întoarcerea la un meniu din stiva de meniuri care a fost deja afişată

  DSPMNUA
  Afişare atribute meniu

  WRKMNU
  Gestionare meniuri

Operaţii pentru descriere mod (*MODD):

- Operaţie de citire

  Nimic
- Operaţie de modificare

  CHGMODD
  Modificare descriere mod
- Operaţiile care nu sunt auditate

  CHGSSNMAX
  Modificare maxim sesiuni

  DSPMODD
  Afişare descriere mod

  ENDMOD
  Terminare mod

  STRMOD
  Pornire mod

  WRKMODD
  Gestionare descrieri mod

Operaţii pentru obiectul modul (*MODULE):

- Operaţie de citire

CRTPGM
O intrare de auditare pentru fiecare obiect modul folosit în timpul unei comenzi CRTPGM

CRTSRVPGM
O intrare de auditare pentru fiecare obiect modul folosit în timpul unei comenzi CRTSRVPGM

UPDPGM
O intrare de auditare pentru fiecare obiect modul folosit în timpul unei comenzi UPDPGM

UPDSRVPGM
O intrare de auditare pentru fiecare obiect modul folosit în timpul unei comenzi UPDSRVPGM

- Operaţie de modificare

  CHGMOD
  Modificare modul

- Operaţiile care nu sunt auditate

  DSPMOD
  Afişare modul

  RTVBNDSRC
  Extragere sursă legătură

  WRKMOD
  Gestionare module

Operaţii pentru fişier de mesaje (*MSGF):

- Operaţie de citire

  DSPMSGD
  Afişare descriere mesaj

  MRGMSGF
  Fişier sursă combinare fişiere de mesaje

  Tipărire
  Tipărire descriere mesaj

  RTVMSG
  Extragere informaţii dintr-un fişier de mesaje

  QMHRTVM
  API-ul de extragere mesaj

  WRKMSGD
  Gestionare descriere de mesaj

- Operaţie de modificare

  ADDMSGD
  Adăugare descriere mesaj

  CHGMSGD
  Modificare descriere mesaj

  CHGMSGF
  Modificare fişier de mesaje

  MRGMSGF
  Combinare fişier de mesaje (fişier-destinaţie şi înlocuire MSGF)

  RMVMSGD
  Înlăturare descriere mesaj

- Operaţiile care nu sunt auditate

OVRMSGF
Înlocuire fişier de mesaje

WRKMSGF
Gestionare fişiere de mesaje

QMHRMFAT
API-ul de extragere atribute fişier de mesaje

Operaţii pentru coada de mesaje (*MSGQ):

- Operaţie de citire

QMHLSTM
API-ul de listare mesaje nonprogram

QMHRMQAT
API-ul de extragere atribute coadă de mesaje nonprogram

DSPLOG
Afişare istoric

DSPMSG
Afişare mesaj

Tipărire
Tipărire mesaje

RCVMSG
Primire mesaj RMV(*NO)

QMHRCVM
API-ul de primire mesaje nonprogram când acţiunea de mesaj nu este *REMOVE.

- Operaţie de modificare

CHGMSGQ
Modificare coadă de mesaje

CLRMSGQ
Curăţare coadă de mesaje

RCVMSG
Primire mesaj RMV(*YES)

QMHRCVM
API-ul de primire mesaje nonprogram când acţiunea de mesaj este *REMOVE.

RMVMSG
Înlăturare mesaj

QMHRMVM
API-ul de înlăturare mesaje nonprogram

SNDxxxMSG
Trimitere mesaj într-o coadă de mesaje

QMHSNDBM
API-ul de trimitere mesaj de întrerupere

QMHSNDM
API-ul de trimitere mesaj nonprogram

QMHSNDRM
API-ul de trimitere mesaj răspuns

SNDRPY
Trmitere răspuns

WRKMSG
Gestionare mesaje

- Operaţiile care nu sunt auditate

WRKMSGQ
Gestionare cozi de mesaje

Programare
Programare operaţii coadă de mesaje

Operaţii pentru grupul de noduri (*NODGRP):

- Operaţie de citire

DSPNODGRP
Afişare grup de noduri

- Operaţie de modificare

CHGNODGRPA
Modificare grup de noduri

Operaţiile pentru lista de noduri (*NODL):

- Operaţie de citire

QFVLSTNL
Listare intrări listă de noduri

- Operaţie de modificare

ADDNODLE
Adăugare intrare listă de noduri

RMVNODLE
Înlăturare intrare listă de noduri

- Operaţiile care nu sunt auditate

WRKNODL
Gestionare listă de noduri

WRKNODLE
Gestionare intrări listă de noduri

Operaţii pentru descriere NetBIOS (*NTBD):

- Operaţie de citire

SAVCFG
Salvare configuraţie

- Operaţie de modificare

CHGNTBD
Modificare descriere NetBIOS

- Operaţiile care nu sunt auditate

Copiere
Opţiunea 3 din WRKNTBD

DSPNTBD
Afişare descriere NetBIOS

RTVCFGSRC
Extragere sursă de configuraţie pentru descrierea NetBIOS

WRKNTBD
Gestionare descriere NetBIOS

Operaţii pentru interfaţa de reţea (*NWID):

- Operaţie de citire

  SAVCFG
  Salvare configuraţie
- Operaţie de modificare

  CHGNWIISDN
  Modificare descriere interfaţă de reţea

  VRYCFG
  Activare sau dezactivare descriere interfaţă de reţea
- Operaţiile care nu sunt auditate

  Copiere
  Opţiunea 3 din WRKNWID

  DSPNWID
  Afişare descriere interfaţă de reţea

  ENDNWIRCY
  Terminare recuperare interfaţă de reţea

  RSMNWIRCY
  Reluare recuperare interfaţă de reţea

  RTVCFGSRC
  Extragere descriere interfaţă de reţea

  RTVCFGSTS
  Extragere stare descriere interfaţă de reţea

  WRKNWID
  Gestionare descriere interfaţă de reţea

  WRKCFGSTS
  Gestionare stare descriere interfaţă de reţea

Operaţii pentru descrierea server de reţea (*NWSD):

- Operaţie de citire

  SAVCFG
  Salvare configuraţie
- Operaţie de modificare

  CHGNWSD
  Modificare descriere server de reţea

  VRYCFG
  Modificare configuraţie
- Operaţiile care nu sunt auditate

  Copiere
  Opţiunea 3 din WRKNWSD

  DSPNWSD
  Afişare descriere server de reţea

RTVCFGSRC
Extragere sursă de configuraţie pentru *NWSD

RTVCFGSTS
Extragere stare de configuraţie pentru *NWSD

WRKNWSD
Gestionare descriere server de reţea

Operaţii pentru coada de ieşire (*OUTQ):

- Operaţie de citire

  STRPRTWTR
  Pornire scriitor imprimantă la o coadă de ieşire

  STRRMTWTR
  Pornire scriitor la distanţă la o coadă de ieşire

- Operaţie de modificare

  Plasare
  Când o intrare este plasată sau îndepărtată din coadă

  CHGOUTQ
  Modificare coadă de ieşire

  CHGSPLFA [5]
  Modificaţi atributele fişierului spool, dacă este mutat într-o coadă de ieşire diferită sau dacă coada de ieşire este auditată

  CLROUTQ
  Curăţare coadă de ieşire

  DLTSPLF [5]
  Ştergere fişier spool

  HLDOUTQ
  Reţinere coadă de ieşire

  RLSOUTQ
  Eliberare coadă de ieşire

- Operaţiile care nu sunt auditate

  CHGSPLFA [5]
  Modificare atribute fişier spool

  CPYSPLF [5]
  Copiere fişier spool

  Creare [5]
  Creare fişier spool

  DSPSPLF [5]
  Afişare fişier spool

  HLDSPLF [5]
  Reţinere fişier spool

  QSPROUTQ
  Extragere informaţii coadă de ieşire

5. Aceasta este de asemenea auditată dacă auditarea de acţiuni (valoarea sistem QAUDLVL sau valoarea profil utilizator AUDLVL) include *SPLFDTA.

RLSSPLF [5]
Eliberare fişier spool

SNDNETSPLF [5]
Trimitere fişier spool reţea

WRKOUTQ
Gestionare coadă de ieşire

WRKOUTQD
Gestionare descriere coadă de ieşire

WRKSPLF
Gestionare fişier spool

WRKSPLFA
Gestionare atribute fişier spool

Operaţii pentru suprapunere (*OVL):

- Operaţie de citire

  Tipărire
  Tipărire fişier spool care referă o suprapunere
- Operaţie de modificare

  Nimic
- Operaţiile care nu sunt auditate

  WRKOVL
  Gestionare suprapuneri

  Tipărire
  Referirea la suprapunere când se creează un fişier spool

Operaţii pentru definiţia de pagină (*PAGDFN):

- Operaţie de citire

  Tipărire
  Tipărirea unui fişier spool care referă la o definiţie de pagină
- Operaţie de modificare

  Nimic
- Operaţiile care nu sunt auditate

  WRKPAGDFN
  Gestionare definiţii de pagină

  Tipărire
  Referirea la definiţia de formular la crearea unui fişier spool

Operaţii pentru segment de pagină (*PAGSEG):

- Operaţie de citire

  Tipărire
  Tipărirea unui fişier spool care referă la un segment de pagină
- Operaţie de modificare

  Nimic
- Operaţiile care nu sunt auditate

  WRKPAGSEG
  Gestionare segmente de pagină

Tipărire
Referirea la segmentul de pagină la crearea unui fişier spool

Operaţii pentru grupul de descriptori tipărire (*PDG):

- Operaţie de citire

  Deschidere
  Când grupul de descriptori tipărire este deschis pentru citire de către un API PrintManager sau verb CPI.

- Operaţie de modificare

  Deschidere
  Când grupul de descriptori tipărire este deschis pentru modificare de către un API PrintManager* sau verb CPI.

- Operaţiile care nu sunt auditate

  CHGPDGPRF
  Modificare profil grup de descriptori tipărire

  WRKPDG
  Gestionare grup de descriptori tipărire

Operaţii pentru program (*PGM):

- Operaţie de citire

  Activare
  Activare program

  Apel Apelare program care nu este deja activat

  ADDPGM
  Adăugare program pentru depanare

  QTEDBGS
  API-ul de înregistrare vizualizare depanare Qte

  QTEDBGS
  API-ul de extragere vederi modul Qte

  // RUN Rulare program în mediu S/36

  RTVCLSRC
  Extragere sursă CL

  STRDBG
  Pornire depanare

- Creare operaţie

  CRTPGM
  Creare program

  UPDPGM
  Actualizare program

- Operaţie de modificare

  CHGCSPPGM
  Modificare program CSP/AE

  CHGPGM
  Modificare program

  CHGS36PGMA
  Modificare atribute program System/36

EDTS36PGMA
Editare atribute program System/36

WRKS36PGMA
Gestionare atribute program System/36

- Operaţiile care nu sunt auditate

ANZPGM
Analiză program

DMPCLPGM
Abandon program CL

DSPCSPOBJ
Afişare obiect CSP

DSPPGM
Afişare program

PRTCMDUSG
Tipărire folosire comandă

PRTCSPAPP
Tipărire aplicaţie CSP/AE

PRTSQLINF
Tipărire informaţii SQL

QBNLPGMI
API-ul de listare informaţii program

QCLRPGMI
API-ul de extragere informaţii program

STRCSP
Pornire utilitare CSP

TRCCSP
Urmărire aplicaţie CSP

WRKOBJCSP
Gestionare obiecte pentru CSP

WRKPGM
Gestionare programe

Operaţii pentru Panoul de grup (*PNLGRP):

- Operaţie citire

ADDSCHIDXE
Adăugare intrare index de căutare

QUIOPNDA
Deschidere Grup panouri pentru API-ul de afişare

QUIOPNPA
Deschidere Grup panouri pentru API-ul de afişare

QUHDSPH
API de afişare ajutor

- Operaţia de modificare

Nimic

- Operaţiile care nu sunt auditate

WRKPNLGRP
Gestionare grupuri de panouri

Operaţiile pentru Disponibilitatea produsului (*PRDAVL):

- Operaţia de modificare

  WRKSPTPRD
  Gestionare produse suportate, când este adăugat sau înlăturat suportul
- Operaţiile care nu sunt auditate

  Citire Nici o operaţie de citire nu este auditată

Operaţiile pentru Definiţia de produs (*PRDDFN):

- Operaţia de modificare

  ADDPRDLICI
  Adăugare informaţii de licenţă produs

  WRKSPTPRD
  Gestionare produse suportate, când este adăugat sau înlăturat suportul
- Operaţiile care nu sunt auditate

  Citire Nici o operaţie de citire nu este auditată

Operaţii pentru Încărcarea de produse (*PRDLOD):

- Operaţia de modificare

  Modificare
  Stare de încărcare produs, listă de biblioteci pentru încărcare produs, listă directoare pentru încărcare produs, limbă principală
- Operaţiile care nu sunt auditate

  Citire Nici o operaţie de citire nu este auditată

Operaţii pentru Formular Query Manager (*QMFORM):

- Operaţie citire

  STRQMQRY
  Pornire cerere Query Management

  RTVQMFORM
  Extragere formular Query Management

  Rulare Rulare cerere

  Exportare
  Exportare formular Query Management

  Tipărire
  Tipărire formular Query Management

  Tipărire formular Query Management folosind formularul

  Folosire
  Accesarea formularului folosind opţiunea 2, 5, 6 sau 9 sau funcţia F13 din meniul Query Management SQL/400.
- Operaţia de modificare

  CRTQMFORM
  Creare formular Query Management

IMPORTARE
Importare formular Query Management

Salvare
Salvare formular folosind o opţiune meniul sau o comandă

Copiere
Opţiunea 3 din funcţia Gestionare formulare Query Manager

- Operaţiile care nu sunt auditate

Gestionare
Când sunt menţionate *QMFORM-urile în ecranul Gestionare

Activ Orice operaţie formular care este făcută pentru formularul 'activ'.

Operaţii pentru Cerere Query Manager (*QMQRY):

- Operaţie citire

RTVQMQRY
Extragere cerere Query Management

Rulare Rulare cerere Query Manager

STRQMQRY
Pornire cerere Query Manager

Exportare
Exportare cerere Query Manager

Tipărire
Tipărire cerere Query Manager

Folosire
Accesaţi cererea folosind funcţia F13 sau opţiunea 2, 5, 6 sau 9 din funcţia Gestionare cereri Query Manager

- Operaţia de modificare

CRTQMQRY
Creare cerere Query Management

Convertire
Opţiunea 10 (Convertire la SQL) din funcţia Gestionare cereri Query Manager

Copiere
Opţiunea 3 din funcţia Gestionare cereri Query Manager

Salvare
Salvare cerere folosind un meniu sau comandă

- Operaţiile care nu sunt auditate

Gestionare
Când sunt menţionate *QMQRY-urile în ecranul Gestionare

Active Orice operaţie cerere care este făcută pentru cererea 'activă'.

Operaţiile pentru Definiţia cerere (*QRYDFN):

- Operaţie citire

ANZQRY
Analiză cerere

Modificare
Modificare cerere folosind un ecran prompt prezentat de WRKQRY sau QRY.

Afişare
Afişare cerere folosind ecranul prompt WRKQRY

Exportare
Exportare formular folosind Query Manager

Exportare
Exportare cerere folosind Query Manager

Tipărire
Tipărire definiţie cerere folosind ecranul prompt WRKQRY

Tipărire formular Query Management

Tipărire cerere Query Manager

Tipărire raport Query Management

QRYRUN
Rulare cerere

RTVQMFORM
Extragere formular Query Management

RTVQMQRY
Extragere cerere Query Management

Rulare Rulare cerere folosind ecranul prompt WRKQRY

Rulare (comanda Query Management)

RUNQRY
Rulare cerere

STRQMQRY
Pornire cerere Query Management

Lansare
Lansare cerere (rulare cerere) în batch folosind ecranul prompt WRKQRY sau sau ecranul Ieşire cerere curentă

- Operaţia de modificare

  Modificare
  Salvare cerere modificată folosind programul cu licenţă Query/400

- Operaţiile care nu sunt auditate

  Copiere
  Copiaţi o cerere folosind opţiunea 3 din ecranul “Gestionare cereri”

  Creare Creaţi o cerere folosind opţiunea 1 din ecranul “Gestionare cereri”

  Ştergere
  Ştergeţi o cerere folosind opţiunea 4 din ecranul “Gestionare cereri”

  Rulare Rulaţi o cerere folosind opţiunea 1 din ecranul “Ieşire cerere curentă” când creaţi sau modificaţi o cerere folosind programul cu licenţă Query/400; Rulaţi o cerere interactiv folosind PF5 când creaţi, afişaţi sau modificaţi o cerere folosind programul cu licenţă Query/400

  DLTQRY
  Ştergere cerere

Operaţii pentru Tabela de translaţie cod referinţă (*RCT):

- Operaţie citire

  Nimic

- Operaţia de modificare

  Nimic
- Operaţiile care nu sunt auditate

  Nimic

Operaţii pentru Lista de răspuns:

Notă: Acţiunile listei de răspuns sunt auditate dacă valoarea sistem de auditare acţiune (QAUDLVL) sau parametrul de auditare acţiune (AUDLVL) din profilul utilizator includ *SYSMGT.

- Operaţiile care sunt auditate

  ADDRPYLE
  Adăugare intrare listă răspuns

  CHGRPYLE
  Modificare intrare listă răspuns

  RMVRPYLE
  Înlăturare intrare listă răspuns

  WRKRPYLE
  Gestionare intrări listă răspuns sistem
- Operaţiile care nu sunt auditate

  Nimic

Operaţii pentru descrierea subsistem (*SBSD):

- Operaţie citire

  ENDSBS
  Terminare subsistem

  STRSBS
  Pornire subsistem
- Operaţia de modificare

  ADDAJE
  Adăugare intrare job autostart

  ADDCMNE
  Adăugare intrare comunicaţii

  ADDJOBQE
  Adăugare intrare coadă joburi

  ADDPJE
  Adăugare intrare job prestart

  ADDRTGE
  Adăugare intrare rutare

  ADDWSE
  Adăugare intrare staţie de lucru

  CHGAJE
  Modificare intrare job autostart

  CHGCMNE
  Modificare intrare comunicaţii

  CHGJOBQE
  Modificare intrare coadă joburi

CHGPJE
Modificare intrare job prestart

CHGRTGE
Modificare intrare rutare

CHGSBSD
Modificare descriere subsistem

CHGWSE
Modificare intrare staţie de lucru

RMVAJE
Înlăturare intrare job autostart

RMVCMNE
Înlăturare intrare comunicaţii

RMVJOBQE
Înlăturare intrare coadă joburi

RMVPJE
Înlăturare intrare job prestart

RMVRTGE
Înlăturare intrare rutare

RMVWSE
Înlăturare intrare staţie de lucru

- Operaţiile care nu sunt auditate

DSPSBSD
Afişare descriere subsistem

QWCLASBS
API-ul de listare subsistem activ

QWDLSJBQ
API-ul de listare coadă joburi subsistem

QWDRSBSD
API-ul de extragere descriere subsistem

WRKSBSD
Gestionare descrieri subsistem

WRKSBS
Gestionare subsisteme

WRKSBSJOB
Gestionare joburi subsistem

Operaţiile pentru indexul de căutare informaţii (*SCHIDX):

- Operaţie citire

STRSCHIDX
Pornire index de căutare

WRKSCHIDXE
Gestionare intrare index de căutare

- Operaţia de modificare (auditată dacă OBJAUD este *CHANGE sau *ALL)

ADDSCHIDXE
Adăugare intrare index de căutare

CHGSCHIDX
Modificare index de căutare

RMVSCHIDXE
Înlăturare intrare index de căutare

- Operaţiile care nu sunt auditate

WRKSCHIDX
Gestionare index de căutare

Operaţiile pentru socket-ul local (*SOCKET):

- Operaţie citire

connect
Legaţi o destinaţie permanentă la un socket şi stabiliţi o conexiune.

DSPLNK
Afişare legături

givedescriptor
API-ul de acordare acces fişier

Qp0lGetPathFromFileID
API-ul de obţinere nume cale sau obiect din ID-ul de fişier

Qp0lRenameKeep
API-ul Redenumire fişier sau director, păstrare nou

Qp0lRenameUnlink
API-ul Redenumire fişier sau director, dezlegare nou

sendmsg
Trimitere datagramă în modul fără conexiune. Se pot folosi buffere multiple.

sendto Trimitere datagramă în modul fără conexiune.

WRKLNK
Gestionare legături

- Operaţia de modificare

ADDLNK
Adăugare legătură

bind Stabilirea unei adrese locale pentru un socket.

CHGAUD
Auditare modificare

CHGAUT
Modificare autorizare

CHGOWN
Modificare proprietar

CHGPGP
Modificare grup primar

CHKIN
Înregistrare

CHKOUT
Debifare

chmod API-ul Modificare autorizaţii fişier

chown API-ul Modificare grup şi proprietar

givedescriptor
API-ul de acordare acces fişier

link API-ul Creare legătură la fişier

Qp0lRenameKeep
API-ul Redenumire fişier sau director, păstrare nou

Qp0lRenameUnlink
API-ul Redenumire fişier sau director, dezlegare nou

RMVLNK
Înlăturare legătură

RNM Redenumire

RST Restaurare

unlink API-ul Înlăturare legătură la fişier

utime API-ul de Setare acces fişier şi timpi de modificare

WRKAUT
Gestionare autorizare

WRKLNK
Gestionare legături

- Operaţiile care nu sunt auditate

close API-ul de închidere fişier

Notă: Închiderea nu este auditată, dar dacă apărea o eşuare de modificare într-un program de ieşire scan_related de închidere, atunci este scrisă o înregistrare de auditare.

DSPAUT
Afişiare autorizare

dup API-ul de duplicare descriptor fişier deschis

dup2 API-ul de duplicare descriptor fişier deschis la un alt descriptor

fcntl API-ul de executare comandă control fişier

fstat API-ul de obţinere informaţii fişier după descriptor

fsync API-ul de sinctonizare modificări în fişier

ioctl API-ul executare cerere control I/O

lstat API-ul de obţinere fişier sau informaţii de legătură

pathconf
API-ul de obţinere variabile nume cale configurabile

read API-ul de citire din fişier

readv API-ul de citire din fişier (Vector)

select API-ul de verificare stare I/O a descriptorilor fişier multipli

stat API-ul de obţinere informaţii fişier

takedescriptor
API-ul de luare acces fişier

write API-ul de scriere în fişier

writev API-ul de scriere în fişier (Vector)

Operaţii pentru scriere dicţionar ajutor (*SPADCT):

- Operaţie citire

  Verificare
  Funcţia silabisire verificare

  Ajutor Funcţia de ajutor silabisire

  Despărţire
  Funcţia de despărţire

  Legare Funcţia de legare

  Sinonime
  Funcţia sinonim

  Bază Folosirea dicţionarului ca bază la crearea unui alt dicţionar

  Verificare
  Folosirea ca dicţionar de verificare la crearea unui alt dicţionar

  Extragere
  Extragere sursă listă de cuvinte de stop

  Tipărire
  Tipărire sursă listă de cuvinte de stop

- Operaţia de modificare

  CRTSPADCT
  Creare dicţionar de adăugare silabisire

- Operaţiile care nu sunt auditate

  Nimic

Operaţii pentru Fişierele spool:

Notă: Acţiunile fişierului spool sunt auditate dacă valoarea sistem de auditare a acţiunii (QAUDLVL) sau parametrul de auditare acţiune (AUDLVL) din profilul utilizator include *SPLFDTA.

- Operaţiile care sunt auditate

  Acces Fiecare acces pentru fiecare utilizator care nu este proprietarul fişierului spool, incluzând:
  - CPYSPLF
  - DSPSPLF
  - SNDNETSPLF
  - SNDTCPSPLF
  - STRRMTWTR
  - API-ul QSPOPNSP

  Modificare
  Modificarea oricăruia din următoarele atribute fişier spool:
  - COPIES
  - DEV
  - FORMTYPE
  - RESTART
  - PAGERANGE

  Creare Crearea unui fişier spool folosind operaţiile de tipărire

  Crearea unui fişier spool folosind API-ul QSPCRTSP

Ştergere
Ştergerea unui fişier spool folosind oricare din următoarele:
- Tipărirea unui fişier spool de pe o imprimantă sau scriitor de dischetă
- Curăţarea cozii de ieşire (CLROUTQ)
- Ştergerea fişierului spool folosind comanda DLTSPLF sau opţiunea de ştergere dintr-un ecran de fişiere spool
- Ştergerea fişierelor spool când un job se termină (ENDJOB SPLFILE(*YES))
- Ştergerea de fişiere spool când se termină un job tipărire (ENDPJ SPLFILE(*YES))
- Trimiterea unui fişier spool la un sistem la distanţă de pe un scriitor la distanţă

Reţinere
Reţinerea unui fişier spool prin oricare din următoarele:
- Folosirea comenzii HLDSPLF
- Folosirea opţiunii de reţinere dintr-un ecran cu fişiere spool
- Tipărirea unui fişier spool care specifică SAVE(*YES)
- Trimiterea unui fişier spool la un sistem la distanţă de pe un scriitor la distanţă când fişierul spool specifică SAVE(*YES)
- Cum reţine un scriitor un fişier spool după ce apare o eroare la procesarea fişierului spool

Citire Citirea unui fişier spool de pe o imprimantă sau scriitor de dischetă

Eliberare
Eliberarea unui fişier spool

Operaţii pentru pachet SQL (*SQLPKG):

- Operaţie citire

  Rulare Când este rulat obiectul *SQLPKG
- Operaţia de modificare

  Nimic
- Operaţiile care nu sunt auditate

  PRTSQLINF
  Tipărire informaţii SQL

Operaţii pentru Programul service (*SRVPGM):

- Operaţie citire

  CRTPGM
  O intrare de auditare pentru fiecare program service folosit în timpul unei comenzi CRTPGM

  CRTSRVPGM
  O intrare de auditare pentru fiecare program service folosit în timpul unei comenzi CRTPGM

  QTEDBGS
  API-ul de înregistrare vizualizare depanare

  QTEDBGS
  API-ul extragere vederi modul

  RTVBNDSRC
  Extragere sursă legătură

  UPDPGM
  O intrare de auditare pentru fiecare program service folosit în timpul unei comenzi UPDPGM.

  UPDSRVPGM
  O intrare de auditare pentru fiecare program service folosit în timpul unei comenzi UPDSRVPGM.

- Creare operaţie

  CRTSRVPGM
  Creare program service

  UPDSRVPGM
  Actualizare program service
- Operaţia de modificare

  CHGSRVPGM
  Modificare program service
- Operaţiile care nu sunt auditate

  DSPSRVPGM
  Afişare program service

  PRTSQLINF
  Tipărire informaţii SQL

  QBNLSPGM
  API-ul de listare informaţii de program service

  QBNRSPGM
  API-ul de extragere informaţii de program service

  WRKSRVPGM
  Gestionare programe serviciu

Operaţii pentru descriere de sesiune (*SSND):

- Nici o operaţie de citire sau modificare nu este auditată pentru tipul de obiect *SSND.

Operaţii pentru Spaţiul de stocare server (*SVRSTG):

- Nici o operaţie de citire sau modificare nu este auditată pentru tipul de obiect *SVRSTG.

Operaţii pentru fişier flux (*STMF):

- Operaţie citire

  CPY Copiere

  DSPLNK
  Afişare legături

  givedescriptor
  API-ul de acordare acces fişier

  MOV Mutare

  open, open64, QlgOpen, QlgOpen64, Qp0lOpen
  API-uri de deschidere fişier

  SAV Salvare

  WRKLNK
  Gestionare legături
- Operaţia de modificare

  ADDLNK
  Adăugare legătură

  CHGAUD
  Auditare modificare

CHGAUT
Modificare autorizare

CHGOWN
Modificare proprietar

CHGPGP
Modificare grup primar

CHKIN
Înregistrare

CHKOUT
Debifare

chmod, QlgChmod
API-uri de modificare autorizări fişier

chown, QlgChown
API-uri de modificare proprietar şi grup

CPY Copiere

creat, creat64, QlgCreat, QlgCreat64
API-uri de creare fişier nou sau rescriere fişier existent

fchmod
API-ul de modificare autorizări fişier după descriptor

fchown
API-ul de modificare grup şi proprietar după descriptor

givedescriptor
API-ul de acordare acces fişier

legătură
API-ul Creare legătură la fişier

MOV Mutare

open, open64, QlgOpen, QlgOpen64, Qp0lOpen
API-uri la deschiderea pentru scriere

Qp0lGetPathFromFileID, QlgGetPathFromFileID
API-uri de obţinere nume cale sau obiect din ID-ul de fişier

Qp0lRenameKeep, QlgRenameKeep
API-uri de redenumire fişier sau director, păstrare nou

Qp0lRenameUnlink, QlgRenameUnlink
API-uri Redenumire fişier sau director, dezlegare nou

RMVLNK
Înlăturare legătură

RNM Redenumire

RST Restaurare

unlink, QlgUnlink
API-uri de înlăturare legătură la fişier

utime, QlgUtime
API-uri de Setare acces fişier şi timpi de modificare

WRKAUT
Gestionare autorizare

WRKLNK
Gestionare legături

- Operaţiile care nu sunt auditate

închidere
API-ul de închidere fişier

DSPAUT
Afişare autorizare

dup API-ul de duplicare descriptor fişier deschis

dup2 API-ul de duplicare descriptor fişier deschis la un alt descriptor

faccessx
Determinaţi accesibilitate fişier

fclear, fclear64
Curăţarea unui fişier

fcntl API-ul de executare comandă control fişier

fpathconf
API-uri de obţinere variabile nume cale configurabile

fstat, fstat64
API-uri de obţinere informaţii fişier după descriptor

fsync API-ul de sinctonizare modificări în fişier

ftruncate, ftruncate64
API-uri de tăiere fişier

ioctl API-ul executare cerere control I/O

lseek, lseek64
API-uri de setare offset citire/scriere

lstat, lstat64
API-uri de obţinere fişier sau informaţii de legătură

pathconf, QlgPathconf
API-uri de obţinere variabile nume cale configurabile

pread, pread64
API-uri de citire din descriptor cu offset

pwrite, pwrite64
API-uri de scriere în descriptor cu offset

read API-ul de citire din fişier

readv API-ul de citire din fişier (Vector)

select API-ul de verificare stare I/O a descriptorilor fişier multipli

stat, stat64, QlgStat, QlgStat64
API-uri de obţinere informaţii fişier

takedescriptor
API-ul de luare acces fişier

write API-ul de scriere în fişier

writev API-ul de scriere în fişier (Vector)

Operaţii pentru legătura simbolică (*SYMLNK):

- Operaţie citire

  CPY Copie

  DSPLNK
  Afişare legături

  MOV Mutare

  readlink
  API-ul de citire valoare a legăturii simbolice

  SAV Salvare

  WRKLNK
  Gestionare legături
- Operaţia de modificare

  CHGOWN
  Modificare proprietar

  CHGPGP
  Modificare grup primar

  CPY Copie

  MOV Mutare

  Qp0lRenameKeep, QlgRenameKeep
  API-uri de redenumire fişier sau director, păstrare nou

  Qp0lRenameUnlink, QlgRenameUnlink
  API-uri Redenumire fişier sau director, dezlegare nou

  RMVLNK
  Înlăturare legătură

  RNM Redenumire

  RST Restaurare

  symlink, QlgSymlink
  API-uri realizare legătură simbolică

  unlink, QlgUnlink
  API-uri de înlăturare legătură la fişier

  WRKLNK
  Gestionare legături
- Operaţiile care nu sunt auditate

  lstat, lstat64, QlgLstat, QlgLstat64
  API-uri legătură stare

Operaţii pentru descrierea maşină S/36 (*S36):

- Operaţie citire

  Nimic
- Operaţia de modificare

  CHGS36
  Modificare configuraţie S/36

  CHGS36A
  Modificare atribute configuraţie S/36

SET Procedură SET

CRTDEVXXX
Când un dispozitiv este adăugat la o tabelă de configuraţie

DLTDEVD
Când un dispozitiv este şters dintr-o tabelă de configuraţie

RNMOBJ
Redenumire descriere dispozitiv

- Operaţiile care nu sunt auditate

DSPS36
Afişare configuraţie System/36

RTVS36A
Extragere atribute configuraţie S/36

STRS36
Pornire S/36

ENDS36
Terminare S/36

Operaţii pentru tabelă (*TBL):

- Operaţie citire

QDCXLATE
Translatare şir de caractere

QTBXLATE
Translatare şir de caractere

QLGRTVSS
Extragere tabelă secvenţă de sortare

CRTLF
Translatarea tabelei în timpul comenzii CRTLF

Read Folosirea Tabelei de secvenţe sortare când se rulează orice comandă care poate specifica o secvenţă de sortare

- Operaţia de modificare

Nimic

- Operaţiile care nu sunt auditate

WRKTBL
Gestionare tabelă

Operaţii pentru indexul utilizator (*USRIDX):

- Operaţie citire

QUSRTVUI
API-ul de extragere intrări indexul utilizator

- Operaţia de modificare

QUSADDUI
API-ul de adăugare intrări în indexul utilizator

QUSRMVUI
API-ul de înlăturare intrări în indexul utilizator

- Operaţiile care nu sunt auditate

Acces Accesul direct la un index utilizator folosind intrucţiunile MI (permise doar pentru un index utilizator al unui domeniu de utilizatori dintr-o bibliotecă specificată în valoarea sistem QALWUSRDMN.

QUSRUIAT
API-ul de extragere atribute index utilizator

Operaţiuni pentru profilul utilizator (*USRPRF):

- Operaţie citire

  Nimic

- Operaţia de modificare

  CHGPRF
  Modificare profil utilizator

  CHGPWD
  Modificare parolă

  CHGUSRPRF
  Modificare profil utilizator

  CHKPWD
  Verificare parolă

  DLTUSRPRF
  Ştergere profil utilizator

  GRTUSRAUT
  Acordare autorizare utilizator (*la-profil-utilizator*)

  QSYCHGPW
  API-ul de modificare parolă

  RSTUSRPRF
  Restaurare profil utilizator

- Operaţiile care nu sunt auditate

  DSPPGMADP
  Afişare programe care adoptă

  DSPUSRPRF
  Afişare profil utilizator

  GRTUSRAUT
  Acordare autorizare utilizator (*de-la-profil-utilizator*)

  PRTPRFINT
  Tipărire valori interne profil

  PRTUSRPRF
  Tipărire profil utilizator

  QSYCUSRS
  API-ul de verificare autorizări speciale utilizator

  QSYLOBJA
  API-ul de listare obiecte autorizate

  QSYLOBJP
  API-ul de listare obiecte care adoptă

  QSYRUSRI
  API-ul de extragere informaţii utilizator

RTVUSRPRF
Extragere profil utilizator

WRKOBJOWN
Gestionare obiecte deţinute

WRKUSRPRF
Gestionare profiluri utilizator

Operaţii pentru coada utilizator (*USRQ):

- Nici o operaţie de citire sau modificare nu este auditată pentru tipul de obiect *USRQ.
- Operaţiile care nu sunt auditate

  Acces Accesul direct la cozi utilizator folosind intrucţiunile MI (permise doar pentru o coadă utilizator a unui domeniu de utilizatori dintr-o bibliotecă specificată în valoarea sistem QALWUSRDMN.

Operaţii pentru spaţiu utilizator (*USRSPC):

- Operaţie citire

  QUSRTVUS
  API-ul de extragere informaţii spaţiu utilizator
- Operaţia de modificare

  QUSCHGUS
  API-ul de modificare informaţii spaţiu utilizator

  QUSCUSAT
  API-ul de modificare atribute spaţiu utilizator
- Operaţiile care nu sunt auditate

  Acces Accesul direct la spaţiu utilizator folosind intrucţiunile MI (permise doar pentru spaţii utilizator ale unui domeniu de utilizatori din bibliotecile specificate în valoarea sistem QALWUSRDMN.

  QUSRUSAT
  API-ul de extragere atribute spaţiu utilizator

Operaţii pentru lista de validare (*VLDL):

- Operaţie citire

  QSYFDVLE
  API-ul de găsire intrare listă de validare
- Operaţia de modificare

  QSYADVLE
  API-ul de adăugare intrare listă de validare

  QSYCHVLE
  API-ul de modificare intrare listă de validare

  QSYRMVLE
  API-ul de înlăturare intrare listă de validare
- Operaţiile care nu sunt auditate

  Acces Accesul direct la spaţiu utilizator folosind intrucţiunile MI (permise doar pentru spaţii utilizator ale unui domeniu de utilizatori din bibliotecile specificate în valoarea sistem QALWUSRDMN.)

  QUSRUSAT
  API-ul de extragere atribute spaţiu utilizator

Operaţii pentru obiectul de personalizare staţie de lucru

- Operaţie citire

Activare
Când un dispozitiv personalizat este activat

RTVWSCST
Extragere obiect de personalizare staţie de lucru (doar când *TRANSFORM este specificat pentru tipul de dispozitiv)

SNDTCPSPLF
Trimitere fişier spool TCP/IP (doar când este specificat TRANSFORM(*YES))

STRPRTWTR
Pornire scriitor imprimantă (doar pentru fişierele spool care sunt tipărite la o imprimantă personalizată folosind funcţia de transformare tipărire gazdă)

STRRMTWTR
Pornire scriitor la distanţă (doar când coada de ieşire este configurată cu CNNTYPE(*IP) şi TRANSFORM(*YES))

Tipărire
Când ieşirea este tipărită direct (nu prin spool) la o imprimantă personalizată folosind funcţia de transformare tipărire gazdă

- Operaţia de modificare

  Nimic
- Operaţiile care nu sunt auditate

  Nimic

Auditare obiect

Anexa F. Macheta intrărilor din jurnalul de auditare

Această anexă conţine informaţii de dispunere pentru toate tipurile de intrări cu cod de jurnal T din jurnalul de auditare (QAUDJRN). Aceste intrări sunt controlate de auditarea de acţiune şi de obiect pe care o definiţi dumneavoastră. Sistemul scrie intrări suplimentare în jurnalul de auditare pentru evenimente ca un IPL sistem sau salvarea receptorului de jurnal. Dispunerea pentru aceste tipuri de intrare poate fi găsită în subiectul Gestiune jurnal din Centrul de informare.

Tabela 154 la pagina 492 conţine dispunerea pentru câmpuri comune pentru toate tipurile de intrare când este specificat OUTFILFMT(*TYPE2) în comanda DSPJRN. Această dispunere, numită QJORDJE2, este definită în fişierul QADSPJR2 din biblioteca QSYS.

Notă: Formatele de ieşire TYPE2 şi *TYPE 4 nu mai sunt actualizate, prin urmare IBM vă recomandă să nu mai folosiţi formatele *TYPE2 şi *TYPE4 şi să folosiţi numai formate *TYPE5.

Tabela 153 la pagina 491 conţine dispunerea pentru câmpuri comune pentru toate tipurile de intrare când este specificat OUTFILFMT(*TYPE4) în comanda DSPJRN. Această dispunere, numită QJORDJE4, este definită în fişierul QADSPJR4 din biblioteca QSYS. Ieşirea *TYPE4 include toate informaţiile *TYPE2 plus informaţii despre identificatori de jurnal, declanşatoare şi restricţii referenţiale.

Tabela 156 la pagina 494 la Tabela 229 la pagina 588 conţin dispuneri pentru fişierele de ieşire de bază de date de model furnizate pentru a defini date care depind de intrare. Puteţi folosi comanda CRTDUPOBJ pentru a crea orice fişier de ieşire gol cu aceeaşi dispunere ca unul din fişierele de ieşire de bază de date de modele. Puteţi folosi comanda DSPJRN pentru a copia intrările selectate din jurnalul de auditare la fişierul de ieşire pentru analizare. “Analizarea intrărilor din jurnalul de auditare cu o interogare sau un program” la pagina 255 furnizează exemple de folosire a fişierelor de ieşire de bază de date de modele. Vedeţi de asemenea subiectul Gestiune jurnal.

Tabela 152 conţine dispunerea pentru câmpuri comune pentru toate tipurile de intrare când este specificat OUTFILFMT(*TYPE5) în comanda DSPJRN. Această dispunere, numită QJORDJE5, este definită în fişierul QADSPJR5 din biblioteca QSYS. Ieşirea *TYPE5 include toate informaţiile *TYPE4 plus informaţii despre biblioteca program, numele de dispozitiv ASP al programului, numărul de dispozitiv ASP al programului, receptor, bibliotecă receptor, nume dispozitiv ASP al receptorului, numărul de dispozitiv ASP al receptorului, număr de braţ, id fir de execuţie, familie de adrese, port la distanţă şi adresă la distanţă.

Tabela 152. Câmpuri antet standard pentru Intrări de jurnal de auditare. Format înregistrare QJORDJE5 (*TYPE5)

Offset	Câmp	Format	Descriere
1	Lungime intrare	Zoned(5,0)	Lungimea toatală a intrării de jurnal inclusiv câmpul de lungime a intrării.
6	Număr de ordine	Char(20)	Aplicat la fiecare intrare de jurnal. Setat iniţial la 1 pentru fiecare jurnal nou sau restaurat. Opţional, resetaţi la 1 când este ataşat un nou receptor.
26	Cod jurnal	Char(1)	Întotdeauna T.
27	Tip intrare	Char(2)	Vedeţi Tabela 155 la pagina 493 pentru o listă de tipuri de de intrări şi descrieri.
29	Amprentă de timp pentru intrare	Char(26)	Data şi ora la care intrarea a fost creată în format amprentă de timp SAA.
55	Nume job	Char(10)	Numele jobului care a provocat generarea intrării.
65	Nume utilizator	Char(10)	Numele profilului utilizator asociat cu jobul [1].
75	Număr de job	Zoned(6,0)	Numărul jobului.

Tabela 152. Câmpuri antet standard pentru Intrări de jurnal de auditare (continuare). Format înregistrare QJORDJE5 (*TYPE5)

Offset	Câmp	Format	Descriere
81	Nume program	Char(10)	Numele programului care a creat intrarea de jurnal. Acesta poate fi de asemenea numele unui program serviciu sau numele parţial al unui fişier clasă folosit într-un program Java compilat. Dacă un program aplicaţie sau un program CL nu au provocat intrarea, câmpul conţine numele unui program furnizat de sistem cum ar fi QCMD. Câmpul are valoarea *NONE dacă este adevărată una din următoarele: • Numele programului nu se aplică la acest tip de intrare. • Numele programului nu a fost disponibil.
91	Bibliotecă program	Char(10)	Numele bibliotecii care conţine programul care a adăugat intrarea de jurnal.
101	Dispozitiv ASP program	Char(10)	Numele dispozitivului ASP care conţine programul care a adăugat intrarea de jurnal.
111	Număr ASP program	Zoned(5,0)	Numărul dispozitivului ASP care conţine programul care a adăugat intrarea de jurnal.
116	Nume obiect	Char(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
126	Bibliotecă obiecte	Char(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
136	Nume membru	Char(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
146	Contor/RRN	Char(20)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
166	Indicator	Char(1)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
167	Identificator ciclu de permanentizare	Char(20)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
187	Profil utilizator	Char(10)	Numele profilului utilizator curent. [1].
197	Nume sistem	Char(8)	Numele sistemului.
205	Identificator jurnal	Char(10)	Folosit pentru jurnalizare. Nu este folosit pentru intrări de jurnal de auditare.
215	Restricţie referenţială	Char(1)	Folosit pentru jurnalizare de fişiere. Nu este folosit pentru intrări de jurnal de auditare.
216	Declanşator	Char(1)	Folosit pentru jurnalizare de fişiere. Nu este folosit pentru intrări de jurnal de auditare.
217	Date incomplete	Char(1)	Folosit pentru jurnalizare de fişiere. Nu este folosit pentru intrări de jurnal de auditare.
218	Ignorat de APY/ RMVJRNCHG	Char(1)	Folosit pentru jurnalizare de fişiere. Nu este folosit pentru intrări de jurnal de auditare.
219	ESD minimizat	Char(1)	Folosit pentru jurnalizare de fişiere. Nu este folosit pentru intrări de jurnal de auditare.
220	Indicator de obiect	Char(1)	Folosit pentru jurnalizare de fişiere. Nu este folosit pentru intrări de jurnal de auditare.
221	Secvenţă sistem	Char(20)	Un număr asignat de sistem pentru fiecare intrare de jurnal.
241	Receptor	Char(10)	Numele receptorului care conţine intrarea de jurnal.
251	Bibliotecă receptor	Char(10)	Numele bibliotecii care conţine receptorul care conţine intrarea de jurnal.
261	Dispozitiv ASP receptor	Char(10)	Numele dispozitivului ASP care conţine receptorul.
271	Număr ASP receptor	Zoned(5,0)	Numărul ASP care conţine receptorul ce conţine intrarea de jurnal.
276	Număr braţ	Zoned(5,0)	Numărul braţului de disc care conţine intrarea de jurnal.
281	Identificator fir de execuţie	Hex(8)	Identifică firul de execuţie din procesul care a adăugat intrarea de jurnal.
289	Identificator hex fir de execuţie	Char(16)	Versiune afişabilă în hex a identificatorului de fir de execuţie.
305	Familie de adrese	Char(1)	Formatul adresei la distanţă pentru această intrare de jurnal.
306	Port la distanţă	Zoned(5,0)	Numărul de port al adresei la distanţă asociate cu intrarea de jurnal.

Tabela 152. Câmpuri antet standard pentru Intrări de jurnal de auditare (continuare). Format înregistrare QJORDJE5 (*TYPE5)

Offset	Câmp	Format	Descriere
311	Adresă la distanţă	Char(46)	Adresa la distanţă asociată cu intrarea de jurnal.
357	Unitate logică de lucru.	Char(39)	Folosit pentru jurnalizare de fişiere. Nu este folosit pentru intrări de jurnal de auditare.
396	ID tranzacţie	Char(140)	Folosit pentru jurnalizare de fişiere. Nu este folosit pentru intrări de jurnal de auditare.
536	Rezervat	Char(20)	Folosit pentru jurnalizare de fişiere. Nu este folosit pentru intrări de jurnal de auditare.
556	Indicatori de valoare de nul	Char(50)	Folosit pentru jurnalizare de fişiere. Nu este folosit pentru intrări de jurnal de auditare.
606	Lungime date specifice intrării	Binary(5)	Lungimea datelor specifice intrării.

Notă: Cele trei câmpuri care încep la offset 55 alcătuiesc numele de job sistem. În majoritatea cazurilor, câmpul nume utilizator de la offset 65 şi numele profil utilizator de la offset 187 au aceeaşi valoare. Pentru joburi prestartate, câmpul nume profil utilizator conţine numele utilizatorului care porneşte tranzacţia. Pentru unele joburi, ambele câmpuri conţin QSYS ca nume utilizator. Câmpul nume profil utilizator din datele specifice intrării conţine utilizatorul care a provocat intrarea. Dacă se foloseşte un API pentru a interschimba profilurile utilizator, câmpul nume profil utilizator conţine numele profilului utilizator nou (interschimbat).

Tabela 153. Câmpuri antet standard pentru Intrări de jurnal de auditare. Format înregistrare QJORDJE4 (*TYPE4)

Offset	Câmp	Format	Descriere
1	Lungime intrare	Zoned(5,0)	Lungimea totală a intrării de jurnal inclusiv câmpul de lungime a intrării.
6	Număr de ordine	Zoned(10,0)	Aplicat la fiecare intrare de jurnal. Setat iniţial la 1 pentru fiecare jurnal nou sau restaurat. Opţional, resetaţi la 1 când este ataşat un nou receptor.
16	Cod jurnal	Char(1)	Întotdeauna T.
17	Tip intrare	Char(2)	Vedeţi Tabela 155 la pagina 493 pentru o listă de tipuri de de intrări şi descrieri.
19	Amprentă de timp pentru intrare	Char(26)	Data şi ora la care intrarea a fost creată în format amprentă de timp SAA.
45	Nume job	Char(10)	Numele jobului care a provocat generarea intrării.
55	Nume utilizator	Char(10)	Numele profilului utilizator asociat cu jobul [1].
65	Număr de job	Zoned(6,0)	Numărul jobului.
71	Nume program	Char(10)	Numele programului care a creat intrarea de jurnal. Acesta poate fi de asemenea numele unui program serviciu sau numele parţial al unui fişier clasă folosit într-un program Java compilat. Dacă un program aplicaţie sau un program CL nu au provocat intrarea, câmpul conţine numele unui program furnizat de sistem cum ar fi QCMD. Câmpul are valoarea *NONE dacă este adevărată una din următoarele: • Numele programului nu se aplică la acest tip de intrare. • Numele programului nu a fost disponibil.
81	Nume obiect	Char(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
91	Nume bibliotecă	Char(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
101	Nume membru	Char(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
111	Contor/RRN	Zoned(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
121	Indicator	Char(1)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
122	ID ciclu de permanentizare	Zoned(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
132	Profil utilizator	Char(10)	Numele profilului utilizator curent. [1].
142	Nume sistem	Char(8)	Numele sistemului.

Tabela 153. Câmpuri antet standard pentru Intrări de jurnal de auditare (continuare). Format înregistrare QJORDJE4 (*TYPE4)

Offset	Câmp	Format	Descriere
150	Rezervat	Char(10)	Folosit pentru jurnalizare de fişiere. Nu este folosit pentru intrări de jurnal de auditare.
160	Restricţie referenţială	Char(1)	Folosit pentru jurnalizare de fişiere. Nu este folosit pentru intrări de jurnal de auditare.
161	Declanşator	Char(1)	Folosit pentru jurnalizare de fişiere. Nu este folosit pentru intrări de jurnal de auditare.
162	(Zonă rezervată)	Char(8)	
170	Indicatori de valori de nul	Char(50)	Folosit pentru jurnalizare de fişiere. Nu este folosit pentru intrări de jurnal de auditare.
220	Lungime date specifice intrării	Binary (4)	Lungimea datelor specifice intrării.

Notă: Cele trei câmpuri care încep la offset 45 alcătuiesc numele de job sistem. În majoritatea cazurilor, câmpul nume utilizator de la offset 55 şi numele profil utilizator de la offset 132 au aceeaşi valoare. Pentru joburi prestartate, câmpul nume profil utilizator conţine numele utilizatorului care porneşte tranzacţia. Pentru unele joburi, ambele câmpuri conţin QSYS ca nume utilizator. Câmpul nume profil utilizator din datele specifice intrării conţine utilizatorul care a provocat intrarea. Dacă se foloseşte un API pentru a interschimba profilurile utilizator, câmpul nume profil utilizator conţine numele profilului utilizator nou (interschimbat).

Tabela 154. Câmpuri antet standard pentru Intrări de jurnal de auditare. Format de înregistrare QJORDJE2 (*TYPE2)

Offset	Field	Format	Descriere
1	Lungime intrare	Zoned(5,0)	Lungimea toatală a intrării de jurnal inclusiv câmpul de lungime a intrării.
6	Număr secvenţă	Zoned(10,0)	Aplicat la fiecare intrare de jurnal. Setat iniţial la 1 pentru fiecare jurnal nou sau restaurat. Opţional, resetaţi la 1 când este ataşat un nou receptor.
16	Cod jurnal	Char(1)	Întotdeauna T.
17	Tip intrare	Char(2)	Vedeti Tabela 155 la pagina 493 pentru o lista de tipuri de de intrari si descrieri.
19	Amprentă de timp	Char(6)	Data sistem la care intrarea a fost făcută.
25	Timpul intrării	Zoned(6,0)	Timpul sistem la care intrarea a fost făcută.
31	Nume job	Char(10)	Numele jobului care a provocat generarea intrarii.
41	Nume utilizator	Char(10)	Numele profilului utilizator asociat cu jobul [1].
51	Număr de job	Zoned(6,0)	Numărul jobului.
57	Nume program	Char(10)	Numele programului care a creat intrarea de jurnal. Acesta poate fi de asemenea numele unui program serviciu sau numele parţial al unui fişier clasă folosit într-un program Java compilat. Dacă un program aplicaţie sau un program CL nu au provocat intrarea, câmpul conţine numele unui program furnizat de sistem cum ar fi QCMD. Câmpul are valoarea *NONE dacă este adevarată una din urmatoarele: • Numele programului nu se aplica la acest tip de intrare. • Numele programului nu a fost disponibil.
67	Nume obiect	Char(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrari de jurnal de auditare.
77	Nume bibliotecă	Char(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
87	Nume membru	Char(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
97	Contor/RRN	Zoned(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
107	Indicator	Char(1)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
108	ID ciclu de permanentizare	Zoned(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
118	Profil utilizator	Char(10)	Numele profilului utilizator curent. [1].
128	Nume sistem	Char(8)	Numele sistemului.

Tabela 154. Câmpuri antet standard pentru Intrări de jurnal de auditare (continuare). Format de înregistrare QJORDJE2 (*TYPE2)

Offset	Field	Format	Descriere
136	(Zonă rezervată)	Char(20)	

[1] Cele trei câmpuri care încep la offset 31 alcătuiesc numele de job sistem. În cele mai multe cazuri, câmpul *Nume utilizator* de la offset-ul 41 şi câmpul *Nume profil utilizator* de la offset-ul 118 au aceeaşi valoare. Pentru joburi prestartate, câmpul *nume profil utilizator* conţine numele utilizatorului care porneşte tranzacţia. Pentru unele joburi, ambele câmpuri conţin QSYS ca nume utilizator. Câmpul *nume profil utilizator* din datele specifice intrării conţine utilizatorul care a provocat intrarea. Dacă se foloseşte un API pentru a interschimba profilurile utilizator, câmpul *nume profil utilizator* conţine numele profilului utilizator nou (interschimbat).

Tabela 155. Tipuri intrare jurnal auditare (QAUDJRN)

Tip intrare	Descriere
AD	Auditare modificări
AF	Eşuare autorizare
AP	Obţinere autorizare adoptată
AU	Modificări atribut
CA	Modificări autorizare
CD	Auditare şir comandă
CO	Creare obiect
CP	Profil utilizator modificat, creat sau restaurat
CQ	Modificare obiect *CRQD
CU	Operaţii cluster
CV	Verificare conexiune
CY	Conexiune criptografică
DI	Directory Server
DO	Ştergere obiect
DS	Resetare parolă securitate DST
EV	Variabile mediu sistem
GR	Înregistrare generică
GS	Descrierea socket a fost dată unui alt job
IP	Comunicaţie între procese
IR	Acţiuni reguli IP
IS	Gestiune securitate internet
JD	Modificare parametru utilizator pentru o descriere job
JS	Acţiuni care afectează joburile
KF	Fişierul inel de chei
LD	Legare, dezlegare sau căutare intrare director
ML	Acţiuni mail servicii office
NA	Atribut reţea modificat
ND	Violare filtru de căutare director APPN
NE	Violare filtru punct final APPN
OM	Mutare sau redenumire obiect
OR	Restaurare obiect
OW	Drept de proprietate obiect modificat
O1	(Acces optic) Fişier unic sau director
O2	(Acces optic) Fişier dual sau director
O3	(Acces optic) Volum
PA	Program modificat pentru adoptare autorizare
PG	Modificare grup primar pentru un obiect
PO	Ieşire tipărită
PS	Comutare (swap) profil
PW	Parolă nevalidă

Tabela 155. Tipuri intrare jurnal auditare (QAUDJRN) (continuare)

Tip intrare	Descriere
RA	Modificare autorizare în timpul restaurării
RJ	Restaurare descriere job cu profil utilizator specificat
RO	Modificare proprietar obiect în timpul restaurării
RP	Restaurare program cu autorizare adoptată
RQ	Restaurare obiect *CRQD
RU	Restaurare autorizare profil utilizator
RZ	Modificare grup primar în timpul restaurării
SD	Modificări aduse directorului de distribuţie sistem
SE	Intrare de rutare subsistem modificată
SF	Acţiuni la fişierele spool
SG	Semnale asincrone
SK	Securizare conexiuni socket
SM	Modificări gestiune sisteme
SO	Acţiuni informaţii utilizator securitate server
ST	Folosire unelte service
SV	Valoare sistem modificată
VA	Modificarea unei liste de control acces
VC	Pornire sau terminare conexiune
VF	Închidere fişiere server
VL	Limită cont depăşită
VN	Conectare sau deconectare reţea
VO	Acţiuni listă de validare
VP	Eroare parolă reţea
VR	Acces resursă reţea
VS	Pornire sau terminare sesiune server
VU	Modificare profil reţea
VV	Modificare stare serviciu
X0	Autentificare reţea
YC	Obiect DLO accesat (modificare)
YR	Obiect DLO accesat (citire)
ZC	Obiect accesat (modificare)
ZM	Acces metodă SOM
ZR	Obiect accesat (citire)

Tabela 156. Intrări jurnal AD (auditare modificare). Fişier descriere câmp QASYADJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	**D** comanda CHGDLOAUD **O** comanda CHGAUD **S** Atributul de scanare a fost modificat folosind comanda CHGATR sau API-ul Qp0lSetAttr API sau când obiectul a fost creat. **U** comanda CHGUSRAUD
157	225	611	Nume obiect	Char(10)	Numele obiectului pentru care auditarea a fost modificată.

Tabela 156. Intrări jurnal AD (auditare modificare) (continuare). Fişier descriere câmp QASYADJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii pentru obiect.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Valoare auditare obiect	Char(10)	Dacă tipul intrării este D, O sau U, câmpul conţine valoarea de auditare specificată. Dacă tipul intrării este S, câmpul conţine valoarea atributului de scanare.
195	263	649	CHGUSRAUD *CMD	Char(1)	Y = Comenzi de aduitare pentru acest utilizator.
196	264	650	CHGUSRAUD *CREATE	Char(1)	Y = Scriere o înregistrare de auditare când acest utilizator creează un obiect.
197	265	651	CHGUSRAUD *DELETE	Char(1)	Y = Scriere o înregistrare de auditare când acest utilizator şterge un obiect.
198	266	652	CHGUSRAUD *JOBDTA	Char(1)	Y = Scriere o înregistrare de auditare când acest utilizator modifică un job.
199	267	653	CHGUSRAUD *OBJMGT	Char(1)	Y = Scriere o înregistrare de auditare când acest utilizator redenumeşte un obiect.
200	268	654	CHGUSRAUD *OFCSRV	Char(1)	Y = Scriere o înregistrare de auditare când acest utilizator execută funcţii office.
201	269	655	CHGUSRAUD *PGMADP	Char(1)	Y = Scriere o înregistrare de auditare când acest utilizator obţine autorizare prin autorizare adoptată.
202	270	656	CHGUSRAUD *SAVRST	Char(1)	Y = Scriere o înregistrare de auditare când acest utilizator mută sau restaurează un obiect.
203	271	657	CHGUSRAUD *SECURITY	Char(1)	Y = Scriere o înregistrare de auditare când acest utilizator execută acţiuni relevante pentru securitate.
204	272	658	CHGUSRAUD *SERVICE	Char(1)	Y = Scriere o înregistrare de auditare când acest utilizator execută funcţii service.
205	273	659	CHGUSRAUD *SPLFDTA	Char(1)	Y = Scriere o înregistrare de auditare când acest utilizator manipulează fişiere spool.
206	274	660	CHGUSRAUD *SYSMGT	Char(1)	Y = Se scrie o înregistrare de auditare când acest utilizator face modificări de gestiune sisteme.
207	275	661	CHGUSRAUD *OPTICAL	Char (1)	Y = Scriere o înregistrare de auditare când acest utilizator accesează dispozitive optice.
208	276	662	(Zonă rezervată)	Char(19)	
227	295	681	Nume DLO	Char(12)	Numele obiectului DLO pentru care auditarea a fost modificată.
239	307	693	(Zonă rezervată)	Char(8)	
247	315	701	Cale folder	Char(63)	Calea folderului.
310			(Zonă rezervată)	Char(20)	
	378	764	(Zonă rezervată)	Char(18)	
	396	782	Lungime nume obiect [1]	Binary(4)	Lungimea numelui obiectului.
330	398	784	CCSID nume obiect[1]	Binary(5)	Identificatorul setului de caractere codate pentru numele obiect.
334	402	788	ID regiune sau ţară nume obiect[1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
336	404	790	ID limbă nume obiect[1]	Char(3)	ID-ul limbă pentru numele obiectului.
339	407	793	(Zonă rezervată)	Char(3)	
342	410	796	ID fişier părinte[1,2]	Char(16)	ID-ul fişierului directorului părinte.
358	426	812	ID fişier obiect[1,2]	Char(16)	ID-ul fişier al obiectului.
374	442	828	Nume obiect[1]	Char(512)	Numele obiectului.
	954	1340	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.

Tabela 156. Intrări jurnal AD (auditare modificare) (continuare). Fişier descriere câmp QASYADJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	970	1356	Nume ASP[5]	Char(10)	Numele dispozitivului ASP.
	980	1366	Număr ASP[5]	Char(5)	Numărul dispozitivului ASP.
	985	1371	CCSID nume cale	Binary(5)	Identificatorul setului de caractere codate pentru numele căii absolute.
	989	1375	ID regiune sau ţară nume cale	Char(2)	ID-ul regiune sau ţară pentru numele cale absolută.
	991	1377	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	994	1380	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	996	1382	Completaţi indicatorului nume cale	Char(1)	Completaţi indicatorul nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele căii absolute complet pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele căii absolute complet pentru obiect.
	997	1383	ID fişier relativ[3]	Char(16)	ID-ul fişier relativ al numelui de cale absolută.
	1013	1399	Nume cale absolută[4]	Char(5002)	Numele cale absolută al obiectului.

1 Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fişiere QOpenSys, "rădăcină" şi sistemele de fişiere definite de utilizator.

2 Un ID care are bitul cel mai din stânga setat şi restul biţilor 0 indică faptul că ID -ul NU este setat.

3 Când indicatorul nume cale absolută (offset 996) este ″N″, acest câmp va conţine ID-ul câmp relativ al numelui căii. Când idicatorului de nume cale absolut este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

4 Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui căii.

5 Dacă obiectul este într-o bibliotecă, acestea sunt informaţiile ASP despre biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informaţiile ASP despre obiect.

Tabela 157. Intrări jurnal AF (Eşuare autorizare). Fişier descriere câmp QASYAFJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.

Tabela 157. Intrări jurnal AF (Eşuare autorizare) (continuare). Fişier descriere câmp QASYAFJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
156	224	610	Tip violare[1]	Char(1)	**A** Neautorizat la obiect
					B Instrucţiunea restricţionată
					C Eşuare validare (vedeţi J5 offset 639)
					D Folosire interfaţă nesuportată, eşuare domeniu obiect
					E Eroare de protecţie spaţiu de stocare hardware, violare spaţiu constant program
					F Eroare autorizaţie ICAPI
					G Eroare autentificare ICAPI
					H Scanare acţiune program de ieşire (vedeţi J5 offset 639)
					I[7] Moştenirea sistem Java nu este permisă
					J Eroare lansare profil job
					N Jetonul profil nu este un jeton regenerabil
					O Eşuare autorizare obiect optic
					P Eroare comutare (swap) profil
					R Eroare de protecţie hardware
					S Încercare de semnare implicită
					T Neautorizat la portul TCP/IP
					U Cerere de permisiune utilizator nevalidă
					V Jetonul profil nu este valid pentru generarea unui nou jeton profil
					W Jetonul profil nu este valid pentru comutare (swap)
					X Violare sistem — vedeţi J5 offset 723 pentru codurile de violare
					Y Neautorizat pentru câmpul curent JUID în timpul unei operaţii de ştergere JUID.
					Z Neautorizat pentru câmpul curent JUID în timpul unei operaţii de setare JUID.
157	225	611	Nume obiect [1, 5]	Char(10)	Numele obiectului.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii în care este obiectul sau numărul corecţiei de LIC care a eşuat la aplicare.[11]
177	245	631	Tip obiect	Char(8)	Tipul obiectului.

Tabela 157. Intrări jurnal AF (Eşuare autorizare) (continuare). Fişier descriere câmp QASYAFJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
185	253	639	Acţiune eroare validare	Char(1)	Acţiunea luată după eroarea de validare detectată, setată doar dacă tipul de violare (J5 offset 610) este C sau H. **A** Translatarea obiectului nu a fost încercată sau a eşuat. Setarea valoare sistem QALWOBJRST a permis obiectului să fie restaurat. Utilizatorul care face restaurarea nu a avut autorizare specială *ALLOBJ şi nivelul de securitate sistem este setat la 10, 20 sau 30. De aceea, toate autorizările la obiect au fost reţinute. **B** Translatarea obiectului nu a fost încercată sau a eşuat. Setarea valoare sistem QALWOBJRST a permis obiectului să fie restaurat. Utilizatorul care face restaurarea nu a avut autorizare specială *ALLOBJ şi nivelul de securitate sistem este setat la 40 sau mai mult. De aceea, toate autorizările la obiect au fost revocate. **C** Translatarea obiectului a avut succes. Copia translatată a fost restaurată în sistem. **D** Translatarea obiectului nu a fost încercată sau a eşuat. Setarea valoare sistem QALWOBJRST a permis obiectului să fie restaurat. Utilizatorul care face restaurarea a avut autorizare specială *ALLOBJ. De aceea, toate autorizările la obiect au fost reţinute. **E** Eroare detectată de timp instalare sistem. **F** Obiectul nu a fost restaurat din cauza semnăturii care nu este în format OS/400. **G** Sistem neasignat sau obiect în stare de moştenire găsite la verificarea sistemului. **H** Obiect în stare utilizator neasignat găsită la verificarea sistemului. **I** Nepotrivire între obiect şi semnătura sa găsită la verificarea sistemului. **J** Certificatul IBM nu a fost găsit la verificarea sistemului. **K** Format de semnătură nevalid găsit la verificarea sistemului. **M** Programul de ieşire scanare a modificat obiectul care a fost scanat **X** Programul de ieşire scanare a dorit marcarea obiectului ca având o eşuare la scanare
186	254	640	Nume job	Char(10)	Numele jobului.
196	264	650	Nume utilizator	Char(10)	Numele utilizator job.
206	274	660	Număr job	Zoned(6,0)	Număr job.
212	280	666	Nume program	Char(10)	Numele programului.

Tabela 157. Intrări jurnal AF (Eşuare autorizare) (continuare). Fişier descriere câmp QASYAFJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
222	290	676	Biblioteca program	Char(10)	Numele bibliotecii unde este găsit programul.
232	300	686	Profil utilizator [2]	Char(10)	Numele utilizatorului care a cauzat eşuarea de autorizare.
242	310	696	Nume staţie de lucru	Char(10)	Numele staţiei de lucru sau tipul staţiei de lucru.
252	320	706	Număr instrucţiune program	Zoned(7,0)	Numărul instrucţiunii programului.
259	327	713	Nume câmp	Char(10)	Numele câmpului.
269	337	723	Cod violare operaţie	Char(3)	Tipul violării de operaţie care a apărut, setat doar dacă tipul violării (J5 offset 610) este X. **HCA** Profilul utilizator unelte service nu este autorizat să execute operaţia de configurare hardware (QYHCHCOP). **LIC** LIC indică faptul că nu a fost aplicată corecţia de LIC din cauza unei violări de semnătură. **SFA** Neautorizat să activeze atributul de mediu pentru accesul fişierului sistem. **CMD** A fost făcută o încercare pentru a folosi o comandă care a fost dezactivată de către administratorul de sistem.
272	340	726	Utilizator office	Char(10)	Numele utilizatorului office.
282	350	736	Nume DLO	Char(12)	Numele obiectului bibliotecă de documente.
294	362	748	(Zonă rezervată)	Char(8)	
302	370	756	Cale folder	Char(63)	Calea folderului.
365	433	819	Office în numele utilizatorului	Char(10)	Utilizator care lucrează în numele unui alt utilizator.
375			(Zonă rezervată)	Char(20)	
	443	829	(Zonă rezervată)	Char(18)	
	461	847	Lungime nume obiect[3]	Binary(4)	Lungimea numelui obiectului.
395	463	849	CCSID nume obiect[3]	Binary(5)	Identificatorul setului de caractere codate pentru numele obiect.
399	467	853	ID regiune sau ţară nume obiect[3]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
401	469	855	ID limbă nume obiect[3]	Char(3)	ID-ul limbă pentru numele obiectului.
404	472	858	(Zonă rezervată)	Char(3)	
407	475	861	ID fişier părinte[3,4]	Char(16)	ID-ul fişierului directorului părinte.
423	491	877	ID fişier obiect[3,4]	Char(16)	ID-ul fişier al obiectului.
439	507	893	Nume obiect[3,6]	Char(512)	Numele obiectului.
	1019	1405	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	1035	1421	Nume ASP[10]	Char(10)	Numele dispozitivului ASP.
	1045	1431	Număr ASP[10]	Char(5)	Numărul dispozitivului ASP.
	1050	1436	CCSID nume cale	Binary(5)	Identificatorul setului de caractere codate pentru numele căii absolute.
	1054	1440	ID regiune sau ţară nume cale	Char(2)	ID-ul regiune sau ţară pentru numele cale absolută.

Tabela 157. Intrări jurnal AF (Eşuare autorizare) (continuare). Fişier descriere câmp QASYAFJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1056	1442	ID limbă nume cale	Char(3)	ID-ul limbaj pentru numele cale absolută.
	1059	1445	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	1061	1447	Completaţi indicatorului nume cale	Char(1)	Completaţi indicatorul nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele căii absolute complet pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele căii absolute complet pentru obiect.
	1062	1448	ID fişier relativ[8]	Char(16)	ID-ul fişier relativ al numelui de cale absolută.
	1078	1464	Nume cale absolută[9]	Char(5002)	Numele cale absolută al obiectului.
		6466	Nume bibliotecă program ASP	Char(10)	Numele ASP pentru biblioteca program
		6476	Numărul bibliotecii program ASP	Char(5)	Numărul ASP pentru biblioteca program

1 Când tipul violării este pentru descrierea ″G″, numele obiectului conţine numele *SRVPGM care a conţinut ieşirea care a detectat eroarea. Pentru mai multe detalii despre tipurile de violări, vedeţi Tabela 126 la pagina 233.

2 Acest câmp conţine numele utilizatorului care a cauzat intrarea. QSYS poate fi utilizator pentru următoarele:

- offset-urile 41 şi 118 pentru înregistrările *TYPE2
- offset-urile 55 şi 132 pentru înregistrările *TYPE4
- offset-urile 65 şi 187 pentru înregistrările *TYPE5

3 Aceste câmpuri sunt folosite doar pentru obiectele din sistemul de fişiere QOpenSys, din sistemul de fişiere "rădăcină", din sistemele de fişiere definite de utilizator şi QFileSvr.400.

4 Un ID care are bitul cel mai din stânga setat şi restul biţilor 0 indică faptul că ID-ul NU este setat.

5 Când tipul violării este ″T″, numele obiectului conţine portul TCP/IP pe care utilizatorul nu are autorizarea să îl acceseze. Valoarea este lăsată aliniată la stânga şi goală. Câmpurile bibliotecă obiect şi tip obiect vor fi goale.

6 Când tipul de violare este O, numele obectului optic este conţinut în câmpul de nume obiect al sistemului de fişiere integrat. Câmpurile ID regiune sau ţară, ID limbă, ID fişier părinte şi ID fişier obiect vor conţine toate spaţii goale.

7 Obiectul clasă Java care a fost creat nu-şi poate extinde clasa sa de bază pentru că ea are atribute sistem Java.

8 Când indicatorul nume cale absolută (offset 1061) este ″N″, acest câmp va conţine ID-ul fişier relativ al numelui căii. Când idicatorului de nume cale absolut este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

9 Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui căii.

10 Dacă obiectul este într-o bibliotecă, acestea sunt informaţiile ASP despre biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informaţiile ASP despre obiect.

11 Când Tip violare este X şi valoarea codului Violare operaţie este LIC, aceasta indică faptul că nu a fost aplicată o corecţie LIC din cauza unei violări de semnătură. Acest câmp va conţine numărul corecţiei LIC a cărei aplicare a eşuat.

Tabela 158. Intrări jurnal AP (autorizare adoptată). Fişier descriere câmp QASYAPJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	**S** Start **E** Terminare **A** Autorizarea adoptată folosită în timpul activării program
157	225	611	Nume obiect	Char(10)	Numele programului, programului de serviciu sau a unui pachet SQL.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Deţinerea profilului utilizator	Char(10)	Numele profilului utilizator a cărui autorizare este adoptată.
195	263	649	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	279	665	Nume ASP[1]	Char(10)	Numele dispozitivului ASP.
	289	675	Număr ASP[1]	Char(5)	Numărul dispozitivului ASP.

1 Dacă obiectul este într-o bibliotecă, acestea sunt informaţiile ASP despre biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informaţiile ASP despre obiect.

Tabela 159. Intrări jurnal AU (Modificări atribut). Fişier descriere câmp QASYAUJ5

Offset			
J5	**Câmp**	**Format**	**Descriere**
610	Tip intrare	Char(1)	Tipul intrării.
			E Atribute de configuraţie EIM
611	Acţiune	Char(3)	Acţiune
			CHG Atribute modificate
614	Nume	Char(100)	Nume atribut
714	Lungime valoare nouă	Binary(4)	Lungime valoare nouă
716	CCSID valoare nouă	Binary(5)	CCSID valoare nouă
720	ID regiune sau ţară valoare nouă	Char(2)	ID regiune sau ţară valoare nouă
722	ID limbă valoare nouă	Char(3)	ID-ul de limbă al noii valori
725	Valoare nouă	Char(2002) [1]	Valoare nouă
2727	Lungime valoare veche	Binary(4)	Lungime valoare veche
2729	CCSID valoare veche	Binary(5)	CCSID valoare veche
2733	ID regiune sau ţară valoare veche	Char(2)	ID regiune sau ţară valoare veche
2735	ID limbă valoare veche	Char(3)	ID-ul de limbă al vechii valori
2738	Valoare veche	Char(2002) [1]	Valoare veche

1 Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea câmpului.

Tabela 160. Intrări jurnal CA (Modificări autorizare). Fişier descriere câmp QASYCAJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Modificările pentru autorizare
157	225	611	Nume obiect	Char(10)	Numele obiectului.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii în care este obiectul.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Nume utilizator	Char(10)	Numele profilului utilizator a cărui autorizare este revocată.
195	263	649	Nume listă de autorizaţii	Char(10)	Numele listei de autorizaţii.
205	273	659	Existenţă obiect	Char(1)	Autorizările acordate sau înlăturate: **Y** *OBJEXIST
206	274	660	Management obiect	Char(1)	**Y** *OBJMGT
207	275	661	Operare obiect	Char(1)	**Y** *OBJOPR
208	276	662	Gestionare liste de autorizare	Char(1)	**Y** *AUTLMGT
209	277	663	Listă de autorizaţii	Char(1)	**Y** Autorizare publică *AUTL
210	278	664	Autorizare citire	Char(1)	**Y** *READ
211	279	665	Autorizare adăugare	Char(1)	**Y** *ADD
212	280	666	Autorizare actualizare	Char(1)	**Y** *UPD
213	281	667	Autorizare ştergere	Char(1)	**Y** *DLT
214	282	668	Autorizare excludere	Char(1)	**Y** *EXCLUDE
215	283	669	Autorizare execuţie	Char(1)	**Y** *EXECUTE
216	284	670	Autorizare de alterare obiect	Char(1)	**Y** *OBJALTER
217	285	671	Autorizare de referire la obiect	Char(1)	**Y** *OBJREF
218	286	672	(Zonă rezervată)	Char(4)	
222	290	676	Tip comandă	Char(3)	Tipul comenzii folosite. **GRT** Acordare **RPL** Acordare cu înlocuire **RVK** Revocare **USR** Operaţia GRTUSRAUT
225	293	679	Nume câmp	Char(10)	Numele câmpului.
235	303	689	(Zonă rezervată)	Char(10)	
245	313	699	Utilizator office	Char(10)	Numele utilizatorului office.
255	323	709	Nume DLO	Char(12)	Numele DLO-ului.
267	335	721	(Zonă rezervată)	Char(8)	

Tabela 160. Intrări jurnal CA (Modificări autorizare) (continuare). Fişier descriere câmp QASYCAJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
275	343	729	Cale folder	Char(63)	Calea folderului.
338	406	792	Office în numele utilizatorului	Char(10)	Utilizator care lucrează în numele unui alt utilizator.
348	416	802	Stare personală	Char(1)	**Y** Stare personală modificată
349	417	803	Cod acces	Char(1)	**A** Cod acces adăugat **R** Cod acces înlăturat
350	418	804	Cod acces	Char(4)	Cod acces.
354			(Zonă rezervată)	Char(20)	
	422	808	(Zonă rezervată)	Char(18)	
	440	826	Lungime nume obiect [1]	Binary(4)	Lungimea numelui obiectului.
374	442	828	CCSID nume obiect[1]	Binary(5)	Identificatorul setului de caractere codate pentru numele obiect.
378	446	832	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
380	448	834	ID limbă nume obiect[1]	Char(3)	ID-ul limbă pentru numele obiectului.
383	451	837	(Zonă rezervată)	Char(3)	
386	454	840	ID fişier părinte[1,2]	Char(16)	ID-ul fişierului directorului părinte.
402	470	856	ID fişier obiect[1,2]	Char(16)	ID-ul fişier al obiectului.
418	486	872	Nume obiect[1]	Char(512)	Numele obiectului.
	998	1384	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	1014	1400	Nume ASP[5]	Char(10)	Numele dispozitivului ASP.
	1024	1410	Număr ASP[5]	Char(5)	Numărul dispozitivului ASP.
	1029	1415	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele căii absolute.
	1033	1419	ID regiune sau ţară nume cale	Char(2)	ID-ul regiune sau ţară pentru numele cale absolută.
	1035	1421	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	1038	1424	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	1040	1426	Completaţi indicatorului nume cale	Char(1)	Completaţi indicatorul nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele căii absolute complet pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele căii absolute complet pentru obiect.
	1041	1427	ID fişier relativ[3]	Char(16)	ID-ul fişier relativ al numelui de cale absolută.
	1057	1443	Nume cale absolută[4]	Char(5002)	Numele cale absolută al obiectului.

Tabela 160. Intrări jurnal CA (Modificări autorizare) (continuare). Fişier descriere câmp QASYCAJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
[1]	Aceste câmpuri sunt folosite doar pentru obiectele din sistemul de fişiere QOpenSys, din sistemul de fişiere "rădăcină", din sistemele de fişiere definite de utilizator şi QFileSvr.400.				
[2]	Un ID care are bitul cel mai din stânga setat şi restul biţilor 0 indică faptul că ID -ul NU este setat.				
[3]	Când indicatorul nume cale (offset 1040) este ″N″, acest câmp va conţine ID-ul fişier relativ al numelui căii. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.				
[4]	Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui căii.				
[5]	Dacă obiectul este într-o bibliotecă, acestea sunt informaţiile ASP despre biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informaţiile ASP despre obiect.				

Tabela 161. Intrări jurnal CD (şir comenzi). Fişier descriere câmp QASYCDJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **C** Rulare comandă **L** Instrucţiune OCL **O** Control operator. **P** procedură S/36 **S** Rulare comandă după ce substituţia comenzii a avut loc **U** Instrucţiune control utilitar
157	225	611	Nume obiect	Char(10)	Numele obiectului.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii în care este obiectul.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Rulare dintr-un program CL	Char(1)	**Y** Da **N** Nu
186	254	640	Şir comenzi	Char(6000)	Comanda care a fost rulată, cu parametri.
		6640	Nume ASP pentru biblioteca comenzii	Char(10)	Nume ASP pentru biblioteca comenzii
		6650	Numărul ASP pentru biblioteca comenzii	Char(5)	Numărul ASP pentru biblioteca comenzii

Tabela 162. Intrări jurnal CO (Creare obiect). Fişier descriere câmp QASYCOJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării.
					N Creare de noi obiecte
					R Înlocuirea unui obiect existent
157	225	611	Nume obiect	Char(10)	Numele obiectului.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii în care este obiectul.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	(Zonă rezervată)	Char(20)	
205	273	659	Utilizator office	Char(10)	Numele utilizatorului office.
215	283	669	Nume DLO	Char(12)	Numele obiectului bibliotecă de documente creat.
227	295	681	(Zonă rezervată)	Char(8)	
235	303	689	Cale folder	Char(63)	Calea folderului.
298	366	752	Office în numele utilizatorului	Char(10)	Utilizator care lucrează în numele unui alt utilizator.
308			(Zonă rezervată)	Char(20)	
	376	762	(Zonă rezervată)	Char(18)	
	394	780	Lungime nume cale	Binary(4)	Lungimea numelui obiectului.
328	396	782	CCSID nume obiect[1]	Binary(5)	Identificatorul setului de caractere codate pentru numele obiect.
332	400	786	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
334	402	788	ID limbă nume obiect[1]	Char(3)	ID-ul limbă pentru numele obiectului.
337	405	791	(Zonă rezervată)	Char(3)	
340	408	794	ID fişier părinte[1,2]	Char(16)	ID-ul fişierului directorului părinte.
356	424	810	ID fişier obiect[1,2]	Char(16)	ID-ul fişier al obiectului.
372	440	826	Nume obiect[1]	Char(512)	Numele obiectului.
	952	1338	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	968	1354	Nume ASP[5]	Char(10)	Numele dispozitivului ASP.
	978	1364	Număr ASP[5]	Char(5)	Numărul dispozitivului ASP.
	983	1369	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele căii absolute.
	987	1373	ID regiune sau ţară nume cale	Char(2)	ID-ul regiune sau ţară pentru numele cale absolută.
	989	1375	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	992	1378	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	994	1380	Completaţi indicatorului nume cale	Char(1)	Completaţi indicatorul nume cale absolută:
					Y Câmpul Nume cale absolută conţine numele căii absolute complet pentru obiect.
					N Câmpul Nume cale absolută nu conţine numele căii absolute complet pentru obiect.
	995	1381	ID fişier relativ[3]	Char(16)	ID-ul fişier relativ al numelui de cale absolută.

Tabela 162. Intrări jurnal CO (Creare obiect) (continuare). Fişier descriere câmp QASYCOJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1011	1397	Nume cale absolută[4]	Char(5002)	Numele cale absolută al obiectului.

[1] Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fişiere QOpenSys, "rădăcină" şi sistemele de fişiere definite de utilizator.

[2] Un ID care are bitul cel mai din stânga setat şi restul biţilor 0 indică faptul că ID -ul NU este setat.

[3] Când indicatorul nume cale (offset 994) este ″N″, acest câmp va conţine ID-ul fişier relativ al numelui căii. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

[4] Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui căii.

[5] Dacă obiectul este într-o bibliotecă, acestea sunt informaţiile ASP despre biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informaţiile ASP despre obiect.

Tabela 163. Intrări jurnal CP (Modificări profil utilizator). Fişier descriere câmp QASYCPJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Modificare la un profil utilizator
157	225	611	Nume profil utilizator	Char(10)	Numele profilului utilizator care a fost modificat.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	256	639	Nume comandă	Char(3)	Tipul comenzii folosite. **CRT** CRTUSRPRF **CHG** CHGUSRPRF **RST** RSTUSRPRF **DST** Resetare parolă QSECOFR folosind DST **RPA** API-ul QSYRESPA
188	256	642	Parolă modificată	Char(1)	**Y** Parolă modificată
189	257	643	Parolă *NONE	Char(1)	**Y** Parola este *NONE.
190	258	644	Parolă expirată	Char(1)	**Y** Parola expirată este *YES **N** Parola expirată este *NO
191	259	645	Autorizare specială la toate obiectele	Char(1)	**Y** Autorizare specială *ALLOBJ
192	260	646	Autorizare specială control job	Char(1)	**Y** Autorizare specială *JOBCTL
193	261	647	Autorizare specială salvare sistem	Char(1)	**Y** Autorizare specială *SAVSYS

Tabela 163. Intrări jurnal CP (Modificări profil utilizator) (continuare). Fişier descriere câmp QASYCPJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
194	262	648	Autorizare specială administrator securitate	Char(1)	**Y** Autorizare specială *SECADM
195	263	649	Autorizare specială control spool	Char(1)	**Y** Autorizare specială *SPLCTL
196	264	650	Autorizare specială service	Char(1)	**Y** Autorizare specială *SERVICE
197	265	651	Autorizare specială auditare	Char(1)	**Y** Autorizare specială *AUDIT
198	266	652	Autorizare specială configuraţie sistem	Char(1)	**Y** Autorizare specială *IOSYSCFG
199	267	653	(Zonă rezervată)	Char(13)	
212	280	666	Profil grup	Char(10)	Numele unui profil grup.
222	290	676	Proprietar	Char(10)	Proprietarul obiectelor create ca membru al unui profil grup.
232	300	686	Autorizare grup	Char(10)	Autorizare profil grup.
242	310	696	Program iniţial	Char(10)	Numele programului iniţial al utilizatorului.
252	320	706	Biblioteca program iniţial	Char(10)	Numele bibliotecii unde este găsit programul iniţial.
262	330	716	Meniu iniţial	Char(10)	Numele meniului iniţial al utilizatorului.
272	340	726	Bibliotecă meniu iniţial	Char(10)	Numele bibliotecii unde este găsit meniul iniţial.
282	350	736	Biblioteca actuală	Char(10)	Numele bibliotecii actuale a utilizatorului.
292	360	746	Calabilităţi limitate	Char(10)	Valorea parametrului de capabilităţi limitate.
302	370	756	Clasă utilizator	Char(10)	Clasa utilizator a utilizatorului.
312	380	766	Limită prioritate	Char(1)	Valoarea parametrului limită prioritate.
313	381	767	Stare profil	Char(10)	Stare profil utilizator.
323	391	777	Tip autorizare grup	Char(10)	Valoarea parametrului GRPAUTTYP.
333	401	787	Profiluri grup suplimentare	Char(150)	Numele a până la 15 profiluri grup suplimentar pentru utilizator.
483	551	937	Identificare utilizator	Char(10)	uid pentru utilizator.
493	561	947	Identificare grup	Char(10)	gid pentru utilizator.
503	571	957	Gestiune parole locale	Char(10)	Valoarea parametrului LCLPWDMGT.

*Tabela 164. Intrări jurnal CQ (modificare *CRQD).* Fişier descriere câmp QASYCQJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.

*Tabela 164. Intrări jurnal CQ (modificare *CRQD) (continuare).* Fişier descriere câmp QASYCQJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Modificare obiect *CRQD
157	225	611	Nume obiect	Char(10)	Numele obiectului care a fost modificat.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii obiect.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
		639	Nume ASP	Char(10)	Nume ASP pentru biblioteca CRQD
		649	Număr ASP	Char(5)	Număr ASP pentru biblioteca CRQD

Tabela 165. Intrări jurnal CU (Operaţii cluster). Fişier descriere câmp QASYCUJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489 şi Tabela 153 la pagina 491 pentru menţionarea de câmp.
	224	610	Tip intrare	Char(1)	Tipul intrării. **M** Operaţie control cluster **R** operaţie de gestiune grup resurse cluster (*GRP)
	225	611	Acţiune intrare	Char(3)	Tipul acţiunii. **ADD** Adăugare **CRT** Creare **DLT** Ştergere **DST** Distribuire **END** Oprire **FLO** Preluare la eroare **LST** Listare informaţii **RMV** Înlăturare **STR** Pornire **SWT** Comutare **UPC** Actualizare atribute
	228	614	Stare	Char(3)	Starea cererii. **ABN** Cererea s-a terminat anormal **AUT** Eşuare autorizare, *IOSYSCFG este necesară **END** Cererea s-a terminat cu succes **STR** Cererea a fost pornită
	231	617	Nume obiect CRG	Char(10)	Nume obiect grup resurse cluster. **Notă:** Această valoare este completată când tipul intrării este R.

Tabela 165. Intrări jurnal CU (Operaţii cluster) (continuare). Fişier descriere câmp QASYCUJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	241	627	Nume bibliotecă CRG	Char(10)	Biblioteca obiect grup de resurse cluster. **Notă:** Această valoare este completată când tipul intrării este R.
	251	637	Nume cluster	Char(10)	Numele clusterului.
	261	647	ID nod	Char(8)	ID-ul nodului.
	269	655	ID nod sursă	Char(8)	ID-ul nodului sursă.
	277	663	Numele utilizator sursă	Char(10)	Numele utilizatorului sistem sursă care a iniţiat cererea.
	287	673	Nume coadă utilizator	Char(10)	Numele cozii utilizator unde sunt trimise răspunsurile.
	297	683	Bibliotecă coadă utilizator	Char(10)	Biblioteca coadă utilizator.
		693	Nume ASP	Char(10)	Numele ASP pentru biblioteca coadă utilizator.
		703	Număr ASP	Char(5)	Număr ASP pentru biblioteca coadă utilizator.

Tabela 166. Intrări jurnal CV (Verificare conexiune). Fişier descriere câmp QASYCVJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489 şi Tabela 153 la pagina 491 pentru menţionarea de câmp.
	224	610	Tip intrare	Char(1)	Tipul intrării. **C** Conexiune stabilită **E** Conexiune terminată **R** Conexiune rejectată

Tabela 166. Intrări jurnal CV (Verificare conexiune) (continuare). Fişier descriere câmp QASYCVJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	225	611	Acţiune	Char(1)	Acţiune luată pentru tipul de conexiune. ″ ″ Conexiune stabilită sau terminată anormal. Folosită pentru Tipul de intrare C sau E. **A** Peer nu a fost cu autentificare. Folosit pentru Tipul de intrare E sau R. **C** Nici un răspuns de la serverul de autentificare. Folosit pentru Tipul de intrare R. **L** Eroare de configuarare LCP. Folosit pentru Tipul de intrare R. **N** Eroare de configuraţie NCP. Folosit pentru Tipul de intrare R. **P** Parola nu este validă. Folosită pentru Tipul de intrare E sau R. **R** Autentificarea a fost rejectată de peer. Folosită pentru Tipul de intrare R. **T** Eroare de configuraţie L2TP. Folosită pentru Tipul de intrare E sau R. **U** Utilizatorul nu este valid. Folosită pentru Tipul de intrare E sau R.
	226	612	Nume profil punct la punct	Char(10)	Numele profil punct la punct.
	236	622	Protocol	Char(10)	Tipul intrării. **L2TP** Protocolul de tunelare nivel 2 **PPP** Protocol punct la punct. **SLIP** Protocol internet linie serială.
	246	632	Metodă de autentificare locală	Char(10)	Tipul intrării. **CHAP** Protocolul de autentificare dialog de confirmare cerere **PAP** Protocol de autentificare parolă. **SCRIPT** Metodă script.
	256	642	Metodă de autentificare la distanţă	Char(10)	Tipul intrării. **CHAP** Protocolul de autentificare dialog de confirmare cerere **PAP** Protocol de autentificare parolă. **RADIUS** Metodă radius. **SCRIPT** Metodă script.
	266	652	Nume obiect	Char(10)	Numele obiect *VLDL.
	276	662	Nume bibliotecă	Char(10)	Numele bilbiotecă obiect *VLDL.
	286	672	Nume utililizator *VLDL	Char(100)	Nume utilizator *VLDL.

Tabela 166. Intrări jurnal CV (Verificare conexiune) (continuare). Fişier descriere câmp QASYCVJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	386	772	Adresă IP locală	Char(40)	Adresa IP locală.
	426	812	Adresă IP la distanţă	Char(40)	Adresa IP la distanţă.
	466	852	Înaintare IP	Char(1)	Tipul intrării. **Y** Înaintarea IP este activă. **N** Înaintarea IP este inactivă.
	467	853	Proxy ARP	Char(1)	Tipul intrării. **Y** Proxy ARP este activat. **N** Proxy ARP nu este activat.
	468	854	Nume radius	Char(10)	Numele profil AAA.
	478	864	Autentificare adresă IP	Char(40)	Autentificare adresă IP.
	518	904	ID sesiune cont	Char(14)	ID sesiune cont.
	532	918	ID multi-sesiune cont	Char(14)	ID multi-sesiune cont.
	546	932	Număr legătură cont	Binary(4)	Număr legătură cont.
	548	934	Tip tunel	Char(1)	Tip tunel: **0** Netunelat **3** L2TP **6** AH **9** ESP
	549	935	Punct final client tunel	Char(40)	Punct final client tunel
	589	975	Punct final server tunel	Char(40)	Punct final server tunel
	629	1015	Timp sesiune cont	Char(8)	Timp sesiune cont. Folosit pentru Tipul de intrare E sau R.
	637	1023	Cauză termnare cont	Binary(4)	Cauză terminare cont. Folosită pentru Tipul de intrare E sau R.
		1025	Nume ASP	Char(10)	Numele ASP pentru biblioteca listei de validare
		1035	Număr ASP	Char(5)	Numărul ASP pentru biblioteca listei de validare

Tabela 167. Intrări jurnal CY (Configuraţie criptografică). Fişier descriere câmp QASYCYJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Funcţie de Control acces **F** Funcţie de Control facilitate **M** Funcţie Cheie master

Tabela 167. Intrări jurnal CY (Configuraţie criptografică) (continuare). Fişier descriere câmp QASYCYJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	225	611	Acţiune	Char(3)	Funcţia configuraţie criptografică executată: **CCP** Definire profil card. **CCR** Definire rol card. **CLK** Setare ceas. **CLR** Ştergere chei primare. **CRT** Creare chei primare. **DCP** Ştergere profil card. **DCR** Ştergere rol card. **DST** Distribuire chei primare. **EID** Setare ID mediu. **FCV** Încărcare/curăţare FCV. **INI** Reiniţializare card. **QRY** Cerere rol sau informaţii profil. **RCP** Înlocuire profil card. **RCR** Înlocuire rol card. **RCV** Primire chei primare. **SET** Setare chei primare. **SHR** Clonare partajări.
	228	614	Profil card	Char(8)	Numele profilului card.
	236	622	Rol card	Char(8)	Rolul profilului card.
	244	630	Nume dispozitiv	Char(10)	Numele dispozitivului criptografic.

Tabela 168. Intrări jurnal DI (Directory Server). fişier descriere câmp QASYDIJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
	224	610	Tip intrare	Char(1)	Tipul intrării. **L** Operaţie LDAP

Tabela 168. Intrări jurnal DI (Directory Server) (continuare). fişier descriere câmp QASYDIJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	225	611	Tip operaţie	Char(2)	Tipul operaţiei LDAP: **AD** Modificare atribut auditare. **AF** Eşuare autorizare. **BN** Legătură cu succes. **CA** Modificare autorizare obiect. **CF** Modificare configuraţie. **CO** Object creare. **CP** Modificare parolă. **DO** Obiect ştergere. **EX** Exportare director LDAP. **IM** Importare director LDAP. **OM** Obiect gestiune (redenumire). **OW** Modificare drept de proprietate. **PW** Parolă eşuată. **UB** Dezlegare cu succes. **ZC** Obiect modificare. **ZR** Obiect citire.
	227	613	Cod eşuare autorizare	Char(1)	Cod pentru eşuările de autorizare. Acest câmp este folosit doar dacă tipul operaţiei (offset 225) este AF. **A** Încercare neautorizată de modificare valoare auditare. **B** Încercare de legare neautorizată. **C** Încercare de creare obiect neautorizată. **D** Încercare de ştergere obiect neautorizată. **E** Încercare de exportare neautorizată. **F** Modificare configuraţie neautorizată (administrator, modificare istoric, bibliotecă backend, publicare) **I** Încercare de importare neautorizată. **M** Încercare de modificare neautorizată. **R** Încercare de citire neautorizată (căutare).
	228	614	Modificare configuraţie	Char(1)	Modificări configuraţie. Acest câmp este folosit doar dacă tipul operaţiei (offset 225) este CF. **A** Modificare ND administrator **C** Modificare istoric activă/inactivă **L** Modificare nume bibliotecă backend **P** Modificare agent de publicare **R** Modificare server replică

Tabela 168. Intrări jurnal DI (Directory Server) (continuare). fişier descriere câmp QASYDIJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	229	615	Cod modificare configuraţie	Char(1)	Cod pentru modificările configuraţiei. Acest câmp este folosit doar dacă tipul operaţiei (offset 225) este CF. **A** Element adăugat la configuraţie **D** Element şters din configuraţie **M** Element modificat
	230	616	Propagare flag	Char(1)	Indică setarea nouă a proprietarului sau valorii de propagare ACL. Acest câmp este folosit doar dacă tipul operaţiei (offset 225) este CA. **T** Adevărat **F** Fals
	231	617	Alegere autentificare legătură	Char(20)	Alegerea de autentificare legătură. Acest câmp este folosit doar dacă tipul operaţiei (offset 225) este BN.
	251	637	Versiune LDAP	Char(4)	Versiunea clientului care face cererea. Acest câmp este folosit doar dacă operaţia a fost făcută prin serverul LDAP. **2** LDAP versiunea 2 **3** LDAP versiunea 3
	255	641	Indicator SSL	Char(1)	Indică dacă SSL a fost folosit în cerere. Acest câmp este folosit doar dacă operaţia a fost făcută prin serverul LDAP. **0** Nu **1** Da
	256	642	Tip cerere	Char(1)	Tipul cererii. Acest câmp este folosit doar dacă operaţia a fost făcută prin serverul LDAP. **A** Autentificat **N** Anonim **U** Neautentificat
	257	643	ID conexiune	Char(20)	ID-ul conexiunii cererii. Acest câmp este folosit doar dacă operaţia a fost făcută prin serverul LDAP.
	277	663	Adresă IP client	Char(50)	Adresa IP şi numărul de port al cererii client. Acest câmp este folosit doar dacă operaţia a fost făcută prin serverul LDAP.
	327	713	CCSID nume utilizator	Bin(5)	Identificatorului de set de caractere codat al numelui utilizator.
	331	717	Lungime nume utilizator	Bin(4)	Lungimea numelui utilizator.
	333	719	Nume utilizator[1]	Char(2002)	Numele utilizatorului LDAP.
	2335	2721	CCSID nume obiect	Bin(5)	Identificatorul set de caractere codat pentru numele obiectului.
	2339	2725	Lungime nume cale	Bin(4)	Lungimea numelui obiectului.
	2341	2727	Nume obiect[1]	Char(2002)	Numele obiectului LDAP.
	4343	4729	CCSID nume proprietar	Bin(5)	Identificatorului de set de caractere codat al numelui proprietarului. Acest câmp este folosit doar dacă tipul operaţiei (offset 225) este OW.

Tabela 168. Intrări jurnal DI (Directory Server) (continuare). fişier descriere câmp QASYDIJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	4347	4733	Lungime nume proprietar	Bin(4)	Lungimea numelui proprietarului. Acest câmp este folosit doar dacă tipul operaţiei este OW.
	4349	4735	Nume proprietar[1]	Char(2002)	Numele proprietarului. Acest câmp este folosit doar dacă tipul operaţiei (offset 225) este OW.
	6351	6737	CCSID nume nou	Bin(5)	Identificatorul set de caractere codat pentru numele nou. Acest câmp este folosit doar dacă tipul operaţiei (offset 225) este OM, OW, ZC sau AF+M. • Pentru tipul operaţie OM, acest câmp va conţine CCSID-ul numelui obiect nou. • Pentru tipul operaţie OW, acest câmp va conţine CCSID-ul numelui proprietar nou. • Pentru tipurile de operaţie ZC sau AF+M, acest câmp va conţine CCSID-ul listei de tipuri de atribute modificate din câmpul Nume nou.
	6355	6741	Lungime nume nou	Bin(4)	Lungimea numelui nou. Acest câmp este folosit doar dacă tipul operaţiei (offset 225) este OM, OW, ZC sau AF+M. • Pentru tipul operaţie OM, acest câmp va conţine lungimea numelui obiect nou. • Pentru tipul operaţie OW, acest câmp va conţine lungimea numelui proprietar nou. • Pentru tipurile de operaţie ZC sau AF+M, acest câmp va conţine lungimea listei de tipuri de atribute modificate din câmpul Nume nou.
	6357	6743	Nume nou[1]	Char(2002)	Numele nou. Acest câmp este folosit doar dacă tipul operaţiei (offset 225) este OM, OW, ZC sau AF+M. • Pentru tipul operaţie OM, acest câmp va conţine numele obiect nou. • Pentru tipul operaţie OW, acest câmp va conţine numele proprietar nou. • Pentru tipurile de operaţie ZC sau AF+M, acest câmp va conţine o listă de tipuri de atribute modificate.
	8359	8745	ID fişier obiect[2]	Char(16)	ID-ul fişier al obiectului pentru exportare.
	8375	8761	Nume ASP[2]	Char(10)	Numele dispozitivului ASP.
	8385	8771	Număr ASP[2]	Char(5)	Numărul dispozitivului ASP.
	8390	8776	Nume cale CCSID[2]	Bin(5)	Identificatorul de set de caractere codat al numelui de cale absolută.
	8394	8780	ID regiune sau ţară nume cale[2]	Char(2)	ID regiune sau ţară al numelui de cale absolută.
	8396	8782	ID limbă nume cale[2]	Char(3)	ID-ul limbă pentru numele de cale absolută.
	8399	8785	Lungime nume cale[2]	Bin(4)	Lungimea numelui căii absolute.
	8401	8787	Indicator nume cale complet[2]	Char(1)	Indicatorul nume cale absolută completă. **Y** Câmpul Nume cale absolută conţine numele căii absolute complet pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele căii absolute complet pentru obiect.
	8402	8788	ID fişier înrudit[2,3]	Char(16)	ID-ul fişier relativ al numelui de cale absolută.

Tabela 168. Intrări jurnal DI (Directory Server) (continuare). fişier descriere câmp QASYDIJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	8418	8804	Nume cale absolută[1,2]	Char(5002)	Numele cale absolută al obiectului.
		13806	Profil utilizator local	Char(10)	Numele profil utilizator local care este mapat la numele utilizator LDAP (J5 offset 719). Spaţiul gol indică faptul că nici un profil utilizator nu este mapat.
		13816	Indicator administrator	Char(1)	Indicatorului administrator pentru numele utilizator LDAP (J5 offset 719).
					Y Utilizatorul LDAP este un administrator.
					N Utilizatorul LDAP nu este un administrator.
					U Nu este cunoscut acum dacă utilizatorul LDAP este un administrator.

1 Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea valorii din câmp.

2 Aceste câmpuri sunt folosite doar dacă tipul operaţiei (offset 225) este EX sau IM.

3 Când indicatorul nume cale (offset 8401) este ″N″, acest câmp va conţine ID-ul fişier relativ al numelui căii. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

Tabela 169. Intrări jurnal DO (Operaţie ştergere). Fişier descriere câmp QASYDOJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării.
					A Obiectul a fost şters sub un control angajat
					C O ştergere în aşteptare a obiectului a fost realizată
					D O creare în aşteptare a obiectului a fost rulată înapoi.
					P Ştergerea obiectului este în curs (ştergera a fost realizată sub controlul angajării)
					R O ştergere în aşteptare a obiectului a fost rulată înapoi.
157	225	611	Nume obiect	Char(10)	Numele obiectului.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii în care este obiectul.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	(Zonă rezervată)	Char(20)	
205	273	659	Utilizator office	Char(10)	Numele utilizatorului office.
215	283	669	Nume DLO	Char(12)	Numele obiectului bibliotecă de documente.
227	295	681	(Zonă rezervată)	Char(8)	
235	303	689	Cale folder	Char(63)	Calea folderului.
298	366	752	Office în numele utilizatorului	Char(10)	Utilizator care lucrează în numele unui alt utilizator.
308			(Zonă rezervată)	Char(20)	
	376	762	(Zonă rezervată)	Char(18)	

Tabela 169. Intrări jurnal DO (Operaţie ştergere) (continuare). Fişier descriere câmp QASYDOJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	394	780	Lungime nume obiect [1]	Binary(4)	Lungimea numelui obiectului.
328	396	782	CCSID nume obiect[1]	Binary(5)	Identificatorul setului de caractere codate pentru numele obiect.
332	400	786	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
334	402	788	ID limbă nume obiect[1]	Char(3)	ID-ul limbă pentru numele obiectului.
337	405	791	(Zonă rezervată)	Char(3)	
340	408	794	ID fişier părinte[1,2]	Char(16)	ID-ul fişierului directorului părinte.
356	424	810	ID fişier obiect[1,2]	Char(16)	ID-ul fişier al obiectului.
372	440	826	Nume obiect[1]	Char(512)	Numele obiectului.
	952	1338	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	968	1354	Nume ASP[5]	Char(10)	Numele dispozitivului ASP.
	978	1364	Număr ASP[5]	Char(5)	Numărul dispozitivului ASP.
	983	1369	CCSID nume cale	Binary5)	Identificatorul set de caractere codat pentru numele căii absolute.
	987	1373	ID regiune sau ţară nume cale	Char(2)	ID-ul regiune sau ţară pentru numele cale absolută.
	989	1375	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	992	1378	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	994	1380	Completaţi indicatorului nume cale	Char(1)	Completaţi indicatorul nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele căii absolute complet pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele căii absolute complet pentru obiect.
	995	1381	ID fişier relativ[3]	Char(16)	ID-ul fişier relativ al numelui de cale absolută.
	1011	1397	Nume cale absolută [4]	Char(5002)	Numele cale absolută al obiectului.

1 Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fişiere QOpenSys, "rădăcină" şi sistemele de fişiere definite de utilizator.

2 Un ID care are bitul cel mai din stânga setat şi restul biţilor 0 indică faptul că ID -ul NU este setat.

3 Când indicatorul nume cale (offset 994) este ″N″, acest câmp va conţine ID-ul fişier relativ al numelui căii. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

4 Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui cale.

5 Dacă obiectul este într-o bibliotecă, acestea sunt informaţiile ASP despre biblioteca obiectului. Dacă obiectul nu este în bibliotecă, acestea sunt informaţiile ASP pentru obiect.

Tabela 170. Intrări jurnal DS (Resetare ID utilizator unelte service furnizate de IBM). Fişier descriere câmp QASYDSJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Resetare parolă ID utilizator unelte service. **C** Modificat cu un ID utilizator unelte service. **P** Parola ID utilizator unelte service a fost modificată.
157	225	611	Resetare ID utilizator unelte service furnizate de IBM	Char(1)	**Y** Cerere pentru resetare ID utilizator unelte service furnizate de IBM
158	226	612	Tip ID utilizator unelte service	Char(10)	Tipul ID utilizator unelte service ***SECURITY** ***FULL** ***BASIC**
168	236	622	Nume nou ID utilizator unelte service	Char(8)	Numele ID utilizator unelte service.
176	244	630	Modificare parolă ID utilizator unelte service	Char(1)	Cerere pentru modificarea parolei ID utilizator unelte service. **Y** Cerere de modificare parolă ID utilizator unelte service.
	245	631	Nume nou ID utilizator unelte service	Char(10)	Numele ID utilizator unelte service.
	255	641	Profil care cere ID utilizator unelte service	Char(10)	Numele ID-ului utilizator unelte service care a cerut modificarea.

Tabela 171. Intrări jurnal EV (variabilă mediu). Fişier descriere câmp QASYEVJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Adăugare **C** Modificare **D** Ştergere

Tabela 171. Intrări jurnal EV (variabilă mediu) (continuare). Fişier descriere câmp QASYEVJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	225	611	Nume trunchiat	Char(1)	Indică dacă este trunchiat numele variabilei de mediu (offset 232). **Y** Numele variabilă de mediu trunchiat. **N** Numele variabilă de mediu netrunchiat.
	226	612	CCSID	Binary(5)	CCSID-ul numelui variabilei de mediu.
	230	616	Lungime	Binary(4)	Lungimea numelui variabilei de mediu.
	232	618	Nume variabilă de mediu[2]	Char(1002)	Numele variabilei de mediu.
	1234	1620	Nume nou trunchiat[1]	Char(1)	Indică dacă este trunchiat numele nou al variabilei de mediu (offset 1241). **Y** Valoare variabilă de mediu trunchiată. **N** Valoare variabilă de mediu netrunchiată.
	1235	1621	Nume nou CCSID[1]	Binary(5)	CCSID-ul numelui variabilă de mediu nou.
	1239	1625	Lungime nume nou[1]	Binary(4)	Lungimea numelui noii variabilei de mediu.
	1241	1627	Nume nou variabilă de mediu[1,2]	Char (1002)	Numele nou variabilă de mediu.

1 Aceste câmpuri sunt folosite când tipul intrării este C.

2 Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui variabilei de mediu.

Tabela 172. Intrări jurnal GR (înregistrare generică). Fişier descriere câmp QASYGRJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489 şi Tabela 153 la pagina 491 pentru menţionarea de câmp.
	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Adăugare ieşire program **C** Monitorizare operaţii resursă şi operaţii de control **D** Ieşire de program înlăturată. **F** Operaţii de înregistrare funcţie. **R** Ieşire de program înlocuită.
	225	611	Acţiune	Char(2)	Acţiune executată. **ZC** Modificare **ZR** Citire
	227	613	Nume utilizator	Char(10)	Nume profil utilizator Pentru tipul de intrare F, acest câmp conţine numele utilizatorului pentru care a fost executată funcţia de înregistrare funcţie.
	237	623	Câmp 1 CCSID	Binary (5)	Valoarea CCSID pentru câmpul 1.

Tabela 172. Intrări jurnal GR (înregistrare generică) (continuare). Fişier descriere câmp QASYGRJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	241	627	Lungime câmp 1	Binary (4)	Lungimea datelor din câmpul 1.
	243	629	Câmp 1	Char(102)[1]	Date câmp 1 Pentru tipul de intrare F, acest câmp conţine descrierea operaţiei de înregistrare funcţie care a fost executată. Valorile posibile sunt: ***REGISTER:** Funcţia a fost înregistrată ***REREGISTER:** Funcţia a fost actualizată ***DEREGISTER:** Funcţia a fost deînregistrată ***CHGUSAGE:** Informaţiile de folosire funcţie s-au modificat ***CHKUSAGE:** Folosirea de funcţie a fost verificată pentru un utilizator şi verificarea a avut succes ***USAGEFAILURE:** Folosirea de funcţie a fost verificată pentru un utilizator şi verificarea nu a avut succes Pentru tipurile de intrare A, D şi R, acest câmp va conţine informaţiile program de ieşire pentru respectiva funcţie care a fost executată. Pentru tipul de intrare C, acest câmp conţine numele funcţiei RMC care este încercat. Valorile posibile sunt: • **mc_reg_event_select** Înregistrează eveniment folosind selecţia de atribut • **mc_reg_event_handle** Înregistrează eveniment folosind tratarea resursă • **mc_reg_class_event** Înregistrează eveniment pentru o clasă de resurse • **mc_unreg_event** Deînregistrează eveniment • **mc_define_resource** Defineşte resursă nouă • **mc_undefine_resource** Nedefineşte resursă • **mc_set_select** Setează valorile atribut resursă folosind selecţia de atribut • **mc_set_handle** Setează valorile atribut resursă folosind tratarea de resursă • **mc_class_set** Setează valorile atribut clasă de sesurse • **mc_query_p_select** Cerere atribute persistente de resursă folosind selecţia de atribute • **mc_query_d_select** Cerere atribute dinamice resursă folosind selecţia de atribute

Tabela 172. Intrări jurnal GR (înregistrare generică) (continuare). Fişier descriere câmp QASYGRJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
243 (cont)					• **mc_query_p_handle** Cerere atribute persistente resursă folosind tratarea resursă **mc_query_d_handle** Cerere atribute dinamice resursă folosind tratarea de resursă **mc_class_query_p** Cerere atribute presistente clasă de resurse **mc_class_query_d** Cerere atribute dinamice clasă de resurse **mc_qdef_resource_class** Cerere definiţie clasă de resurse **mc_qdef_p_attribute** Cerere definiţie atribut persistent **mc_qdef_d_attribute** Cerere definiţie atribut dinamic **mc_qdef_sd** Cerere de date structurate **mc_qdef_valid_values** Cerere definiţie pentru valori valide de atribut persistent **mc_qdef_actions** Cerere definiţie acţiuni resursă **mc_invoke_action** Invocare acţiune pentru resursă **mc_invoke_class_action** Invocare acţiune pentru o clasă de resurse
	345	731	Câmpul 2 CCSID	Binary (5)	Valoarea CCSID pentru câmpul 2.
	349	735	Lungime câmp 2	Binary (4)	Lungimea datelor din câmpul 2.
	351	737	Câmpul 2	Char (102)[1]	Date câmp 2 Pentru tipul de intrare F, acest câmp conţine numele funcţiei pe care s-a lucrat. Pentru tipul de intrare C, acest câmp conţine numele resursei sau clasei de resurse pentru care a fost încercată operaţia.
	453	839	Câmpul 3 CCSID	Binary (5)	Valoarea CCSID pentru câmpul 3.
	457	843	Lungime câmp 3	Binary (4)	Lungimea datelor din câmpul 3.

Tabela 172. Intrări jurnal GR (înregistrare generică) (continuare). Fişier descriere câmp QASYGRJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	459	845	Câmp 3	Char(102)[1]	Date câmp 3. Pentru tipul de intrare F, acest câmp conţine setarea de folosire pentru un utilizator. Există o valoare pentru acest câmp doar dacă operaţia de înregistrare funcţie este una din următoarele: ***REGISTER:** Când operaţia este *REGISTER, acest câmp conţine valoarea de folosire implicită. Numele utilizator va fi *DEFAULT. ***REREGISTER:** Când operaţia este *REREGISTER, acest câmp conţine valoarea de folosire implicită. Numele utilizator va fi *DEFAULT. ***CHGUSAGE:** Când operaţia este *CHGUSAGE, acest câmp conţine valoarea de folosire pentru utilizatorului specificat în câmpul nume utilizator. Pentru tipul de intrare C, acest câmp conţine rezultatul pentru orice verificare de autorizaţii care a fost făcută pentru operaţia indicată la câmpul 1. Următoarele sunt valori posibile: • *NOAUTHORITYCHECKED: Dacă operaţia indicată la câmpul 1 nu necesită o verificare de autorizaţie sau dacă, dintr-un motiv oarecare, nu a fost încercată nici o verificare de autorizaţie. • *AUTHORITYPASSED: Când ID-ul utilizator mapat indicat în Nume profil utilizator a fost admis cu succes de către verificarea de autorizaţie corespunzătoare pentru operaţia indicată în câmpul 1 pentru resursa sau clasa de resurse indicate în câmpul 2. • *AUTHORITYFAILED: Când ID-ul utilizator mapat indicat în Nume profil utilizator a eşuat verificarea de autorizaţie corespunzătoare pentru operaţia indicată în câmpul 1 pentru resursa sau clasa de resurse indicate în câmpul 2.
	561	947	Câmp 4 CCSID	Binary (5)	Valoarea CCSID pentru câmpul 4.
	565	951	Lungime câmp 4	Binary (4)	Lungimea datelor din câmpul 4.
	567	953	Câmp 4	Char(102)[1]	Date câmp 4. Pentru tipul de intrare F, acest câmp conţine setarea de permitere *ALLJOB pentru funcţie. Există o valoare pentru acest câmp doar dacă operaţia de înregistrare funcţie este una din următoarele: ***REGISTER** ***REREGISTER**

[1] Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea câmpului.

Tabela 173. Intrări jurnal GS (acordare descriptor). Fişier descriere câmp QASYGSJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489,Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **G** Acordare descriptor **R** Primire descriptor **U** Nu se poate folosi descriptor
157	225	611	Nume job	Char(10)	Numele jobului.
167	235	621	Nume utilizator	Char(10)	Numele utilizatorului.
177	245	631	Număr job	Zoned (6,0)	Numărul jobului.
183	251	637	Nume profil utilizator	Char (10)	Numele profilului utilizator.
	261	647	JUID	Char (10)	Identitatea utilizator job al jobului destinaţie. (Această valoare se aplică doar la înregistrările de auditare subtipul G)

Tabela 174. Intrări jurnal IP (comunicaţii între procese). Fişier descriere câmp QASYIPJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Modificări de autorizare şi/sau proprietate **C** Creare **D** Ştergere **F** Eşuare autorizare **G** Obţinere **M** Ataşare memorie partajată **Z** Semafor normal închis sau detaşare memorie partajată
157	225	611	Tip IPC	Char(1)	Tip IPC **M** Memorie partajată **N** Semafor normal **Q** Coadă de mesaje **S** Semafore
158	226	612	Tratare IPC	Binary(5)	ID de tratare IPC
162	230	616	Proprietar nou	Char(10)	Proprietar nou de entitate IPC
172	240	626	Proprietar vechi	Char(10)	Proprietar vechi de entitate IPC

Tabela 174. Intrări jurnal IP (comunicaţii între procese) (continuare). Fişier descriere câmp QASYIPJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
182	250	636	Autorizare proprietar	Char(3)	Autorizare proprietar la entitatea IPC ***R** citire ***W** scriere ***RW** citire şi scriere
185	253	639	Grup nou	Char(10)	Grup asociat cu entitatea IPC
195	263	649	Grup vechi	Char(10)	Grup anterior asociat cu entitatea IPC
205	273	659	Autorizare grup	Char(3)	Autorizare grup la entitatea IPC ***R** citire ***W** scriere ***RW** citire şi scriere
208	276	662	Autorizare publică	Char(3)	Autorizare publică la entitatea IPC ***R** citire ***W** scriere ***RW** citire şi scriere
211	279	665	Nume semafor CCSID	Binary(5)	CCSID-ul numelui semaforului.
216	283	669	Nume semafor lungime	Binary(4)	Lungimea numelui semaforului.
218	285	671	Nume semafor	Char(2050)	Numele semaforului. **Notă:** Acesta este un câmp de lungime variabilă. Primele 2 caractere conţin lungimea numelui semaforului.

Tabela 175. Intrări jurnal IR (Acţiuni reguli IP). Fişier descriere câmp QASYIRJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489 şiTabela 153 la pagina 491 pentru listarea de câmpuri.
	224	610	Tip intrare	Char(1)	Tipul intrării. **L** Au fost încărcate reguli IP de pe un fişier. **N** Reguli IP au fost descărcate pentru o conexiune securitate IP **P** Reguli IP au fost încărcate pentru o conexiune securitate IP **R** Reguli IP au fost citite şi copiate într-un fişier. **U** Au fost descărcate (înlăturate) reguli.
	225	611	Nume fişier	Char(10)	Numele fişierului QSYS folosit pentru a încărca sau primi regulile IP. Această valoare este goală dacă fişierul folosit nu a fost în sistemul de fişiere QSYS.
	235	621	Bibliotecă fişiere	Char(10)	Numele bibliotecii fişiere QSYS.

Tabela 175. Intrări jurnal IR (Acţiuni reguli IP) (continuare). Fişier descriere câmp QASYIRJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	245	631	Rezervat	Char(18)	
	263	649	Lungime nume fişier	Binary (4)	Lungimea numelui fişier.
	265	651	CCSID nume fişier[1]	Binary (5)	Identificatorul set de caractere codat pentru numele fişier.
	269	655	ID fişier regiune sau ţară[1]	Char(2)	ID-ul de regiune sau ţară pentru numele fişier.
	271	657	ID limbă fişier[1]	Char(3)	ID-ul limbă pentru numele fişierului.
	274	660	Rezervat	Char(3)	
	277	663	ID fişier părinte[1, 2]	Char(16)	ID-ul fişierului directorului părinte.
	293	679	ID fişier obiect[1, 2]	Char(16)	ID-ul fişier al fişierului.
	309	695	Nume fişier[1]	Char(512)	Numele fişierului.
	821	1207	Secvenţă conexiune	Char(40)	Numele conexiunii.
	861	1247	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	877	1263	Nume ASP	Char(10)	Numele dispozitivului ASP.
	887	1273	Număr ASP[5]	Char(5)	Numărul dispozitivului ASP.
	892	1278	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele căii absolute.
	896	1282	ID regiune sau ţară nume cale	Char(2)	ID-ul regiune sau ţară pentru numele cale absolută.
	898	1284	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	901	1287	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	903	1289	Completaţi indicatorului nume cale	Char(1)	Completaţi indicatorul nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele căii absolute complet pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele căii absolute complet pentru obiect.
	904	1290	ID fişier relativ[3]	Char(16)	ID-ul fişier relativ al numelui de cale absolută.
	920	1306	Nume cale absolută[4]	Char(5002)	Numele cale absolută al obiectului.

1 Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fişiere QOpenSys şi 'root'.

2 Dacă ID-ul are cel mai din stânga bit setat şi restul de biţi zero, ID-ul **nu** este setat.

3 Când indicatorul nume cale (offset 903) este ″N″, acest câmp va conţine ID-ul fişier relativ al numelui căii. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

4 Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea câmpului.

5 Dacă obiectul este într-o bibliotecă, acestea sunt informaţiile ASP despre biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informaţiile ASP despre obiect.

Tabela 176. Intrări jurnal IS (gestiune securitate internet). Fişier descriere câmp QASYISJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489 şi Tabela 153 la pagina 491 pentru menţionarea de câmp.
	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Eşuare (acest tip nu mai este folosit) **C** Normal (acest tip nu mai este folosit) **U** Utilizator mobil (acest tip nu mai este folosit) **1** Negociere IKE fază 1 SA **2** Negociere IKE fază 2 SA
	225	611	Adresă IP locală	Char(15)	Adresă IP locală.
	240	626	Port ID client local	Char(5)	Port ID client local.
	245	631	Adresă IP la distanţă	Char (15)	Adresă IP la distanţă.
	260	646	Port ID client la distanţă	Char (5)	Port ID client la distanţă (valid pentru faza 2).
	265	651	ID mobil	Char(256)	ID mobil. Acest câmp nu mai este folosit.
	521	907	Codul rezultat	Char(4)	Rezultat negociere: **0** Cu succes **1–30** Erori specifice protocol (documentate în ISAKMP RFC2408, găsit la: http://www.ietf.org) **82xx** erori specifice iSeries VPN Key Manager
	525	911	CCSID	Bin(5)	Identificatorul set de caractere codat • ID local • Valoare ID client local • ID la distanţă • Valoare ID client la distanţă
	529	915	ID local	Char(256)	Identificator IKE local
	785	1171	Tip ID client local	Char(2)	Tipul ID-ului client (valid pentru faza 2): **1** Adresă IP versiunea 4 **2** Nume domeniu complet calificat **3** Nume domeniu complet calificat utilizator **4** Subreţea IP versiunea 4 **7** Interval adresă IP versiunea 4 **9** Nume distinctiv **11** Identificator cheie
	787	1173	Valoare ID client local	Char(256)	ID client local (valid pentru faza 2)
	1043	1429	Protocol ID client local	Char(4)	Protocol ID client local (valid pentru faza 2)
	1047	1433	ID la distanţă	Char(256)	Identificator IKE la distanţă

Tabela 176. Intrări jurnal IS (gestiune securitate internet) (continuare). Fişier descriere câmp QASYISJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1303	1689	Tip ID client la distanţă	Char(2)	Tipul ID-ului client (valid pentru faza 2) **1** Adresă IP versiunea 4 **2** Nume domeniu complet calificat **3** Nume domeniu complet calificat utilizator **4** Subreţea IP versiunea 4 **7** Interval adresă IP versiunea 4 **9** Nume distinctiv **11** Identificator cheie
	1305	1691	Valoare ID client la distanţă	Char(256)	ID client la distanţă (valid pentru faza 2)
	1561	1947	Protocol ID client la distanţă	Char(4)	Protocol ID client la distanţă (valid pentru faza 2)

Tabela 177. Intrări jurnal JD (modificare descriere job). Fişier descriere câmp QASYJDJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Profilul utilizator specificat pentru parametrul USER al descrierii de job
157	225	611	Descriere job	Char(10)	Numele descrierii de job modificate care a avut parametrul USER modificat.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii în care este obiectul.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Tip comandă	Char(3)	Tipul comenzii folosite. **CHG** comanda CHGJOBD (Change Job Description - Modificare descriere job) **CRT** comanda CRTJOBD (Create Job Description - Creare descriere job)
188	256	642	Utilizator vechi	Char(10)	Numele profilului utilizator specificat pentru parametrul USER înainte ca descrierea de job să se fi modificat.
198	266	652	Utilizator nou	Char(10)	Numele profilului USER specificat pentru parametrul utilizator înainte ca descrierea de job să se fi modificat.
		662	Nume ASP	Char(10)	Nume ASP pentru biblioteca JOBD
		672	Număr ASP	Char(5)	Număr ASP pentru biblioteca JOBD

Tabela 178. Intrări jurnal JS (modificare job). Fişier descriere câmp QASYJSJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării.
					A comanda ENDJOBABN
					B Lansare
					C Modificare
					E Terminare
					H Reţinere
					I Deconectare
					M Modificare profil sau profil de grup
					N Comanda ENDJOB
					P Ataşare job imediat batch sau prestart
					Q Modificare atributele cerere
					R Eliberare
					S Pornire
					T Modificare profil sau profil de grup folosind un jeton de profil.
					U CHGUSRTRC
					V Dispozitiv virtual modificat de către API-ul QWSACCDS.
157	225	611	Tip job	Char(1)	Tipul jobului.
					A Autostart
					B Batch
					I Interactiv
					M Monitorizare subsistem
					R Cititor
					S Sistem
					W Scriitor
					X SCPF

Tabela 178. Intrări jurnal JS (modificare job) (continuare). Fişier descriere câmp QASYJSJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
158	226	612	Subtip job	Char(1)	Subtipul jobului. **' '** Nici un subtip **D** Batch imediat **E** Cerere start procedură **J** Prestart **P** Driver dispozitiv de tipărire **Q** Cerere **T** MRT **U** Utilizator spool alternativ
159	227	613	Nume job	Char(10)	Prima parte a numelui de job calificat pe care se operează.
169	237	623	Nume utilizator job	Char(10)	A doua parte a numelui de job calificat pe care se operează.
179	247	633	Număr job	Char(6)	A treia parte a numelui de job calificat pe care se operează.
185	253	639	Nume dispozitiv	Char(10)	Numele dispozitivului
195	263	649	Profil utilizator efectiv[2]	Char(10)	Numele profilului utilizator efectiv pentru firul de execuţie
205	273	659	Nume descriere job	Char(10)	Numele descrierii job pentru job
215	283	669	Bibliotecă descriere job	Char(10)	Numele bibliotecii pentru descrierea job
225	293	679	Numel coadă job	Char(10)	Numele cozii de joburi pentru job
235	303	689	Bibliotecă coadă joburi	Char(10)	Numele bibliotecii pentru coada de joburi
245	313	699	Nume coadă ieşire	Char(10)	Numele cozii de ieşire pentru job
255	323	709	Bibliotecă coadă ieşire	Char(10)	Numele bibliotecii pentru coada de ieşire
265	333	719	Dispozitiv imprimantă	Char(10)	Numele cozii dispozitivului imprimantă pentru job
275	343	729	Listă de biblioteci[2]	Char(430)	Lista de biblioteci pentru job
705	773	1159	Nume profil grup efectiv[2]	Char(10)	Numele profilului grup efectiv pentru firul de execuţie
715	783	1169	Profiluri grup suplimentare[2]	Char(150)	Numele profilurilor grup suplimentare pentru firul de execuţie.
	933	1319	Descriere JUID	Char(1)	Descrie înţelesul câmpului JUID: **' '** Câmpul JUID conţine valoarea pentru JOB. **C** API-ul JUID de curăţare a fost apelat. Câmpul JUID conţine noua valoare. **S** API-ul JUID de setare a fost apelat. Câmpul JUID conţine noua valoare.
	934	1320	Câmp JUID	Char(10)	Conţine valoarea JUID
	944	1330	Profil utilizator real	Char(10)	Numele profilului utilizator real pentru firul de execuţie.
	954	1340	Profil utilizator salvat	Char(10)	Numele profilului utilizator salvat pentru firul de execuţie.

Tabela 178. Intrări jurnal JS (modificare job) (continuare). Fişier descriere câmp QASYJSJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	964	1350	Profil grup real	Char(10)	Numele profilului de profil grup real pentru firul de execuţie.
	974	1360	Profil grup salvat	Char(10)	Numele profilului de profil grup salvat pentru firul de execuţie.
	984	1370	Utilizator real modificat[3]	Char(1)	Profilul utilizator real a fost modificat. **Y** Da **N** Nu
	985	1371	Utilizator efectiv modificat[3]	Char(1)	Profilul utilizator efectiv a fost modificat. **Y** Da **N** Nu
	986	1372	Utilizator salvat modificat[3]	Char(1)	Profilul utilizator salvat a fost modificat **Y** Da **N** Nu
	987	1373	Grup real modificat[3]	Char(1)	Profilul grup real a fost modificat. **Y** Da **N** Nu
	988	1374	Grup efectiv modificat[3]	Char(1)	Profilul grup efectiv a fost modificat. **Y** Da **N** Nu
	989	1375	Grup salvat modificat[3]	Char(1)	Profilul grup salvat a fost modificat. **Y** Da **N** Nu
	990	1376	Grupuri suplimentare modificate[3]	Char(1)	Profilurile grup suplimentare au fost modificate. **Y** Da **N** Nu
	991	1377	Numărul listă biblioteci[4]	Bin(4)	Numărul de biblioteci din câmpul extensie listă de biblioteci (offset 993).
	993	1379	Extensie listă de biblioteci[4,5]	Char(2252)	Extensia la lista de biblioteci pentru job.
		3631	Grup ASP ASP de biblioteci	Char(10)	Grup ASP ASP de biblioteci
		3641	Nume ASP	Char(10)	Nume ASP pentru biblioteca JOBD
		3651	Număr ASP	Char(5)	Număr ASP pentru biblioteca JOBD

[1] Acest câmp este gol dacă jobul este în coada de mesaje şi nu rulează.

[2] Când înregitrarea de auditare JS este generată din cauză că un job execută o operaţie într-un alt job, atunci acest câmp va conţine date din firul de execuţie iniţial al jobului pe care se operează. În toate celelalte cazuri, câmpul va conţine date din firul de execuţie care a executat operaţia.

[3] Acest câmp este folosit doar când tipul intrării (offset 224) este M sau T.

[4] Acest câmp este folosit doar dacă numărul de biblioteci din lista de biblioteci depăşeşte dimensiunea câmpului la offset-ul 343.

[5] Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea datelor din câmp.

Tabela 179. Intrări jurnal KF (Fişier inel de chei). Fişier descriere câmp QASYKFJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489 şi Tabela 153 la pagina 491 pentru listarea de câmpuri.
	224	610	Tip intrare	Char(1)	Tipul intrării.
					C Operaţie certificat
					K Operaţie fişier inel de chei
					P Parolă incorectă
					T Operaţie rădăcină de încredere
	225	611	Operaţie certificat	Char(3)	Tip acţiune[4].
					ADK Certificat cu cheie privată adăugată
					ADD Certificat adăugat
					REQ Certificat cerut
					SGN Certificat semnat
	228	614	Operaţie inel de chei	Char(3)	Tip acţiune[5].
					ADD Pereche inele chei adăugată
					DFT Pereche inele chei desemnată ca implicită
					EXP Pereche inele chei exportată
					IMP Pereche inele chei importată
					LST Listează etichetele perechilor de inele de chei într-un fişier
					PWD Modifică parola fişier inel de chei
					RMV Pereche inele chei înlăturată
					INF Extragere informaţii pereche inel de chei
					2DB Fişier inel de chei convertit la un format bază de date de chei
					2YR fişier bază de date de chei convertit la fişier inel de chei
	231	617	Operaţie root de încredere	Char(3)	Tip acţiune[6].
					TRS Pereche inele chei desemnată ca root de încredere
					RMV Desemnare root de încredere înlăturată
					LST Listează root-urile de încredere
	234	620	Rezervat	Char(18)	
	252	638	Lungime nume cale	Binary(4)	Lungime nume fişier inel de chei
	254	640	CCSID nume obiect	Binary(5)	CCSID nume fişier inel de chei
	258	644	ID regiune sau ţară nume obiect	Char(2)	ID ţară sau regiune nume fişier inel de chei
	260	646	ID limbă nume obiect	Char(3)	ID limbă nume fişier inel de chei
	263	649	Rezervat	Char(3)	
	266	652	ID fişier părinte	Char(16)	OD fişier direcotr părinte inel de chei

Tabela 179. Intrări jurnal KF (Fişier inel de chei) (continuare). Fişier descriere câmp QASYKFJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	282	668	ID fişier obiect	Char(16)	Nume fişier director inel de chei
	298	684	Nume obiect	Char(512)	Nume fişier inel de chei
	810	1196	Rezervat	Char(18)	
	828	1214	Lungime nume obiect	Binary(4)	Lungime nume fişier destinaţie sau sursă
	830	1216	CCSID nume obiect	Binary(5)	CCSID nume fişier destinaţie sau sursă
	834	1220	ID regiune sau ţară nume obiect	Char(2)	ID regiune sau ţară nume fişier destinaţie sau sursă
	836	1222	ID limbă nume obiect	Char(3)	ID limbă nume fişier destinaţie sau sursă.
	839	1225	Rezervat	Char(3)	
	842	1228	ID fişier părinte	Char(16)	ID fişier director părinte destinaţie sau sursă.
	858	1244	ID fişier obiect	Char(16)	ID fişier director destinaţie sau sursă
	874	1260	Nume obiect	Char(512)	Nume fişier destinaţie sau sursă.
	1386	1772	Lungime etichetă certificat	Binary(4)	Lungime etichetă certificat.
	1388	1774	Etichetă certificat[1]	Char(1026)	Etichetă certificat.
	2414	2800	ID fişier obiect	Char(16)	ID fişier fişier inel de chei.
	2430	2816	Nume ASP	Char(10)	Numele dispozitivului ASP.
	2440	2826	Număr ASP	Char(5)	Numărul dispozitivului ASP.
	2445	2831	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele căii absolute.
	2449	2835	ID regiune sau ţară nume cale	Char(2)	ID-ul regiune sau ţară pentru numele cale absolută.
	2451	2837	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	2454	2840	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	2456	2842	Completaţi indicatorului nume cale	Char(1)	Completaţi indicatorul nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele căii absolute complet pentru fişierul inel de chei. **N** Câmpul Nume cale absolută nu conţine numele căii absolute complet pentru fişierul inel de chei.
	2457	2843	ID fişier relativ[2]	Char(16)	ID-ul fişier relativ al numelui de cale absolută.
	2473	2859	Nume cale absolută[1]	Char(5002)	Numele cale absolută al fişierului inel de chei.
	7475	7861	ID fişier obiect	Char(16)	ID-ul fişier al fişierului destinaţie sau sursă.
	7491	7877	Nume ASP	Char(10)	Nume ASP fişier destinaţie sau sursă
	7501	7887	Număr ASP	Char(5)	Număr ASP fişier destinaţie sau sursă
	7506	7892	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele căii absolute.
	7510	7896	ID regiune sau ţară nume cale	Char(2)	ID-ul de regiune sau ţară pentru numele de cale absolută.
	7512	7898	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	7515	7901	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.

Tabela 179. Intrări jurnal KF (Fişier inel de chei) (continuare). Fişier descriere câmp QASYKFJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	7517	7903	Completaţi indicatorului nume cale	Char(1)	Completaţi indicatorul nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele căii absolute complet pentru fişierul destinaţie sau sursă. **N** Câmpul Nume cale absolută nu conţine numele căii absolute complet pentru fişierul destinaţie sau sursă.
	7518	7904	ID fişier relativ[3]	Char(16)	ID-ul fişier relativ al numelui de cale absolută.
	7534	7920	Nume cale absolută[1]	Char(5002)	Numele cale absolută al fişierului destinaţie sau sursă.

1 Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui căii.

2 Când indicatorul de nume cale (offset 2456) este ″N″, acest câmp va conţine ID-ul de fişier relativ al numelui căii absolute la offset-ul 2473. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

3 Când indicatorul de nume cale (offset 7517) este ″N″, acest câmp va conţine ID-ul de fişier relativ al numelui căii absolute la offset-ul 7534. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

4 Câmpul va conţine spaţii goale când nu este o operaţie de certificat.

5 Câmpul va conţine spaţii goale când nu este o operaţie de fişier inel de chei.

6 Câmpul va conţine spaţii goale când nu este o operaţie de root de încredere.

Tabela 180. Intrări jurnal LD (director de căutare, legare, dezlegare). Fişier descriere câmp QASYLDJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **L** Legare director **U** Dezlegare director **K** Căutare director
157			(Zonă rezervată)	Char(20)	
	225	611	(Zonă rezervată)	Char(18)	
	243	629	Lungime nume obiect [1]	Binary (4)	Lungimea numelui obiectului.
177	245	631	CCSID nume obiect[1]	Binary(5)	Identificatorul setului de caractere codate pentru numele obiect.
181	249	635	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
183	251	637	ID limbă nume obiect[1]	Char(3)	ID-ul limbă pentru numele obiectului.
186	254	640	(Zonă rezervată)	Char(3)	
189	257	643	ID fişier părinte[1,2]	Char(16)	ID-ul fişierului directorului părinte.

Tabela 180. Intrări jurnal LD (director de căutare, legare, dezlegare) (continuare). Fişier descriere câmp QASYLDJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
205	273	659	ID fişier obiect[1,2]	Char(16)	ID-ul fişier al obiectului.
221	289	675	Nume obiect[1]	Char(512)	Numele obiectului.
	801	1187	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	817	1203	Nume ASP	Char(10)	Numele dispozitivului ASP.
	827	1213	Număr ASP	Char(5)	Numărul dispozitivului ASP.
	832	1218	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele căii absolute.
	836	1222	ID regiune sau ţară nume cale	Char(2)	ID-ul de regiune sau ţară pentru numele de cale absolută.
	838	1224	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	841	1227	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	843	1229	Completaţi indicatorului nume cale	Char(1)	Completaţi indicatorul nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele căii absolute complet pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele căii absolute complet pentru obiect.
	844	1230	ID fişier înrudit[1]	Char(16)	ID-ul fişier relativ al numelui de cale absolută.
	860	1246	Nume cale absolută[2]	Char(5002)	Numele cale absolută al obiectului.

1 Când indicatorul de nume cale (offset 843) este ″N″, acest câmp va conţine ID-ul d fişier relativ al numelui căii absolute. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

2 Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui căii.

Tabela 181. Intrări jurnal ML (Acţiuni mail). Fişier descriere câmp QASYMLJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **O** Istoric de mailuri deschis
157	225	611	Profil utilizator	Char(10)	Nume profil utilizator.
167	235	621	ID utilizator	Char(8)	Identificator utilizator
175	243	629	Adresă	Char(8)	Adresă utilizator

Tabela 182. Intrări jurnal NA (Modificare atribut). Fişier descriere câmp QASYNAJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Modificare la atributul reţea. **T** Modificare la atributul TCP/IP.
157	225	611	Atribut	Char(10)	Numele atributului.
167	235	621	Valorea nouă atribut	Char(250)	Valoarea atributului după ce a fost modificat.
417	485	871	Valorea veche atribut	Char(250)	Valoarea atributului înainte de a fi modificat.

Tabela 183. Intrări de jurnal ND (Filtru de căutare director APPN). Fişier descriere câmp QASYNDJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Violare filtru de căutare director
157	225	611	Nume punct de control filtrat	Char(8)	Nume punct de control filtrat
165	233	619	NETID punct de control filtrat	Char(8)	NETID punct de control filtrat
173	241	627	Nume locaţie CP filtrat	Char(8)	Nume locaţie CP filtrat.
181	249	635	NETID locaţie CP filtrat	Char(8)	NETID locaţie CP filtrat.
189	257	643	Nume locaţie partener	Char(8)	Nume locaţie partener.
197	265	651	NETID locaţie partener	Char(8)	NETID locaţie partener.
205	273	659	Sesiune intrare	Char(1)	Sesiune intrare. **Y** Aceasta este o sesiune intrare **N** Aceasta nu este o sesiune intrare
206	274	660	Sesiune ieşire	Char(1)	Sesiune ieşire. **Y** Aceasta este o sesiune ieşire **N** Aceasta nu este o sesiune ieşire

Pentru informaţii suplimentare despre Filtrul de căutare director şi Punctul final APPN, vedeţi Centrul de informare (vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii).

Tabela 184. Intrări de jurnal NE (Filtru punct final APPN). Fişier descriere câmp QASYNEJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Violare filtru punct final.
157	225	611	Nume locaţie locală	Char(8)	Nume locaţie locală.
165	233	619	Nume locaţie la distanţă	Char(8)	Nume locaţie la distanţă.
173	241	627	NETID la distanţă	Char(8)	NETID la distanţă.
181	249	635	Sesiune intrare	Char(1)	Sesiune intrare. **Y** Aceasta este o sesiune intrare **N** Aceasta nu este o sesiune intrare
182	250	636	Sesiune ieşire	Char(1)	Sesiune ieşire. **Y** Aceasta este o sesiune ieşire **N** Aceasta nu este o sesiune ieşire

Pentru informaţii suplimentare despre Filtrul de căutare director şi Punctul final APPN, vedeţi Centrul de informare (vedeţi "Cerinţe preliminare şi informaţii înrudite" la pagina xvi pentru detalii).

Tabela 185. Intrări jurnal OM (Modificare gestiune obiect). Fişier descriere câmp QASYOMJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **M** Obiect mutat la o bibliotecă diferită. **R** Obiect redenumit.
157	225	611	Nume obiect vechi	Char(10)	Numele vechi al obiectului.
167	235	621	Nume bibliotecă vechi	Char(10)	Numele bibliotecii în care este obiectul vechi.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Nume obiect nou	Char(10)	Numele nou al obiectului.
195	263	649	Nume bibliotecă nou	Char(10)	Numele bibliotecii în care a fost mutat obiectul.
205	273	659	(Zonă rezervată)	Char(20)	
225	293	679	Utilizator office	Char(10)	Numele utilizatorului office.
235	303	689	Nume document sau folder vechi	Char(12)	Numele vechi al folderului sau documentului.
247	315	701	(Zonă rezervată)	Char(8)	
255	323	709	Cale folder veche	Char(63)	Calea veche a folderului.

Tabela 185. Intrări jurnal OM (Modificare gestiune obiect) (continuare). Fişier descriere câmp QASYOMJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
318	386	772	Folder nou sau nume document	Char(12)	Numele nou al folderului sau documentului.
330	398	784	(Zonă rezervată)	Char(8)	
338	406	792	Cale folder nouă	Char(63)	Calea nouă a folderului.
401	469	855	Office în numele utilizatorului	Char(10)	Utilizator care lucrează în numele unui alt utilizator.
411			(Zonă rezervată)	Char(20)	
	479	865	(Zonă rezervată)	Char (18)	
	497	883	Lungime nume cale	Binary (4)	Lungimea câmpului nume obiect vechi.
431	499	885	CCSID nume obiect[1]	Binary(5)	Identificatorul setului de caractere codate pentru numele obiect.
435	503	889	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
437	505	891	ID limbă nume obiect[1]	Char(3)	ID-ul limbă pentru numele obiectului.
440	508	894	(Zonă rezervată)	Char(3)	
443	511	897	Fişier părinte vechi[1,2]	Char(16)	ID-ul fişier al directorului părinte vechi.
459	527	913	ID fişier obiect vechi[1,2]	Char(16)	ID-ul fişier al obiectului vechi.
475	543	929	Nume obiect vechi[1]	Char(512)	Numele obiectului vechi.
987	1055	1441	ID fişier părinte nou[1,2]	Char(16)	ID fişier al directorului părinte nou.
1003	1071	1457	Nume obiect nou[1,2,6]	Char(512)	Numele nou al obiectului.
	1583	1969	ID fişier obiect[1,2]	Char(16)	ID-ul fişier al obiectului.
	1599	1985	Nume ASP[7]	Char(10)	Numele dispozitivului ASP.
	1609	1995	Număr ASP[7]	Char(5)	Numărul dispozitivului ASP.
	1614	2000	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele căii absolute.
	1618	2004	ID regiune sau ţară nume cale	Char(2)	ID-ul de regiune sau ţară pentru numele de cale absolută.
	1620	2006	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	1623	2009	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	1625	2011	Completaţi indicatorului nume cale	Char(1)	Completaţi indicatorul nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele căii absolute complet pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele căii absolute complet pentru obiect.
	1626	2012	ID fişier relativ[3]	Char(16)	ID-ul fişier relativ al numelui de cale absolută.
	1642	2028	Nume cale absolută[5]	Char(5002)	Numele cale absolută vechi al obiectului.
	6644	7030	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	6660	7046	Nume ASP[8]	Char(10)	Numele dispozitivului ASP.
	6670	7056	Număr ASP[8]	Char(5)	Numărul dispozitivului ASP.

Tabela 185. Intrări jurnal OM (Modificare gestiune obiect) (continuare). Fişier descriere câmp QASYOMJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	6675	7061	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele căii absolute.
	6679	7065	ID regiune sau ţară nume cale	Char(2)	ID-ul de regiune sau ţară pentru numele de cale absolută.
	6681	7067	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	6684	7070	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	6686	7072	Completaţi indicatorului nume cale	Char(1)	Completaţi indicatorul nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele căii absolute complet pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele căii absolute complet pentru obiect.
	6687	7073	ID fişier înrudit[4]	Char(16)	ID-ul fişier relativ al numelui de cale absolută.
	6703	7089	Nume cale absolută[5]	Char(5002)	Numele cale absolută nou al obiectului.

1 Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fişiere QOpenSys, "rădăcină" şi sistemele de fişiere definite de utilizator.

2 Un ID care are bitul cel mai din stânga setat şi restul biţilor 0 indică faptul că ID -ul NU este setat.

3 Când indicatorul de nume cale (offset 1625) este ″N″, acest câmp va conţine ID-ul de fişier relativ al numelui căii absolute la offset-ul 1642. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

4 Când indicatorul de nume cale (offset 6686) este ″N″, acest câmp va conţine ID-ul de fişier relativ al numelui căii absolute la offset-ul 6703. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

5 Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui căii.

6 Nu există nici un câmp lungime asociat pentru această valoare. Şirul este completat cu null dacă nu este de lungime de 512 caractere.

7 Dacă obiectul vechi este într-o bibliotecă, acestea sunt informaţiile ASP bibliotecii obiectului. Dacă obiectul vechi nu este într-o bibliotecă, acestea sunt informaţiile ASP ale obiectului.

8 Dacă obiectul nou este într-o bibliotecă, acestea sunt informaţiile ASP bibliotecii obiectului. Dacă obiectul nou nu este în bibliotecă, acestea sunt informaţiile ASP pentru obiect.

Tabela 186. Intrări jurnal OR (restaurare obiect)(. Fişier descriere câmp QASYORJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **N** Un obiect nou a fost restaurat pentru sistem. **E** Un obiect existent a fost restaurat pentru sistem.
157	225	611	Nume obiect restaurat	Char(10)	Numele obiectului restaurat.

Tabela 186. Intrări jurnal OR (restaurare obiect)((continuare). Fişier descriere câmp QASYORJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
167	235	621	Nume bibliotecă restaurat	Char(10)	Numele bibliotecii obiectului restaurat.
177	245	631	Tip obiect.	Char(8)	Tipul obiectului.
185	253	639	Nume obiect salvat	Char(10)	Numele obiectului salvat.
195	263	649	Nume bibliotecă salvată	Char(10)	Numele bibliotecii din care este salvat obiectul
205	273	659	Stare program[1]	Char(1)	**I** A fost restaurat un program în stare de moştenire. **Y** A fost restaurat un program în stare sistem. **N** A fost restaurat un program în stare utilizator.
206	274	660	Comandă sistem[2]	Char(1)	**Y** A fost restaurată o comandă sistem. **N** A fost restaurată o comandă în stare utilizator.
207			(Zonă rezervată)	Char(18)	
	275	661	Mod SETUID	Char(1)	Idicatorul mod SETUID. **Y** Bitul mod SETUID pentru obiectul restaurat este activ. **N** Bitul mod SETUID pentru obiectul restaurat nu este activ.
	276	662	Mod SETGID	Char(1)	Idicatorul mod SETGID. **Y** Bitul mod SETGID pentru obiectul restaurat este activ. **N** Bitul mod SETGID pentru obiectul restaurat nu este activ.
	277	663	Stare semnătură	Char(1)	Starea semnăturii pentru obiectul restaurat. **B** Semnătura nu a fost în format OS/400 **E** Semnătura există dar nu este verificată **F** Semnătura nu se potriveşte cu conţinutul obiectului **I** Semnătură ignorată **N** Obiect de nesemnat **S** Semnătura este validă **T** Semnătură fără încredere **U** Obiect nesemnat

Tabela 186. Intrări jurnal OR (restaurare obiect)((continuare). Fişier descriere câmp QASYORJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	278	664	Atribut scanare	Char(1)	Dacă fişierul a fost un obiect sistem de fişiere integrat, valoarea atributului de scanare pentru acel obiect a fost
					Y *YES
					N *NO
					C *CHGONLY Vedeţi comanda CHGATR pentru descrieri ale acestor valori.
	279	665	Rezervat	Char(14)	
225	293	679	Utilizator office	Char(10)	Numele utilizatorului office.
235	303	689	Restaurare nume DLO	Char(12)	Numele obiectului bibliotecii de documente al obiectului restaurat.
247	315	701	(Zonă rezervată)	Char(8)	
255	323	709	Cale folder restaurare	Char(63)	Folderul în care a fost restaurat DLO.
318	386	772	Nume DLO salvare	Char(12)	Numele DLO al obiectului salvat.
330	398	784	(Zonă rezervată)	Char(8)	
338	406	792	Cale folder salvare	Char(63)	Folderul din care a fost salvat DLO.
401	469	855	Office în numele utilizatorului	Char(10)	Utilizator care lucrează în numele unui alt utilizator.
411			(Zonă rezervată)	Char(20)	
	479	865	(Zonă rezervată)	Char(18)	
	497	883	Lungime nume cale	Binary (4)	Lungimea câmpului Nume obiect vechi.
431	499	885	CCSID nume obiect[3]	Binary(5)	identificator de set de caractere codate pentru numele obiect.
435	503	889	ID regiune sau ţară nume obiect[3]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
437	505	891	ID limbă nume obiect[3]	Char(3)	ID-ul limbă pentru numele obiectului.
440	508	894	(Zonă rezervată)	Char(3)	
443	511	897	ID fişier părinte[3,4]	Char(16)	ID-ul fişierului directorului părinte.
459	527	913	ID fişier obiect[3,4]	Char(16)	ID-ul fişier al obiectului.
475	543	929	Nume obiect[3]	Char(512)	Numele obiectului.
	1055	1441	ID fişier vechi	Char(16)	ID-ul fişier al obiectului vechi.
	1071	1457	ID fişier mediu	Char(16)	ID-ul fişier (FID) care a fost restaurat în fişierul de mediu. **Notă:** FID-ul memorat pe mediu este FID-ul pe care l-a avut obiectul în sistemul sursă.
	1087	1473	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	1103	1489	Nume ASP[7]	Char(10)	Numele dispozitivului ASP.
	1113	1499	Număr ASP[7]	Char(5)	Numărul dispozitivului ASP.
	1118	1504	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele căii absolute.
	1122	1508	ID regiune sau ţară nume cale	Char(2)	ID-ul de regiune sau ţară pentru numele de cale absolută.

Tabela 186. Intrări jurnal OR (restaurare obiect)((continuare). Fişier descriere câmp QASYORJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1124	1510	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	1127	1513	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	1129	1515	Completaţi indicatorului nume cale	Char(1)	Completaţi indicatorul nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele căii absolute complet pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele căii absolute complet pentru obiect.
	1130	1516	ID fişier relativ[5]	Char(16)	ID-ul fişier relativ al numelui de cale absolută.
	1146	1532	Nume cale absolută[6]	Char(5002)	Numele cale absolută al obiectului.

1 Acest câmp are o intrare doar dacă obiectul care a fost restaurat este un program.

2 Acest câmp are o intrare doar dacă obiectul care a fost restaurat este o comandă.

3 Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fişiere QOpenSys şi "rădăcină".

4 Un ID care are bitul cel mai din stânga setat şi restul biţilor 0 indică faptul că ID -ul NU este setat.

5 Când indicatorul de nume cale (offset 1129) este ″N″, acest câmp conţine ID-ul de fişier relativ al numelui de cale absolută. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

6 Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui căii.

7 Dacă obiectul este într-o bibliotecă, acestea sunt informaţiile ASP despre biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informaţiile ASP despre obiect.

Tabela 187. Intrări jurnal OW (modificare drept de proprietate). Fişier descriere câmp QASYOWJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Modificare proprietar obiect
157	225	611	Nume obiect	Char(10)	Numele obiectului.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii în care este obiectul.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Proprietar vechi	Char(10)	Proprietarul vechi al obiectului.
195	263	649	Proprietar nou	Char(10)	Proprietarul nou al obiectului.
205	273	659	(Zonă rezervată)	Char(20)	
225	293	679	Utilizator office	Char(10)	Numele utilizatorului office.
235	303	689	Nume DLO	Char(12)	Numele obiectului bibliotecă de documente.
247	315	701	(Zonă rezervată)	Char(8)	
255	323	709	Cale folder	Char(63)	Calea folderului.
318	386	772	Office în numele utilizatorului	Char(10)	Utilizator care lucrează în numele unui alt utilizator.
328			(Zonă rezervată)	Char(20)	
	396	782	(Zonă rezervată)	Char(18)	

Tabela 187. Intrări jurnal OW (modificare drept de proprietate) (continuare). Fişier descriere câmp QASYOWJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	414	800	Lungime nume cale	Binary (4)	Lungimea numelui obiect nou.
348	416	802	CCSID nume obiect[1]	Binary(5)	Identificatorul setului de caractere codate pentru numele obiect.
352	420	806	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
354	422	808	ID limbă nume obiect[1]	Char(3)	ID-ul limbă pentru numele obiectului.
357	425	811	(Zonă rezervată)	Char(3)	
360	428	814	ID fişier părinte[1,2]	Char(16)	ID-ul fişierului directorului părinte.
376	444	830	ID fişier obiect[1,2]	Char(16)	ID-ul fişier al obiectului.
392	460	846	Nume obiect[1]	Char(512)	Numele obiectului.
	972	1358	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	988	1374	Nume ASP[5]	Char(10)	Numele dispozitivului ASP.
	998	1384	Număr ASP[5]	Char(5)	Numărul dispozitivului ASP.
	1003	1389	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele căii absolute.
	1007	1393	ID regiune sau ţară nume cale	Char(2)	ID-ul de regiune sau ţară pentru numele de cale absolută.
	1009	1395	ID limbă nume cale	Char(3)	ID-ul limbă pentru numele de cale absolută.
	1012	1398	Lungime nume cale	Binary(4)	Lungimea numelui căii absolute.
	1014	1400	Completaţi indicatorului nume cale	Char(1)	Completaţi indicatorul nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele căii absolute complet pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele căii absolute complet pentru obiect.
	1015	1401	ID fişier relativ[3]	Char(16)	ID-ul fişier relativ al numelui de cale absolută.
	1031	1417	Nume cale absolută[4]	Char(5002)	Numele cale absolută al obiectului.

1 Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fişiere QOpenSys şi "rădăcină".

2 Un ID care are bitul cel mai din stânga setat şi restul biţilor 0 indică faptul că ID -ul NU este setat.

3 Când indicatorul de nume cale (offset 1014) este ″N″, acest câmp conţine ID-ul de fişier relativ al numelui de cale absolută. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

4 Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui căii.

5 Dacă obiectul este într-o bibliotecă, acestea sunt informaţiile ASP despre biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informaţiile ASP despre obiect.

Tabela 188. Intrări jurnal O1 (Acces optic). fişier descriere câmp QASY01JE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.

Tabela 188. Intrări jurnal O1 (Acces optic) (continuare). fişier descriere câmp QASY01JE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
156	224	610	Tip intrare.	Char(1)	R-Citire U-Actualizare D-Ştergere C-Creare director X-Eliberare fişier reţinut
157	225	611	Tip obiect	Char(1)	F-Fişier D-Sfârşit director S-Spaţiu de stocare
158	226	612	Tip acces	Char(1)	D-Date fişier A-Atribute director fişier R-Restaurare operaţie S-Salvare operaţie
159	227	613	Nume dispozitiv	Char(10)	Nume LUD bibliotecă
169	237	623	Nume CSI	Char(8)	Nume obiect parte
177	245	631	Bibliotecă CSI	Char(10)	Bibliotecă obiect parte
187	255	641	Nume volum	Char(32)	Nume volum optic
219	287	673	Nume obiect	Char(256)	Nume fişier/director optic
		929	Nume ASP	Char(10)	Nume ASP pentru biblioteca CSI
		939	Număr ASP	Char(5)	Număr ASP pentru biblioteca CSI

Notă: Această intrare este folosită pentru auditarea următoarelor funcţii:

- Deschidere fişier sau director
- Creare director
- Ştergere director fişiere
- Modificare sau extragere atribute
- Eliberare fişier optic reţinut

Tabela 189. Intrări jurnal O2 (Acces optic). Fişier descriere câmp QASY02JE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare.	Char(1)	C-Copiere R-Redenumire B-Copie de rezervă a directorului sau fişierului S-Salvare fişier reţinut M-Mutare fişier
157	225	611	Tip obiect	Char(1)	F-Fişier D-Director

Tabela 189. Intrări jurnal O2 (Acces optic) (continuare). Fişier descriere câmp QASY02JE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
158	226	612	Nume dispozitiv sursă	Char(10)	Nume LUD bibliotecă sursă
168	236	622	Nume CSI sursă	Char(8)	Nume obiect parte sursă
176	244	630	Bibliotecă CSI sursă	Char(10)	Bibliotecă obiect parte sursă
186	254	640	Nume volum Sursă	Char(32)	Nume volum optic sursă
218	286	672	Nume Obj Src	Char(256)	Numele fişier/director optic sursă
474	542	928	Nume dispozitiv tgt	Char(10)	Numele LUD bibliotecă destinaţie
484	552	938	Nume CSI tgt	Char(8)	Numele obiect parte destinaţie
492	560	946	Bibliotecă CSI tgt	Char(10)	Bibliotecă obiect parte destinaţie
502	570	956	Nume volum tgt	Char(32)	Nume volum optic destinaţie
534	602	988	Nume obj tgt	Char(256)	Nume fişier/director optic destinaţie
		1244	Nume ASP	Char(10)	Numele ASP pentru biblioteca CSI sursă
		1254	Număr ASP	Char(5)	Numărul ASP pentru biblioteca CSI sursă
		1259	Numele ASP pentru biblioteca CSI destinaţie	Char(10)	Numele ASP pentru biblioteca CSI destinaţie
		1269	Numărul ASP pentru biblioteca CSI destinaţie	Char(5)	Numărul ASP pentru biblioteca CSI destinaţie

Tabela 190. Intrări jurnal O3 (Acces optic). fişier descriere câmp QASY03JE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare.	Char(1)	I-Iniţializare N-Redenumire B-Copie de rezervă volum C-Conversie volum copie de rezervă la primar M-Importare E-Exportare L-Modificare listă de autorizare A-Modificare atribute volum R-Citire absolută
157	225	611	Nume dispozitiv	Char(10)	Nume LUD bibliotecă
167	235	621	Nume CSI	Char(8)	Nume obiect parte
175	243	629	Bibliotecă CSI	Char(10)	Bibliotecă obiect parte

Tabela 190. Intrări jurnal O3 (Acces optic) (continuare). fişier descriere câmp QASY03JE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
185	253	639	Nume volum vechi	Char(32)	Nume volum optic vechi
217	285	671	Nume volum nou [1]	Char(32)	Nume volum optic nou
249	317	703	Listă Auth veche [2]	Char(10)	Listă de autorizaţie veche
259	327	713	Listă auth nouă [3]	Char(10)	Listă de autorizaţie nouă
269	337	723	Adresă [4]	Binary(5)	Blocul de pornire
273	341	727	Lungime [4]	Binary(5)	Citire lungime
		731	Nume ASP	Char(10)	Nume ASP pentru biblioteca CSI
		741	Număr ASP	Char(5)	Număr ASP pentru biblioteca CSI

1 Acest câmp conţine numele volumului nou pentru funcţiile Iniţializare, Redenumire şi Conversie; el conţine numele volumului copie de rezervă pentru funcţiile Copiere de rezervă. El conţine numele volum pentru Importare, Exportare, Modificare listă autorizaţie, Modificare atribute volum şi Citire sector.

2 Folosit doar pentru Importare, Exportare şi Modificare listă autorizaţie.

3 Folosit doar pentru Modificare listă autorizaţie.

4 Folosit doar pentru Citire sector.

Tabela 191. Intrări jurnal PA (Adoptare program). Fişier de descriere câmp QASYPAJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării.
					A Modificaţi programul pentru a adopta autorizarea proprietarului.
					J Programul Java adoptă autorizarea proprietarului.
					M Modificaţi valorile SETUID, SETGID ale obiectului sau Redenumirea restricţionată şi indicatorul mod dezlegare.
157	225	611	Nume program[3]	Char(10)	Numele programului.
167	235	621	Bibliotecă program[3]	Char(10)	Numele bibliotecii unde este găsit programul.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Proprietar	Char(10)	Numele proprietarului.
	263	649	modul IXVTX	Char(1)	redenumirea restricţionată şi indicatorul de mod de dezlegare (ISVTX).
					Y Indicatorul de mod ISVTX este activ pentru obiect.
					N Indicatorul de mod ISVTX nu este activ pentru obiect.
	263	649	Rezervat	Char(17)	

Tabela 191. Intrări jurnal PA (Adoptare program) (continuare). Fişier de descriere câmp QASYPAJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	281	667	Lungine nume obiect[1]	Binary (4)	Lungimea numelui obiectului.
	283	669	CCSID nume obiect[1]	Binary(5)	identificator de set de caractere codate pentru numele obiect.
	287	673	ID regiune sau ţară nume obiect	Char(2)	ID-ul de regiune sau ţară pentru numele obiect.
	289	675	ID limbă nume obiect[1]	Char(3)	ID-ul limbă pentru numele obiectului.
	292	678	Rezervat	Char(3)	
	295	681	ID părinte[1, 2, 3]	Char(16)	ID fişier părinte
	311	697	ID fişier obiect [3]	Char(16)	ID-ul fişier pentru obiect
	327	713	Nume obiect[1]	Char(512)	Numele obiect pentru obiect.
	839	1225	Mod SETUID	Char(1)	Indicatorul de mod ID utilizator efectiv set (SETUID).
				Y	Bitul de mod SETUID este activ pentru obiect.
				N	Bitul de mod SETUID nu este activ pentru obiect.
	840	1226	Mod SETGID	Char(1)	Indicatorul de mod ID grup efectiv set (SETGID).
				Y	Bitul de mod SETGID este activ pentru obiect.
				N	Bitul de mod SETGID nu este activ pentru obiect.
	841	1227	Proprietar grup primar	Char(10)	Numele proprietarului grup primar.
	851	1237	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	867	1253	Nume ASP[6]	Char(10)	Numele dispozitivului ASP.
	877	1263	Număr ASP[6]	Char(5)	Numărul dispozitivului ASP.
	882	1268	CCSID nume cale	Binary(5)	Identificatorul de set de caractere codat pentru numele de cale absolută.
	886	1272	ID regiune sau ţară nume cale	Char(2)	ID-ul de regiune sau ţară pentru numele de cale absolută.
	888	1274	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	891	1277	Lungime nume cale	Binary(4)	Lungimea numelui de cale absolut.
	893	1279	Completaţi indicatorul nume cale	Char(1)	Completaţi indicatorul de nume cale absolută:
				Y	Câmpul Nume cale absolută conţine numele complet pentru cale absolută pentru obiect.
				N	Câmpul Nume cale absolută nu conţine numele complet pentru cale absolută pentru obiect.
	894	1280	ID fişier înrudit[4]	Char(16)	ID fişier înrudit pentru numele de cale absolută.
	910	1296	Nume cale absolută[5]	Char(5002)	Numele cale absolută al obiectului.

Tabela 191. Intrări jurnal PA (Adoptare program) (continuare). Fişier de descriere câmp QASYPAJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
[1]	Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fişiere QOpenSys şi "rădăcină".				
[2]	Un ID care are bitul cel mai din stânga setat şi restul zero indică faptul că ID-ul NU este setat.				
[3]	Când tipul de intrare este ″J″, câmpurile nume program şi nume bibliotecă vor conţine ″*N″. În plus, ID-ul de fişier părinte şi ID-ul de fişier obiect vor conţine zerouri binare.				
[4]	Când indicatorul de nume cale (offset 893) este ″N″, acest câmp va conţine ID-ul d fişier relativ al numelui căii absolute. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.				
[5]	Acesta este câmpul lungime variabilă. Primii 2 octeţi conţin lungimea numelui cale.				
[6]	Dacă obiectul este într-o bibliotecă, acestea sunt informaţiile ASP bibliotecii obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informaţiile ASP ale obiectului.				

Tabela 192. Intrări jurnal PG (Modificare grup primar). Fişier descriere câmp QASYPGJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Modificaţi grupul primar.
157	225	611	Nume obiect	Char(10)	Numele obiectului.
167	235	621	Biblioteca obiectului	Char(10)	Numele bibliotecii unde este găsit obiectul.
177	245	631	Tipul obiectului	Char(8)	Tipul obiectului.
185	253	639	Grup primar vechi	Char(10)	Grupul primar anterior pentru obiect.[5]
195	263	649	Grup primar nou	Char(10)	Grupul primar nou pentru obiect.
					Autorizările pentru grupul primar nou:
205	273	659	Existenţă obiect	Char(1)	**Y** *OBJEXIST
206	274	660	Gestiune obiect	Char(1)	**Y** *OBJMGT
207	275	661	Obiect operaţional	Char(1)	**Y** *OBJOPR
208	276	662	Modificare obiect	Char(1)	**Y** *OBJALTER
209	277	663	Referinţă obiect	Char(1)	**Y** *OBJREF
210	278	664	(Zonă rezervată)	Char(10)	
220	288	674	Gestiune listă autorizaţii	Char(1)	**Y** *AUTLMGT
221	289	675	Autorizare citire	Char(1)	**Y** *READ
222	290	676	Adăugare autorizare	Char(1)	**Y** *ADD
223	291	677	Actualizare autorizare	Char(1)	**Y** *UPD
224	292	678	Ştergere autorizare	Char(1)	**Y** *DLT

Tabela 192. Intrări jurnal PG (Modificare grup primar) (continuare). Fişier descriere câmp QASYPGJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
225	293	679	Execuţie autorizare	Char(1)	**Y** *EXECUTE
226	294	680	(Zonă rezervată)	Char(10)	
236	304	690	Excludere autorizare	Char(1)	**Y** *EXCLUDE
237	305	691	Revocare grup primar vechi	Char(1)	**Y** Revocare autorizare pentru grupul primar anterior. **' '** Nu revocaţi autorizarea pentru grupul primar anterior.
238	306	692	(Zonă rezervată)	Char (20)	
258	326	712	Utilizator de tip office	Char(10)	Numele utilizatorului de tip office.
268	336	722	Nume DLO	Char(12)	Numele obiectului bibliotecă documente sau al directorului.
280	348	734	(Zonă rezervată)	Char(8)	
288	356	742	Cale director	Char(63)	Calea directorului.
351	419	805	Office în numele Utilizatorului	Char(10)	Utilizatorul care lucrează în numele altui utilizator.
361			(Zonă rezervată)	Char(20)	
	429	815	(Zonă rezervată)	Char(18)	
	447	833	Lungime nume obiect[1]	Binary (4)	Lungimea numelui obiect.
381	449	835	CCSID nume obiect[1]	Binary(5)	identificator de set de caractere codate pentru numele obiect.
385	453	839	ID regiune sau ţară nume obiect[1]	Char(2)	ID-ul regiune sau ţară pentru numele obiect.
387	455	841	ID-ul limbaj nume obiect[1]	Char(3)	ID-ul limbaj pentru numele obiect.
390	458	844	(Zonă rezervată)	Char(3)	
393	461	847	ID fişier părinte[1,2]	Char(16)	ID-ul fişier al directorului părinte.
409	477	863	ID fişier obiect[1,2]	Char(16)	ID-ul fişier al obiectului.
425	493	879	Nume obiect[1]	Char(512)	Numele obiectului.
	1005	1391	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
		1407	Nume ASP[6]	Char(10)	Numele dispozitivului ASP.
		1417	Număr ASP[6]	Char(5)	Numărul dispozitivului ASP.
	1035	1422	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele de cale absolută.
	1040	1426	ID regiune sau ţară nume cale	Char(2)	ID-ul de regiune sau ţară pentru numele de cale absolută.
	1042	1428	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	1045	1431	Lungime nume cale	Binary(4)	Lungimea numelui de cale absolută.
	1047	1433	Completaţi indicatorul nume cale	Char(1)	Completaţi indicatorul de nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele complet pentru cale absolută pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele complet pentru cale absolută pentru obiect.
	1048	1434	ID fişier înrudit[3]	Char(16)	ID fişier înrudit pentru numele de cale absolută.

Tabela 192. Intrări jurnal PG (Modificare grup primar) (continuare). Fişier descriere câmp QASYPGJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1064	1450	Nume cale absolută[4]	Char(5002)	Numele cale absolută al obiectului.

1 Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fişiere QOpenSys şi "rădăcină".

2 Un ID care are bitul cel mai din stânga setat şi restul zero indică faptul că ID-ul NU este setat.

3 Când indicatorul de nume cale (offset 1047) este ″N″, acest câmp va conţine ID-ul d fişier relativ al numelui căii absolute. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

4 Acesta este câmpul lungime variabilă. Primii 2 octeţi conţin lungimea numelui cale.

5 O valoare de *N înseamnă că valoarea Grup primar vechi nu a fost disponibilă.

6 Dacă obiectul este într-o bibliotecă, acestea sunt informaţiile ASP bibliotecii obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informaţiile ASP ale obiectului.

Tabela 193. Intrări jurnal PO (Ieşire imprimantă). Fişier descriere câmp QASYPOJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip ieşire	Char(1)	Tipul ieşirii.
					D Tipărire directă
					R Trimitere către sistemul la distanţă pentru tipărire
					S Fişier din spool tipărit
157	225	611	Stare după tipărire	Char(1)	**D** Şters după tipărire
					H Reţinere după tipărire
					S Salvat după tipărire
					' ' Tipărire directă
158	226	612	Nume job	Char(10)	Prima parte a numelui de job calificat.
168	236	622	Nume utilizator job	Char(10)	A doua parte a numelui de job calificat.
178	246	632	Număr job	Zoned(6,0)	A treia parte a numelui de job calificat.
184	252	638	Profil utilizator	Char(10)	Profilul utilizator care a creat ieşirea.
194	262	648	Coadă ieşire	Char(10)	Coada ieşire care conţine fişierul spool.[1]
204	272	658	Numele bibliotecă coadă ieşire	Char(10)	Numele bibliotecii care conţine coada de ieşire.[1]
214	282	668	Nume dispozitiv	Char(10)	Dispozitivul unde ieşirea a fost tipărită[2].
224	292	678	Tip dispozitiv	Char(4)	Tipul dispozitivului imprimantă[2].
228	296	682	Model dispozitiv	Char(4)	Modelul dispozitivul imprimantă[2].
232	300	686	Numele fişier dispozitiv	Char(10)	Numele fişierului dispozitiv folosit pentru a accesa imprimanta.
242	310	696	Bibliotecă fişier dispozitiv	Char(10)	Numele bibliotecii pentru fişierul dispozitiv.
252	320	706	Numele fişier spool	Char(10)	Numele fişierului spool[1]

Tabela 193. Intrări jurnal PO (Ieşire imprimantă) (continuare). Fişier descriere câmp QASYPOJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
262	330	716	Număr fişier spool scurt	Char(4)	Numărul fişierului spool [1]. Setaţi la spaţii dacă este prea lung.
266	334	720	Tip formular	Char(10)	Tipul de formular al fişierului spool.
276	344	730	Date utilizator	Char(10)	Datele utilizator asociate cu fişierul spool [1].
286			(Zonă rezervată)	Char(20)	
	354	740	Număr fişier spool	Char(6)	Numărul fişierului spool.
	360	746	Zonă rezervată	Char(14)	
306	374	760	Sistem la distanţă	Char(255)	Numele sistemului la distanţă la care este trimisă tipărirea.
561	629	1015	Coadă tipărire sistem la distanţă	Char(128)	Numele cozii de ieşire de pe sistemul la distanţă.
	757	1143	Numele sistem job fişier spool	Char (8)	Numele sistemului pe care există fişierul spool.
	765	1151	Data de creare fişier spool	Char (7)	Data de creare fişier spool (CYYMMDD)
	772	1158	Timp de creare fişier spool	Char(6)	Timpul de creare fişier spool (HHMMSS).
		1164	Nume ASP	Char(10)	Nume ASP pentru biblioteca dispozitiv
		1174	Număr ASP	Char(5)	Numărul ASP pentru biblioteca fişier dispozitiv
		1179	Numele ASP coadă ieşire	Char(10)	Nume ASP pentru biblioteca coadă ieşire.
		1189	Numărul ASP coadă de ieşire	Char(5)	Numărul ASP pentru biblioteca cozii de ieşire.

1 Acest câmp este gol dacă tipul ieşirii este direct tipărit.

2 Acest câmp este gol dacă tipul ieşirii este tipărit la distanţă.

Tabela 194. Intrări jurnal PS (Interschimbare profil). Fişier descriere câmp QASYPSJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.

Tabela 194. Intrări jurnal PS (Interschimbare profil) (continuare). Fişier descriere câmp QASYPSJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Interschimbare profil în timpul passthrough. **E** Terminare lucru în numele relaţiei. **H** Tratare profil generată de API-ul QSYGETPH. **I** Toate jetoanele profil au fost respinse **M** Numărul maxim de jetoane profil care au fost generate. **P** Jeton profil general pentru utilizator. **R** Toate jetoanele profil pentru un utilizator au fost îndepărtate. **S** Pornire lucru în numele relaţiei **V** Profil utilizator autentificat
157	225	611	Profil utilizator	Char(10)	Nume profil utilizator.
167	235	621	Locaţie sursă	Char(8)	Locaţie sursă pass-through.
175	243	629	Profil utilizator destinaţie original	Char(10)	Profilul original utilizator destinaţie pass-through.
185	253	639	Profil nou utilizator destinaţie	Char(10)	Profil nou utilizator destinaţie pass-through.
195	263	649	Utilizator office	Char(10)	Pornirea şi oprirea utilizatorului office în numele relaţiei.
205	273	659	În numele utilizatorului	Char(10)	Utilizatorul în numele căruia lucrează utilizatorul office.
215	283	669	Tip jeton profil	Char(1)	Tipul jetonului profil care a fost generat. **M** Jeton profil uz-multiplu **R** Jeton profil regenerat de uz-multiplu **S** Jeton profil uz-singular
216	284	670	Timeout jeton profil	Binary(4)	Numărul de secunde în care jetonul profil este valid.

Tabela 195. Intrări jurnal PW (Parolă). Fişier descriere câmp QASYPWJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.

Tabela 195. Intrări jurnal PW (Parolă) (continuare). Fişier descriere câmp QASYPWJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
156	224	610	Tip intrare violare	Char(1)	Tipul violării **A** Eşuare de legătură APPC **D** Numele ID utilizator unelte service nu este valid **E** Parola ID utilizator unelte service nu este validă **P** Parolă nevalidă **S** Parola de decriptare SQL nu este validă **U** Numele utilizator nu este valid **X** ID-ul utilizator unelte service este dezactivat **Y** ID-ul utilizator unelte service nu este valid **Z** Parola ID utilizator unelte service nu este validă
157	225	611	Nume utilizator	Char(10)	Numele utilizator job sau numele ID utilizator unelte service.
167	235	621	Nume dispozitiv	Char(40)	Numele dispozitivului sau dispozitivului de comunicaţii pe care a fost introdusă parola sau ID-ul utilizator. Dacă tipul intrării este X, Y sau Z, acest câmp va conţine numele uneltei service care este accesată.
207	275	661	Numele locaţiei la distanţă	Char(8)	Numele locaţiei la distanţă pentru legătura APPC.
215	283	669	Nume locaţie locală	Char(8)	Numele locaţiei locale pentru legătura APPC.
223	291	677	ID reţea	Char(8)	ID-ul reţea pentru legătura APPC.
		685[2]	Nume obiect	Char(10)	Numele obiectului care este decriptat.
		695	Bibliotecă obiect	Char(10)	Biblioteca pentru obiectul care este decriptat.
		705	Tipul obiectului	Char(8)	Tipul obiectului care este decriptat.
		713	Nume ASP[1]	Char(10)	Numele dispozitivului ASP.
		723	Număr ASP[1]	Char(5)	Numărul dispozitivului ASP.

1 Dacă obiectul este într-o bibliotecă, acestea sunt informaţiile ASP pentru biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informaţiile ASP pentru obiect.

2 Dacă numele obiectului este *N şi tipul violării este S, utilizatorul a încercat să decripteze date într-o variabilă gazdă.

Tabela 196. Intrări jurnal RA (Modificare autorizare pentru obiectul restaurat). Fişier descriere câmp QASYRAJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Modificări aduse autorizării pentru obiectul restaurat
157	225	611	Nume obiect	Char(10)	Numele obiectului.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii în care este obiectul.

Tabela 196. Intrări jurnal RA (Modificare autorizare pentru obiectul restaurat) (continuare). Fişier descriere câmp QASYRAJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Nume listă de autorizare	Char(10)	Numele listei de autorizare.
195	263	649	Autorizare publică	Char(1)	**Y** Autorizarea publică setată la *EXCLUDE.
196	264	650	Autorizare privată	Char(1)	**Y** Autorizare privată îndepărtată.
197	265	651	AUTL îndepărtată	Char(1)	**Y** Lista de autorizaţii îndepărtat din obiect.
198	266	652	(Zonă rezervată)	Char(20)	
218	286	672	Nume DLO	Char(12)	Numele obiectului de bibliotecă de documente.
230	298	684	(Zonă rezervată)	Char(8)	
238	306	692	Cale director	Char(63)	Directorul care conţine obiectul bibliotecă de documente.
301			(Zonă rezervată)	Char(20)	
	369	755	(Zonă rezervată)	Char(18)	
	387	773	Lungime nume obiect	Binary(4)	Lungimea numelui obiectului.
321	389	775	CCSID nume obiect[1]	Binary(5)	identificator de set de caractere codate pentru numele obiect.
325	393	779	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiune sau ţară pentru numele obiect.
327	395	781	ID-ul limbaj nume obiect [1]	Char(3)	ID-ul limbaj pentru numele obiect.
330	398	784	(Zonă rezervată)	Char(3)	
333	401	787	ID fişier părinte[1,2]	Char(16)	ID-ul fişier al directorului părinte.
349	417	803	ID fişier obiect[1,2]	Char(16)	ID-ul fişier al obiectului.
365	433	819	Nume obiect[1]	Char(512)	Numele obiectului.
	945	1331	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	961	1347	Nume ASP[5]	Char(10)	Numele dispozitivului ASP.
	971	1357	Număr ASP[5]	Char(5)	Numărul dispozitivului ASP.
	976	1362	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele de cale absolută.
	980	1366	ID regiune sau ţară nume cale	Char(2)	ID-ul de regiune sau ţară pentru numele de cale absolută.
	982	1368	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	985	1371	Lungime nume cale	Binary(4)	Lungimea numelui de cale absolută.
	987	1373	Completaţi indicatorul nume cale	Char(1)	Completaţi indicatorul de nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele complet pentru cale absolută pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele complet pentru cale absolută pentru obiect.
	988	1374	ID fişier relativ[3]	Char(16)	ID fişier înrudit pentru numele de cale absolută.

Tabela 196. Intrări jurnal RA (Modificare autorizare pentru obiectul restaurat) (continuare). Fişier descriere câmp QASYRAJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1004	1390	Nume cale absolută [4]	Char(5002)	Numele cale absolută al obiectului.

[1] Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fişiere QOpenSys şi "rădăcină".

[2] Un ID care are bitul cel mai din stânga setat şi restul zero indică faptul că ID-ul NU este setat.

[3] Când indicatorul de nume cale (offset 987) este ″N″, acest câmp va conţine ID-ul d fişier relativ al numelui căii absolute. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

[4] Acesta este câmpul lungime variabilă. Primii 2 octeţi conţin lungimea numelui cale.

[5] Dacă obiectul este într-o bibliotecă, acestea sunt informaţiile ASP bibliotecii obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informaţiile ASP ale obiectului.

Tabela 197. Intrări jurnal RJ (Restaurare descriere job). Fişier descrierere câmp QASYRJJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** restaurarea unei descrieri job care a avut specificat un profil utilizator în parametrul USER.
157	225	611	Nume descriere job	Char(10)	Numele descrierii de job restaurate.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii în care a fost restaurată descrierea de job.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Nume utilizator	Char(10)	Numele profilului utilizator specificat în descrierea de job.
		649	Nume ASP	Char(10)	Nume ASP pentru biblioteca JOBD
		659	Număr ASP	Char(5)	Număr ASP pentru biblioteca JOBD

Tabela 198. Intrări jurnal RO (Modificare drept de proprietate pentru obiectul restaurat). Fişier descriere câmp QASYROJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Retaurarea obiectelor care au dreptul de proprietate modificat când sunt resturate
157	225	611	Nume obiect	Char(10)	Numele obiectului.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii în care este obiectul.

Tabela 198. Intrări jurnal RO (Modificare drept de proprietate pentru obiectul restaurat) (continuare). Fişier descriere câmp QASYROJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Proprietar vechi	Char(10)	Numele proprietarului înainte ca dreptul de proprietate să fie modificat.
195	263	649	Proprietar nou	Char(10)	Numele proprietarului după ce dreptul de proprietate a fost modificat.
205	273	659	(Zonă rezervată)	Char(20)	
225	293	679	Nume DLO	Char(12)	Numele obiectului bibliotecă de documente.
237	305	691	(Zonă rezervată)	Char(8)	
245	313	699	Cale director	Char(63)	Directorul în care a fost restaurat obiectul.
308			(Zonă rezervată)	Char(20)	
	376	762	(Zonă rezervată)	Char(18)	
	394	780	Lungime nume obiect[1]	Binary(4)	Lungimea numelui obiectului.
328	396	782	CCSID nume obiect[1]	Binary(5)	identificator de set de caractere codate pentru numele obiect.
332	400	786	ID regiune sau ţară nume obiect[1]	Char(2)	ID-ul regiune sau ţară pentru numele obiect.
334	402	788	ID-ul limbaj nume obiect[1]	Char(3)	ID-ul limbaj pentru numele obiect.
337	405	791	(Zonă rezervată)	Char(3)	
340	408	794	ID fişier părinte[1,2]	Char(16)	ID-ul fişier al directorului părinte.
356	424	810	ID fişier obiect[1,2]	Char(16)	ID-ul fişier al obiectului.
372	440	826	Nume obiect[1]	Char(512)	Numele obiectului.
	952	1338	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	968	1354	Nume ASP[5]	Char(10)	Numele dispozitivului ASP.
	978	1364	Număr ASP[5]	Char(5)	Numărul dispozitivului ASP.
	983	1369	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele de cale absolută.
	987	1373	ID regiune sau ţară nume cale	Char(2)	ID-ul de regiune sau ţară pentru numele de cale absolută.
	989	1375	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	992	1378	Lungime nume cale	Binary(4)	Lungimea numelui de cale absolută.
	994	1380	Completaţi indicatorul nume cale	Char(1)	Completaţi indicatorul de nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele complet pentru cale absolută pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele complet pentru cale absolută pentru obiect.
	995	1381	ID fişier relativ[3]	Char(16)	ID fişier înrudit pentru numele de cale absolută.
	1011	1397	Nume cale absolută[4]	Char(5002)	Numele cale absolută al obiectului.

Tabela 198. Intrări jurnal RO (Modificare drept de proprietate pentru obiectul restaurat) (continuare). Fişier descriere câmp QASYROJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**

[1] Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fişiere QOpenSys şi "rădăcină".

[2] Un ID care are bitul cel mai din stânga setat şi restul zero indică faptul că ID-ul NU este setat.

[3] Când indicatorul de nume cale (offset 994) este ″N″, acest câmp va conţine ID-ul d fişier relativ al numelui căii absolute. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

[4] Acesta este câmpul lungime variabilă. Primii 2 octeţi conţin lungimea numelui cale.

[5] Dacă obiectul este într-o bibliotecă, acestea sunt informaţiile ASP bibliotecii obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informaţiile ASP ale obiectului.

Tabela 199. Intrări RP (Restaurare programe care adoptă autorizare). Fişierul descriere câmp QASYRPJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Restaurare programe care adoptă autorizarea proprietarului
157	225	611	Nume program	Char(10)	Numele programului
167	235	621	Bibliotecă program	Char(10)	Numele bibliotecii în care este localizat programul
177	245	631	Tip obiect	Char(8)	Tipul obiectului
185	253	639	Nume proprietar	Char(10)	Numele proprietarului
	263	649	(Zonă rezervată)	Char(18)	
	281	667	Lungime nume obiect[1]	Binary (4)	Lungimea numelui obiectului.
	283	669	CCSID nume obiect[1]	Binary (5)	Identificatorul set de caractere codat pentru numele obiectului.
	287	673	ID regiune sau ţară nume obiect[1]	Char (2)	ID-ul regiune sau ţară pentru numele obiect.
	289	675	ID limbă nume obiect[1]	Char (3)	ID-ul limbă pentru numele obiectului.
	292	678	(Zonă rezervată)	Char (3)	
	295	681	ID fişier părinte[1,2]	Char (16)	ID-ul fişier al directorului părinte.
	311	697	ID fişier obiect[1,2]	Char (16)	ID-ul fişier al obiectului.
	327	713	Nume obiect[1]	Char (512)	Numele obiectului.
	839	1225	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	855	1241	Nume ASP[5]	Char(10)	Numele dispozitivului ASP.
	865	1251	Număr ASP[5]	Char(5)	Numărul dispozitivului ASP.
	870	1256	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele de cale absolută.
	874	1260	ID regiune sau ţară nume cale	Char(2)	ID-ul de regiune sau ţară pentru numele de cale absolută.
	876	1262	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	879	1265	Lungime nume cale	Binary(4)	Lungimea numelui de cale absolută.

Tabela 199. Intrări RP (Restaurare programe care adoptă autorizare) (continuare). Fişierul descriere câmp QASYRPJE/J4/J5

	Offset				
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	881	1267	Completaţi indicatorul nume cale	Char(1)	Completaţi indicatorul de nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele complet pentru cale absolută pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele complet pentru cale absolută pentru obiect.
	882	1268	ID fişier relativ[3]	Char(16)	ID fişier înrudit pentru numele de cale absolută.
	898	1284	Nume cale absolută[4]	Char(5002)	Numele cale absolută al obiectului.

1 Aceste câmpuri sunt folosite doar pentru obiectele din QOpenSys şi sistemul de fişiere 'root'.

2 Dacă un ID care are cel mai din stânga bit setat şi restul de biţi zero, ID-ul **nu** este setat.

3 Când indicatorul de nume cale (offset 994) este ″N″, acest câmp va conţine ID-ul d fişier relativ al numelui căii absolute. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

4 Acesta este câmpul lungime variabilă. Primii 2 octeţi conţin lungimea numelui cale.

5 Dacă obiectul este într-o bibliotecă, acestea sunt informaţiile ASP bibliotecii obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informaţiile ASP ale obiectului.

Tabela 200. Intrări jurnal RQ (Restaurare obiect descriptor de modificare cerere). Fişier descriere câmp QASYRQJE/J4/J5

	Offset				
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Restauraţi obiectul *CRQD care adoptă autorizare.
157	225	611	Nume obiect	Char(10)	Numele descriptorului de modificare cerere.
167	235	621	Bibliotecă obiect	Char(10)	Numele bibliotecii unde este găsit descriptorul de modificare cerere.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
		639	Nume ASP	Char(10)	Nume ASP pentru biblioteca CRQD
		649	Număr ASP	Char(5)	Număr ASP pentru biblioteca CRQD

Tabela 201. Intrări jurnal RU (Restaurare autorizare pentru profil utilizator). Fişier de descriere câmp QASYRUJE/J4/J5

	Offset				
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Restaurare autorizare pentru profilurile utilizator

Tabela 201. Intrări jurnal RU (Restaurare autorizare pentru profil utilizator) (continuare). Fişier de descriere câmp QASYRUJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
157	225	611	Nume utilizator	Char(10)	Numele profilului utilizator a cărui autorizare a fost restaurată.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
	253	639	Autorizare restaurată	Char(1)	Indică dacă toate autorizările au fost restaurate pentru utilizator. **A** Toate autorizaările au fost restaurate **S** Unele autorizări nu au fost restaurate

Tabela 202. Intrări jurnal RZ (Modificare grup primar pentru obiectul restaurat). Fişier descriere câmp QASYRZJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Grup primar modificat.
157	225	611	Nume obiect	Char(10)	Numele obiectului.
167	235	621	Bibliotecă obiect	Char(10)	Numele bibliotecii unde este găsit obiectul.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Grup primar vechi	Char(10)	Grupul primar anterior pentru obiect.
195	263	649	Grup primar nou	Char(10)	Grupul primar nou pentru obiect.
205	273	659	(Zonă rezervată)	Char(20)	
225	293	679	Nume DLO	Char(12)	Numele obiectului bibliotecă de documente.
237	305	691	(Zonă rezervată)	Char(8)	
245	313	699	Cale director	Char(63)	Directorul în care a fost restaurat obiectul.
308			(Zonă rezervată)	Char(20)	
	376	762	(Zonă rezervată)	Char(18)	
	394	780	Lungime nume obiect [1]	Binary(4)	Lungimea numelui obiectului.
328	396	782	CCSID nume obiect [1]	Binary(5)	identificator de set de caractere codate pentru numele obiect.
332	400	786	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiune sau ţară pentru numele obiect.
334	402	788	ID-ul limbaj nume obiect [1]	Char(3)	ID-ul limbaj pentru numele obiect.
337	405	791	(Zonă rezervată)	Char(3)	
340	408	794	ID fişier părinte [1,2]	Char(16)	ID-ul fişier al directorului părinte.
356	424	810	ID fişier obiect [1,2]	Char(16)	ID-ul fişier al obiectului.
372	440	826	Nume obiect [1]	Char(512)	Numele obiectului.
	952	1338	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	968	1354	Nume ASP	Char(10)	Numele dispozitivului ASP.
	978	1364	Număr ASP	Char(5)	Numărul dispozitivului ASP.

Tabela 202. Intrări jurnal RZ (Modificare grup primar pentru obiectul restaurat) (continuare). Fişier descriere câmp QASYRZJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	983	1369	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele de cale absolută.
	987	1373	ID regiune sau ţară nume cale	Char(2)	ID-ul de regiune sau ţară pentru numele de cale absolută.
	989	1375	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	992	1378	Lungime nume cale	Binary(4)	Lungimea numelui de cale absolută.
	994	1380	Completaţi indicatorul nume cale	Char(1)	Completaţi indicatorul de nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele complet pentru cale absolută pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele complet pentru cale absolută pentru obiect.
	995	1381	ID fişier relativ[3]	Char(16)	ID fişier înrudit pentru numele de cale absolută.
	1011	1397	Nume cale absolută[4]	Char(5002)	Numele cale absolută al obiectului.

1 Aceste câmpuri sunt folosite doar pentru obiectele din sistemele de fişiere QOpenSys şi "rădăcină".

2 Un ID care are bitul cel mai din stânga setat şi restul zero indică faptul că ID-ul NU este setat.

3 Când indicatorul de nume cale (offset 1014) este ″N″, acest câmp conţine ID-ul de fişier relativ al numelui de cale absolută. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

4 Acesta este câmpul lungime variabilă. Primii 2 octeţi conţin lungimea numelui cale.

Tabela 203. Intrări jurnal SD (Modificare director de distribuţie sistem). Fişier de descriere câmp QASYSDJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **S** Modificare director sistem

Tabela 203. Intrări jurnal SD (Modificare director de distribuţie sistem) (continuare). Fişier de descriere câmp QASYSDJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
157	225	611	Tip modificare	Char(3)	**ADD** Adăugare intrare director **CHG** Modificare intrare director **COL** Intrare colector **DSP** Afişare intrare director **OUT** Cerere fişier ieşire **PRT** Tipărire intrare director **RMV** Îndepărtare intrare director **RNM** Redenumire intrare director **RTV** Extragere detalii **SUP** Intrare furnizor
160	228	614	Tip înregistrare	Char(4)	**DIRE** Director **DPTD** Detalii departament **SHDW** Umbră director **SRCH** Căutare director
164	232	618	Sistem origine	Char(8)	Sistemul origine a modificării
172	240	626	Profil utilizator	Char(10)	Profilul utilizator care face modificarea
182	250	636	Cerere sistem	Char(8)	Sistemul care cere modificarea
190	258	644	Cerere funcţie	Char(6)	**INIT** Iniţializare **OFFLIN** Inţializare în stare de neconectare **REINIT** Reiniţializare **SHADOW** Umbrire normală **STPSHD** Oprire umbrire
196	264	650	ID utilizator	Char(8)	ID-ul utilizator care este modificat
204	272	658	Adresă	Char(8)	Adresa care este modificată
212	280	666	ID utilizator reţea	Char(47)	ID-ul utilizator reţea care este modificat

Tabela 204. Intrări jurnal SE (Modificare intrare rutare subsistem). Fişier descriere câmp QASYSEJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Intrare rutare subsistem modificată
157	225	611	Nume subsistem	Char(10)	Numele obiectului

Tabela 204. Intrări jurnal SE (Modificare intrare rutare subsistem) (continuare). Fişier descriere câmp QASYSEJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii în care este obiectul
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Nume program	Char(10)	Numele programului care a modificat intrarea de rutare.
195	263	649	Nume bibliotecă	Char(10)	Numele bibliotecii pentru program
205	273	659	Număr secvenţă	Char(4)	Numărul de secvenţă
209	277	663	Numele comandă	Char(3)	Tipul comenzii folosite **ADD** ADDRTGE **CHG** CHGRTGE **RMV** RMVRTGE
		666	Nume ASP pentru biblioteca SBSD	Char(10)	Nume ASP pentru biblioteca SBSD
		676	Număr ASP pentru biblioteca SBSD	Char(5)	Număr ASP pentru biblioteca SBSD
		681	Nume ASP pentru biblioteca program	Char(10)	Nume ASP pentru biblioteca program
		691	Număr ASP pentru biblioteca program	Char(5)	Număr ASP pentru biblioteca program

Tabela 205. Intrări jurnal SF (Acţiune către fişierul spool). Fişier descriere câmp QASYSFJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip acces	Char(1)	Tipul intrării **A** Fişier din spool citit **C** Fişier din spool creat **D** Fişier din spool şters **H** Fişier din spool reţinut **I** Creaţi un fişier inline **R** Fişier din spool eliberat **U** Fişier din spool cu securitate relevantă. **V** Sunt modificate doar atributele fişierului spool cu securitate nerelevantă.
157	225	611	Nume fişier bază de date	Char(10)	Numele fişierul bază de date care conţine fişierul spool
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii pentru fişierul bază de date
177	245	631	Tip obiect	Char(8)	Tipul obiectului fişierului bază de date
185	253	639	Zonă rezervată	Char(10)	
195	263	649	Nume membru	Char(10)	Numele mombrului fişier.

Tabela 205. Intrări jurnal SF (Acţiune către fişierul spool) (continuare). Fişier descriere câmp QASYSFJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
205	273	659	Numel fişier spool	Char(10)	Numele fişierului spool [1].
215	283	669	Număr fişier spool scurt	Char(4)	Numărul fişierului spool [1]. Dacă numărul fişierului spool este mai mare de 4 octeţi, acest câmp va fi gol şi va fi folosit câmpul Număr fişier spool (J5 offset 693).
219	287	673	Nume coadă ieşire	Char(10)	Numele cozii de ieşire care conţine fişierul spool.
229	297	683	bibliotecă coadă ieşire	Char(10)	Numele bibliotecii pentru coada de ieşire.
239			Zonă rezervată	Char(20)	
	307	693	Număr fişier spool	Char(6)	Numărul fişierului spool.
	313	699	Zonă rezervată	Char(14)	
259	327	713	Copii vechi	Char(3)	Numărul copiilor vechi din fişierul spool
262	330	716	Copii noi	Char(3)	Numărul copiilor noi din fişierul spool
265	333	719	Imprimantă veche	Char(10)	Imprimanta veche pentru fişierul spool
275	343	729	Imprimantă nouă	Char(10)	Imprimanta nouă pentru fişierul spool
285	353	739	Coadă de ieşire nouă	Char(10)	Coada de ieşire nouă pentru fişierul spool
295	363	749	Bibliotecă coadă ieşire nouă	Char(10)	Biblioteca pentru noua coadă de ieşire
305	373	759	Tip formular vechi	Char(10)	Tipul formularului vechi al fişierului spool
315	383	769	Tip formular nou	Char(10)	Tipul formularului nou al fişierului spool
325	393	779	Pagină de repornire veche	Char(8)	Pagina de repornire veche pentru fişierul spool
333	401	787	Pagina de repornire nouă	Char(8)	Pagina de repornire nouă pentru fişierul spool
341	409	795	Început interval pagină veche	Char(8)	Început interval pagină veche al fişierului spool
349	417	803	Pornire interval pagină nouă	Char(8)	Început interval pagină nouă al fişierului spool
357	425	811	Sfârşit interval pagină veche	Char(8)	Sfârşit interval pagină veche al fişierului spool
365	433	819	Sfârşit interval pagină nouă	Char(8)	Sfârşit interval pagină nouă al fişierului spool
	441	827	Nume job fişier spool	Char(10)	Numele jobului fişier spool.
	451	837	Utilizator job fişier spool	Char(10)	Utilizatorul pentru jobul fişier spool.
	461	847	Numărul job fişier spool	Char(6)	Numărul pentru jobul fişier spool.
	467	853	Desenator vechi	Char(8)	Desenator sursă vechi.
	475	861	Desenator nou	Char(8)	Desenator sursă nou.
	483	869	Nume definiţie pagină veche	Char(10)	Nume definiţie pagină veche.
	493	879	Bibliotecă definiţie pagină veche	Char(10)	Nume bibliotecă definiţie pagină veche
	503	889	Nume definiţie pagină nouă	Char(10)	Nume definiţie pagină nouă.

Tabela 205. Intrări jurnal SF (Acţiune către fişierul spool) (continuare). Fişier descriere câmp QASYSFJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	513	899	Bibliotecă definiţie pagină nouă	Char(10)	Bibliotecă definiţie pagină nouă.
	523	909	Nume definiţie formular vechi	Char(10)	Nume definiţie formular vechi.
	533	919	Bibliotecă definiţie formular vechi	Char(10)	Nume bibliotecă definiţie formular vechi.
	543	929	Numele definiţiei noi de formular	Char(10)	Numele definiţiei noi de formular
	553	939	Bibliotecă definiţie formular nouă	Char(10)	Nume bibliotecă definiţie formular nou.
	563	949	Opţiunea 1 veche definită de utilizator	Char(10)	Opţiunea 1 veche definită de utilizator.
	573	959	Opţiunea 2 veche definită de utilizator	Char(10)	Opţiunea 2 veche definită de utilizator.
	583	969	Opţiunea 3 veche definită de utilizator	Char(10)	Opţiunea 3 veche definită de utilizator.
	593	979	Opţiunea 4 veche definită de utilizator	Char(10)	Opţiunea 4 veche definită de utilizator.
	603	989	Opţiunea 1 nouă definită de utilizator	Char(10)	Opţiunea 1 nouă definită de utilizator.
	613	999	Opţiunea 2 nouă definită de utilizator	Char(10)	Opţiunea 2 nouă definită de utilizator.
	623	1009	Opţiunea 3 nouă definită de utilizator	Char(10)	Opţiunea 3 nouă definită de utilizator.
	633	1019	Opţiunea 4 nouă definită de utilizator	Char(10)	Opţiunea 4 nouă definită de utilizator.
	643	1029	Obiect vechi definit de utilizator	Char(10)	Nume obiect vechi definit de utilizator.
	653	1039	Bibliotecă obiecte veche definită de utilizator	Char(10)	Nume bibliotecă vechi definit de utilizator.
	663	1049	Tip obiect vechi definit de utilizator	Char(10)	Tip obiect vechi definit de utilizator.
	673	1059	Obiect nou definit de utilizator	Char(10)	Obiect nou definit de utilizator.
	683	1069	Bibliotecă obiecte nouă definită de utilizator	Char(10)	Nume nou bibliotecă obiecte definit de utilizator.

Tabela 205. Intrări jurnal SF (Acţiune către fişierul spool) (continuare). Fişier descriere câmp QASYSFJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	693	1079	Tip obiect nou definit de utilizator	Char(10)	Tip de obiect nou definit de utilizator.
	703	1089	Nume sistem job fişier spool	Char(8)	Numele sistemului pe care există fişierul spool.
	711	1097	Data de creare fişier spool	Char(7)	Data de creare fişier spool (CYYMMDD).
	718	1104	Timp de creare fişier spool	Char(6)	Timp de creare fişier spool (HHMMSS).
		1110	Numele datelor vechi definite de utilizator	Char(255)	Numele datelor vechi definite de utilizator
		1365	Numele datelor noi definite de utilizator	Char(255)	Numele datelor noi definite de utilizator
		1620	Nume fişier ASP	Char(10)	Nume ASP pentru biblioteca de fişier bază de date.
		1630	Număr fişier ASP	Char(5)	Număr ASP pentru biblioteca fişierului bază de date.
		1635	Nume ASP coadă de ieşire	Char(10)	Nume ASP pentru biblioteca coadă ieşire.
		1645	Numărul ASP coadă de ieşire	Char(5)	Numărul ASP pentru biblioteca cozii de ieşire.
		1650	Nume ASP nou coadă de ieşire	Char(10)	Nume ASP pentru biblioteca cozii de ieşire nouă.
		1660	Număr ASP nou pentru coada de ieşire	Char(5)	Număr ASP pentru biblioteca cozii de ieşire nouă.

1 Acest câmp este gol când tipul intrării este I (tipărire inline).

Tabela 206. Intrări jurnal SG (Semnale asincrone). Fişier descriere câmp QASYSGJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489 şi Tabela 153 la pagina 491 pentru listarea de câmpuri.
	224	610	Tip intrare.	Char(1)	Tipul intrării. **A** Semnal asincron iSeries procesat **P** Semnal asincron de mediu de spaţiu de adrese private (PASE) procesat
	225	611	Număr semnal	Char(4)	Număr semnalului care a fost procesat.

Tabela 206. Intrări jurnal SG (Semnale asincrone) (continuare). Fişier descriere câmp QASYSGJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	229	615	Acţiune de tratare	Char(1)	Acţiunea luată pentru acest semnal. **C** Continuaţi procesul **E** Excepţie semnal **H** Tratare prin invocarea funcţiei de prindere semnal **S** Opriţi procesul **T** Terminaţi procesul **U** Terminaţi cererea
	230	616	Sursă semnal	Char(1)	Sursa semnalului. **M** Sursa maşină **P** Sursă proces **Notă:** Când valoarea sursei de semnal este maşină. valorile job sursă sunt goale.
	231	617	Nume job sursă	Char(10)	Prima parte a numelui calificat al jobului sursă.
	241	627	Numele utilizator job sursă	Char(10)	Partea a doua a numelui calificat al jobului sursă.
	251	637	Numărul jobului sursă	Char(6)	A treia parte a numelui calificat al jobului sursă.
	257	643	Utilizator curent job sursă	Char(10)	Profil utiliator curent pentru jobul sursă.
	267	653	Amprentă de timp la generare	Char(8)	Formatul *DTS al timpului la care a fost generat semnalul. **Notă:** API-ul QWCCVTDT poate fi folosit pentru a converti o amprentă de timp *DTS la alte formate.

Tabela 207. Intrări jurnal SK (Conexiuni socket securizate). Fişier de descriere câmp QASYSKJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489 şi Tabela 153 la pagina 491 pentru listarea de câmpuri.
	224	610	Tip intrare	Char(1)	**A** Accptare **C** Conectare **D** Adresă DHCP asignată **F** Mail filtrat **P** Port indisponibil **R** Rejectare mail **U** Adresă DHCP neasignată
	225	611	Adresă IP locală[3]	Char(15)	Adresa IP locală.
	240	626	Port local	Char(5)	Portul local.
	245	631	Adresa IP la distanţă.[3]	Char(15)	Adresa IP la distanţă.

Tabela 207. Intrări jurnal SK (Conexiuni socket securizate) (continuare). Fişier de descriere câmp QASYSKJ4/J5

	Offset				
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	260	646	Port la distanţă	Char(5)	Portul la distanţă.
	265	651	Descriptor socket	Bin(5)	Descriptorul de socket.
	269	655	Filtrare descriere	Char(10)	Filtrul de mail specificat.
	279	665	Lungime date filtru	Bin(4)	Lungimea datelor filtru.
	281	667	Date filtru[1]	Char(514)	Datele filtru.
	795	1181	Familie de adrese	Char(10)	Familia de adrese. ***IPV4** Protocol internet versiunea 4 ***IPV6** Protocol internet versiunea 6
	805	1191	Adresa IP locală	Char(46)	Adresa IP locală.
	851	1237	Adresa IP la distanţă [2]	Char(46)	Adresa IP la distanţă
	897	1283	Adresa MAC	Char(32)	Adresa MAC a clientului care face cererea.
	929	1315	Nume gazdă	Char(255)	Numle gazdă a clientului care face cererea.

1 Acesta este câmpul lungime variabilă. Primii 2 octeţi conţin lungimea câmpului.

2 Când tipul intrării este D, acest câmp conţine adresa IP asignată de serverul DHCP clientului care a făcut cererea.

3 Aceste câmpuri suportă doar adrese IPv4.

Tabela 208. Intrări jurnal SM (Modificare gestiune sisteme). Fişier de descriere câmp QASYSMJE/J4/J5

	Offset				
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare.	Char(1)	Funcţie accesată **B** Listă copie de rezervă modificată **C** Opiuni de curăare automată **D** DRDA **F** Sistem de fişiere HFS **N** Operaţie fişier reţea **O** Opţiuni copie de rezervă modificate **P** Planificare de pornire/oprire alimentare **S** Listă de răspunsuri sistem **T** Timpi de recuperare cale de acces modificaţi

Tabela 208. Intrări jurnal SM (Modificare gestiune sisteme) (continuare). Fişier de descriere câmp QASYSMJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
157	225	611	Tip acces	Char(1)	**A** Adăugare **C** Modificare **D** Ştergere **R** Îndepărtare **S** Afişare **T** Extragere sau primire
158	226	612	Număr secvenţă	Char(4)	Numărul secvenţă al acţiunii
162	230	616	ID mesaj	Char(7)	ID mesaj asociat cu acţiunea
169	237	623	Nume bază de date relaţională	Char(18)	Numele pentru baza de date relaţională
187	255	641	Nume sistem de fişiere	Char(10)	Numele pentru sistemul de fişiere
197	265	651	Opţiune copie de rezervă modificată	Char(10)	Opţiunea copie de rezervă care a fost modificată
207	275	661	Modificare listă copie de rezervă	Char(10)	Numele listei copie de rezervă care a fost modificată
217	285	671	Nume fişier reţea	Char(10)	Numele fişierului reţea care a fost folosit
227	295	681	Membru fişier reţea	Char(10)	Numele membrului fişierului reţea
237	305	691	Numărul fişierului reţea	Zoned(6,0)	Numărul fişierului reţea
243	311	697	Proprietar fişier reţea	Char(10)	Numele profilului utilizator care deţine fişierul reţea
253	321	707	Utilizatorul care a generat fişierul reţea	Char(8)	Numele profilului utilizator care a generat fişierul reţea
261	329	715	Adresa care a generat fişierul reţea	Char(8)	Adresa care a generat fişierul reţea

Tabela 209. Intrări jurnal SO (Acţiuni informaţii utilizator de securitate server). Fişier descriere câmp QASYSOJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării **A** Adăugare intrare **C** Modificare intrare **R** Îndepărtare intrare **T** Extragere intrare
157	225	611	Profil utilizator	Char(10)	Numele profilului utilizator.

Tabela 209. Intrări jurnal SO (Acţiuni informaţii utilizator de securitate server) (continuare). Fişier descriere câmp QASYSOJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	235	621	Tip intrare informaţii utilizator	Char(1)	**N** Tip intrare nespecificată. **U** Intrarea este o intrare de informaţii aplicaţie utilizator. **Y** Intrarea este o intrare de autentificare server.
	236	622	Parolă memorată	Char(1)	**N** Parolă nememorată **S** Nici o modificare **Y** Parola este memorată.
	237	623	Nume server	Char(200)	Numele serverului.
	437	823	(Zonă rezervată)	Char(3)	
	440	826	Lungime ID utilizator	Binary (4)	Lungimea ID-ului utilizator.
	442	828	(Zonă rezervată)	Char(20)	
	462	848	ID utilizator	Char(1002)[1]	ID-ul pentru utilizator.

1 Acesta este câmpul lungime variabilă. Primii 2 octeţi conţin lungimea câmpului.

Tabela 210. Intrări jurnal ST (Acţiune unelte service). Fişier descriere câmp QASYSTJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării **A** Înregistrare service

Tabela 210. Intrări jurnal ST (Acţiune unelte service) (continuare). Fişier descriere câmp QASYSTJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
157	225	611	Unealtă service	Char(2)	Tipul intrării.
					AN ANZJVM
					CS STRCPYSCN
					CD QTACTLDV
					CE QWTCTLTR
					CT DMPCLUTRC
					DC DLTCMNTRC
					DD DMPDLO
					DJ DMPJVM
					DO DMPOBJ
					DS DMPSYSOBJ, QTADMPTS
					EC ENDCMNTRC
					ER ENDRMTSPT
					HD QYHCHCOP (DASD)
					HL QYHCHCOP (LPAR)
					JW QPYRTJWA
					PC PRTCMNTRC
					PE PRTERRLOG
					PI PRTINTDTA
					PS QP0FPTOS
					SE QWTSETTR
					SC STRCMNTRC
					SJ STRSRVJOB
					SR STRRMTSPT
					ST STRSST
					TA TRCTCPAPP
					TC TRCCNN (*FORMAT specified)
					TE ENDTRC, ENDPEX
					TI TRCINT sau TRCCNN (*ON, *OFF sau *END specificat)
					TS STRTRC, STRPEX
159	227	613	Nume obiect	Char(10)	Numele obiectului accesat
169	237	623	Nume bibliotecă	Char(10)	Numele bibliotecii pentru obiect
179	247	633	Tip obiect	Char(8)	Tipul obiectului
187	255	641	Nume job	Char(10)	Prima parte a numelui de job calificat
197	265	651	Nume utilizator job	Char(10)	A doua parte a numelui de job calificat
207	275	661	Număr job	Zoned(6,0)	A treia parte a numelui de job calificat
213	281	667	Nume obiect	Char(30)	Numele obiectului pentru DMPSYSOBJ

Tabela 210. Intrări jurnal ST (Acţiune unelte service) (continuare). Fişier descriere câmp QASYSTJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
243	311	697	Nume bibliotecă	Char(30)	Numele bibliotecii pentru obiect pentru DMPSYSOBJ
273	341	727	Tip obiect	Char(8)	Tipul obiectului
281	349	735	Nume DLO	Char(12)	Numele obiectului bibliotecă de documente
293	361	747	(Zonă rezervată)	Char(8)	
301	369	755	Cale director	Char(63)	Directorul care conţine obiectul bibliotecă de documente
	432	818	Câmp JUID	Char(10)	JUID a jobului destinaţie.
	442	828	Acţiune de urmărire din timp[1]	Char(10)	Acţiunea cerută pentru căutarea de job din timp ***ON** Căutarea din timp activată ***OFF** Urmărire din timp dezactivată ***RESET** Urmărire din timp ezactivată şi informaţiile de urmărire şterse.
	452	838	Opţiune de urmărire aplicaţie[2]	Char(1)	Opţiunea de urmărire specificată în TRCTCPAPP. **Y** Colecţia de informaţii de urmărire pornită **N** Colecţia de informaţii de urmărire oprită şi informaţiile de urmărire scrise în fişierul spool **E** Colecţia de informaţii de urmărire terminată şi toate informaţiile de urmărire şterse (nici o ieşire creată)
	453	839	Aplicaţie urmărită[2]	Char(10)	Numele aplicaţiei care este urmărită.
	463	849	Profil unelte service[3]	Char(10)	Numele profilului unelte service folosite pentru STRSST.
		859	ID nod sursă	Char(8)	ID nod sursă
		867	Utilizator sursă	Char(10)	Utilizator sursă
		877	Numele ASP pentru biblioteca de obiecte	Char(10)	Numele ASP pentru biblioteca de obiecte
		887	Număr ASP pentru biblioteca de obiecte	Char(5)	Număr ASP pentru biblioteca de obiecte
		892	Numele ASP pentru biblioteca de obiecte DMPSYSOBJ	Char(10)	Numele ASP pentru biblioteca de obiecte DMPSYSOBJ
		902	Număr ASP pentru biblioteca de obiecte DMPSYSOBJ	Char(5)	Număr ASP pentru biblioteca de obiecte DMPSYSOBJ

[1] Acest câmp este folosit doar când tipul intrării (offset 225) este CE.

[2] Acest câmp este folosit doar când tipul intrării (offset 225) este TA.

[3] Acest câmp este folosit doar când tipul intrării (offset 225) este ST.

Tabela 211. Intrări jurnal SV (Acţiune pentru valoarea sistem). Fişier descriere câmp QASYSVJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Modificare pentru valorile sistem **B** Modificare pentru atributele service **C** Modificare pentru ceasul sistem
157	225	611	Valoare sistem sau atribut service	Char(10)	Numele valorii sistem sau atributului service
167	235	621	Valoare nouă	Char(250)	Valoarea la care valoarea sistem sau atributul sistem a fost modificată
417	485	871	Valoare veche	Char(250)	Valoarea valorii sistem sau atributului sistem înainte sa fie modificată
667	735	1121	Continuarea valorii noi	Char(250)	Continuarea valorii la care valoarea sistem sau atributul sistem au fost modificate.
917	985	1371	Continuarea valorii vechi	Char(250)	A fost modificată continuarea valorii sistem sau atributului sistem.

Tabela 212. Intrări jurnal VA (Modificarea listei de cotrol acces). Fişier descriere câmp QASYVAJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Stare	Char(1)	Starea cererii. **S** Cu succes **F** Eşuare
157	225	611	Nume server	Char(10)	Numele descrierii server reţea care a înregistrat evenimentul.
167	235	621	Dată server	Char(6)	Data la care a fost reţinut în istoric evenimentul pe serverul reţea.
173	241	627	Timp server	Zoned(6,0)	Timpul la care a fost reţinut în istoric evenimentul pe serverul reţea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului care a lansat cererea pentru a modifica lista de control acces.
187	255	641	Nume solicitant	Char(10)	Numele utilizatorului care a lansat cererea.
197	265	651	Acţiune executată	Char(1)	Acţiunea executată în profilul de control acces: **A** Adăugare **C** Modificare **D** Ştergere
198	266	652	Nume resursă	Char(260)	Numele resursei de modificat.

Tabela 213. Intrări jurnal VC (Terminare şi oprire conexiune). Fişier descriere câmp QASYVCJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Acţiune de conectare.	Char(1)	Acţiunea de conectare care a apărut. **S** Pornire **E** Terminare **R** Refuzare
157	225	611	Nume server	Char(10)	Numele descrierii server reţea care a înregistrat evenimentul.
167	235	621	Data server	Char(6)	Data la care a fost reţinut în istoric evenimentul pe serverul reţea.
173	241	627	Timp server	Zoned(6,0)	Timpul la care a fost reţinut în istoric evenimentul pe serverul reţea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului asociat cu cererea de conectare.
187	255	641	Utilizator conexiune	Char(10)	Numele utilizatorului asociat cu cererea de conectare.
197	265	651	ID conectare	Char(5)	Pornirea sau oprirea ID-ului de conectare.
202	270	656	Motiv refuzare	Char(1)	Motivul refuzării conectării: **A** Deconectare automată (timeout), partajare îndepărtată sau lipsă de permisiuni administrative **E** Eroare, deconectare sesiune sau parolă incorectă **N** Deconectare normală sau limită de nume utilizator **P** Nici o permisiune de acces la resursa partajată
203	271	657	Nume reţea	Char(12)	Numele reţea asociat cu conexiunea.

Tabela 214. Intrări jurnal VF (Închiderea fişierelor server). Fişier descriere câmp QASYVFJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Motiv închidere	Char(1)	Motivul pentru care fişierul a fost închis. **A** Deconectare administrativă **N** Deconectare client normală **S** Deconectare sesiune
157	225	611	Nume server	Char(10)	Numele descrierii server reţea care a înregistrat evenimentul.
167	235	621	Dată server	Char(6)	Data la care a fost reţinut în istoric evenimentul pe serverul reţea.

Tabela 214. Intrări jurnal VF (Închiderea fişierelor server) (continuare). Fişier descriere câmp QASYVFJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
173	241	627	Timp server	Zoned(6,0)	Timpul la care a fost reţinut în istoric evenimentul pe serverul reţea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului care cere închiderea.
187	255	641	Utilizator conexiune	Char(10)	Numele utilizatorului care cere închiderea.
197	265	651	ID fişier	Char(5)	ID-ul fişierului care a fost închis.
202	270	656	Durată	Char(6)	Numărul de secunde în care fişierul a fost deschis.
208	276	662	Nume resursă	Char(260)	Numele resursei care deţine fişierul accesat.

Tabela 215. Intrări jurnal VL (Limită cont depăşită). fişier descriere câmp QASYVLJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Motiv	Char(1)	Motivul pentru care limita a fost depăşită. **A** Cont expirat **D** Cont dezactivat **L** Orele de logare depăşite **U** Necunoscut sau indisponibil **W** Staţie de lucru nevalidă
157	225	611	Nume server	Char(10)	Numele descrierii server reţea care a înregistrat evenimentul.
167	235	621	Dată server	Char(6)	Data la care a fost reţinut în istoric evenimentul pe serverul reţea.
173	241	627	Timp server	Zoned(6,0)	Timpul la care a fost reţinut în istoric evenimentul pe serverul reţea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului cu violare limită cont.
187	255	641	Utilizator	Char(10)	Numele utilizatorului cu violare limită cont.
197	265	651	Nume resursă	Char(260)	Numele resursei care este folosită.

Tabela 216. Intrări jurnal VN (Logare şi delogare reţea). Fişier descriere câmp QASYVNJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip logare	Char(1)	Tipul evenimentului care a apărut: **F** Cerere delogare **O** Cerere logare **R** Logare refuzată

Tabela 216. Intrări jurnal VN (Logare şi delogare reţea) (continuare). Fişier descriere câmp QASYVNJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
157	225	611	Nume server	Char(10)	Numele descrierii server reţea care a înregistrat evenimentul.
167	235	621	Dată server	Char(6)	Data la care a fost reţinut în istoric evenimentul pe serverul reţea.
173	241	627	Timp server	Zoned(6,0)	Timpul la care a fost reţinut în istoric evenimentul pe serverul reţea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului pentru eveniment.
187	255	641	Utilizator	Char(10)	Utilizatorul care s-a logat sau s-a delogat.
197	265	651	Privilegiu utilizator	Char(1)	Privilegiul utilizatorului care se loghează: **A** Administrator **G** Musafir **U** Utilizator
198	266	652	Motiv refuzare	Char(1)	Motivul refuzării încercării de logare: **A** Access refuzat **F** Dezactivare forţată datorită limitei de logare **P** Parolă incorectă
199	267	653	Motiv adiţional	Char(1)	Detalii despre refuzul accesului: **A** Cont expirat **D** Cont dezactivat **L** Ore de logare nevalide **R** ID solicitant nevalid **U** Necunoscut sau indisponibil

Tabela 217. Intrări jurnal VO (Listă de validare). Fişier descriere câmp QASYVOJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489 şi Tabela 153 la pagina 491 pentru listarea de câmpuri.
	224	610	Tip intrare	Char(1)	Tipul intrării. **A** Adăugare intrare în lista de validare **C** Modificare intrare în lista de validare **F** Căutare intrare în lista de validare **R** Îndepărtare intrare în lista de validare **U** Verificare fără succes a unei intrări în lista de validare **V** Verificare cu succes a unei intrări în lista de validare

Tabela 217. Intrări jurnal VO (Listă de validare) (continuare). Fişier descriere câmp QASYVOJ4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	225	611	Tip fără succes	Char(1)	Tipul unei verificări fără succes. **E** Datele criptate sunt incorecte **I** ID-ul intrării nu a fost găsit **V** Lista de validare nu a fost găsită
	226	612	Lista de validare	Char(10)	Numele listei de validare.
	236	622	Nume bibliotecă	Char(10)	Numele bibliotecii în care este lista de validare.
	246	632	Date criptate	Char(1)	Valoare date de criptat. **Y** Datele de criptat au fost specificate în cerere. **N** Datele de criptat nu au fost specificate în cerere
	247	633	Date intrare	Char(1)	Valore date de intrare **Y** Datele de intrare au fost specificate în cerere. **N** Datele de intrare nu au fost specificate în cerere.
	248	634	Lungime ID intrare	Binary(4)	Lungimea ID-ului intrării.
	250	636	Lungime date	Binary(4)	Lungimea datelor de intrare.
	252	638	Atribut de date criptate	Char (1)	Date criptate. **' '** nu a fost specificat un atribut de date criptate. **0** Datele de criptat pot fi folosite pentru a verifica o intrare. Aceasta este situaţia implicită. **1** Datele de criptat pot fi folosite pentru a verifica o intrare şi datele pot fi întoarse într-o operaţie de căutare.
	253	639	Atribut de certificat X.509	Char (1)	Certificat X.509
	254	640	(Zonă rezervată)	Char (28)	
	282	668	ID intrare	Byte(100)	ID-ul intrare
	382	768	Date intrare	Byte(1000)	Datele de intrare.
		1768	Numele ASP pentru biblioteca listei de validare	Char(10)	Numele ASP pentru biblioteca listei de validare
		1778	Numărul ASP pentru biblioteca listei de validare	Char(5)	Numărul ASP pentru biblioteca listei de validare

Tabela 218. Intrări jurnal VP (Eroare parolă reţea). Fişier descriere câmp QASYVPJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.

Tabela 218. Intrări jurnal VP (Eroare parolă reţea) (continuare). Fişier descriere câmp QASYVPJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
156	224	610	Tip eroare	Char(1)	Tipul erorii care a a apărut. **P** Eroare parolă
157	225	611	Nume server	Char(10)	Numele descrierii server reţea care a înregistrat evenimentul.
167	235	621	Dată server	Char(6)	Data la care evenimentul a fost logat pe serverul reţea.
173	241	627	Timp server	Zoned(6,0)	Timpul la care a fost reţinut în istoric evenimentul pe serverul reţea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului care a iniţiat cererea.
187	255	641	Utilizator	Char(10)	Numele utilizatorului care a încercat să se logheze.

Tabela 219. Intrări jurnal VR (Accces resursă reţea). Fişier descriere câmp QASYVRJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Stare	Char(1)	Starea de acces. **F** Accesul la resursă a eşuat **S** Accesul la resursă a reuşit
157	225	611	Nume server	Char(10)	Numele descrierii server reţea care a înregistrat evenimentul.
167	235	621	Dată server	Char(6)	Data la care evenimentul a fost logat pe serverul reţea.
173	241	627	Timp server	Zoned(6,0)	Timpul la care a fost reţinut în istoric evenimentul pe serverul reţea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului care cere resursa.
187	255	641	Utilizator	Char(10)	Numele utilizatorului care cere resursa.
197	265	651	Tip operaţie	Char(1)	Tipul operaţiei care este executată: **A** Atributele de resursă modificate **C** Instanţa resursei create **D** Resursă ştearsă **P** Permisiuni resursă modificate **R** Citire de date sau rulare de la o resursă **W** Date scrise într-o resursă **X** Resursa nu funcţiona
198	266	652	Cod retur	Char(4)	Codul retur este primit dacă accesul la resursă este garantat.
202	270	656	Mesaj server	Char(4)	Codul mesaj este trimis când accesul este garantat.
206	274	660	ID fişier	Char(5)	ID-ul fişierului care este accesat.
211	279	665	Nume resursă	Char(260)	Numele resursep care este folosită.

Tabela 220. Intrări jurnal VS (Sesiune server). Fişier descriere câmp QASYVSJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Acţiune sesiune	Char(1)	Acţiunea sesiune care a apărut.
					E Terminare sesiune
					S Pornire sesiune
157	225	611	Nume server	Char(10)	Numele descrierii server reţea care a înregistrat evenimentul.
167	235	621	Dată server	Char(6)	Data la care evenimentul a fost logat pe serverul reţea.
173	241	627	Timp server	Zoned(6,0)	Timpul la care a fost reţinut în istoric evenimentul pe serverul reţea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului care cere sesiune.
187	255	641	Utilizator	Char(10)	Numele utilizatorului care cere sesiunea.
197	265	651	Privilegiu utilizator	Char(1)	Nivelul de privilegiu al utilizatorului pentru pornirea de sesiune:
					A Administrator
					G Musafir
					U Utilizator
198	266	652	Cod motiv	Char(1)	codul motiv pentru terminarea sesiunii.
					A Deconectare administrator
					D Deconectarea automată (timeout), partajare îndepărtată sau lipsă de permisiuni administrative
					E Eroare, deconectare sesiune sau parolă incorectă
					N Deconectare normală sau limită de nume utilizator
					R Restricţie cont

Tabela 221. Intrări jurnal VU (Modificare profil reţea). Fişier descriere câmp QASYVUJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip	Char(1)	Tipul înregistrării care a fost modificată.
					G Înregistrare grup
					U Înregistrare utilizator
					M Informaţii globale profil utilizator
157	225	611	Nume server	Char(10)	Numele descrierii server reţea care a înregistrat evenimentul.
167	235	621	Dată server	Char(6)	Data la care evenimentul a fost logat pe serverul reţea.

Tabela 221. Intrări jurnal VU (Modificare profil reţea) (continuare). Fişier descriere câmp QASYVUJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
173	241	627	Timp server	Zoned(6,0)	Timpul la care a fost reţinut în istoric evenimentul pe serverul reţea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului care cere modificarea profilului utilizator.
187	255	641	Utilizator	Char(10)	Numele utilizatorului care cere modificarea profilului utilizator.
197	265	651	Acţiune	Char(1)	Acţiune cerută: **A** Adăugare **C** Modificare **D** Ştergere **P** Parolă incorectă
198	266	652	Nume resursă	Char(260)	Numele resursei.

Tabela 222. Intrări jurnal VV (modificare stare service). Fişier descriere câmp QASYVVJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Tipul intrării: **C** Stare service modificată **E** Server oprit **P** Server în pauză **R** Server repornit **S** Server pornit
157	225	611	Nume server	Char(10)	Numele descrierii server reţea care a înregistrat evenimentul.
167	235	621	Dată server	Char(6)	Data la care evenimentul a fost logat pe serverul reţea.
173	241	627	Timp server	Zoned(6,0)	Timpul la care a fost reţinut în istoric evenimentul pe serverul reţea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului care cere modificarea.
187	255	641	Utilizator	Char(10)	Numele utilizatorului care cere modificarea.
197	265	651	Stare	Char(1)	Starea cererii serviciului: **A** Serviciu activ **B** Pornirea serviciului în aşteptare **C** Continuare serviciu în aşteptare **E** Oprirea aşteptării pentru serviciu **H** Aducerea în pauză a serviciului **I** Serviciu în pauză **S** Serviciu oprit
198	266	652	Cod serviciu	Char(8)	Codul serviciului cerut.
206	274	660	Set text	Char(80)	Textul care este setat de către cererea serviciului.

Tabela 222. Intrări jurnal VV (modificare stare service) (continuare). Fişier descriere câmp QASYVVJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
286	354	740	Valoare retur	Char(4)	Valoarea retur din operaţia de modificare.
290	358	744	Serviciu	Char(20)	Serviciul care fost modificat.

Tabela 223. Intrări jurnal X0 (Autentificare reţea). Fişier descriere câmp QASYX0JE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.

Tabela 223. Intrări jurnal X0 (Autentificare reţea) (continuare). Fişier descriere câmp QASYX0JE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
156	224	610	Tip intrare	Char(1)	Tipul intrării:
					1 Tichet serviciu valid
					2 Principalele serviciu nu se potrivesc
					3 Principalele client nu se potrivesc
					4 Nepotrivire adresă IP tichet
					5 Eşuare decriptare tichet
					6 Eşuare decriptare autentificator
					7 Regiunea nu este în regiunile locale client
					8 Tichetul este o încercare de repetiţie
					9 Tichetul nu este încă valid
					A Decriptare eroare sumă de control KRB_AP_PRIV sau KRB_AP_SAFE
					B Nepotrivire adresă IP la distanţă
					C Nepotrivire adresă IP locală
					D Eroare amprentă de timp KRB_AP_PRIV sau KRB_AP_SAFE
					E eroare repetiţie KRB_AP_PRIV sau KRB_AP_SAFE
					F eroare ordine secvenţă KRB_AP_PRIV sau KRB_AP_SAFE
					K acceptare GSS — acreditare expirată
					L acceptare GSS — eroare sumă de control
					M acceptare GSS — legături canale
					N desfăşurare GSS sau context expirat verificare GSS
					O desfăşurare GSS sau decodare/decriptare verificare GSS
					P desfăşurare GSS sau eroare sumă de control verificare GSS
					Q desfăşurare GSS sau eroare secvenţă verificare GSS
	225	611	Cod stare	Char(8)	Starea cererii
	233	619	Valoare stare GSS	Char(8)	Valoare stare GSS
	241	627	Adresă IP la distanţă	Char(21)	Adresă IP la distanţă
	262	648	Adresă IP locală	Char(21)	Adresa IP locală
	283	669	Adrese criptate	Char(256)	Adrese IP criptate
	539	925	Indicator adrese criptate	Char(1)	Indicator adrese IP criptate
					Y toate adresele incluse
					N nu toate adresele incluse
					X nefurnizat

Tabela 223. Intrări jurnal X0 (Autentificare reţea) (continuare). Fişier descriere câmp QASYX0JE/J4/J5

Offset				
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	540	926	Flag-uri tichet	Char(8)	Flag-uri tichet
	548	934	Timp autentificare tichet	Char(8)	Timp autentificare tichet
	556	942	Timp pornire tichet	Char(8)	Timp pornire tichet
	564	950	Timp oprire tichet	Char(8)	Timp oprire tichet
	572	958	Timp reînnoire tichet	Char(8)	Reînnoire tichet înainte de timp
	580	966	Marcare timp mesaj	Char(8)	Marcare timp X0E
	588	974	Marcare timp expirare GSS	Char(8)	Marcare timp expirare acreditare GSS sau marcare timp expirare context
	596	982	CCSID Principal server	Binary(5)	CCSID Principal server (din tichet)
	600	986	Lungime Principal server	Binary(4)	Lungime Principal server (din tichet)
	602	988	Indicator Principal server	Char(1)	Indicator Principal server (din tichet) **Y** Principal server complet **N** Principal server incomplet **X** nefurnizat
	603	989	Principal server	Char(512)	Principal server (din tichet)
	1115	1501	CCSID parametru Principal server	Binary(5)	CCSID Parametru Principal server (din tichet)
	1119	1505	Lungime Parametru Principal server	Binary(4)	Lungime parametru Principal server (din tichet)
	1121	1507	Indicator parametru Principal server	Char(1)	CCSID Parametru Principal server (din tichet) **Y** Principal server complet **N** Principal server incomplet **X** nefurnizat
	1122	1508	Parametru Principal server	Char(512)	Parametrul Principal server din tichet trebuie să se potrivească
	1634	2020	CCSID Principal client	Binary(5)	CCSID Principal client (din autentificator)
	1638	2024	Lungime Principal client	Binary(4)	Lungime Principal client (din autentificator)
	1640	2026	Indicator Principal client	Char(1)	Indicator Principal client (din autentificator) **Y** Principal client complet **N** Principal client incomplet **X** nefurnizat
	1641	2027	Principal client	Char(512)	Principal client din autentificator
	2153	2539	CCSID Principal client	Binary(5)	CCSID Principal client (din tichet)
	2157	2543	Lungime Principal client	Binary(4)	Lungime Principal client (din tichet)

Tabela 223. Intrări jurnal X0 (Autentificare reţea) (continuare). Fişier descriere câmp QASYX0JE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
	2159	2545	Indicator Principal client	Char(1)	Indicator Principal client (din tichet) **Y** Principal client complet **N** Principal client incomplet **X** nefurnizat
	2160	2546	Principal client	Char(512)	Principal client din tichet
	2672	3058	CCSID Principal server GSS	Binary(5)	CCSID Principal server (din acreditare GSS)
	2676	3062	Lungime Principal server GSS	Binary(4)	Lungime Principal server (din acreditare GSS)
	2678	3064	Indicator Principal serverg GSS	Char(1)	Indicator Principal server (din acreditare GSS) **Y** Principal server complet **N** Principal server incomplet **X** nefurnizat
	2679	3065	Principal server GSS	Char(512)	Principal server din acreditare GSS
	3191	3577	CCSID Principal local GSS	Binary(5)	CCSID Nume principal local GSS
	3195	3581	Lungime Principal local GSS	Binary(4)	Lungime nume principal local GSS
	3197	3583	Indicator Principal local GSS	Char(1)	Indicator nume principal local GSS **Y** Principal local complet **N** Principal local incomplet **X** nefurnizat
	3198	3584	Principal local GSS	Char(512)	Principal local GSS
	3710	4096	CCSID Principal la distanţă GSS	Binary(5)	CCSID Nume principal la distanţă GSS
	3714	4100	Lungime Principal la distanţă GSS	Binary(4)	Lungime nume principal la distanţă GSS
	3716	4102	Indicator Principal la distanţă GSS	Char(1)	Indicator nume principal la distanţă GSS **Y** Principal la distanţă complet **N** Principal la distanţă incomplet **X** nefurnizat
	3717	4103	Principal la distanţă GSS	Char(512)	Principal la distanţă GSS

Tabela 224. Intrări jurnal X1 (Jeton identitate). Fişier descriere câmp QASYX1JE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.

Tabela 224. Intrări jurnal X1 (Jeton identitate) (continuare). Fişier descriere câmp QASYX1JE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
156	224	610	Tip intrare	Char(1)	Tipul intrării: **D** Delegare jeton identitate cu succes **F** Delegare jeton identitate eşuată **G** Obţinere cu succes a utilizatorului din jetonul identitate **U** Obţinerea utilizatorului din jetonul identitate a eşuat
	225	611	Cod motiv	Binary (5)	cod motiv pentru cererea eşuată: **9** Nepotrivire lungime jeton **10** Nepotrivire identificator EIM **11** Nepotrivire ID instanţă aplicaţie **12** Semnătură jeton nevalidă **13** Jeton identitate nevalid **14** Utilizator destinaţie nevalid **16** Tratare cheie nevalidă **17** Versiune jeton nesuportată **18** Cheie publică negăsită **Notă:** La o eşuare, doar informaţiile care au fost validate până la punctul eşuării for fi completate în câmpurile text.
		615	Rezervat	Char(7)	Rezervat
		622	CCSID date	Binary(5)	CCSID-ul datelor din câmpurile text
		626	Lungime receptor	Binary(5)	Lungimea datelor din câmpul receptorului.
		630	Receptor	Char(508)	Receptorul jetonului identitate care fie a eşuat cererea fie a avut succes. Datele din acest câmp vor fi în formatul: <EIMID>eimID_receptor </EIMID> <APPID>RECEIVER_appID </APPID> <TIMESTAMP>amprentă_timp_receiver </TIMESTAMP>. Amprenta de timp va fi inclusă doar în cererile de delegare.
		1138	Lungime expeditor	Binary(5)	Lungimea datelor din câmpul expeditorului.
		1142		Char(508)	Expeditorul jetonului identitate care fie a eşuat cererea fie a avut succes. Datele din acest câmp vor fi în formatul: <EIMID>eimID_expeditor</EIMID> <APPID>appID_expeditor</APPID> <TIMESTAMP>amprentă_timp_expeditor</TIMESTAMP>
		1650	Lungime iniţiator	Binary(5)	Lungimea datelor din câmpul iniţiatorului.
		1654	Iniţiator	Char(508)	Iniţiatorul cererii jeton identitate. Dacă expeditorul şi iniţiatorul sunt aceiaşi, câmpul cu lungimea iniţiator va fi 0. Datele din acest câmp vor fi în formatul: <EIMID>eimID_iniţiator</EIMID> <APPID>appID_iniţiator</APPID> <TIMESTAMP>amprentă_timp_iniţiator</TIMESTAMP>
		2162	Lungime lanţ	Binary(5)	Lungimea datelor din câmpul lanţ.

Tabela 224. Intrări jurnal X1 (Jeton identitate) (continuare). Fişier descriere câmp QASYX1JE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
		2166	Lanţ	Char(2036)	Lanţul expeditorilor între iniţiator şi ultimul expeditor. Lanţul va fi în ordinea de la cel din urmă la cel dintâi. Dacă nu există alţi expeditori, atunci câmpul lungime lanţ va fi 0. Acest câmp poate fi trunchiat dacă modificarea este mai mare decât lungimea acestui câmp. Datele din acest câmp vor fi în formatul: <SNDRz><EIMID>sndrz_eimID</EIMID> <APPID>sndrz_appID</APPID> <TIMESTAMP>sndrz_timestamp </TIMESTAMP> </SNDRz> <SNDRy>...</SNDRy>...
		4202	Intrări lanţ	Binary(5)	Numărul de intrări din câmpul lanţ.
		4206	Intrări lanţ disponibile	Binary(5)	Numărul intrărilor disponibile pentru lanţul expeditorilor. Acest număr poate fi mai mare decât numărul de intrări din câmp în cazul în care câmpul este trunchiat.
		4210	Lungime registry sursă	Binary(5)	Lungimea datelor din câmpul registry sursă.
		4214	Registry sursă	Char(508)	Registry sursă specificat în jetonul identitate.
		4722	Lungime utilizator registry sursă	Binary(5)	Lungimea datelor din câmpul utilizator registry sursă.
		4726	Utilizator registry sursă	Char(508)	Utilizatorul registry sursă specificat în jetonul identitate.
		5234	Lungime registry destinaţie	Binary(5)	Lungimea datelor din câmpul registry destinaţie.
		5238	Registry destinaţie	Char(508)	Registry destinaţie specificat.
		5746	Lungime utilizator registry destinaţie	Binary(5)	Lungimea datelor din câmpul utilizator registry destinaţie.
		5750	Utilizator registry destinaţie	Char(508)	Utilizatorul registry destinaţie spre care indică jetonul identitate. Acest câmp este completat într-o preluare utilizator cu succes din cererea jeton identitate.

Tabela 225. Intrări jurnal YC (Modificarea obiectului DLO). Fişier descriere câmp QASYYCJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Acces obiect **C** Modificarea unui obiect DLO
157	225	611	Nume obiect	Char(10)	Numele obiectului
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii
177	245	631	Tip obiect	Char(8)	Tipul obiectului
185	253	639	Utilizator office	Char(10)	Profilul utilizator al utilizatorului office
195	263	649	Nume document sau director	Char(12)	Numele documentului sau directorului
207	275	661	(Zonă rezervată)	Char(8)	

Tabela 225. Intrări jurnal YC (Modificarea obiectului DLO) (continuare). Fişier descriere câmp QASYYCJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
215	283	669	Cale director	Char(63)	Directorul care conţine obiectul bibliotecă de documente
278	346	732	În numele utilizatorului	Char(10)	Utilizatorul care lucrează în numele altui utilizator.
288	356	742	Tip acces	Packed(5,0)	Tipul de acces [1]

1 Vedeţi Tabela 230 la pagina 590 pentru o listă de coduri pentru tipurile de acces.

Tabela 226. Intrări jurnal YR (Citirea obiectului DLO). Fişier descriere câmp QASYYRJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Acces obiect **R** Citirea unui obiect DLO
157	225	611	Nume obiect	Char(10)	Numele obiectului
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii
177	245	631	Tip obiect	Char(8)	Tipul obiectului
185	253	639	Utilizator office	Char(10)	Profilul utilizator al utilizatorului office
195	263	649	Nume document sau director	Char(12)	Numele obiectului bibliotecă de documente
207	275	661	(Zonă rezervată)	Char(8)	
215	283	669	Cale director	Char(63)	Directorul care conţine obiectul bibliotecă de documente
278	346	732	În numele utilizatorului	Char(10)	Utilizatorul care lucrează în numele altui utilizator.
288	356	742	Tip acces	Packed(5,0)	Tipul de acces [1]

1 Vedeţi Tabela 230 la pagina 590 pentru o listă de coduri pentru tipurile de acces.

Tabela 227. Intrări jurnal ZC (Modificare obiect). Fişier descriere câmp QASYZCJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Acces obiect **C** Modificarea unui obiect **U** Modernizarea accesului deschis către un obiect
157	225	611	Nume obiect	Char(10)	Numele obiectului
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii în care este localizat obiectul
177	245	631	Tip obiect	Char(8)	Tipul obiectului
185	253	639	Tip acces	Packed(5,0)	Tipul de acces [1]

Tabela 227. Intrări jurnal ZC (Modificare obiect) (continuare). Fişier descriere câmp QASYZCJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
188	256	642	Date specifice de acces	Char(50)	Date specifice despre acces Când tipul obiect este *IMGCLG, acest câmp conţine următorul format: **Char 3** Numărul index al intrării catalog de imagini. **Blank** Indică faptul că operaţia a fost pentru un catalog de imagini. **Char 32** ID-ul volum al intrării catalog de imagini. **Blank** Indică faptul că operaţia a fost pentru un catalog de imagini. **Char 1** Tipul de acces pentru intrare. Valorile posibile sunt listate mai jos. **Blank** Indică faptul că operaţia a fost pentru un catalog de imagini. **R** Fişierul care conţine catalogul de imagini este numai-scriere. **W** Fişierul care conţine intrarea catalog de imagini poate fi citit/scris. **Char 1** Protecţia la scriere pentru intrare. **Blank** Indică faptul că operaţia a fost pentru un catalog de imagini. **Y** Fişierul care conţine intrarea catalog de imagini este protejat la scriere. **N** Fişierul care conţine intrarea catalog de imagini nu este protejat la scriere. **Char 10** Numele dispozitivului virtual. **Blank** Indică faptul că operaţia a fost pentru un catalog de imagini sau că respectivul catalog de imagini nu este în stare Pregătit. **Char 3** Nefolosit.
238			(Zonă rezervată)	Char(20)	
	306	692	(Zonă rezervată)	Char(18)	
	324	710	Lungime nume obiect [2]	Binary (4)	Lungimea numelui obiectului.
258	326	712	CCSID nume obiect [2]	Binary(5)	identificator de set de caractere codate pentru numele obiect.
262	330	716	ID regiune sau ţară nume obiect [2]	Char(2)	ID-ul regiune sau ţară pentru numele obiect.
264	332	718	ID limbă nume obiect[2]	Char(3)	ID-ul limbă pentru numele obiectului.

Tabela 227. Intrări jurnal ZC (Modificare obiect) (continuare). Fişier descriere câmp QASYZCJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
267	335	721	(Zonă rezervată)	Char(3)	
270	338	724	ID fişier părinte[2, 3]	Char(16)	ID-ul fişier al directorului părinte.
286	354	740	ID fişier obiect[2, 3]	Char(16)	ID-ul fişier al obiectului.
302	370	756	Nume obiect[2]	Char(512)	Numele obiectului.
	882	1268	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	898	1284	Nume ASP[6]	Char(10)	Numele dispozitivului ASP.
	908	1294	Număr ASP[6]	Char(5)	Numărul dispozitivului ASP.
	913	1299	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele de cale absolută.
	917	1303	ID regiune sau ţară nume cale	Char(2)	ID-ul de regiune sau ţară pentru numele de cale absolută.
	919	1305	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	922	1308	Lungime nume cale	Binary(4)	Lungimea numelui de cale absolută.
	924	1310	Completaţi indicatorul nume cale	Char(1)	Completaţi indicatorul de nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele complet pentru cale absolută pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele complet pentru cale absolută pentru obiect.
	925	1311	ID fişier înrudit[4]	Char(16)	ID fişier înrudit pentru numele de cale absolută.
	941	1327	Nume cale absolută[5]	Char(5002)	Numele cale absolută al obiectului.

1 Vedeţi Tabela 230 la pagina 590 pentru o listă de coduri pentru tipurile de acces.

2 Aceste câmpuri sunt folosite doar pentru obiectele din QOpenSys, sistemele de fişiere "rădăcină" şi sistemele de fişiere definite de utilizator.

3 Un ID care are bitul cel mai din stânga setat şi restul zero indică faptul că ID-ul NU este setat.

4 Când indicatorul de nume cale (offset 924) este ″N″, acest câmp va conţine ID-ul d fişier relativ al numelui căii absolute. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

5 Acesta este câmpul lungime variabilă. Primii 2 octeţi conţin lungimea numelui cale.

6 Dacă obiectul este într-o bibliotecă, acestea sunt informaţiile ASP bibliotecii obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informaţiile ASP ale obiectului.

Tabela 228. Intrări de jurnal ZM (Acces metodă SOM). Fişier descriere câmp QASYZMJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1				Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224		Tip acces	Char(1)	Tipul de acces
157	225		Existenţă obiect	Char(1)	Existenţă obiect Y
158	226		Gestiune obiect	Char(1)	Gestiune obiect Y

Tabela 228. Intrări de jurnal ZM (Acces metodă SOM) (continuare). Fişier descriere câmp QASYZMJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
159	227		Operaţional obiect	Char(1)	Operaţional obiect Y
160	228		Modificare obiect	Char(1)	Modificare obiect Y
161	229		Referinţă obiect	Char(1)	referinţă obiect Y
162	230		Rezervat	Char(10)	Câmp rezervat
172	240		Gestiune listă	Char(1)	Gestiune listă de autorizaţie
173	241		Citire	Char(1)	Citire Y
174	242		Adăugare	Char(1)	Adăugare Y
175	243		Actualizare	Char(1)	Actualizare Y
176	244		Ştergere	Char(1)	Ştergere Y
177	245		Execuţie	Char(1)	Execuţie Y
178	246		Rezervat	Char(10)	Câmp rezervat
188	256		ID fişier clasă	Char(16)	ID-ul de fişier al clasei
204	272		ID-ul de fişier obiect	Char(16)	ID-ul fişier al obiectului
220	288		Nume metodă	Char(4096)	Numele metodei

Tabela 229. Intrări jurnal ZR (Citire obiect). Fişier descriere câmp QASYZRJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi Tabela 152 la pagina 489, Tabela 153 la pagina 491 şi Tabela 154 la pagina 492 pentru menţionarea câmpului.
156	224	610	Tip intrare	Char(1)	Acces obiect **R** Citirea unui obiect
157	225	611	Nume obiect	Char(10)	Numele obiectului
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii în care este localizat obiectul
177	245	631	Tip obiect	Char(8)	Tipul obiectului
185	253	639	Tip acces	Packed(5,0)	Tipul de acces [1]

Tabela 229. Intrări jurnal ZR (Citire obiect) (continuare). Fişier descriere câmp QASYZRJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
188	256	642	Date specifice de acces	Char(50)	Date specifice despre acces. Când tipul obiect este *IMGCLG, acest câmp conţine următorul format: **Char 3** Numărul index al intrării catalog de imagini. **Blank** Indică faptul că operaţia a fost pentru un catalog de imagini. **Char 32** ID-ul volum al intrării catalog de imagini. **Blank** Indică faptul că operaţia a fost pentru un catalog de imagini. **Char 1** Tipul de acces pentru intrare. Valorile posibile sunt menţionate mai jos. **Blank** Indică faptul că operaţia a fost pentru un catalog de imagini. **R** Fişierul care conţine catalogul de imagini este numai-scriere. **W** Fişierul care conţine intrarea catalog de imagini poate fi citit/scris. **Char 1** Protecţia la scriere pentru intrare. **Blank** Indică faptul că operaţia a fost pentru un catalog de imagini. **Y** Fişierul care conţine intrarea catalog de imagini este protejat la scriere. **N** Fişierul care conţine intrarea catalog de imagini nu este protejat la scriere. **Char 10** Numele dispozitivului virtual. **Blank** Indică faptul că operaţia a fost pentru un catalog de imagini sau că respectivul catalog de imagini nu este în stare Pregătit. **Char 3** Nefolosit.
238			(Zonă rezervată)	Char(20)	
	306	692	(Zonă rezervată)	Char(18)	
	324	710	Lungime nume obiect [2]	Binary(4)	Lungimea numelui obiectului.
258	326	712	CCSID nume obiect [2]	Binary(5)	identificator de set de caractere codate pentru numele obiect.
262	330	716	ID regiune sau ţară nume obiect [2]	Char(2)	ID-ul regiune sau ţară pentru numele obiect.
264	332	718	ID limbă nume obiect[2]	Char(3)	ID-ul limbă pentru numele obiectului.
267	335	721	(Zonă rezervată)	Char(3)	
270	338	724	ID fişier părinte[2,3]	Char(16)	ID-ul fişier al directorului părinte.
286	354	740	ID fişier obiect[2,3]	Char(16)	ID-ul fişier al obiectului.

Tabela 229. Intrări jurnal ZR (Citire obiect) (continuare). Fişier descriere câmp QASYZRJE/J4/J5

Offset					
JE	**J4**	**J5**	**Câmp**	**Format**	**Descriere**
302	370	756	Nume obiect[2]	Char(512)	Numele obiectului.
	882	1268	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	898	1284	Nume ASP	Char(10)	Numele dispozitivului ASP.
	908	1294	Număr ASP	Char(5)	Numărul dispozitivului ASP.
	913	1299	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele de cale absolută.
	917	1303	ID regiune sau ţară nume cale	Char(2)	ID-ul de regiune sau ţară pentru numele de cale absolută.
	919	1305	ID limbă nume cale	Char(3)	ID limbă pentru numele de cale absolută.
	922	1308	Lungime nume cale	Binary(4)	Lungimea numelui de cale absolută.
	924	1310	Completaţi indicatorul nume cale	Char(1)	Completaţi indicatorul de nume cale absolută: **Y** Câmpul Nume cale absolută conţine numele complet pentru cale absolută pentru obiect. **N** Câmpul Nume cale absolută nu conţine numele complet pentru cale absolută pentru obiect.
	925	1311	ID fişier înrudit[4]	Char(16)	ID fişier înrudit pentru numele de cale absolută.
	941	1327	Nume cale absolută[5]	Char(5002)	Numele cale absolută al obiectului.

1 Vedeţi Tabela 230 pentru o listă de coduri pentru tipurile de acces.

2 Aceste câmpuri sunt folosite doar pentru obiectele din QOpenSys, sistemele de fişiere "rădăcină" şi sistemele de fişiere definite de utilizator.

3 Un ID care are bitul cel mai din stânga setat şi restul zero indică faptul că ID-ul NU este setat.

4 Când indicatorul de nume cale (offset 924) este ″N″, acest câmp va conţine ID-ul d fişier relativ al numelui căii absolute. Când idicatorului de nume cale este ″Y″, acest câmp va conţine 16 octeţi de zerouri hexa.

5 Acesta este câmpul lungime variabilă. Primii 2 octeţi conţin lungimea numelui cale.

Tabela 230 listează codurile de acces folosite pentru intrările jurnal auditare obiecte din fişierele QASYYCJE/J4/J5, QASYYRJE/J4/J5, QASYZCJE/J4/J5 şi QASYZRJE/J4/J5.

Tabela 230. Codurile numerice pentru tipurile de acces

Cod	Tip acces	Cod	Tip acces	Cod	Tip acces
1	Adăugare	26	Încărcare	51	Trimitere
2	Activare program	27	Listare	52	Pornire
3	Analiză	28	Mutare	53	Transfer
4	Aplicare	29	Combinare	54	Urmărire
5	Apel sau TFRCTL	30	Deschidere	55	Verificare
6	Configurare	31	Tipărire	56	Alimentare
7	Modificare	32	Cerere	57	Lucru
8	Verificare	33	Revendicare	58	Atribut DLO citire/modificare
9	Închidere	34	Recepţie	59	Securitate DLO citire/modificare
10	Curăţare	35	Citire	60	Conţinut DLO citire/modificare

Tabela 230. Codurile numerice pentru tipurile de acces (continuare)

Cod	Tip acces	Cod	Tip acces	Cod	Tip acces
11	Comparaţie	36	Reorganizare	61	Toate părţile DLO citire/modificare
12	Anulare	37	Eliberare	62	Adăugare constrângere
13	Copiere	38	Îndepărtare	63	Modificare constrângere
14	Creare	39	Redenumire	64	Înlăturare constrângere
15	Conversie	40	Înlocuire	65	Pornire procedură
16	Depanare	41	Continuare	66	Obţinere acces la **OOPOOL
17	Ştergere	42	Restaurare	67	Semnare obiect
18	Abandon	43	Extragere	68	Înlătuarea tuturor semnăturilor
19	Afişare	44	Rulare	69	Curăţare obiect semnat
20	Editare	45	Revocare	70	MOUNT
21	Oprire	46	Salvare	71	Descărcare
22	Fişier	47	Salvare cu eliberare spaţiu de stocare	72	Oprire derulare înapoi
23	Acordare	48	Salvare şi ştergere		
24	Reţinere	49	Lansare		
25	Iniţializare	50	Setare		

Anexa G. Comenzile şi meniurile pentru comenzi de securitate

Această anexă descrie comenzile şi meniurile pentru uneltele de securitate. Exemple despre folosirea comenzilor sunt incluse în acest manual.

Două meniuri sunt disponibile pentru uneltele de securitate:

- Meniul SECTOOLS (Unelte securitate) pentru a rula comenzile în mod interactiv.
- Meniul SECBATCH (Lansare sau Planificare rapoarte de securitate pentru batch) pentru a rula comenzile de rapoarte în batch. Meniul SECBATCH are două părţi. Prima parte a meniului foloseşte comanda Lansare Job (SBMJOB) pentru a lansa rapoarte pentru procesarea imediată în batch.

  A doua parte a meniului foloseşte comanda Adăugare intrare planificată a jobului (ADDJOBSCDE). O folosiţi pentru a planifica rapoartele de securitate care să fie rulate regulat la un anumit moment de timp speicificat.

Opţiunile din meniul cu unelte de securitate

Următorul este partea despre meniul SECTOOLS care se referă la profilurile utilizator. Pentru a accesa acest meniu, tastaţi GO SECTOOLS

```
SECTOOLS                        Unelte de securitate

Selectaţi unul din următoarele:

  Gestionare profiluri
     1. Analizare parolelor implicite

     2. Afişarea listei de profiluri active
     3. Modificarea listei de profiluri active
     4. Analizarea activităţii profilului

     5. Afişarea planificatorului de activare
     6. Modificarea intrării planificatorului de activare

     7. Afişarea planificatorului de expirare
     8. Modificarea expirării intrării de planificare
```

Tabela 231 descrie aceste opţiuni de meniuri şi comenzile asociate:

Tabela 231. Comenzi unelte pentru Profiluri utilizatori

Meniul[1] Opţiune	**Nume comandă**	**Descriere**	**Fişier bază de date folosit**
1	ANZDFTPWD	Folosiţi comanda Analizare parole implicite pentru a raporta şi a lua acţiuni pe profilurile utilizatori care au o parolă egală cu cea a numelui profilului utilizator.	QASECPWD[2]
2	DSPACTPRFL	Folosiţi comanda Afişare listă de profiluri active pentru a afişa sau tipări lista de profiluri utilizatori care sunt exceptaţi de la procesarea ANZPRFACT.	QASECIDL[2]

Tabela 231. Comenzi unelte pentru Profiluri utilizatori (continuare)

Meniul[1] Opţiune	**Nume comandă**	**Descriere**	**Fişier bază de date folosit**
3	CHGACTPRFL	Folosiţi comanda Modificare listă de profiluri activă pentru a adăuga sau înlătura profiluri de utilizatori din lista de excepţii pentru comanda ANZPRFACT. Un profil utilizator care este în lista de profiluri active este permament activ (doar dacă înlăturaţi profilul din listă). Comanda ANZPRFACT nu dezactivează un profil care este în lista de profiluri active, nedepinzând de cât de mult timp a fost profilul inactiv.	QASECIDL[2]
4	ANZPRFACT	Folosiţi comanda Analizare activitate profil pentru a dezactiva profilurile utilizator care nu au fost folosite un anumit număr de zile specificat. După ce folosiţi comanda ANZPRFACT pentru a specifica numărul de zile, sistemul rulează jobul ANZPRFACT în fiecare noapte. Puteţi folosi comanda CHGACTPRFL pentru a exclude profilurile utilizator de a fi dezactivate.	QASECIDL[2]
5	DSPACTSCD	Folosiţi comanda Afişare planificator activare profiluri pentru a afişa sau a tipări informaţii despre planificator pentru activarea sau dezactivarea profilurilor de utilizatori specifice. Creaţi planificatorul cu ajutorul comenzii CHGACTSCDE.	QASECACT[2]
6	CHGACTSCDE	Folosiţi comanda Modificare intrare planificare pentru a face ca un profil de utilizator să fie disponibil pentru semnare doar la momente specificate din zi sau săptămână. Pentru fiecare profil de utilizator pentru care faceţi planificarea, sistemul creează intrări de planificare a jobului pentru orele de activare şi dezactivare.	QASECACT[2]
7	DSPEXPSCDE	Folosiţi comanda Afişare planificare expirare pentru a afişa sau tipări lista de profiluri de utilizatori care sunt planificaţi pentru a fi dezactivaţi sau înlăturaţi din sistem în viitor. Folosiţi comanda CHGEXPSCDE pentru a seta profilurile de utilizatori care vor expira.	QASECEXP[2]
8	CHGEXPSCDE	Folosiţi comanda Modificare intrări de expirare pentru a planifica un profil utilizator pentru înlăturare. Puteţi înlătura profilul temporar (prin dezactivarea lui) sau îl puteţi şterge din sistem. Această comandă foloseşte o intrare de planificator de joburi care rulează în fiecare zi la 00:01 (1 minut după miezul nopţii). Jobul priveşte în fişierul QASECEXP pentru a determina dacă orice profiluri utilizator sunt setate pentru a expira în acea zi. Folosiţi comanda DSPEXPSCD pentru a afişa profilurile utilizatori care sunt planificate pentru expirare.	QASECEXP[2]
9	PRTPRFINT	Folosiţi comanda Tipărire profiluri interne pentru a tipări un report cu informaţiile interne despre numărul de întrări într-un obiect profil utilizator (*USRPRF).	

Tabela 231. Comenzi unelte pentru Profiluri utilizatori (continuare)

Meniul[1] Opţiune	Nume comandă	Descriere	Fişier bază de date folosit
Note: 1. Opţiunile sunt din meniul SECTOOLS. 2. Fişierul este în biblioteca QUSRSYS.			

Puteţi apăsa pe pagină jos în meniu pentru a vedea opţiunile suplimentare. Tabela 232 descrie opţiunile meniu şi comenzile asociate pentru auditarea securităţii:

Tabela 232. Comenzi unelte pentru auditarea de securitate

Meniu[1] Opţiune	Nume comandă	Descriere	Fişier bază de date folosit
10	CHGSECAUD	Folosiţi comanda Modificare auditare securitate pentru a seta auditarea securităţii şi pentru a modifica valorile de sistem care controlează auditarea de securitate. Când rulaţi comanda CHGSECAUD, sistemul creează jurnalul de auditare de securitate (QAUDJRN) dacă nu există deja. Comanda CHGSECAUD furnizează opţiuni care simplifică setarea QAUDLVL (nivel de auditare) şi pentru valorile de sistem QAUDLVL2 (extensie de nivel de auditare). Puteţi specifica *ALL pentru a activa toate setările de nivel de auditare. Sau, puteţi specifica *DFTSET pentru a activa cele mai comune setări folosite (*AUTFAIL, *CREATE, *DELETE, *SECURITY, şi *SAVRST). **Notă:** Dacă folosiţi uneltele de securitate pentru a seta auditarea, fiţi siguri că planificaţi pentru gestiunea primitorilor jurnalului de auditare. Altfe, se poate să întâlniţi imediat probleme la utilizarea disc-ului.	
11	DSPSECAUD	Folosiţi comanda Afişare auditare securitate pentru a afişa informaţii despre jurnalul de auditare securitate şi valorile de sistem care controlează auditarea de securitate.	
Note: 1. Opţiunile sunt din meniul SECTOOLS.			

Cum se foloseşte meniul batch securitate

Următoarea este prima parte a meniului SECBATCH:

```
SECBATCH         Submit or Schedule Security Reports To Batch
                                                                    Sistem:
Select one of the following:

  Submit Reports to Batch
     1. Adopting objects
     2. Audit journal entries
     3. Authorization list authorities
     4. Command authority
     5. Command private authorities
     6. Communications security
     7. Directory authority
     8. Directory private authority
     9. Document authority
    10. Document private authority
    11. File authority
    12. File private authority
    13. Folder authority
```

Atunci când selectaţi o opţiune din acest meniu, vedeţi ecranul Lansare job (SBMJOB), după cum urmează:

```
                            Lansare job (SBMJOB)
Introduceţi opţiunile şi apăsaţi Enter.

Comandă de rulat . . . . . . . . . . . > PRTADPOBJ USRPRF(*ALL
_____________________________________________
_____________________________________________
_____________________________________________...
Nume job . . . . . . . . . . . .   *JOBD         Nume, *JOBD
Descriere job. . . . . . . .   *USRPRF          Nume, *USRPRF
  Bibliotecă. . . . . . . . . .                   Nume, *LIBL, *CURLIB
Coadă job . . . . . . . . . . .   *JOBD         Nume, *JOBD
  Bibliotecă. . . . . . . . . .   __              Nume, *LIBL, *CURLIB
Prioritate job (în JOBQ)  . . . .  *JOBD        1-9, *JOBD
Prioritate ieşire (în OUTQ) . . .   *JOBD        1-9, *JOBD
Dispozitiv tipărire . . . . . . .   *CURRENT     Nume, *CURRENT, *USRPRF...
```

Dacă vreţi să modificaţi opţiunea implicită pentru comandă, puteţi apăsa F4 (Prompt) din linia *Comanda de rulare*.

Pentru a vedea Planificarea rapoartelor batch, mergeţi o pagină în jos la meniul SECBATCH. Prin folosirea opţiunilor din această parte a meniului, puteţi de exemplu să configuraţi sistemul să ruleze versiuni modificate ale rapoartelor regulat.

```
SECBATCH         Submit or Schedule Security Reports To Batch
                                                                  Sistem:
Select one of the following:

    28. User objects
    29. User profile information
    30. User profile internals
    31. Check object integrity

  Schedule Batch Reports
    40. Adopting objects
    41. Audit journal entries
    42. Authorization list authorities
    43. Command authority
    44. Command private authority
    45. Communications security
    46. Directory authority
```

Puteţi apăsa page down pentru opţiuni suplimentare ale meniului. Atunci când selectaţi o opţiune din această parte a meniului, vedeţi ecranul Adăugare intrare planificator de joburi:

```
                     Adăugare intrare planif. job (ADDJOBSCDE)

Introduceţi opţiunile şi apăsaţi Enter.

Nume job . . . . . _____                    Nume, *JOBD
Comnadă de rulat . . . . . > PRTADPOBJ USRPRF(*ALL)
_____________________________________________
_____________________________________________
_____________________________________________
_____________________________________________...
Frecvenţă  . . . . . _______ *ONCE, *WEEKLY, *MONTHLY
Dată planificare, sau. . . . . *CURRENT      Date, *CURRENT, *MONTHST
Zi planificare . . . . . *NONE         *NONE, *ALL, *MON, *TUE.
+ pentru mai multe valori
Oră planificare  . . . . . *CURRENT      Oră, *CURRENT
```

Puteţi să poziţionaţi cursorul pe linia *Comandă de rulat* şi apăsaţi F4 (Prompt) pentru a alege diferite setări pentru raport. Ar trebui să asociaţi un nume de job cu sens astfel încât să recunoaşteţi intrarea atunci când afişaţi intrările din planificarea de joburi.

Opţiunile din meniul batch securitate

Tabela 233descriere opţiunile meniului şi comenzile asociate pentru rapoartele de securitate.

Atunci când rulaţi rapoarte de securitate, sistemul afişează doar informaţii care îndeplinesc ambele criterii de selecţie pe care le specificaţi şi criteriul de selecţie pentru unealtă. De exemplu, descrierea de job care specifică numele profil utilizator şi securitate relevantă. De aceea, raportul descriere de job (PRTJOBDAUT)tipăreşte descrieri de job din biblioteca specificată numai dacă autorizaţia publică pentru descrierea de job nu este *EXCLUDE *şi* dacă descrierea de job specifică nu nume profil utilizator în parametrul USER.

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

Dacă un anumit raport printează mai multe informaţii decât vă aşteptaţi, consultaţi informaţiile de ajutor online pentru a afla criteriile de selecţie pentru raport.

Tabela 233. Comenzi pentru rapoarte securitate

Meniu[1] Opţiune	**Nume comandă**	**Descriere**	**Fişier bază de date folosit**
1, 40	PRTADPOBJ	Folosiţi comanda Tipărire obiecte adoptare pentru a tipări o listă de obiecte ca adoptă autorizarea pentru profilul de utilizator specificat. Puteţi specifica un profil singur, un nume de profil generic (ca de exemplu toate profilurile care încep cu Q), sau toate profilurile pe sistem. Acest raport are două versiuni. Raportul complet listează toate obiectele adoptate care îndeplinesc criteriile de selecţie. Raportul modificat listează diferenţele între obiectele adoptate care sunt curent pe sistem şi obiectele adoptate care au fost pe sistem ultima oară când rulează raportul.	QSECADPOLD[2]
2, 41	DSPAUDJRNE	Folosiţi comanda Afişare intrări jurnal de auditare pentru a afişa sau tipări informaţii despre intrările din jurnalul de auditare de securitate. Puteţi selecta tipuri de intrări specifice, utilizatori specifice, şi o perioadă de timp.	QASYxxJ5[3]

Tabela 233. Comenzi pentru rapoarte securitate (continuare)

Meniu[1] Opţiune	**Nume comandă**	**Descriere**	**Fişier bază de date folosit**
3, 42	PRTPVTAUT *AUTL	Când folosiţi comanda Tipărire autorizări private pentru obiectele *AUTL, primiţi o listă a tuturor listelor de autorizări pe sistem. Raportul include utilizatorii care sunt autorizaţi pentru fiecare listă şi ce autorizări au utilizatorii pentru liste. Folosiţi această informaţie pentru a vă ajuta să analizaţi sursele de autorizări de obiecte pe sistemul dumneavoastră. Raportul are trei versiuni. Reportul complet listează toate listele de autorizate pe sistem. Raportul modificat listează adăugările şi modificările pentru autorizări de când aţi rulat ultima oară raportul. Raportul şters listează utilizatorii ale căror autorizări pentru listele de autorizare au fost şterse de la ultima rulare a raportului. Când tipăriţi raportul complet, aveţi opţiunea de a tipări o listă de obiecte pentru fiecare listă de autorizare securizată. Sistemul va crea un raport separat pentru fiecare listă de autorizare.	QSECATLOLD[2]
6, 45	PRTCMNSEC	Folosiţi comanda Tipărire securitate comunicaţie pentru a tipări setările relevante pentru securitate pentru obiectele are afectează comunicaţia pe sistemul dumneavoastră. Setările afectează cum utilizatorii şi joburile pot intra pe sistemul dumneavoastră. Această comandă produce două rapoarte: un raport care afişează setările pentru listele de configurare pe sistem şi un raport care listează parametrii relevanţi pentru securitate pentru descriptorii de linie, pentru controlere şi pentru descrierile dispozitivelor. Fiecare din aceste rapoarte au o versiune completă şi o versiune modificată.	QSECCMNOLD[2]
15, 54	PRTJOBDAUT	Folosiţi comandă Tipărire autorizare descriere job pentru a tipări o listă a descriptorilor de joburi care specifică un profil de utilizator şi au autorizările publice care nu sunt *EXCLUDE. Raportul arată autorizările speciale pentru profilul utilizatorului care este specificat în descrierea de job. Acest raport are două versiuni. Raportul complet listează toate obiectele de descriere de joburi care îndeplinesc criteriile de selecţie. Raportul modificat listează diferenţele între obiectele de descriere a jobului care sunt curent pe sistem şi obiectele de descriere de job care au fost pe sistem ultima dată când s-a rulat raportul.	QSECJBDOLD[2]

Tabela 233. Comenzi pentru rapoarte securitate (continuare)

Meniu[1] **Opţiune**	**Nume comandă**	**Descriere**	**Fişier bază de date folosit**
Vedeţi nota 4	PRTPUBAUT	Folosiţi comanda Tipărire obiecte autorizate pentru publicare pentru a tipări o listă de obiecte ale cărei autorizare publică nu este *EXCLUDE. Când rulaţi comanda, specificaţi tipul obiectului şi biblioteca sau bibliotecile pentru raport. Folosiţi comanda PRTPUBAUT pentru a tipări imformaţii despre obiecte pe care fiecare utilizator de pe sistem le poate accesa. Acest raport are două versiuni. Raportul complet listează toate obiectele care îndeplinesc criteriile de selecţie. Raportul modificat listează diferenţele între obiectele specificate care sunt curent pe sistem şi obiectele (de acelaşi tip în aceaşi bibliotecă) care au fost pe sistem ultima oară când aţi rulat raportul.	QPBxxxxxx[5]
Vedeţi nota 4.	PRTPVTAUT	Folosiţi comanda Tipărire autorizări private pentru a tipări o listă de autorizări private pentru obiecte pentru tipurile specificate în biblioteca specificată. Folosiţi acest raport pentru a vă ajuta să determinaţi sursele de autorizări pentru obiecte. Acest raport are trei versiuni. Raportul complet listează toate obiectele care îndeplinesc criteriile de selecţie. Raportul modificat listează diferenţele între obiectele specificate care sunt curent pe sistem şi obiectele (de acelaşi tip în aceaşi bibliotecă) care au fost pe sistem ultima dată când s-a rulat raportul. Raportul şters listează utilizatorii ale căror autorizări pentru un obiect au fost şterse de când aţi tipărit ultima dată raportul.	QPVxxxxxx[5]
24, 63	PRTQAUT	Folosiţi Tipărire raport coadă pentru a tipări setările de securitate pentru cozile de ieşire şi cozile de joburi pe sistemul dumneavoastră. Aceste setări controlează cine poate vizualiza şi modifica intrări în coada de ieşire sau coada de job. Acest raport are două versiuni. Raportul complet listează toate cozile de ieşire şi obiectele cozii de job care îndeplinesc criteriul de selecţie. Raportul modificat listează diferenţele între obiectele cozii de ieşire şi cozii de job care sunt curent pe sistem şi între obiectele cozii de ieşire şi cozii de job care au fost pe sistem ultima dată când aţi rulat raportul.	QSECQOLD[2]

Tabela 233. Comenzi pentru rapoarte securitate (continuare)

Meniu[1] Opţiune	**Nume comandă**	**Descriere**	**Fişier bază de date folosit**
25, 64	PRTSBSDAUT	Folosiţi comanda Tipărire descriere subsistem pentru a tipări intrările de comunicaţie relevante de securitate pentru descrierile de subsistem pe sistemul dumneavoastră. Aceste setări controlează cum poate porni lucrul pe sistemul dumneavoastră şi cum pot porni joburile. Raportul tipăreşte o descriere de subsistem doar are intrări de comunicaţii care specifică un nume de profil de utilizator. Acest raport are două versiuni. Raportul complet listează toate obiectele de descriere de subsistem care întrunesc criteriile de selecţie. Raportul modificat listează diferenţele între descrierea subsistemului care sunt curent pe sistem şi obiectele descrierii subsistemului care au fost pe sistem ultima oară când aţi rulat raportul.	QSECSBDOLD[2]
26, 65	PRTSYSSECA	Folosiţi comanda Tipărire atribute de securitate sistem pentru a tipări o listă de valori de sistem relevante de securitate şi atribute de reţea. Raportul arată valoarea curentă şi valoarea recomandată.	
27, 66	PRTTRGPGM	Folosiţi comanda Tipărire programe declanşare pentru a tipări o listă de programe declanşare care sunt asociate cu fişierele bazei de date pe sistemul dumneavoastră. Acest raport care două versiuni. Raportul complet listează toate programele declanşate care sunt asignate şi întrunesc criteriul dumneavoastră de selecţie. Raportul modificat listează programele declanşate care au asignate de la ultima oară când aţi rulat raportul.	QSECTRGOLD[2]
28, 67	PRTUSROBJ	Folosiţi comanda Tipărire obiecte utilizator pentru a tipări o listă de obiecte utilizator (obiecte care nu sunt furnizate de către IBM) care sunt într-o bibliotecă. Puteţi folosi acest raport pentru a tipări o listă de obiecte utilizator care sunt într-o bibliotecă (ca de exemplu QSYS) care este în porţiunea de sistem în lista bibliotecii. Acest raport are două versiuni. Raportul complet listează toate obiectele utilizator care îndeplinesc criteriul de selecţie. Raportul modificat listează diferenţele între obiectele utilizator care sunt curent pe sistem şi obiectele utilizator care sunt pe sistem ultima oară când aţi rulat raportul.	QSECPUOLD[2]
29, 68	PRTUSRPRF	Folosiţi comanda Tipărire profil utilizator pentru a analiza profilurile utilizator care îndeplinesc criteriile specificate. Puteţi selecta profilurile utilizator bazate pe autorizările specificate, clasele de utilizator, sau o nepotrivire între autorizările speciale şi clasa de utilizator. Puteţi tipări informaţiile de autorizare, informaţiile despre mediu, sau informaţiile despre parolă.	
30, 69	PRTPRFINT	Folosiţi comanda Tipărire profil intern pentru a tipări un raport cu informaţiile interne a numărului intrărilor conţinute într-un obiect profil utilizator (*USRPRF).	

Tabela 233. Comenzi pentru rapoarte securitate (continuare)

Meniu[1] Opţiune	Nume comandă	Descriere	Fişier bază de date folosit
31, 70	CHKOBJITG	Folosiţi comanda Verificare integritate obiect pentru a determina dacă obiectele operabile (ca de exemplu programele) au fost modificate fără a folosi un compilator. Această comandă vă poate ajuta să detectaţi încercările de a introduce un program virus în sistemul dumneavoastră sau pentru a modifica un program pentru a realiza instrucţiuni neautorizate.	

Note:

1. Opţiunile sunt din meniul SECBATCH.
2. Acest fişier este în biblioteca QUSRSYS.
3. xx este un tip de intrare de două caractere. De exemplu, fişierul de ieşire model pentru intrările de jurnal AE este QSYS/QASYAEJ5. Fişierele de ieşire model sunt descrise în Anexa F din această carte.
4. Meniul SECTOOLS conţine opţiuni pentru tipurile obiect care sunt obişnuit scopul administratorilor de securitate. De exemplu, folosiţi opţiunile 11 sau 50 pentru a rula comanda PRTPUBAUT pe obiectele *FILE. Folosiţi opţiunile generale (18 şi 57) pentru a specifica tipul de obiect. Folosiţi opţiunile 12 şi 15 pentru a rula comanda PRTPVTAUT pentru obiectele *FILE. Folosiţi opţiunile generale (19 şi 58) pentru a specifica tipul de obiect.
5. xxxxxx din numele fişierului este tipul obiectului. De exemplu, fişierul pentru obiectele program este numit QPBPGM pentru autorizaţiile publice şi QPVPGM pentru autorizaţiile private. Fişierele sunt în biblioteca QUSRSYS.

   Fişierul conţine un membru pentru fiecare bibliotecă pentru care aţi tipărit un raport. Numele membru este acelaşi ca şi numele bibliotecă.

Comenzile pentru personalizarea securităţii

Tabela 234 descrie comenzile pe care le puteţi folos pentru a personaliza securitatea pe sistemul dumneavoastră. Aceste comenzi sunt în meniul SECTOOLS:

Tabela 234. Comenzi pentru Personalizarea sistemului dumneavoastră

Meniu[1] Option	Nume comandă	Descriere	Fişier bază de date folosit
60	CFGSYSSEC	Folosiţi comanda Configurare securitate sistem pentru a seta valorile sistem de securitate relevante la configurările recomandate. Comanda setează deasemenea auditarea de securitate pe sistemul dumneavoastră. “Valorile setate de comanda Configurare securitate sistem” descrier ce face comanda.	
61	RVKPUBAUT	Folosiţi comanda Revocare autorizaţie publică pentru a seta autorizaţia publică la *EXCLUDE pentru un set de comenzi sensibile la securitate pe sistemul dumneavoastră. “Ce face comanda Revocare autorizare publică” la pagina 603listează acţiunile pe care le realizează comanda RVKPUBAUT.	

Note:

1. Opţiuni sunt din meniul SECTOOLS.

Valorile setate de comanda Configurare securitate sistem

Tabela 235 la pagina 602listează valorile sistem care sunt setate când rulaţi comanda CFGSYSSEC. Comanda CFGSYSSEC rulează un program care este numit QSYS/QSECCFGS.

Tabela 235. Valori setate de comanda CFGSYSSEC

Nume valoare sistem	Setare	Descriere valoare sistem
QAUTOCFG	0 (Nu)	Configurare automată a noilor dispozitive
QAUTOVRT	0	Numărul de descrieri de dispozitive virtuale pe care le va crea automat sistemul dacă nu este disponibil pentru a fi folosit nici un dispozitiv.
QALWOBJRST	*NONE	Dacă programele de stare sistem şi programele care adoptă autorizaţie pot fi restaurare
QDEVRCYACN	*DSCMSG (Deconectare cu mesaj)	Acţiunea sistem atunci când comunicaţiile sunt restabilite
QDSCJOBITV	120	Perioada de timp înainte ca sistemul să acţioneze la un job deconectat
QDSPSGNINF	1 (Da)	Dacă utilizatorii văd ecranul cu informaţii de semnare
QINACTITV	60	Perioada de timp înainte ca sistemul să acţioneze la un job interactiv inactiv
QINACTMSGQ	*ENDJOB	Acţiunile realizate de sistem pentru un job inactiv
QLMTDEVSSN	1 (Da)	Dacă utilizatorii sunt limitaţi la semnarea pe un singur dispozitiv la un moment dat
QLMTSECOFR	1 (Da)	Dacă utilizatorii *ALLOBJ şi *SERVICE sunt limitaţi la anumite dispozitive
QMAXSIGN	3	Câte încercări consecutive, fără succes de semnare sunt permise
QMAXSGNACN	3 (Ambele)	Dacă sistemul dezactivează dezactivează staţia de lucru sau profilul utilizator atunci când limita QMAXSIGN este atinsă.
QRMTSIGN	*FRCSIGNON	Cum manipulează sistemul o încercare de semnare la distanţă (passthrough sau TELNET).
QRMTSVRATR	0 (Off)	Permite ca sistemul să fie analizaz la distanţă.
QSECURITY [1]	50	Nivelul de securitate care este impus
QPWDEXPITV	60	Cât de des trebuie să-şi modifice utilizatorii parolele
QPWDMINLEN	6	Lungime minimă pentru parole
QPWDMAXLEN	8	Lungime maximă pentru parole
QPWDPOSDIF	1 (Da)	Dacă fiecare poziţie dintr-o parolă trebuie să difere de aceeaşi poziţie din vechea parolă
QPWDLMTCHR	Vedeţi nota 2	Caractere care nu sunt permise în parolă
QPWDLMTAJC	1 (Da)	Dacă numere adiacente sunt interzise în parole
QPWDLMTREP	2 (Nu pot fi repetate consecutiv)	Dacă sunt interzise caractere repetate în parole
QPWDRQDDGT	1 (Da)	Dacă parolele trebuie să aibă cel puţin un număr
QPWDRQDDIF	1 (32 parole unice)	Câte parole unice sunt necesare înainte ca o parolă să poată fi repetată
QPWDVLDPGM	*NONE	Programul ieşire utilizator pe care sistem îl apelează pentru a valida parolele

Note:

1. Dacă rulaţi curent cu QSECURITY de 30 sau mai puţin, revedeţi informaţiile din Capitolul 2 din această carte înainte de a modifica la un nivel de securitate mai înalt.
2. Caracterele restricţionate sunt stocate în ID CPXB302 în fişierul de mesaje QSYS/QCPFMSG. Sunt livrate ca AEIOU@$#. Puteţi folosi comanda Modificare descriere mesaj (CHGMSGD) pentru a modifica caracterele restricţionate.

Comanda CFGSYSSEC setează deasemenea parola la *NONE pentru următoarele profiluri utilizator furnizate de IBM:

QSYSOPR

QPGMR
QUSER
QSRV
QSRVBAS

În sfârşit, comanda CFGSYSSEC configurează auditarea de securitate conformcu valorile pe care le-aţi specificat folosind comanda Modificare auditare securitate(CHGSECAUD).

Modificarea programului

Dacă unele dintre aceste setări nu sunt corespunzătoare cu instalarea dumneavoastră, puteţi crea propria versiune de program care procesează comanda. Realizaţi următoarele:

__ Pasul 1. Folosiţi comanda Extragere sursă CL (RTVCLSRC) pentru a copia sursa pentru programul care rulează atunci când folosiţi comanda CFGSYSSEC. Programul pentru extragere este QSYS/QSECCFGS. Atunci când extrageţi, daţi-i un *nume diferit*.

__ Pasul 2. Editaţi programul pentru a realiza modificările. Apoi compilaţi-l. Atunci când îl compilaţi, asiguraţi-vă că *nu* înlocuiţi programul QSYS/QSECCFGS furnizat de IBM. Programul dumneavoastră ar trebuie să aibă un nume diferit.

__ Pasul 3. Folosiţi comanda Modificare comandă (CHGCMD) pentru a modifica parametrul de comandă (PGM) pentru comanda CFGSYSSEC. Setaţi valoarea PGM la numele programului dumneavoastră. De exemplu, dacă creaţi un program în biblioteca QGPL care este numit MYSECCFG, veţi introduce următoarele:

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

Notă: Dacă modificaţi programul QSYS/QSECCFGS, IBM nu poate garanta sau implica reabilitate, serviabilitate, performanţele sau funcţionabilitatea programului. Garanţiile implicate de fabricţie si potrivire cu un anumit scop nu sunt acordate explicit.

Ce face comanda Revocare autorizare publică

Puteţi folosi comanda Revocare autorizaţie publică (RVKPUBAUT) pentru a seta autorizaţia publică*EXCLUDE pentru un set de comenzi şi programe. Comanda RVKPUBAUT rulează un program care este numit QSYS/QSECRVKP. Deoare este livrat, QSECRVKP revocă autorizaţia publică (prin setarea la *EXCLUDE) pentru comenzile care sunt listate în Tabela 236 la pagina 604 şi interfeţele programabile pentru aplicaţii (API) care sunt listate în Tabela 237 la pagina 604. Atunci când soseşte sistemul dumneavoastră, aceste comenzi şi API-uri au autorizaţia publică setată la *USE.

Comenzile care sunt listate în Tabela 236 la pagina 604 şi API-urile care sunt listate în Tabela 237 la pagina 604 toate realizează funcţii pe sistemul dumneavoastră care pot furniza o opurtunitate pentru a dăuna. Ca administrator de securitate, ar trebui să autorizaţi explicit utilizatorii să ruleze aceste comenzi şi programe decât să le faceţi disponibile tuturor utilizatorilor de pe sistem.

Atunci când rulaţi comanda RVKPUBAUT, specificaţi biblioteca care conţine aceste comenzi. Biblioteca implicită este QSYS. Dacă aveţi mai mult de un limbaj naţional pe sistem, trebuie să rulaţi comanda pentru fiecare bibliotecă QSYSxxx.

Tabela 236. Comenzi ale căror autorizaţii publice sunt setate de comanda RVKPUBAUT

ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGE
ADDPJE	CHGWSE	RMVWSE
ADDRTGE	CPYCFGL	RSTLIB
ADDWSE	CRTCFGL	RSTOBJ
CHGAJE	CRTCTLAPPC	RSTS36F
CHGCFGL	CRTDEVAPPC	RSTS36FLR
CHGCFGLE	CRTSBSD	RSTS36LIBM
CHGCMNE	ENDRMTSPT	STRRMTSPT
CHGCTLAPPC	RMVAJE	STRSBS
CHGDEVAPPC	RMVCFGLE	WRKCFGL

API-urile din Tabela 237 sunt toate în biblioteca QSYS:

Tabela 237. Programe ale căror autorizaţii publice sunt setate de comanda RVKPUBAUT

QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

Pe V3R7, când rulaţi comanda RVKPUBAUT, sistemul setează autorizaţia publică pentru directorul rădăcină la *USE (numai dacă nu este deja *USE sau mai puţin).

Modificarea programului

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

__ Pasul 1. Folosiţi comanda Extragere sursă CL (RTVCLSRC) pentru a copia sursa pentru programul care ruleză atunci când folosiţi comanda RVKPUBAUT. Programul pentru a fi extras este QSYS/QSECRVKP. Atunci când îl extrageţi, daţi-i *un nume diferit*.

__ Pasul 2. Editaţi programul pentru a realiza modificările. Apoi compilaţi-l. Atunci când îl compilaţi, asiguraţi-vă că *nu* înlocuiţi programul furnizat de IBM QSYS/QSECRVKP. Programul dumneavoastră ar trebui să aibă un nume diferit.

__ Pasul 3. Folosiţi comanda Modificare comandă (CHGCMD) pentru a modifica programul să proceseze parametrul de comandă (PGM) pentru comanda RVKPUBAUT. Setaţi valoarea PGM la numele programului dumneavoastră. De exemplu, dacă creaţi un program în biblioteca QGPL care se numeşte MYRVKPGM, veţi introduce următoarele:

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

Notă: Dacă modificaţi programul QSYS/QSECRVKP, IBM nu poate garanta sau implica încredere, serviabilitate, performanţe sau funcţionabilitate pentru program. Garanţiile implicate pentru fabricare sau potrivirea cu un anumit scop nu sunt acordate explicit.

Anexa H. Observaţii

Aceste informaţii au fost elaborate pentu produsele şi serviciile oferite în S.U.A. Este posibil ca

IBM să nu ofere în alte ţări produsele, serviciile sau caracteristicile 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 este responsabilitatea utilizatorului să evalueze şi să verifice funcţionarea oricărui produs, program sau serviciu non-IBM.

IBM poate avea brevete sau aplicaţii în curs de brevetare care să acopere subiectele descrise în acest document. Oferirea acestui document nu vă conferă nici o licenţă cu privire la aceste patente. Puteţi trimite solicitări de licenţă, în scris, la:

| IBM Director of Licensing
| IBM Corporation
| North Castle Drive
| Armonk, NY 10504-1785
| U.S.A.

Pentru cererile de licenţă privind informaţii (DBCS) pe doi octeţi, contactaţi Departamentul de proprietate intelectuală IBM din ţara dumneavoastră sau trimiteţi cereri, în scris, la:

| IBM World Trade Asia Corporation
| Licensing
| 2-31 Roppongi 3-chome, Minato-ku
| Tokyo 106-0032, Japan

Următorul paragraf nu se aplică în cazul Angliei sau al altor ţări unde asemenea prevederi nu sunt în concordanţă cu legile locale:INTERNATIONAL BUSINESS MACHINES CORPORATION OFERĂ ACEASTĂ PUBLICAŢIE "CA ATARE", FARĂ NICI UN FEL DE GARANŢIE, EXPRIMATĂ SAU PRESUPUSĂ, INCLUSIV, DAR NELIMITÂNDU-SE LA ELE, GARANŢIILE IMPLICITE DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME, DE VANDABILITATE SAU DE POTRIVIRE LA UN ANUMIT SCOP. Unele state nu permit declinarea responsabilităţii pentru garanţiile exprese sau deduse în anumite tranzacţii, de aceea este posibil ca această declaraţie să nu fie valabilă în cazul dumneavoastră.

Aceste informaţii pot include inexactităţi tehnice sau erori de tipărire. Informaţiile incluse aici sunt modificate periodic; aceste modificări vor fi încorporate în noi ediţii ale publicaţiei. IBM poate aduce îmbunătăţiri şi/sau modifcări produsului (produselor) şi/sau programului (programelor) descrise în această publicaţie în orice moment fără notificare.

În cadrul acestor informaţii se face referire la site-uri Web non-IBM numai pentru a oferi ajutor, fără ca aceasta să reprezinte în vreun fel susţinerea acelor site-uri Web. Materialele de pe site-urile Web respective nu fac parte din materialelor pentru acest produs IBM, iar utilizarea acestor site-uri Web se face pe propriul risc.

IBM poate folosi sau distribui informaţiile pe care le furnizaţi în orice mod crede că este corespunzător, fără a atrage asupra sa nici o obligaţie faţă de dumneavoastră.

Posesorii de licenţă asupra acestui program care doresc să obţină informaţii despre el în scopul de a activa: (i) schimbul de informaţii între programele create independent şi alte programe (inclusiv acesta) şi (ii) folosirea mutuală a informaţiilor care au fost schimbate trebuie să contacteze:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N

Rochester, MN 55901
U.S.A.

Aceste informaţii pot fi disponibile cu condiţia repectării termenilor şi condiţiilor, iar în unele cazuri cu plata unor taxe.

Programul cu licenţă descris în aceste informaţii şi toate materialele licenţiate disponibile pentru el sunt furnizate de către IBM conform termenilor IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code sau orice acord echivalent între noi.

Toate datele de performanţă din acest document au fost determinate într-un mediu controlat. De aceea, rezultatele obţinute în alte medii de funcţionare pot fi diferite. Unele măsurători s-ar putea să fi fost făcute pe sisteme la nivel de dezvoltare şi nu există nici o garanţie că aceste măsurători vor fi identice pe sistemele disponibile pe piaţă. Mai mult decât atât, unele măsurători s-ar putea să fi fost estimate prin extrapolare. Rezultatele reale pot fi diferite. Utilizatorii acestui document trebuie să verifice datele aplicabile pentru mediul lor specific.

Informaţiile privind produsele non-IBM au fost obţinute de la furnizorii acestor produse, din anunţurile lor publicate sau din alte surse disponibile publicului. IBM 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.

Toate declaraţiile privind direcţiile de viitor şi intenţiile IBM-ului pot fi schimbate sau se poate renunţa la ele, fără notificare prealabilă şi reprezintă doar scopuri şi obiective.

Toate preţurile IBM arătate sunt preţurile cu amănuntul sugerate de IBM, sunt curente şi pot fi modificate fără notificare. Preţurile dealer-ului pot fi diferite.

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.

LICENŢĂ COPYRIGHT:

Aceste informaţii conţin exemple de programe de aplicaţii în limbaje sursă, care ilustrează tehnici de programare pe diferite platforme de operare. Puteţi copia, modifica şi distribui aceste exemple de programe sub orice formă fără să plătiţi ceva către IBM, în scopul dezvoltării, folosirii, promovării sau distribuirii programelor de aplicaţie conforme cu interfaţa de programare a aplicaţiilor pentru platforma de operare pentru care au fost scrise exemplele de program. Aceste exemple nu au fost testate amănunţit în toate condiţiile. De aceea, IBM nu poate garanta sau sugera că acestea sunt fiabile, capabile de service sau funcţionale.

EXCEPTÂND GARANŢIILE OBLIGATORII, CARE NU POT FI EXCLUSE, IBM, DEZVOLTATORII DE PROGRAME ŞI FURNIZORII SĂI NU ACORDĂ NICI O GARANŢIE SAU CONDIŢIE, EXPRESĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANŢIILE SAU CONDIŢIILE IMPLICITE DE VANDABILITATE, DE POTRIVIRE PENTRU UN ANUMIT SCOP SAU DE NEÎNCĂLCARE A UNUI DREPT, REFERITOARE LA PROGRAM SAU LA SUPORTUL TEHNIC, DACĂ ESTE CAZUL.

ÎN NICI O ÎMPREJURARE IBM, DEZVOLTATORII SĂI DE PROGRAME SAU FURNIZORII NU VOR FI RESPONSABILI PENTRU ORICARE DINTRE URMĂTOARELE PAGUBE, CHIAR DACĂ AU FOST INFORMAŢI ÎN LEGĂTURĂ CU POSIBILITATEA PRODUCERII LOR:

1. PIERDEREA SAU DETERIORAREA DATELOR;
2. PAGUBE SPECIALE, ACCIDENTALE SAU INDIRECTE SAU PREJUDICII ECONOMICE DE CONSECINŢĂ; SAU

3. PIERDERI REFERITOARE LA PROFIT, AFACERI, BENEFICII, REPUTAŢIE SAU ECONOMII PLANIFICATE.

UNELE JURISDICŢII NU PERMIT EXCLUDEREA SAU LIMITAREA PREJUDICIILOR INCIDENTALE SAU INDIRECTE, CAZ ÎN CARE ESTE POSIBIL CA UNELE SAU TOATE LIMITĂRILE SAU EXCLUDERILE DE MAI SUS SĂ NU FIE VALABILE PENTRU DUMNEAVOASTRĂ.

Fiecare copie sau orice porţiune din aceste exemple de pogram sau orice lucrare derivată din acestea trebuie să includă un anunţ de copyright de genul următor:

Dacă vizualizaţi aceste informaţii folosind o copie electronică, fotografiile şi ilustraţiile color s-ar putea să nu apară.

Mărci comerciale

Următorii termeni sunt mărci comerciale ale International Business Machines Corporation în Statele Unite, în alte ţări sau ambele:

- 400
- AIX
- AS/400
- COBOL/400
- DB2
- DB2 Universal Database
- Domino
- DRDA
- e(logo)server
- eServer
- i5/OS
- IBM
- iSeries
- Lotus
- MQSeries
- MVS
- NetServer
- Notes
- OfficeVision
- Operating System/400
- OS/2
- OS/400
- Print Services Facility
- PrintManager
- Redbooks
- RPG/400
- SAA
- SecureWay
- SQL/400
- System/36
- System/38
- SystemView
- WebSphere
- zSeries

Microsoft, Windows, Windows NT şi emblema (logo) Windows sunt mărci comerciale ale Microsoft Corporation în Statele Unite, în alte ţări sau ambele.

Java şi toate mărcile comerciale bazate pe Java sunt mărci comerciale ale Sun Microsystems, Inc. în Statele Unite, în alte ţări sau ambele.

Linux este marcă comercială a lui Linus Torvalds în Statele Unite, în alte ţări sau ambele.

Alte nume de companii, produse sau servicii ar putea fi mărci comerciale sau mărci de serviciu ale altora.

Termenii şi condiţiile pentru descărcarea şi tipărirea informaţiilor

Permisiunile pentru folosirea informaţiilor pe care le-aţi selectat pentru descărcare sunt acordate în următorii termeni şi condiţii şi cu indicarea acceptării lor de către dumneavoastră.

Uz personal: Puteţi reproduce aceste informaţii pentru uzul dumneavoastră personal şi necomercial cu condiţia ca toate notele de proprietate să fie păstrate. Nu puteţi distribui, afişa sau face lucrări derivative din aceste informaţii sau orice alte porţiuni din ele, fără acordul explicit al IBM.

Uz comercial: Puteţi reproduce, distribui şi afişa aceste informaţii doar în întreprinderea dumneavoastră cu condiţia ca toate notele de proprietate să fie păstrate. Nu puteţi face lucrări derivative ale acestor informaţii, sau să reproduceţi, să distribuiţi sau să afişaţi aceste informaţii sau orice alte porţiuni din ele în afara întreprinderii dumneavoastră, fără acordul explicit al IBM.

Cu excepţia acestei permisiuni explicite, nici o altă permisiune, licenţă sau drepturi nu sunt acordate, fie explicite sau implicite, pentru informaţii sau alte date, software sau alte proprietăţi intelectuale conţinute în acestea.

IBM îşi păstrează dreptul de a retrage permisiunile acordate aici oricând, la discreţia sa, dacă folosirea Publicaţiilor este în detrimentul intereselor sale sau, după cum este determinat de IBM sau dacă instrucţiunile de mai sus nu sunt urmate corespunzător.

Nu puteţi descărca, exporta sau re-exporta 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 INFORMAŢII. PUBLICAŢIILE SUNT FURNIZATE ″AŞA CUM SUNT″ ŞI FĂRĂ GARANŢIE DE NICI UN FEL, FIE EXPLICITĂ, FIE IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA ELE, GARANŢIILE SUBÎNŢELESE DE NEÎNCĂLCARE A UNUI DREPT, DE VANDABILITATE SAU DE POTRIVIRE PENTRU UN ANUMIT SCOP.

Toate materialele au copyright IBM Corporation.

Prin descărcarea sau tipărirea de informaţii de pe acest sit, v-aţi dat acordul pentru aceşi termeni şi aceste condiţii.

Informaţii înrudite

Ar putea fi nevoie să citiţi alte cărţi IBM pentru mai multe informaţii detaliate despre un anumit subiect. Următoarele cărţi IBM iSeries conţin informaţii de care aţi putea avea nevoie.

Securitatea avansată

- *Tips and Tools for Securing Your iSeries*, SC41-5300-07furnizează un set de sugestii practice pentru utilizarea caracteristicilor de securitate ale iSeries şi pentru stabilirea procedurilor de operare legate de securitate. Această carte descrie de asemenea cum se face setarea şi utilizarea securităţii şi a uneltelor de securitate care fac parte din OS/400. Vedeţi iSeries: CD-ROM manuale suplimentare Centrul de informare.
- *Implementing iSeries 400 Security, 3rd Edition* de Wayne Madden şi Carol Woodbury. Loveland, Colorado: 29th Street Press, o divizie a Duke Communication International, 1998. Furnizează îndrumări şi sugestii practice pentru planificarea, setarea şi gestionarea securităţii iSeries.

  Număr de comandă ISBN
  1–882419–78–2

Salvarea de rezervă şi recuperarea

- *Backup and Recovery*, SC41-5304-07 furnizează informaţii despre planificarea unei strategii de salvare de rezervă şi de recuperare, despre salvarea informaţiilor din sistemul dumneavoastră şi despre recuperarea sistemului, a pool-urilor de memorie auxiliară şi a opţiunilor de protejare a discului. Vedeţi iSeries: CD-ROM manuale suplimentare Centrul de informare.
- Informaţii suplimentare de salvare de rezervă şi de recuperare pot fi găsite în Centrul de informare. Vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru informaţii suplimentare.

Informaţii privind securitatea de bază şi securitatea fizică

- Subiectul Securitatea de bază a sistemului şi planificarea din Centrul de informare explică de ce este necesară securitatea, defineşte conceptele importante şi furnizează informaţii despre planificarea, implementarea şi monitorizarea securităţii de bază în sistem. Vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii.

Programul licenţait iSeries Access pentru Windows

- Subiectul iSeries Access pentru Windows din Centrul de informare furnizează informaţii tehnice despre programele iSeries Access pentru Windows pentru toate versiunile de iSeries Access pentru Windows. Vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii.

Comunicaţiile şi conectarea în reţea

- *SNA Distribution Services*, SC41-5410-01 furnizează informaţii despre configurarea unei reţele pentru SNADS (Systems Network Architecture distribution services) şi configurarea unei punţi VM/MVS (Virtual Machine/Multiple Virtual Storage). În plus, sunt discutate funcţiile de distribuire a obiectelor, serviciile pentru biblioteca de documente şi serviciile pentru directorul de distribuţie sistem.
- *Remote Work Station Support*, SC41-5402-00 furnizează informaţii despre cum se face setarea şi utilizarea suportului pentru staţie de lucru la distanţă, cum ar fi passthrough staţie de afişare, facilitate de comandă gazdă distribuită şi ataşament la distanţă 3270. Vedeţi iSeries: CD-ROM manuale suplimentare Centrul de informare.
- Centrul de informare furnizează informaţii despre procesarea de fişiere la distanţă. El descrie cum se face definirea unui fişier la distanţă în DDM (distributed data management) OS/400, cum se face crearea unui fişier DDM, ce utilitare de fişiere sunt suportate prin DDM şi cerinţele DDM OS/400 în raport cu alte sisteme. Vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii.
- Centrul de informare furnizează informaţii care descriu cum se face utilizarea şi configurarea TCP/IP şi a mai multor aplicaţii TCP/IP, cum ar fi FTP, SMTP şi TELNET. Vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii.

Criptarea

- *Cryptographic Support/400*, SC41-3342-00 descrie capabilităţile de securitate de date ale produsului program cu licenţă Cryptographic Facility. El explică cum se face utilizarea facilităţii şi furnizează informaţii de referinţă pentru programatori. Vedeţi iSeries: CD-ROM manuale suplimentare Centrul de informare.

Operaţiile de sistem generale

- ″Operaţiile de sistem de bază″ din Centrul de informare furnizează informaţii privind modul în care se face pornirea şi oprirea sistemului şi cum se face tratarea problemelor de sistem. Vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii suplimentare.

Instalarea programelor livrate de IBM şi configurarea sistemului

- *Local Device Configuration*, SC41-5121-00 furnizează informaţii despre cum se face o configurare iniţială şi cum se face modificarea acelei configuraţii. Conţine de asemenea informaţii conceptuale despre configurarea dispozitivelor. Vedeţi iSeries: CD-ROM manuale suplimentare Centrul de informare.
- *Install, upgrade, or delete OS/400 and related software*, SC41-5120-08 furnizează proceduri pas-cu-pas pentru instalarea iniţială, pentru instalarea programelor cu licenţă, pentru PTF-uri şi pentru limbi secundare de la IBM. Vedeţi iSeries: CD-ROM manuale suplimentare Centrul de informare.

Sistemul de fişiere integrat

- Subiectele Sisteme de fişiere şi Administrare din Centrul de informare furnizează o privire generală asupra sistemul de fişiere integrat, inclusiv ce este, cum poate fi folosit şi ce interfeţe sunt disponibile. Vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii.

Internetul

- *AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet* SG24–4929 discută problemele legate de securitate şi riscurile conectării serverului iSeries la Internet. Vi se oferă exemple, recomandări, sugestii şi tehnici pentru aplicaţii.
- *iSeries and the Internet*, G325–6321, vă ajută să vă rezolvaţi problemele potenţiale de securitate pe care le puteţi avea la conectarea iSeries la Internet. Pentru informaţii suplimentare, vizitaţi următoarea pagină de bază IBM I/T (Information Technology) Security : `http://www.ibm.com/security`
- *Cool Title About the AS/400 and Internet*, SG24-4815, vă poate ajuta să înţelegeţi şi apoi să utilizaţi Internetul (sau reţeaua dumneavoastră internă) de pe iSeries. Vă ajută să înţelegeţi cum se folosesc funcţiile şi caracteristicile. Această carte vă iniţiază pentru a folosi e-mail-ul, transferul de fişiere, emularea de terminal, gopher, HTTP şi 5250 pentru gateway HTML.

IBM Lotus Domino

- URL-ul http://www.lotus.com/ldd/doc furnizează informaţii despre Lotus Notes, Domino şi IBM Domino pentru iSeries. Din acest site web puteţi descărca informaţii în formatul de bază de date Domino (.NSF) şi în formatul Adobe Acrobat (.PDF), puteţi căuta în baza de date şi puteţi afla cum puteţi obţine manuale tipărite.

Suportul optic

- *Optical Support*, SC41-5310-04 furnizează informaţii despre funcţii care sunt unice pentru *Optical Support*. Conţine de asemenea informaţii folositoare pentru utilizarea şi înţelegerea dispozitivelor CD, a dispozitivelor de bibliotecă de mediu optic ataşate direct şi a dispozitivelor de bibliotecă de mediu optic ataşate la LAN. Vedeţi iSeries: CD-ROM manuale suplimentare Centrul de informare.

Tipărirea

- Centrul de informare furnizează informaţii despre elementele şi conceptele de tipărire ale sistemului, despre suportul de fişier imprimantă şi de spool de tipărire pentru operaţiile de tipărire şi despre conectarea imprimantei. Vedeţi “Cerinţe preliminare şi informaţii înrudite” la pagina xvi pentru detalii.

Programarea

- *CL Programming*, SC41-5721-06, furnizează o discutare amplă a subiectelor de programare, incluzând o discuţie generală asupra obiectelor şi a bibliotecilor, asupra programării CL, asupra controlului de flux şi a comunicaţiei între programe, asupra gestionării obiectelor din programele CL şi asupra creării de programe CL. Alte subiecte includ mesajele predefinite şi improvizate şi tratarea mesajelor, definirea şi crearea de comenzi şi meniuri definite de utilizator, testarea aplicaţiilor, incluzând modul de depanare, puncte de întrerupere, urmăriri şi

funcţii de afişare. Vedeţi iSeries: CD-ROM manuale suplimentare Centrul de informare.

- Subiectul CL din Centrul de informare (vedeţi "Cerinţe preliminare şi informaţii înrudite" la pagina xvi pentru detalii) furnizează o descriere completă a limbajului CL (control language - limbaj de control) iSeries şi a comenzilor lui din OS/400. Comenzile OS/400 sunt utilizate pentru a accesa funcţii ale programului licenţiat Operating System/400 (5738-SS1). Toate comenzile CL non-OS/400 — acelea asociate cu celelalte programe cu licenţă, incluzând toate limbile şi diversele utilitare — sunt descrise în alte cărţi care suportă acele programe cu licenţă.
- Subiectul Programare din Centrul de informare furnizează informaţii despre multe dintre limbajele şi utilitarele disponibile în iSeries. El conţine rezumate ale:
  - Tuturor comenzilor CL iSeries (din programele OS/400 şi din toate celelalte programe cu licenţă), sub diferite forme.
  - Informaţiilor înrudite cu comenzile CL, cum ar fi mesajele de eroare care pot fi monitorizate de fiecare comandă şi fişierele livrate de IBM care sunt utilizate de unele comenzi.
  - Obiectelor livrate de IBM, incluzând biblioteci.
  - Valorilor sistem livrate de IBM.
  - Cuvintelor cheie DDS pentru fişiere fizice, logice, de afişare, de imprimantă şi ICF.
  - Instrucţiunilor REXX şi ale funcţiilor încorporate.
  - Altor limbaje (cum ar fi RPG) şi altor utilitare (cum ar fi SEU şi SDA).
- Centrul de informare conţine mai multe subiecte privind Administrarea sistemelor şi Controlul funcţionării din iSeries. Unele din aceste subiecte includ colecţii de date de performanţă, administrare de valori sistem şi administrare de spaţiu de stocare. Pentru detalii despre accesarea Centrului de informare, vedeţi "Cerinţe preliminare şi informaţii înrudite" la pagina xvi.
- *Work Management*, SC41-5306-03 furnizează informaţii despre cum se face crearea şi modificarea unui mediu de administrare a operaţiilor. Vedeţi iSeries: CD-ROM manuale suplimentare Centrul de informare.
- Subiectul API din Centrul de informare (vedeţi "Cerinţe preliminare şi informaţii înrudite" la pagina xvi pentru detalii) furnizează informaţii despre cum se face crearea, utilizarea şi ştergerea obiectelor care ajută la gestionarea performanţei de sistem, utilizarea eficientă a spool-ului şi întreţinerea eficientă a fişierelor bază de date. Această carte include de asemenea informaţii despre crearea şi întreţinerea de programe pentru obiectele sistem şi despre extragerea OS/400 informaţiilor prin operaţii cu obiecte, fişiere bază de date, joburi şi fişiere spool.

Utilitare

- *ADTS for AS/400: Source Entry Utility*, SC09-2605-00furnizează informaţii despre folosirea utilitarului SEU (source entry utility) din ADT (Application Development Tools) pentru a crea şi edita membrii sursă. Cartea explică cum se face pornirea şi terminarea unei sesiuni SEU şi cum se face utilizarea numeroaselor caracteristici ale acestui editor de text. Cartea conţine exemple pentru a ajuta atât utilizatorii noi, cât şi pe cei experimentaţi să realizeze diverse operaţii de editare, de la cele mai simple comenzi de linie până la utilizarea prompturilor predefinite pentru limbajele de nivel înalt şi pentru formate de date. Vedeţi iSeries: CD-ROM manuale suplimentare Centrul de informare.
- Subiectul Bază de date DB2 Universal pentru iSeries din Centrul de informare furnizează o privire generală despre cum se face proiectarea, scrierea, rularea şi testarea instrucţiunile SQL/400*. Descrie de asemenea SQL interactiv (Structured Query Language) şi furnizează exemple despre cum se scriu instrucţiunile SQL în programe COBOL, RPG, C, FORTRAN şi PL/I. Vedeţi "Cerinţe preliminare şi informaţii înrudite" la pagina xvi pentru detalii.
- Subiectul Bază de date DB2 Universal pentru iSeries din Centrul de informare furnizează informaţii despre cum se face:
  - Construirea, întreţinerea şi rularea de interogări SQL
  - Crearea de rapoarte de la cele mai simple la cele complexe
  - Construirea, actualizarea, gestionarea, interogarea şi raportarea în tabelele bazei de date, utilizând o interfaţă bazată pe formulare
  - Definirea şi modelarea interogărilor SQL şi a rapoartelor pentru includerea în programe de aplicaţie

  Vedeţi "Cerinţe preliminare şi informaţii înrudite" la pagina xvi pentru detalii.

Index

Caractere speciale

A

B

C

D

E

F

G

H

I

Î

J

L

M

N

O

P

Q

R

S

Ş

T

U

V

W

Z

Comentarii cititori

iSeries
Referinţe privind securitatea
Versiunea 5

Publicaţia nr. SA12-6497-08

Apreciem comentariile dumneavoastră despre această publicaţie. Nu ezitaţi să ne trimiteţi comentariile despre anumite erori sau lipsuri, despre claritatea, organizarea şi conţinutul subiectelor din această carte. Comentariile pe care le trimiteţi trebuie să se refere la informaţiile din acest manual şi la modul în care sunt prezentate.

Pentru întrebări cu caracter tehnic şi informaţii despre produse şi preţuri vă rugăm să luaţi legătura cu sucursala IBM din localitatea dumneavoastră, cu partenerul de afaceri IBM sau cu reprezentantul de vânzări autorizat.

Pentru întrebări generale, vă rugăm sunaţi la ″Hallo IBM″ (număr de telefon 01803/313233).

Când trimiteţi comentarii la IBM, acordaţi IBM-ului dreptul ne-exclusiv de a utiliza sau distribui aceste comentarii în orice mod pe care îl consideră corespunzător, fără ca din aceasta să rezulte vreo obligaţie faţă de dumneavoastră.

Comentarii:

Vă mulţumim pentru ajutorul acordat.

Pentru a trimite comentariile:
- Trimiteţi comentariile la adresa de pe spatele acestui formular.
- Trimiteţi un fax la următorul număr: Alte ţări: 1-507-253-5192
- Trimiteţi comentariile prin e-mail la: RCHCLERK@us.ibm.com

Dacă doriţi un răspuns de la IBM, vă rugăm să completaţi următoarele informaţii:

Nume	Adresă
Companie sau organizaţie	
Număr de telefon	Adresă de e-mail

Comentarii cititori
SA12-6497-08

IBM

IBM CORPORATION
ATTN DEPT 542 IDCLERK
3605 HWY 52 N
ROCHESTER MN

Tipărit în S.U.A.

SA12-6497-08