System i

Securitatea
Referinţă securitate

Versiunea 6 Ediţia 1

SA12-6497-10

System i

Securitatea
Referinţă securitate

Versiunea 6 Ediţia 1

SA12-6497-10

Notă

Înainte de a folosi aceste informaţii şi produsul la care se referă, citiţi informaţiile din Anexa I, “Observaţii”, la pagina 717.

Această ediţie este valabilă pentru IBM i5/OS (număr de produs 5761-SS1) versiunea 6, ediţia 1, modificarea 0 şi pentru toate ediţiile şi modificările ulterioare până se specifică altceva în noile ediţii. Această versiune nu rulează pe toate modelele RISC şi nici pe modelele CISC.

Această ediţie înlocuieşte SC41-5302-09.

Cuprins

Ce este nou în V6R1

Citiţi despre informaţiile noi sau modificate semnificativ în colecţia de subiecte Referinţă securitate.

Valori de sistem noi

Blocare modificare parolă (QPWDCHGBLK)
Valoarea de sistem Blocare modificare parolă (QPWDCHGBLK) specifică perioada de timp cât este blocată modificarea unei parole după o modificare anterioară.

Avertisment expirare parolă (QPWDEXPWRN)
Valoarea de sistem Avertisment expirare parolă (QPWDEXPWRN) specifică la câte zile înainte de expirarea parolei începe afişarea mesajelor privind expirarea parolei atunci când se loghează un utilizator.

Reguli parole (QPWDRULES)
Valoarea de sistem Reguli parole (QPWDRULES) specifică regulile folosite pentru a verifica dacă o parolă este formată corect. Puteţi specifica mai multe valori pentru QPWDRULES, dacă nu specificaţi *PWDSYSVAL.

Listă specificare cifru SSL (QSSLCSL)
Valoarea de sistem Listă specificare cifru SSL (QSSLCSL) determină ce listă de specificare cifru va fi suportată de System SSL.

Control cifru SSL (QSSLCSLCTL)
Valoarea de sistem Control cifru SSL (QSSLCSLCTL) specifică dacă sistemul sau utilizatorul controlează valoarea de sistem Listă specificare cifru SSL (QSSLCSL).

Protocoale SSL (QSSLPCL)
Valoarea de sistem Protocoale SSL (QSSLPCL) specifică protocoalele SSL suportate de System SSL.

Cum puteţi vedea ce este nou sau modificat

Pentru a vă ajuta să vedeţi unde au fost făcute modificări tehnice, centrul de informare foloseşte:

- Imaginea » pentru a marca locul unde încep informaţiile noi sau modificate.
- Imaginea «, pentru a marca locul în care se termină informaţiile noi sau modificate.

În fişierele PDF, puteţi vedea bare de revizuire (|) în marginea din stânga a informaţiilor noi sau modificate.

Capitolul 1. Introducere în securitatea System i

Familia de sisteme IBM acoperă un interval larg de utilizatori. Securitatea pe platforma System i este suficient de flexibilă pentru a îndeplini cerinţele acestui interval larg de utilizatori şi situaţii.

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. Trebuie să înţelegeţi caracteristicile şi opţiunile disponibile, astfel încât să le puteţi adapta la cerinţele dumneavoastră de securitate.

Securitatea sistemului are trei obiective importante:

Confidenţialitatea:
- Protejarea împotriva dezvăluirii informaţiilor către persoane neautorizate
- Restricţionarea accesului la informaţiile confidenţiale
- Protejarea faţă de utilizatorii de sistem curioşi şi persoanele străine

Integritatea:
- Protejarea împotriva modificărilor neautorizate de date
- Restricţionarea manipulării datelor la programele autorizate
- Asigurarea că datele sunt de încredere

Disponibilitatea:
- Prevenirea modificărilor accidentale sau a distrugerii datelor
- Protejarea împotriva încercărilor persoanelor străine de a folosi abuziv sau a distruge resursele sistemului

Securitatea sistemului este deseori asociată cu ameninţări externe, cum ar fi cele reprezentate de hacker-i sau firme concurente. Însă adesea principalul beneficiu al unui sistem de securitate bine conceput este protejarea împotriva accidentelor de sistem produse de utilizatorii de sistem autorizaţi. Într-un sistem fără caracteristici de securitate corespunzătoare, apăsarea unei taste greşite ar putea determina ştergerea unor informaţii importante. Securitatea sistemului poate împiedica acest tip de accidente.

Nici cele mai bune funcţii de sistem pentru securitate nu pot duce la rezultate bune fără o bună planificare. Securitatea setată pe porţiuni mici, fără planificare, poate crea confuzie. Este dificil de întreţinut şi de auditat. Planificarea nu înseamnă 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. Această colecţie de subiecte conţine recomandări pentru a aduce sistemul la un nivel rezonabil de securitate. Când evaluaţi recomandările, ţineţi cont de cerinţele de securitate ale instalării dumneavoastră.

Securitatea fizică

Securitatea fizică include protejarea unităţii sistem, a dispozitivelor sistemului şi a mediilor de stocare cu copii de rezervă faţă de deteriorarea accidentală sau intenţionată. Majoritatea măsurilor pe care le luaţi pentru a asigura securitatea fizică a sistemului dumneavoastră sunt externe sistemului. Însă sistemul este echipat şi cu o cheie IPL, care împiedică executarea unor funcţii neautorizate de la unitatea de sistem.

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

Informaţii înrudite

Planificarea securităţii fizice

Securitatea cheii IPL

Puteţi extrage şi modifica poziţia cheii IPL folosind API-ul QWCRIPLA (Extragere atribute IPL) sau comanda CHGIPLA (Modificare atribute IPL).

Cheia IPL de pe panoul de control 940x controlează accesul la diverse funcţii ale panoului de control al sistemului.

Caracteristica pentru cheie IPL vă permite accesul de utilizator de la distanţă la funcţii suplimentare, disponibile de la panoul de control. De exemplu, se poate controla de unde va realiza maşina IPL-ul şi în ce mediu, i5/OS sau DST (Dedicated Service Tools - Unelte de service dedicate).

Valoarea de sistem i5/OS QRMTSRVATR controlează accesul de la distanţă. La livrare, această valoare este dezactivată, nefiind permisă ignorarea 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.

Referinţe înrudite

“Atributul de service la distanţă (QRMTSRVATR)” la pagina 39
Atributul de service la distanţă (QRMTSRVATR) controlează posibilitatea de a analiza de la distanţă problemele de service ale sistemului. Valoarea permite analizarea sistemului de la distanţă.

Nivelul de securitate

Platforma System i oferă cinci niveluri de securitate. Prin setarea valorii de sistem QSECURITY, puteţi alege ce nivel de securitate doriţi să aplice sistemul.

Nivelul 10:
Nivelul 10 nu mai este suportat.

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 destinat platformelor System i cu cerinţe mari de securitate, fiind conceput să îndeplinească cerinţele de securitate Common Criteria (CC).

Referinţe înrudite

Capitolul 2, “Folosirea valorii de sistem QSecurity”, la pagina 9
Puteţi alege gradul de securitate pe care doriţi să îl impună sistemul prin setarea valorii de sistem QSECURITY (security level - nivel de securitate).

Valorile de sistem

Valorile de sistem permit personalizarea multor caracteristici ale platformei System i. Puteţi folosi valorile de sistem pentru a defini setările de securitate pentru tot sistemul.

De exemplu, puteţi specifica următoarele setări:

- 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.

Concepte înrudite

Capitolul 3, “Valorile de sistem de securitate”, la pagina 23
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.

Semnarea

Puteţi impune integritatea prin semnarea obiectelor software pe care le folosiţi.

O componentă cheie a securităţii este *integritatea*: posibilitatea de a vă asigura că obiectele din sistem nu au fost modificate. Software-ul sistemului de operare System i este protejat prin semnături digitale.

Semnarea software-ului este importantă mai ales dacă obiectul a fost transmis prin Internet sau a fost stocat pe un mediu despre care credeţi că a fost modificat. Semnătura digitală poate fi folosită pentru a detecta modificarea obiectului.

Semnăturile digitale şi utilizarea lor pentru verificarea integrităţii software-ului pot fi gestionate 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 să optaţi pentru semnarea programelor (toate programele licenţiate livrate cu sistemul sunt semnate).

Puteţi restricţiona adăugarea semnăturilor digitale într-un depozit de certificate digitale folosind API-ul Adăugare verificator şi puteţi restricţiona resetarea parolelor pentru depozitul de certificate digitale. SST (System Service Tools - Unelte de service sistem) furnizează o nouă opţiune de meniu, numită ″Work with system security″ (Lucru cu securitate sistem), unde puteţi restricţiona adăugarea certificatelor digitale.

Informaţii înrudite

Folosirea semnăturilor digitale pentru a proteja integritatea software-ului

Digital Certificate Manager

Activarea semnării unice

Semnarea unică este un proces de autentificare în care un utilizator poate accesa mai multe sisteme introducând o singură dată ID-ul de utilizator şi parola. În reţele eterogene din zilele noastre, cu sisteme partiţionate şi mai multe platforme, administratorii trebuie să rezolve complexităţile gestionării identificării şi autentificării pentru utilizatorii de reţea.

Pentru a activa un mediu de semnare unică, IBM furnizează două tehnologii care lucrează împreună, pentru a permite utilizatorilor să se logheze cu numele de utilizator şi parola Windows şi apoi să fie autentificaţi pe platformele System i

din reţea. NAS (Network Authentication Service) şi EIM (Enterprise Identity Mapping) sunt cele două tehnologii pe care trebuie să le configureze un administrator pentru a activa un mediu de semnare unică. Windows 2000, Windows XP, AIX şi z/OS folosesc protocolul Kerberos pentru a autentifica utilizatorii în reţea. Un sistem securizat, centralizat, numit centru de distribuire a cheilor, îi autentifică în reţea pe principali (utilizatorii Kerberos).

NAS permite unei platforme System i să participe în regiunea Kerberos, iar EIM furnizează un mecanism pentru asocierea principalilor Kerberos cu un singur identificator EIM, care reprezintă utilizatorul respectiv în întreaga întreprindere. Identificatorului EIM îi pot fi asociate şi alte identităţi de utilizator, cum ar fi un nume de utilizator i5/OS. Când un utilizator se loghează în reţea şi accesează o platformă System i, nu este promptat pentru un ID de utilizator şi o parolă. Dacă autentificarea Kerberos reuşeşte, aplicaţiile pot căuta asocierea cu identificatorul EIM pentru a găsi numele de utilizator i5/OS. Utilizatorul nu mai are nevoie de o parolă pentru a se loga pe platforma System i, deoarece este deja autentificat prin protocolul Kerberos. Administratorii pot gestiona central identităţile de utilizator cu EIM, iar utilizatorii din reţea trebuie să gestioneze o singură parolă. Puteţi activa semnarea unică prin configurarea tehnologiilor NAS şi EIM pe sistem.

Informaţii înrudite

Scenariu: Crearea unui mediu de test cu semnare unică

Profilurile de utilizator

Pe sistemul de operare i5/OS, 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. Următoarea listă descrie unele dintre caracteristicile de securitate importante 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.

Concepte înrudite

Capitolul 4, “Profilurile de utilizator”, la pagina 73
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.

Profiluri de grup

Un *profil de grup* este un tip special de profil de utilizator. În loc să acordaţi autorizarea fiecărui utilizator individual, puteţi folosi un profil de grup ca să definiţi autorizarea pentru un grup de utilizatori.

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.

Concepte înrudite

“Planificarea profilurilor de utilizator” la pagina 238
Un profil de grup este o unealtă folositoare când mai mulţi utilizatori au cerinţe de securitate similare. Puteţi crea direct fişiere grup sau puteţi face un profil existent un profil de grup. Când folosiţi profiluri de grup, puteţi gestiona autorizarea mai eficient şi reduce numărul de autorizări private individuale pentru obiecte.

“Dreptul de proprietate al grupului asupra obiectelor” la pagina 143
Acest subiect furnizează informaţii detaliate despre dreptul de proprietate al grupului asupra obiectelor.

“Grupul primar pentru un obiect” la pagina 144
Puteţi specifica un grup primar pentru un obiect.

“Copierea profilurilor de utilizator” la pagina 118
Puteţi crea un profil de utilizator copiind alt profil de utilizator sau profil de grup.

Securitatea resurselor

Capacitatea de a accesa un obiect este numită *autorizare*. Securitatea resurselor în sistemul de operare i5/OS vă permite să controlaţi autorizările obiectelor, care definesc cine poate folosi ce obiecte şi cum pot fi folosite acele obiecte.

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. Următoarea listă descrie caracteristicile securităţii resurselor:

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

Liste de autorizare
Obiectele cu nevoi similare de securitate trebuie să fie grupate într-o listă. Autorizare poate fi acordată listei în loc de a fi acordată obiectelor individuale.

Proprietate asupra obiectului
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 responsabilitatea pentru securitatea informaţiilor dumneavoastră.

Grup primar
Puteţi specifica un grup primar pentru un obiect. Autorizarea grupului primar este stocată cu obiectul. Utilizarea grupurilor primare poate simplifica administrarea autorizărilor 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 apoi să securizaţi 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 eficient de a securiza informaţiile, oferind o performanţă bună.

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.

Păstrător de autorizare
Un păstrător de autorizare stochează informaţiile de autorizare pentru un fişier de bază de date descris de

program. Informaţiile de autorizare rămân chiar dacă fişierul este şters. Păstrătorii 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. Puteţi folosi instrucţiuni SQL pentru a gestiona această autorizare.

Concepte înrudite

Capitolul 5, “Securitatea resurselor”, la pagina 131
Această secţiune descrie fiecare dintre componentele securităţii resurselor şi cum funcţionează împreună pentru a proteja informaţiile despre sistem. Explică de asemenea cum să se utilizeze comanda CL şi afişează organizarea de securitate resursă pe sistemul dvs.

Jurnalul de auditare de securitate

Puteţi folosi jurnalele de auditare de securitate pentru a audita eficienţa securităţii sistemului.

Sistemul de operare i5/OS oferă posibilitatea de a înregistra într-un jurnal de auditare de securitate evenimente de securitate selectate. Mai multe valori de sistem, valori de profil de utilizator şi valori de obiecte controlează ce evenimente sunt înregistrate în jurnal.

Concepte înrudite

Capitolul 9, “Auditarea securităţii pe System i”, la pagina 257
Această secţiune descrie tehnici pentru auditarea eficienţei securităţii de pe sistemul dumneavoastră.

Securitatea Common Criteria

Common Criteria este un cadru de lucru pentru evaluarea independentă, analizarea şi testarea produselor pe baza unui set de cerinţe de securitate.

Pe data de 10 august 2005, IBM a primit pentru i5/OS V5R3M0 certificarea Common Criteria Evaluated Assurance Level (EAL) 4, plus ALC_FLR.2 CAPP (Controlled Access Protection Profile), Versiunea 1.d, 8 octombrie 1999. Pentru a achiziţiona sistemul evaluat, comandaţi Common Criteria FC 1930 sub 5722-SS1.

Clienţii ar trebui să comande acest număr de caracteristică numai dacă este necesară rularea în configuraţie Common Criteria.

Produsul apare pe pagina Validated Products List de pe situl Web Common Criteria Evaluation and Validation Scheme(http://www.nsa.gov/ia/industry/niap.cfm).

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 independent* (iASP) şi *pool de discuir 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. Începând cu V5R2, modificările funcţionale aduse pool-urilor de discuri independente au implicaţii asupra securităţii sistemului. 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. Utilizatorul nu va avea nici o autorizare specială şi parola va fi setată la *NONE.

Pool-urile de disc independente suportă multe obiecte bazate pe bibliotecă şi sisteme de fişiere definite de utilizator. Există însă mai multe obiecte care nu sunt permise pe pool-urile de discuri independente. În i5/OS V5R1, puteţi folosi pool-uri de disc independente doar cu sisteme de fişiere definite de utilizator.

Informaţii înrudite

Tipurile de obiecte suportate şi nesuportate

Capitolul 2. Folosirea valorii de sistem QSecurity

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

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.

Nivelurile de securitate

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 40 de securitate” la pagina 14.

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. Nivelurile de securitate: compararea funcţiilor

Funcţia	Nivelul 20	Nivelul 30	Nivelul 40	Nivelul 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

Tabela 1. Nivelurile de securitate: compararea funcţiilor (continuare)

Funcţia	Nivelul 20	Nivelul 30	Nivelul 40	Nivelul 50
Profilul de utilizator este creat automat.	Nu	Nu	Nu	Nu
Capabilităţile de auditare securitate disponibile.	Da	Da	Da	Da
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
Protecţia îmbunătăţită a spaţiului de stocare hardware este impusă pentru tot spaţiul 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 al 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 20.

Autorizările speciale implicite

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.

Puteţi de asemenea restricţiona utilizatorii cu autorizările *SECADM şi *ALLOBJ, astfel încât să nu poată modifica cu ajutorul comenzii 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 să restricţionaţi modificările asupra valorilor de sistem de securitate şi o listă completă a valorilor de sistem afectate, consultaţi Valorile de sistem de securitate.

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 clase de utilizator după nivelul de securitate

	Clase de utilizatori				
Autoriz. specială	***SECOFR**	***SECADM**	***PGMR**	***SYSOPR**	***USER**
*ALLOBJ	All	10 sau 20	10 sau 20	10 sau 20	10 sau 20
*AUDIT	All				
*IOSYSCFG	All				
*JOBCTL	All	10 sau 20	10 sau 20	All	
*SAVSYS	All	10 sau 20	10 sau 20	All	10 sau 20
*SECADM	All	All			
*SERVICE	All				
*SPLCTL	All				

Notă: Subiectele “Clasă utilizator” la pagina 79 şi “Autorizarea specială” la pagina 84 furnizează informaţii suplimentare despre clasele de utilizator şi despre autorizările speciale.

Considerente

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.

La nivelul de securitate 30 (sau mai mic), utilizatorii pot apela interfeţe de sistem care schimbă la profilul de utilizator QSECOFR sau permit utilizatorilor accesul la resurse la care nu au acces în mod normal. La nivelul de securitate 40, utilizatorilor nu le este permis să apeleze direct aceste interfeţe. De aceea, nivelul de securitate 40 sau mai mare este recomandat.

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 rulaţi sistemul la nivelul de securitate 50, aţi putea observa un efect asupra performanţei datorită 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. Folosirea nivelului de securitate 30 de la început vă oferă flexibilitatea de a securiza câteva resurse critice

când aveţi nevoie fără a trebui să testaţi toate aplicaţiile din nou.

Concepte înrudite

"Nivelul de securitate" la pagina 2
Platforma System i oferă cinci niveluri de securitate. Prin setarea valorii de sistem QSECURITY, puteţi alege ce nivel de securitate doriţi să aplice sistemul.

Operaţii înrudite

"Dezactivarea nivelului de securitate 50" la pagina 21
După trecerea la nivelul de securitate 50, se poate să realizaţi că trebuie să treceţi înapoi la nivelul de securitate 30 sau 40 temporar. De exemplu, aţi putea avea nevoie să testaţi aplicaţii noi pentru erori de integritate; sau aţi putea descoperi probleme de integritate care nu apar la niveluri de securitate mai mici.

Nivelul 10 de securitate

La nivelul 10 de securitate, nu aveţi protecţie de securitate. De aceea, nivelul 10 de securitate nu este recomandat.

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, "profiluri de utilizator furnizate de IBM", la pagina 317 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 20 de securitate

Nivelul de securitate 20 furnizează funcţii suplimentare de securitate decât nivelul 10. Totuşi, deoarece la nivelul de securitate 20 toate profilurile sunt create cu autorizare specială *ALLOBJ implicit, nici nivelul de securitate 20 nu este recomandat.

Nivelul de securitate 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.

Trecerea la nivelul 20 de la nivelul 10

Când treceţi de la nivelul 10 la nivelul 20, orice profiluri de utilizator care au fost create automat la nivelul 10 sunt păstrate. Parola pentru fiecare profil de utilizator care a fost creat la nivelul 10 este aceeaşi cu numele profilului de utilizator. Nu sunt făcute modificăriautorizărilor speciale din profilurile de utilizator.

Luaţi în considerare realizarea următoarei liste de acitivăţi recomandate dacă aveţi de gând să treceţi de la nivelul 10 la nivelul 20 după ce sistemul a fost în producţie:

- 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 “Valorile implicite pentru profilurile de utilizator” la pagina 317 din Anexa B, “profiluri de utilizator furnizate de IBM”, la pagina 317 pentru orice modificări pe care doriţi să le faceţi asupra profilurilor create automat la nivelul de securitate 10.

Modificarea la nivel 20 de la un nivel mai înalt

Când modificaţi de la un nivel mai înalt de securitate la nivelul 20, sunt adăugate autorizări speciale profilurilor de utilizator. Făcând aceasta, utilizatorul are, cel puţin, autorizarea specială implicită pentru clasa de utilizatori.

Când modificaţi la nivelul 20 de la un nivel mai înalt de securitate, sistemul adaugă autorizarea specială *ALLOBJ tuturor profilurilor de utilizator. Aceasta permite utilizatorilor să vizualizeze, să modifice sau să şteargă orice obiect din sistem.

Citiţi Tabela 2 la pagina 11 pentru a vedea cum diferă autorizările speciale între nivelul 20 şi nivelurile de securitate mai înalte.

Nivelul 30 de securitate

Nivelul de securitate 30 furnizează funcţii suplimentare de securitate decât nivelul de securitate 20.

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.

Modificarea la nivel 30 de la un nivel mai mic

Când treceţi la nivelul de securitate 30 de la un nivel de securitate mai mic, sistemul modifică toate profilurile de utilizator pentru a actualiza autorizările speciale următoarea dată când realizaţi un 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 11 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. Luaţi în considerare realizarea următoarelor activităţi recomandate:

- Pentru fiecare aplicaţie, setaţi autorizările corespunzătoare pentru obiectele de aplicaţie.
- Testaţi fiecare aplicaţie folosind profiluri de utilizator reale sau profiluri de utilizator de test speciale.
  - Înlăturaţi autorizarea specială *ALLOBJ din profilurile de utilizator care sunt 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 test, acordaţi autorizări corespunzătoare pentru obiecte aplicaţie profilurilor de utilizator de producţie care ar trebui să aibă acces la aplicaţie.
- 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. Puteţi acorda acestor utilizatori autorizare *CHANGE asupra dispozitivelor selectate, acorda autorizarea QSECOFR *CHANGE dispozitivelor sau să modificaţi valoarea de sistem QLMTSECOFR la 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.

Referinţe înrudite

"Definirea modului în care pot fi accesate informaţii" la pagina 132
Puteţi defini ce operaţii pot fi realizate asupra obiectelor, datelor şi câmpurilor.

Nivelul 40 de securitate

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 compară modul în care sunt suportate funcţiile de securitate la nivelurile 30, 40 şi 50.

Tabela 3. Comparaţia nivelurilor de securitate 30, 40 şi 50

Descriere scenariu	Nivelul 30	Nivelul 40	Nivelul 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]; operaţia eşuează.	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 poate reuşi.	Intrare jurnal AF; [1] operaţia eşuează.	Intrare jurnal AF; [1] operaţia eşuează.
Este făcută o încercare de a restaura un program care nu are o valoare de validare. [2]	Nu este făcută nici o validare. Programul trebuie convertit înainte să poată fi folosit.	Nu este făcută nici o validare. Programul trebuie convertit înainte să poată fi folosit.	Nu este făcută nici o validare. Programul trebuie convertit înainte să poată 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.
Este făcută o încercare de a modifica spaţiul asociat al unui program.	Încercarea are succes.	Intrare jurnal AF;[1] operaţia eşuează.	Intrare jurnal AF;[1] operaţia eşuează.
Este făcută o încercare de a modifica spaţiul de adrese al unui job.	Încercarea are succes.	Intrare jurnal AF;[1] operaţia eşuează.	Intrare jurnal AF;[1] operaţia eşuează.
Un program în stare utilizator încearcă să apeleze sau să transfere controlul unui program de domeniu sistem.	Încercarea are succes.	Intrare jurnal AF;[1] operaţia eşuează.	Intrare jurnal AF;[1] operaţia eşuează.
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.

Tabela 3. Comparaţia nivelurilor de securitate 30, 40 şi 50 (continuare)

Descriere scenariu	Nivelul 30	Nivelul 40	Nivelul 50
Un program stare utilizator trimite un mesaj de excepţie unui program stare sistem care nu este imediat deasupra sa în stiva de apeluri.	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, 3] operaţia eşuează.[3]	Intrare jurnal AF;[1, 3] operaţia eşuează. [3]

[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, “Auditarea securităţii pe System i”, la pagina 257 pentru informaţii suplimentare despre funcţiile de auditare.

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

[3] 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 la pagina 14, 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 folosirii de interfeţe nesuportate

La nivelul de securitate 40 sau mai mare, sistemul împiedică încercările de a apela direct programe sistem care nu sunt documentate ca interfeţe call-level.

De exemplu, apelarea directă a programului de procesare a comenzii pentru comanda SIGNOFF eşuează.

Sistemul foloseşte atributul de domeniu al unui obiect şi atributul de stare al unui program pentru a forţa 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. Puteţi accesa obiecte care sunt domeniu *SYSTEM folosind comanda corespunzătoare sau API. Stările *SYSTEM şi *INHERIT sunt rezervate pentru programele livrate de IBM.

  Puteţi afişa starea unui program folosind comanda Afişare program (DSPPGM). Puteţi afişa starea unui program de service folosind comanda Afişare program service (DSPSRVPGM).

Tabela 4 arată regulile de acces pentru domeniu şi stare:

Tabela 4. Domeniu şi acces stare

	Domeniu obiect	
Stare program	***USER**	***SYSTEM**
*USER	DA	NO [1]
*SYSTEM	DA	DA

[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:

Când următoarele condiţii sunt îndeplinite, o intrare de eşuare autorizare (AF), tip violare D sau R, este scrisă în jurnalul QAUDJRN:

- Funcţia de auditare este activă
- Valoarea de sistem QAUDLVL include *PGMFAIL
- Este făcută o încercare de a folosi o interfaţă nesuportată

Protejarea descrierilor de job

Dacă un nume de profil de utilizator este folosit ca valoare pentru câmpul Utilizator într-o descriere de job, orice joburi lansate cu o descriere de job pot rula sub acel profil de utilizator. Deci un utilzator neautorizat ar putea lansa un job pentru a rula sub profilul de utilizator specificat în descrierea de job.

La nivelul de securitate 40 şi mai mare, jobul ar putea eşua dacă utilizatorul care lansează jobul nu are autorizare *USE asupra descrierii de job şi a profilului de utilizator specificat în descrierea de job. La nivelul de securitate 30, jobul rulează dacă cel care l-a lansat are autorizarea *USE pentru descrierea de job.

Intrare jurnal:

Când următoarele condiţii sunt îndeplinite, o intrare AF, tip violare J, este scrisă în jurnalul QAUDJRN:

- Funcţia de auditare este activă
- Valoarea de sistem QAUDLVL include *AUTFAIL
- Un utilizatorul lansează un job, în timp ce utilizatorul nu este autorizat asupra profilului de utilizator din descrierea de job.

Semnarea fără ID şi parolă de utilizator

Nivelul de securitate determină cum controlează sistemul semnarea fără ID şi parolă de utilizator.

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.

Intrare jurnal:

Când următoarele condiţii sunt îndeplinite, o intrare AF, tip violare S, este scrisă în jurnalul QAUDJRN:

- Funcţia de auditare este activă
- Valoarea de sistem QAUDLVL include *AUTFAIL
- Un utilizator încearcă să se logheze fără a introduce un ID utilizator şi parolă şi descrierea subsistemului îi permite

Notaţi că încercarea eşuează la nivelul de securitate 40 şi mai mare.

Concepte înrudite

"Descrierile de subsistem" la pagina 205
Descrierile de subsisteme realizează mai multe funcţii în sistem.

Protecţia îmbunătăţită a spaţiului de stocare hardware

Protecţia îmbunătăţită a spaţiului de stocare permite ca blocurile cu informaţii de sistem din memorie să fie definite ca 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.

Protecţia îmbunătăţită a spaţiului de stocare hardware este suportată pe toate modelele System i.

Intrare jurnal:

Când sunt îndeplinite următoarele condiţii, în jurnalul QAUDJRN este scrisă o intrare AF, tip violare R:

- Funcţia de auditare este activă
- Valoarea de sistem QAUDLVL include *PGMFAIL
- Un program încearcă să scrie într-o zonă de memorie protejată de caracteristica de protecţie spaţiu de stocare hardware îmbunătăţită

Protejarea spaţiului asociat al unui program

Pentru programe OPM, la nivelul de securitate 40 şi mai mare, spaţiului asociat unui obiect program nu poate fi modificat direct de programe stare utilizator. Pentru programe ILE, spaţiului asociat unui obiect program nu poate fi modificat de programe stare utilizator la niciun nivel de securitate.

Protejarea 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

Interfeţe pentru sistemul de operare i5/OS sunt programele de stare sistem din domeniul utilizator. Când parametrii sunt transmişi între programe 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 Common Criteria. Aţi putea observa un efect asupra performanţeo datorită acestei verificări suplimentare.

Validarea programelor care sunt restaurate

Când este creat un program, sistemul calculează o valoare de validare, care este stocată 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 se potrivesc, sistemul acţionează conform valorilor de sistem Forţare conversie la restaurare (QFRCCVNRST) şi Permitere restaurare obiect (QALWOBJRST).

În plus faţă de o listă 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,Verificare obiect la restaurare (QVFYOBJRST), QFRCCVNRST şi

QALWOBJRST, se comportă ca o serie de filtre pentru a determina dacă un program va fi restaurat fără modificare, dacă va fi reconstruit (convertit) pe măsură ce este restaurat sau dacă nu va fi restaurat în sistem.

Notă: Programele de stare sistem trebuie să aibă o semnătură digitală IBM validă. Altfel, nu pot fi restaurate, indiferent de cum sunt setate valorile de 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 continuă cu al doilea filtru, valoarea de sistem QFRCCVNRST. Cu această valoare de sistem specificaţi dacă să convertiţi programe, programe de service 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 fost pasate primelor două filtre acestea continuă la filtrul final, valoarea de sistem QALWOBJRST. Această valoare de sistem controlează dacă obiectele cu atribute sensibile la securitate pot fi sau nu restaurate.

Observaţii:

1. Programele create pentru sistemul de operare i5/OS pot conţine informaţii care permit programului să fie reconstruit la momentul restaurării, fără a cere sursa programului.
2. Programele create pentru i5/OS versiunea 5, ediţia 1 şi mai recente, conţin informaţiile necesare pentru reconstruire chiar când observabilitatea programului este înlăturată.
3. Programele create pentru ediţiile dinainte de versiunea 5, ediţia 1 pot fi reconstruite doar la restaurare dacă observabilitatea programului nu a fost ştearsă.

Referinţe înrudite

“Valorile de sistem referitoare la securitate” la pagina 36
Acest subiect introduce valorile de sistem legate de securitate din sistemul de operare i5/OS.

Trecerea la nivelul de securitate 40

Înainte de a migra la nivelul 40, asiguraţi-vă că toate aplicaţiile rulează cu succes la nivelul de securitate 30. Nivelul de securitate 30 vă oferă oportunitatea de a testa securitatea resurselor pentru toate aplicaţiile.

Urmaţi aceşti paşi 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 290 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. Monitorizaţi jurnalul de auditare pentru intrări *AUTFAIL şi *PGMFAIL în timp ce rulaţi toate aplicaţiile la nivelul de securitate 30. Fiţi în special atent la următoarele coduri motiv din intrările de tipul AF:

   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 17 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

Aţi putea avea nevoie să treceţi înapoi la nivelul 30 de la nivelul 40 temporar deoarece trebuie să testaţi aplicaţii noi pentru erori de integritate. Sau, aţi putea descoperi că nu aţi testat suficient 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 de 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, sunt adăugate unele autorizări speciale tuturor profilurilor de utilizator. (Vedeţi Tabela 2 la pagina 11.) Aceasta înlătură protecţia de securitate a resurselor.

Nivelul 50 de securitate

Nivelul de securitate 50 este proiectat pentru a îndeplini unele din cerinţele definite de conformitatea CAPP pentru CC. Nivelul de securitate 50 furnizează protecţie a integrităţii îmbunătăţită, în plus de ce este furnizat de nivelul de securitate 40, pentru instalări cu cerinţe stricte de securitate.

Funcţiile de securitate incluse pentru nivelul de securitate 50 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

Cele mai multe obiecte sunt create în domeniul sistem. Când rulaţi sistemul 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 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. Consultaţi “Permiterea obiectelor din domeniul de utilizator (QALWUSRDMN)” la pagina 25 pentru mai multe informaţii.

  Operaţii înrudite

  “Modificarea la nivelul de securitate 50”
  Dacă nivelul curent de securitate este 10 sau 20, modificaţi nivelulu de securitate la 40 înainte de a-l modifica la 50. Dacă nivelul curent de securitate este 30 sau 40, trebuie să evaluaţi valoarea QALWUSRDMN şi să recompilaţi unele programe pentru a pregăti nivelul de securitate 50.

Restricţionarea manipulării mesajelor

Mesajele trimise între programe furnizează un potenţial de expunere a integrităţii.

La nivelul de securitate 50, puteţi restricţiona mesajele trimise între programe pentru a proteja integritatea sistemului.

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 apeluri, un mesaj de excepţie poate fi trimis programului 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, unele blocuri de control interne, cum ar fi blocul de control lucru, nu pot fi modificate de un program stare utilizator. La nivelul de securitate 50, nu poate fi modificat nici un bloc de control intern. Aceasta includecalea de date deschisă (ODP), spaţiile pentru comenzile şi programele CL şi blocul de control job mediu S/36.

Modificarea la nivelul de securitate 50

Dacă nivelul curent de securitate este 10 sau 20, modificaţi nivelulu de securitate la 40 înainte de a-l modifica la 50. Dacă nivelul curent de securitate este 30 sau 40, trebuie să evaluaţi valoarea QALWUSRDMN şi să recompilaţi unele programe pentru a pregăti nivelul de securitate 50.

Majoritatea măsurilor de securitate suplimentare care sunt impuse la nivelul de securitate 50 nu cauzează intrărilor de 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 18 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 valoarea de sistem QALWUSRDMN. Controlarea obiectelor de domeniu utilizator este importantă pentru integritatea sistemului.
- 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/400 sau RPG* ale mediului 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.

Concepte înrudite

“Restricţionarea obiectelor de domeniu utilizator” la pagina 19
Cele mai multe obiecte sunt create în domeniul sistem. Când rulaţi sistemul la nivelul de securitate 40 sau 50, obiectele de domeniu sistem pot fi accesate doar prin folosirea comenzilor şi API-urilor furnizate.

Dezactivarea nivelului de securitate 50

După trecerea la nivelul de securitate 50, se poate să realizaţi că trebuie să treceţi înapoi la nivelul de securitate 30 sau 40 temporar. De exemplu, aţi putea avea nevoie să testaţi aplicaţii noi pentru erori de integritate; sau aţi putea descoperi probleme de integritate care nu apar la niveluri de securitate mai mici.

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 de 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, sunt adăugate unele autorizări speciale tuturor profilurilor de utilizator. Aceasta înlătură protecţia de securitate a resurselor.

Referinţe înrudite

Capitolul 2, “Folosirea valorii de sistem QSecurity”, la pagina 9
Puteţi alege gradul de securitate pe care doriţi să îl impună sistemul prin setarea valorii de sistem QSECURITY (security level - nivel de securitate).

Capitolul 3. Valorile de sistem de securitate

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 să împiedicaţi 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 că valorile de sistem sunt libere să fie modificate în timpul IPL-ului.

Puteţi restricţiona următoarele valori de sistem folosind opţiunea de blocare:

Tabela 5. Valorile de sistem care pot fi blocate

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

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 de utilizator 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. Tastaţi ID-ul dumneavoastră utilizator 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 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**.

Concepte înrudite

"Valorile de sistem" la pagina 3
Valorile de sistem permit personalizarea multor caracteristici ale platformei System i. Puteţi folosi valorile de sistem pentru a defini setările de securitate pentru tot sistemul.

Valorile de sistem generale pentru securitate

Acest subiect introduce valorile de sistem generale pe care le puteţi folosi pentru a controla securitatea pe sistemul de operare i5/OS.

Privire generală:

Valorile de sistem de securitate generale vă permit să setaţi funcţia de securitate pentru a suporta deciziile pe care le faceţi când dezvoltaţi politica de securitate. De exemplu, în politica de securitate afirmaţi că sistemele care conţin informaţii confidenţiale, cum ar fi conturi client sau inventare de state de plată, au nevoie de un nivel mai strict de securitate decât sistemele folosite pentru testarea aplicaţiilor care sunt dezvoltate în companie. Puteţi apoi planifica şi seta un nivel de securitate pe aceste sisteme care corespunde cu deciziile pe care le faceţi când dezvoltaţi politica de securitate.

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).

Valorile de sistem generale care controlează securitatea în sistem sunt după cum urmează:

QALWUSRDMN
Permitere obiecte de domeniu utilizator în biblioteci

QCRTAUT
Creare autorizare publică implicită

QDSPSGNINF
Afişare informaţii de semnare

QFRCCVNRST
Forţare conversaţie 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

Permiterea obiectelor din domeniul de utilizator (QALWUSRDMN)

Tuturor obiectelor le este asignat un atribut de domeniu când sunt create. Un domeniu este o caracteristică a unui obiect care controlează cum pot accesa programele obiectul. Valoarea de sistem Permitere obiecte domeniu utilizator (QALWUSRDMN) specifică căror biblioteci le este permis să conţină obiecte domeniu utilizator de tip *USRSPC, *USRIDX şi *USRQ.

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. Restricţia nu se aplică la obiecte domeniu utilizator de tip program (*PGM), program server (*SRVPGM) şi pachete SQL (*SQLPKG).

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi Valori de sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorile de sistem de securitate şi 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. Aceasta este o valoare livrată.
***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.

Valore 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.

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. Aceasta limitează numărul de utilizatori care pot folosi interfaţa MI pentru a citi sau modifica datele din obiectele domeniu utilizator din aceste biblioteci fără a fi auditate.

Notă: Dacă rulaţi comanda Pretindere spaţiu de stocare (RCLSTG), obiectele domeniu utilizator ar putea trebui mutate în şi din biblioteca QRCL (pretindere spaţiu de stocare). Pentru a rula comanda RCLSTG cu succes, ar putea fi nevoie 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 Autorizare pentru obiecte noi (QCRTAUT) specifică autorizarea publică pentru un obiect nou creat.

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. Consultaţi Valori de sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorile de sistem de securitate şi 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, inclusiv QSYS, au o valoare CRTAUT de *SYSVAL. Dacă modificaţi valoarea de sistem QCRTAUT la altceva decât *CHANGE, aţi putea întâlni probleme la semnarea în dispozitive noi sau create automat. Pentru a evita probleme când modificaţi QCRTAUT la ceva diferit de *CHANGE, asiguraţi-vă că toate descrierile de dispozitiv şi cozile de mesaje asociate au o autorizare PUBLIC de *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 Afişare informaţii logare (QDSPSGNINF) determină dacă ecranul Informaţii semnare este arătat după semnare.

Ecranul Informaţii semnare afişează:

- Data ultimei semnări
- Orice verificări de parole care nu au fost valide
- Numărul de zile până când parola expiră (dacă parola va expira în zilele de avertisment expirare parolă (QPWDEXPWRN)))

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

Password verifications not valid . . . . . :   3

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

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi Valori de sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorile de sistem de securitate şi 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: 1 (Ecranul este arătat) este recomandată astfel încât utilizatorii să poată monitoriza încercarea de folosire a profilurilor lor şi când este necesară o parolă nouă.

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 Interval timeout job inactiv (QINACTITV) specifică în minute cât permite sistemul unui job să fie inactiv înainte de a lua 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

Sesiuni de emulare prin System i Access sunt incluse. 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. 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 determină sistemul care 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 System i Access ar putea părea inactiv sistemului dacă utilizatorul realizează funcţii PC, cum ar fi editarea unui document, fără a interacţiona cu sistemul.

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 minute

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

Valoarea de sistem Coadă de mesaje timeout job inactiv (QINACTMSGQ) specifică ce acţiune ia sistemul când intervalul de timeout job inactiv pentru un job a fost atins.

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 10. Valorile posibile pentru valoarea de sistem QPWDLMTCHR:

***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. Consultaţi “Intervalul de timeout pentru job deconectat (QDSCJOBITV)” la pagina 38 pentru mai multe informaţii. **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] Subiectul Control funcţionare descrie joburile de grup şi joburile secundare.	

Valoare recomandată: *DSCJOB este recomandat dacă utilizatorii nu rulează joburi System i Access. Folosirea *DSCJOB când unele joburi System i Access rulează este echivalentă cu terminarea joburilor. Poate cauza pierderi semnificative de informaţii. Folosiţi opţiunea *message-queue* dacă aveţi programul licenţiat System i Access. Subiectul Programare CL arată un exemplu de scriere a unui program pentru manipularea mesajelor.

Folosirea unei cozi de mesaje: Un utilizator sau un program poate monitoriza coada de mesaje şi să ia o acţiune după cum este necesar, cum ar fi 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 System i 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 Limitare sesiune dispozitiv (QLMTDEVSSN) specifică dacă numărul de sesiuni dispozitiv permise pentru un utilizator este limitat.

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 valoare restricţionată. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 11. Valorile posibile pentru valoarea de sistem QLMTDEVSSN:

0	Utilizatorul nu este limitat la un anumit număr de sesiuni dispozitiv.
1	Utilizatorul este limitat la un singură sesiune dispozitiv.
2 - 9	Utilizatorul este limitat la numărul specificat de sesiuni dispozitiv.

Valoare recomandată: 1 (Da) este recomandat deoarece limitarea utilizatorilor la un singur dispozitiv reduce probabilitatea partajării parolelor şi lăsarea dispozitivelor nesupravegheate.

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

Limitarea responsabilului cu securitatea (QLMTSECOFR)

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

Valoarea sistem QLMTSECOFR este forţată doar de la nivelul de securitate 30 în sus. “Staţii de lucru” la pagina 201 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. Consultaţi Valori de sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorile de sistem de securitate şi 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.

Tabela 12. Valorile posibile pentru valoarea de sistem QLMTSECOFR: (continuare)

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 (Yes)

Numărul maxim de încercări de semnare (QMAXSIGN)

Valoarea de sistem Încercă maxime de semnare (QMAXSIGN) controlează numărul de încercări consecutive de semnare sau de verificare parolă care nu sunt corecte de către utilizatori locali sau de la distanţă.

Încercările incorect de semnare sau de verificare parolă poate fi cauzate de un ID utilizator care nu este corect, o parolă care nu este corectă sau autoriza inadecvată pentru a folosi o staţie de lucru.

Când numărul maxim de încercări de semnare sau verificare de parolă este atins, valoarea de sistem QMAXSGNACN este folosită pentru a determina acţiunea care va fi luată. Un mesaj CPF1393 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 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.

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi Valori de sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorile de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 13. Valorile posibile pentru valoarea de sistem QMAXSIGN:

3	Un utilizator poate încerca maxim 3 încercări de semnare sau de verificare parolă.
***NOMAX**	Sistemul permite un număr nelimitat de încercări incorecte de semnare sau de verificare parolă. Aceasta dă posibilităţi nelimitate unui potenţial intrus să ghicească o combinaţie validă de ID utilizator şi parolă.
limit	Specificaţi o valoare între 1 şi 25. Numărul recomandat de încercări de semnare sau verificare parolă este trei. Tipic, trei încercări sunt suficiente pentru a corecta erorile de tastare dar destul de puţine pentru a ajuta la împiedicarea accesului neautorizat.

Valoare recomandată: 3

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

Valoarea de sistem Acţiune când limita de încercări de logări este atinsă (QMAXSGNACN) determină ce face sistemul când pe o staţie de lucru este atins numărul maxim de încercări de semnare sau verificare parolă.

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi 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 de utilizator este dezactivat când numărul de încercări de semnare incorecte atinge valoarea de sistem QMAXSIGN, indiferent dacă încercările de semnare incorecte au fost de la aceleaşi dispozitive sau de la dispozitive diferite. O permisiuni sau verificare de parolă validă resetează numărul de încercări de semnare incorecte în profilul de utilizator.

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 30 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 Păstrare securitate server (QRETSVRSEC) determină dacă informaţii de autentificare decriptibile asociate cu profiluri de utilizator sau intrări listă de validare (*VLDL) pot fi păstrate pe sistemul gazdă. Aceasta nu include parola profilului de utilizator System i.

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 la 0 şi rularea comenzii Curăţare date securitate server (CLRSVRSEC). Dacă aveţi un număr mare de profiluri de utilizator sau liste de validare pe sistem comanda CLRSVRSEC ar putea rula pentru o perioadă 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 intrare. 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. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi 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

Concepte înrudite

“Folosirea listelor de validare” la pagina 242
Obiectele listei de validare furnizează o metodă pentru aplicaţii de a stoca în siguranţă informaţii de autentificare utilizatori.

Pornirea şi repornirea de la distanţă (QRMTIPL)

O parte a planului de securitate a sistemului este de a determina dacă veţi permite utilizatorilor la distanţă să pornească şi să repornească sistemul. Valoarea de sistem Pornire şi repornire de la distanţă (QRMTIPL) vă oferă abilitatea de a porni sistemul de la distanţă folosind telefonul şi un modem sau semnalul SPCN.

Când QRMTIPL este setat la 1 (Da), orice telefon va face ca sistemul să repornească. Chiar dacă această valoare de sistem se referă la opţiunile de repornire ale sistemului, are implicaţii de securitate. Evident nu vreţi ca cineva să repornească neavizat sistemele. Totuşi, dacă folosiţi un sistem la distanţă pentru a administra sistemul va trebui să permiteţi repornire de la distanţă.

Tabela 16. Valorile posibile pentru valoarea de sistem pornire şi repornire de la distanţă (QRMTIPL)

0	Nu permiteţi pornire şi repornire de la distanţă
1	Permisiunea de pornire şi repornire la distanţă

Informaţii înrudite

Repornire valori sistem: Permitere pornire şi repornire de la distanţă

Controlul semnării de la distanţă (QRMTSIGN)

Valoarea de sistem Control semnare de la distanţă (QRMTSIGN) specifică modul în acre sistemul tratează cererile de semare de la distanţă.

Exemple de semnări de la distanţă sunt sesiunile pass-through cu staţia de afişare din alt sistem, funcţia de staţie de lucru a programului licenţiat System i Access şi accesul TELNET.

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 17. Valorile posibile pentru valoarea de sistem QRMTSIGN:

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

Tabela 17. Valorile posibile pentru valoarea de sistem QRMTSIGN: (continuare)

***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.

Valoare recomandată: *REJECT este recomandat dacă nu vreţi să permiteţi acces pass-through sau System i Access. Dacă nu permiteţi acces pass-through sau System i Access, folosiţi *FRCSIGNON sau *SAMEPRF.

Cartea Remote Workstation 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 de fişiere integrat la deschidere ieşire.
- QIBM_QP0L_SCAN_CLOSE — Scanare sistem de fişiere integrat la închidere ieşire.

Pentru informaţii suplimentare despre sisteme de fişiere integrate, consultaţi subiectul Sistem de fişiere integrat.

Tabela 18. 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.

Valoare recomandată: Valoarea recomandată este *ROOTOPNUD astfel încât sistemele de fişiere ″root″ (/), QOpenSys şi definite de utilizator sunt scanare când oricine înregistrează programe de ieşire în punctele de ieşire legate de scanare ale sistemului de fişiere integrat.

Referinţe înrudite

“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.

Informaţii înrudite

Directoare *TYPE2

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.

QSCANFSCTL lucrează cu valoarea de sistem scanare sisteme de fişiere pentru a furniza elemente de control mai fine despre cum şi ce este scanat în sistemul de fişiere integrat. Puteţi alege opţiuni de scanare diferite sau puteţi selecta să

folosiţi opţiunile implicite de scanare. De asemeneao, puteţi selecta mai multe opţiuni de scanare care controlează cum şi ce vor scana programele înregistrate de ieşire. Aceste opţiuni sunt descrise în următoarea tabelă:

Tabela 19. 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.
***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 actualizare). 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.

Valoare recomandată: Dacă vreţi cele mai restrictive valori pentru specificate pentru scanarea sistemului de fişiere integrat, atunci setările recomandate sunt *ERRFAIL şi *NOWRTUPG. Acestea asigură că orice eşuare de la programele de ieşire de scanare împiedică operaţiile asociate, precum şi nu acordă 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 perioadei de instalare.

Referinţe înrudite

“Scanarea sistemelor de fişiere (QSCANFS)” la pagina 33
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.

Controlul memoriei de partajare (QSHRMEMCTL)

Valoarea de sistem Partajare control memorie (QSHRMEMCTL) defineşte căror utilizatori le este permis să folosească memorie partajată sau memorie mapată care are capabilitate de scriere.

Mediul poate conţine aplicaţii, fiecare rulând un job diferit, dar partajând pointeri cu aceste aplicaţii. Folosirea acestor API-uri furnizează performanţă mai bună a aplicaţiilor şi fluidizarea dezvoltării aplicaţiilor permiţând memorie partajată şi fişiere flux între aceste aplicaţii diferite şi joburi. Totuşi, folosirea acestor API-uri ar putea reprezenta un risc pentru sistemul şi bunurile dumneavoastră. Un programator poate avea acces la scriere şi poate adăuga, modifica şi şterge intrări din memoria partajată sau fişier flux.

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. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 20. Valorile 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)

Cu atributul *USEADPAUT(*YES), valoarea de sistem Folosire autorizare adoptată (QUSEADPAUT) defineşte ce utilizatori pot crea programe.

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 autorizare, el poate crea, modifica sau actualiza programe sau programe servicii cu atributul USEADPAUT(*YES). Autorizarea la lista de autorizare nu poate veni de la o autorizare adoptată.

Dacă o listă de autorizare este numită în valoarea de sistem şi lista de autorizare 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 autorizare nu există.

Dacă sunt cerute mai multe funcţii în comandă sau API şi lista de autorizare lipseşte, funcţia nu este executată.

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 21. Valorile posibile pentru valoarea de sistem QUSEADPAUT:

nume listă de autorizare	Este semnalat un mesaj diagnostic pentru a indica faptul că programul este creat cu USEADPAUT(*NO) dacă toate următoarele sunt adevărate: • Utilizatorul nu are autorizare la lista de autorizări menţionată. • Nu mai există şi alte erori când programul sau programul serviciu este creat.
***NONE**[1]	Toţi utilizatorii pot crea, modifica sau actualiza programe şi programe de service pentru a folosi autorizarea programului care le-a apelat dacă utilizatorul are autorizare necesară asupra programului sau programului de service.
[1] *NONE indică că nu este folosită nicio listă de autorizaţi şi implicit tuturor utilizatorilor le va fi permis să acceseze programe care folosesc autorizare adoptată.	

Valoare recomandată: Pentru maşini de producţie, creaţi o listă de autorizare cu autorizarea *PUBLIC(*EXCLUDE). Specificaţi această listă de autorizare 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 autorizare pentru valoarea de sistem QUSEADPAUT. Acest lucru este important în special pentru mediile de dezvlotare de aplicaţii.

Valorile de sistem referitoare la securitate

Acest subiect introduce valorile de sistem legate de securitate din sistemul de operare i5/OS.

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 devin efective imediat. IPL-ul nu este necesar.

Următoarele informaţii sunt descrieri ale valorilor de sistem suplimentare care se leagă de securitatea sistemului. 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 discutată de asemenea în subiectul Valori de sistem joburi: Interval timeout pentru joburi deconectate.

QRMTSRVATR
Atribut service la distanţă

| **QSSLCSL**
| Listă de specificare cifru SSL

| **QSSLCSLCTL**
| Control cifru SSL

| **QSSLPCL**
| Protocoale SSL

Concepte înrudite

"Validarea programelor care sunt restaurate" la pagina 17
Când este creat un program, sistemul calculează o valoare de validare, care este stocată 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.

Configurarea automată a dispozitivelor (QAUTOCFG)

Valoarea de sistem Configurare automată dispozitiv (QAUTOCFG) configurează automat dispozitive ataşate local. Valoarea specifică dacă dispozitivele care sunt adăugate în sistem sunt configurate automat.

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 22. 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: La iniţierea setării sistemului sau la adăugarea de multe dispozitive noi, valoarea de sistem ar trebui 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 Configurare automată dispozitive virtuale (QAUTOVRT) specifică dacă dispozitivele pass-through virtuale şi dispozitivele virtuale ecran întreg TELNET (spre dosebire de dispozitiv virtuale funcţie staţie de lucru) sunt configurate automat.

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. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 23. Valorile posibile pentru valoarea de sistem QAUTOVRT:

0	Nici un dispozitiv virtual nu este creat automat.

Tabela 23. Valorile posibile pentru valoarea de sistem QAUTOVRT: (continuare)

număr-de- 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.

Valoare recomandată: 0

Informaţii înrudite

Remote Workstation Support

Setarea TCP/IP

Acţiunea la recuperarea dispozitivelor (QDEVRCYACN)

Valoarea de sistem Acţiune recuperare dispozitiv (QDEVRCYACN) specifică ce acţiune să luaţi când are loc o eroare de I/E pentru o staţie de lucru a unui job interactiv.

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 24. 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 o valoare *MSG sau *DSCMSG este specificată, acţiunea de recuperare dispozitiv nu este realizată până când jobul realizează următoarea operaţie de I/E. Într-un mediu LAN/WAN, aceasta permite unui dispozitiv să se deconecteze şi altuia să se conecteze, folosind aceeaşi adresă, înainte ca următoarea operaţie de I/E pentru job să aibă loc. Jobul poate reveni dintr-un mesaj de eroare de I/E şi continua rularea pe un al doilea dispozitiv. Pentru a evita aceasta, specificaţi 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.

Intervalul de timeout pentru job deconectat (QDSCJOBITV)

Valoarea de sistem Interval timeout job deconectat (QDSCJOBITV) determină dacă şi când sistemul opreşte un job deconectat. Intervalul este specificat în minute.

Dacă setaţi valoarea de sistem QINACTMSGQ pentru 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. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 25. 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.
time-in-minutes	Specifcă o valoare între 5 şi 1440.

Valoare recomandată: 120

Atributul de service la distanţă (QRMTSRVATR)

Atributul de service la distanţă (QRMTSRVATR) controlează posibilitatea de a analiza de la distanţă problemele de service ale sistemului. Valoarea permite analizarea sistemului de la distanţă.

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Valorile permise pentru valoarea de sistem QRMTSRVATR sunt:

Tabela 26. Valorile posibile pentru valoarea de sistem QRMTSRVATR:

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

Valoare recomandată: 0

Concepte înrudite

“Securitatea cheii IPL” la pagina 2
Puteţi extrage şi modifica poziţia cheii IPL folosind API-ul QWCRIPLA (Extragere atribute IPL) sau comanda CHGIPLA (Modificare atribute IPL).

Listă specificare cifru SSL (QSSLCSL)

Valoarea de sistem Listă specificare cifru SSL (QSSLCSL) determină ce listă de specificare cifru va fi suportată de System SSL.

System SSL foloseşte secvenţa de valori din QSSLCSL pentru a ordona lista implicită de specificare cifru System SSL. Intrările listei implicite de specificare cifru sunt definite de sistem şi pot fi modificate între ediţii. Dacă o suită implicită de cifruri este înlăturată din valoarea de sistem QSSLCSL, este de asemenea înlăturată din lista de specificare cifru implicită. Suita implicită de cifruri este adăugată în lista de specificare cifru când suita de cifruri este adăugată în valoarea de sistem QSSLCSL. Nu puteţi adăuga alte suite de cifruri în lista implicită de specificare cifru înafară de setul definit de sistem pentru ediţie. De asemenea, o suită de cifruri nu poate fi adăugată la QSSLCSL dacă valoarea de protocol SSL necesară pentru suita de cifruri nu este setată pentru valoarea de sistem QSSLPCL (listă protocoale SSL).

Valorile valorii de sistem QSSLCSL sunt numai citire dacă valoarea de sistem Control cifru SSL (QSSLCSLCTL) nu este setată la *USRDFN.

Valorile permise pentru valoarea de sistem QSSLCSL sunt după cum urmează:

- *RSA_AES_128_CBC_SHA

- *RSA_RC4_128_SHA
- *RSA_RC4_128_MD5
- *RSA_AES_256_CBC_SHA
- *RSA_3DES_EDE_CBC_SHA
- *RSA_DES_CBC_SHA
- *RSA_EXPORT_RC4_40_MD5
- *RSA_EXPORT_RC2_CBC_40_MD5
- *RSA_NULL_SHA
- *RSA_NULL_MD5
- *RSA_RC2_CBC_128_MD5
- *RSA_3DES_EDE_CBC_MD5
- *RSA_DES_CBC_MD5

Notă: Trebuie să aveţi autorizări speciale *IOSYSCFG, *ALLOBJ şi *SECADM pentru a modifica această valoare de sistem.

Pentru informaţii suplimentare despre valorile livrate, puteţi să consultaţi subiectul Listă specificare cifru SSL din colecţia de subiecte Valorile de sistem.

Informaţii înrudite

Valori sistem securitate: Listă specificare cifru SSL

Proprietăţi SSL sistem

Control cifru SSL (QSSLCSLCTL)

Valoarea de sistem Control cifru SSL (QSSLCSLCTL) specifică dacă sistemul sau utilizatorul controlează valoarea de sistem Listă specificare cifru SSL (QSSLCSL).

Valorile permise pentru valoarea de sistem QSSLCSLCTL sunt după cum urmează:

- *OPSYS
- *USRDFN

Notă: Trebuie să aveţi autorizări speciale *IOSYSCFG, *ALLOBJ şi *SECADM pentru a modifica această valoare de sistem.

Pentru informaţii suplimentare despre valorile livrate, puteţi să consultaţi subiectul Control cifru SSL din colecţia de subiecte Valorile de sistem.

Informaţii înrudite

Valori sistem securitate: Listă cifru SSL

Protocoale SSL (QSSLPCL)

Valoarea de sistem Protocoale SSL (QSSLPCL) specifică protocoalele SSL suportate de System SSL.

Valorile permise pentru valoarea de sistem QSSLPCL sunt după cum urmează:

- *OPSYS
- *TLSV1
- *SSLV2
- *SSLV3

Notă: Trebuie să aveţi autorizări speciale *IOSYSCFG, *ALLOBJ şi *SECADM pentru a modifica această valoare de sistem.

| Pentru informaţii suplimentare despre valorile livrate, puteţi să consultaţi subiectul Protocoale SSL din colecţia de
| subiecte Valorile de sistem.

| **Informaţii înrudite**

| Valori sistem securitate: Protocoale SSL

Valorile de sistem pentru restaurare referitoare la securitate

Acest subiect introduce valorile de sistem restaurare legate de securitate pe sistemul de operare i5/OS.

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 devin efective imediat. IPL-ul nu este necesar.

Următoarele informaţii sunt descrieri ale valorilor de sistem care se leagă de restaurarea obiectelor legate de securitate din sistem care ar trebui de asemenea luate în considerare la restaurarea obiectelor. Vedeţi Tabela 19 la pagina 34pentru 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

În continuare sunt prezentate aceste valori de sistem. Sunt afişate opţiunile posibile. Opţiunile care sunt subliniate sunt valorile implicite ale sistemului.

Concepte înrudite

“Restaurarea programelor” la pagina 252
Restaurarea programelor pe sistemul dumneavoastră ce sunt obţinute de la o sursă necunoscută pun o problemă de securitate. Acest subiect furnizează informaţii despre factorii care ar trebui luaţi în considerare la restaurarea programelor.

Verificarea obiectului la restaurare (QVFYOBJRST)

Valoarea de sistem Verificare obiect la restaurare (QVFYOBJRST) determină dacă obiectele trebuie să aibă semnături digitale pentru a fi restaurate în sistem.

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 Verificare obiect la restaurare (QVFYOBJRST). Acesta este folosit pentru a controla restaurarea unor obiecte care pot fi semnate digital. Al doilea filtru este valoarea de sistem Forţare conversie 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 Permitere obiecte la restaurare (QALWOBJRST). Specifică dacă pot fi restaurate obiectele cu atribute sensibile la securitate.

Dacă Digital Certificate Manager (i5/OS opţiunea 34) nu este instalat în sistem, toate obiectele cu excepţia celor semnate de o sursă de sistem de încredere sunt tratate ca nesemnate la determinarea efecterlor valorii de sistem QVFYOBJRST în timpul unei operaţii de restaurare.

Programele, programele de service şi obiectele modul care sunt create sau convertite într-un sistem cu o ediţie anterioară de V6R1 sunt tratate ca nesemnate când sunt restaurate pe un sistem V6R1 sau mai recent. La fel, programele, programele de service şi obiectele modul care sunt create sau convertite pe o ediţie V6R1 sau mai recentă sunt tratate ca nesemnate când sunt restaurate pe un sistem anterior faţă de V6R1.

Modificarea acestei valori de sistem devine imediat efectivă.

Observaţii:

1. Această valoare de sistem este o valoare restricţionată. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.
2. Obiectele care au atributul stare-sistem şi obiectele care au atributul stare-moştenită trebuie să aibă o semnătură validă dintr-o sursă de încredere a sistemului. Obiectele din PTF-ul LIC trebuie de asemenea să aibă o semnătură validă dintr-o sursă de înceredere a sistemului. Dacă aceste obiecte nu au o semnătură validă, acestea nu pot fi restaurate, indiferent de valoarea valorii de sistem QVFYOBJRST.

Atenţie: Când sistemul este livrat,valoarea de sistem QVFYOBJRST este setată la 3. Dacă modificaţi valoarea QVFYOBJRST, este important să setaţi valoarea QVFYOBJRST la 3 sau la o valoare mai mică înainte de a instala o nouă ediţie a sistemului de operare i5/OS.

Tabela 27. Valorile posibile pentru valoarea de sistem QVFYOBJRST:

1	Nu verificaţi semnăturile la restaurare. Restauraţi toate obiectele stare utilizator indiferent de semnătura lor. Nu folosiţi această valoare dacă nu aveţi obiecte semnate de restaurat care vor eşua verificarea semnăturii dintr-un motiv acceptabil.
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. Folosiţi această valoare doar dacă anumite obiecte pe care vreţi să le restauraţi conţin semnături care nu sunt valide. În general, nu este recomandat să restauraţi obiecte cu semnături care nu sunt valide în sistem.
3	Verificaţi semnăturile la restaurare. Restauraţi comenzile şi obiectele stare utilizator nesemnate. Restauraţi comenzile şi obiectele stare utilizator semnate numai dacă semnăturile sunt valide. Folosiţi această valoare pentru operaţii normale, când aşteptaţi unele din obiectele pe care le restauraţi să fie nesemnate, dar vreţi să vă asiguraţi că toate obiectele semnate au semnături care sunt 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.

Tabela 27. Valorile posibile pentru valoarea de sistem QVFYOBJRST: (continuare)

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. Folosiţi această valoare doar dacă anumite obiecte pe care vreţi să le restauraţi conţin semnături care nu sunt valide, dar nu vreţi posibilitatea de a restaura obiecte nesemnate. În general, nu este recomandat să restauraţi obiecte cu semnături care nu sunt valide în sistem.
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.

Unele comenzi folosesc o semnătură care nu include 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 la o comandă care nu are un astfel de program.
- Modificarea parametrului ″unde îi este permis să ruleze″.
- Modificarea parametrului ″permitere utilizator limitat″.

Dacă vreţi, puteţi adăuga propria semnătură la aceste comenzi care include aceste zone ale obiectului comandă.

Valoare recomandată: 3

Forţarea conversiei la restaurare (QFRCCVNRST)

Valoarea de sistem Forţare conversie la restaurare (QFRCCVNRST) poate forţa conversia unor tipuri de obiecte în timpul unei restaurări. Această valoare de sistem poate de asemenea împiedica unele obiecte să fie restaurate.

Valoarea de sistem QFRCCVNRST specifică dacă să convertiţi următoarele tipuri de obiecte la o restaurare:

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

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. Specificarea *YES şi *RQD în parametrul FRCOBJCVN este aceeaşi cu specificarea ’2’ pentru această valoare de sistem şi poate înlocui valoarea de sistem când este setată la 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 Verificare obiect la restaurare(QVFYOBJRST), controlează restaurarea unor obiecte care pot fi semnate digital. Doar obiectele care pot trece de primele două filtre sunt procesate de al treilea filtru, valoarea de sistem Permitere restaurare obiect (QALWOBJRST), care specifică dacă obiectele cu atribute sensibile la securitate pot fi restaurate.

Dacă Digital Certificate Manager (i5/OS opţiunea 34) nu este instalat în sistem, toate obiectele cu excepţia celor semnate de o sursă de sistem de încredere sunt tratate ca nesemnate la determinarea efecterlor valorii de sistem QFRCCNVRST în timpul unei operaţii de restaurare.

Programele, programele de service şi obiectele modul care sunt create sau convertite într-un sistem cu o ediţie anterioară de V6R1 sunt tratate ca nesemnate când sunt restaurate pe un sistem V6R1 sau mai recent. La fel, programele, programele de service şi obiectele modul care sunt create sau convertite pe o ediţie V6R1 sau mai recentă sunt tratate ca nesemnate când sunt restaurate pe un sistem anterior faţă de V6R1.

Valoarea livrată a QFRCCVNRST este 1. Pentru toate valorile QFRCCVNRST un obiect care ar trebui convertit dar 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. Consultaţi Valori de sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorile de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela de mai jos rezumă valorile permise pentru QFRCCVNRST:

Tabela 28. Valori QFRCCVNRST

0	Nu convertiţi nimic. Nu împiedicaţi restaurarea nici unui obiect.
1	Vor fi convertite obiectele cu erori de validare.
2	Obiectele vor fi convertite dacă conversia lor este necesară pentru sistemul de operare curent sau maşina curentă sau dacă au o eroare de validare.
3	Obiectele care sunt suspectate de a fi fost modificate, obiectele care conţin erori de validare şi obiectele care necesită conversie pentru a fi folosite în versiunea curentă a sistemului de operare sau pe maşina curentă vor fi convertite.
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:** Obiectele (semnate şi nesemnate) care au erori de validare, sunt suspectate de a fi fost modifiacte sau necesită conversie pentru a fi folosite pe versiunea curentă a sistemului de operare sau pe maşina curentă vor fi convertite; sau vor fi restaurate dacă nu sunt convertite.
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, sunt suspectate de a fi fost modificate sau care necesită conversie pentru a fi folosite în versiunea curentă a sistemului de operare sau pe maşina curentă 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, sau 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 Permite restaurare obiecte sensibile la securitate (QALWOBJRST) determină dacă obiectele care sunt sensibile la securitate pot fi restaurate în sistem.

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 Verificare obiect la restaurare (QVFYOBJRST). Acesta este folosit pentru a controla restaurarea unor obiecte care pot fi semnate digital. Al doilea filtru este valoarea de sistem Forţare conversie 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 Permitere obiecte la restaurare (QALWOBJRST). Specifică dacă pot fi restaurate obiectele cu atribute sensibile la securitate. O puteţi folosi pentru a împiedica pe oricine să restaureze un obiect stare sistem sau un obiect care adoptă autorizarea.

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 i5/OS.
- 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. Consultaţi Valori de sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorile de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

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

Tabela 29. Valorile posibile pentru valoarea de sistem QALWOBJRST:

***ALL**	Orice obiect poate fi restaurat pe sistem de către un utilizator cu autorizarea corectă.
***NONE**	Obiectele sensibile la securitate, cum ar fi programele de stare sistem sau programele care adoptă autorizare, nu pot fi restaurate în sistem.
***ALWSYSSTT**	Obiectele sistem şi cele care moştenesc stare pot fi restaurate în sistem.
***ALWPGMADP**	Obiectele care adoptă autorizare pot fi restaurate în 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 pentru a vă proteja sistemul de programe care pot cauza 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 restauraţeţi regulat programe şi aplicaţii în sistem, ar putea fi necesar să setaţi valoarea de sistem QALWOBJRST la *ALWPGMADP.

Valorile de sistem pentru parole

Acest subiect descrie valorile de sistem care se aplică la parole. Aceste valori de sistem obligă utilizatorii să modifice parolele regulat şi ajută la împiedicarea utilizatorilor de a aloca parole triviale sau uşor de ghicit. Acestea se pot asigura că parolele îndeplinesc cerinţele reţelei de comunicaţii.

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 (cu excepţia QPWDLVL). IPL-ul nu este necesar.

Valorile de sistem controlează parolele:

| **QPWDCHGBLK**
| Blocare modificare parolă

QPWDEXPITV
Interval de expirare

| **QPWDEXPWRN**
| Avertisment expirare parolă

QPWDLVL
Nivel parolă

QPWDLMTCHR
Caractere restricţionate

QPWDLMTAJC
Caractere adiacente restricţionate

QPWDLMTREP
Caractere repetate restricţionate

QPWDMINLEN
Lungime minimă

QPWDMAXLEN
Lungime maximă

QPWDPOSDIF
Diferenţă poziţie caracter

QPWDRQDDIF
Diferenţă necesară

QPWDRQDDGT
Necesitate caracter numeric

| **QPWDRULES**
| Reguli parolă

QPWDVLDPGM
Program validare parolă

Valorile de sistem de compunere parolă sunt forţate doar când parola este modificată folosind comanda CHGPWD, opţiunea de meniu ASSIST pentru a modifica o parolă sau API-ul QSYCHGPW. Acestea nu sunt forţate când parola este setată folosind comanda CRTUSRPRF sau CHGUSRPRF.

Sistemul împiedică un utilizator să seteze parola egală cu numele profilului de utilizator folosind comanda CHGPWD, meniul ASSIST sau API-ul QSYCHGPW în oricare din următoarele condiţii.

- Valoarea de sistem Reguli parolă (QPWDRULES) are o valoare de *PWDSYSVAL şi valoarea de sistem Lungime minimă parolă (QPWDMINLEN) are o valoare diferită de 1.
- Valoarea de sistem Reguli parolă (QPWDRULES) are o valoare de *PWDSYSVAL şi valoarea de sistem Lungime maximă parolă (QPWDMAXLEN) are o valoare diferită de 10.
- Valoarea de sistem Reguli parolă (QPWDRULES) are o valoare de *PWDSYSVAL şi modificaţi oricare din valorilor de sistem control parolă de la valorile implicite.

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

Informaţii înrudite

Valori sistem: Privire generală parolă

Blocare modificare parolă (QPWDCHGBLK)

Valoarea de sistem Blocare modificare parolă (QPWDCHGBLK) specifică perioada de timp în care o parolă este blocată la modificare după operaţia anterioară de modificare parolă.

O modificare la această valoare de sistem se petrece imediat.

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi subiectul Valori sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 30. Valorile posibile pentru valoarea de sistem QPWDCHGBLK:

***NONE**	Parola poate fi modificată oricând.
1 - 99	O parolă nu poate fi modificată în numărul specificat de ore după o operaţie de modificare de parolă anterioară reuşită.

Intervalul de expirare a parolei (QPWDEXPITV)

Valoarea de sistem Interval expirare parolă (QPWDEXPITV) controlează numărul de zile permite înainte de modificarea 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.

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

Previous sign-on . . . . . . . . . . . . . :   10/30/99  14:15:00

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

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 31. 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: între 30 şi 90

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

Avertisment expirare parolă (QPWDEXPWRN)

Valoarea de sistem Avertisment expirare parolă (QPWDEXPWRN) specifică numărul de zile înainte de expirarea parolei la care să se înceapă afişarea de mesaje de expirare parolă când un utilizator se loghează.

O modificare la această valoare de sistem se petrece imediat.

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi subiectul Valori sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 32. Valorile posibile pentru valoarea de sistem QPWDEXPWRN:

7	Specifică că mesajul de avertisment de expirare parolă ar trebuie să înceapă să fie afişat cu 7 zile înainte de expirarea parolei.
1 - 99	Specifică numărul de zile înainte de expirarea parolei cu cât să înceapă a fi afişate mesaje de avertisment de expirare parolă.

Valoarerecomandată: 14 (zile)

Nivel parolă (QPWDLVL)

Nivelul de parolă al sistemului poate fi setat pentru a permite profilurilor de 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 pentru a permite o frază-parolă ca valoare a parolei. Termenul *frază-parolă* este uneori folosit în industria calculatoarelor pentru a descrie o valoare de parolă care poate fi foarte lungă şi are câteva restricţii asupra caracterelor 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 într-o frază-parolă sunt că nu poate începe cu un asterisc (*) şi blancurile de la sfârşit vor fi înlăturate. Înainte de a modifica nivelul de parolă al sistemului, revedeţi secţiunea Planificarea modificărilor nivelului de parolă.

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi Valori de sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorile de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 33. Valorile 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 caracterele $, @, # şi liniuţă de subliniere. • QPWDLVL 0 ar trebui folosit dacă sistemul comunică cu alte platforme System i din reţea şi acele sisteme rulează cu o valoare QPWDLVL de 0 sau o ediţie a sistemului de operare mai mică decât V5R1M0. • QPWDLVL 0 ar trebui folosită dacă sistemul dumneavoastră comunică cu orice alt sistem care limitează lungimea parolelor de 1-10 caractere. • QPWDLVL 0 trebuie folosit dacă sistemul comunică cu produsuli5/OS Support pentru Windows Network Neighborhood i5/OS NetServer) şi sistemul comunică cu alte sisteme folosind parolei între 1 şi 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 i5/OS NetServer pentru clienţi Windows 95/98/ME vor fi înlăturate din sistem. **Notă:** Produsul i5/OS Netserver va funcţiona cu clienţi Windows NT/2000/XP/Vista când nivelul de parolă este 1 sau 3. Dacă folosiţi suportul client pentru produsul i5/OS NetServer, nu puteţi folosi QPWDLVL valoarea 1. QPWDLVL 1 îmbunătăţeşte securitatea platformelor System i înlăturând toate parolele i5/OS NetServer din sistem.
2	Sistemul suportă parole de profil de 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 o revenire la QPWDLVL 0 sau 1 cât timp parola creată la QPWDLVL 2 sau 3 îndeplineşte cerinţele de lungime şi sintaxă ale unei parole valide la QPWDLVL 0 sau 1. • QPWDLVL 2 poate fi folosit dacă sistemul comunică cu produsul i5/OS Support pentru Windows Network Neighborhood i5/OS NetServer) cât timp parola are între 1 şi 14 caractere. • QPWDLVL 2 nu poatea fi folosit dacă sistemul comunică cu alte platforme System i dintr-o reţea şi acele sisteme rulează o valoare QPWDLVL de 0 sau 1 sau o ediţie a sistemului de operare mai veche decât 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 de 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. • QPWDLVL 3 nu poate fi folosit dacă sistemul comunică cu alte platforme System i dintr-o reţea şi acele sisteme rulează cu o valoare QPWDLVL de 0 sau 1 sau o ediţie a sistemului de operare mai veche decât V5R1M0. • QPWDLVL 3 nu poate fi folosit dacă sistemul dumneavoastră comunică cu orice alt sistem care limitează lungimea parolelor de 1-10 caractere. • QPWDLVL 3 nu poate fi folosit dacă sistemul comunică cu produsul i5/OS Support pentru Windows Network Neighborhood i5/OS NetServer. **Notă:** Produsul i5/OS Netserver va funcţiona cu clienţiWindows NT/2000/XP/Vista când nivelul de parolă este 1 sau 3. 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 valorile nivelului de parolă curent şi în aşteptare, folosiţi comanda Afişare atribute securitate (DSPSECA).

Lungimea minimă a parolelor (QPWDMINLEN)

Valoarea de sistem Lungimea minimă a parolelor (QPWDMINLEN) controlează numărul minim de caractere dintr-o parolă.

Observaţii:

1. Această valoare de sistem este o valoare restricţionată. Consultaţi Valori de sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorile de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.
2. Dacă valoarea de sistem QPWDRULES specifică orice valoare diferită de *PWDSYSVAL, această valoare de sistem nu poate fi modificată şi valoarea sa va fi ignorată când sunt verificate parole noi pentru a vedea dacă sunt formate corect.

Tabela 34. 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 este recomandat pentru a împiedica utilizatorii să asigneze parole care sunt uşor de ghicit, cum ar fi iniţialele numelui sau un singur caracter.

Lungimea maximă a parolelor (QPWDMAXLEN)

Valoarea de sistem Lungimea maximă a parolelor (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 îndeplinesc cerinţele reţelei dumneavoastră.

Observaţii:

1. Această valoare de sistem este o valoare restricţionată. Consultaţi Valori de sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorile de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.
2. Dacă valoarea de sistem QPWDRULES specifică orice valoare diferită de *PWDSYSVAL, această valoare de sistem nu poate fi modificată şi valoarea sa va fi ignorată când sunt verificate parole noi pentru a vedea dacă sunt formate corect.

Tabela 35. Valorile 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 Diferenţă necesară în parole (QPWDRQDDIF) controlează dacă parola trebuie să fie diferită de parolele anterioare.

Această valoare furnizează securitate suplimentară împiedicând utilizatorii să specifice parole care au fost 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. Această valoare de sistem este o valoare restricţionată. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 36. Valorile posibile pentru valoarea de sistem QPWDRQDDIF:

Valoare	*Număr de parole anterioare verificate pentru duplicate*
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 o valoare de 5 sau mai mică pentru a împiedica folosirea de parole repetate. Folosiţi o combinaţie a valorii de sistem Diferenţă necesară în parole (QPWDRQDDIF) şi valoarea de sistem Interval expirare parolă (QPWDEXPITV) pentru a împiedica o parolă să fie refolosită 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 timp de aproximativ 9 luni.

Restricţionarea caracterelor pentru parole (QPWDLMTCHR)

Valoarea de sistem Caractere restricţionate pentru parole (QPWDLMTCHR) limitează folosirea anumitor caractere 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.

Observaţii:

1. Această valoare de sistem este o valoare restricţionată. Consultaţi Valori de sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorile de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.
2. Dacă valoarea de sistem QPWDRULES specifică orice valoare diferită de *PWDSYSVAL, această valoare de sistem nu poate fi modificată şi valoarea sa va fi ignorată când sunt verificate parole noi pentru a vedea dacă sunt formate corect.

Tabela 37. Valorile posibile pentru valoarea de sistem QPWDLMTCHR:

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

Valoare recomandată: A, E, I, O sau U. Ar putea fi de asemenea necesar să împiedicaţi folosirea caracterelor speciale (#, $ şi @) pentru compatibilitatea cu alte sisteme.

Restricţionarea cifrelor consecutive pentru parole (QPWDLMTAJC)

Valoarea de sistem Restricţie de cifre consecutive pentru parole (QPWDLMTAJC) limitează folosirea de caractere numerice unul lângă altul (adiacent) 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.

Observaţii:

1. Această valoare de sistem este o valoare restricţionată. Consultaţi Valori de sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorile de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.
2. Dacă valoarea de sistem QPWDRULES specifică orice valoare diferită de *PWDSYSVAL, această valoare de sistem nu poate fi modificată şi valoarea sa va fi ignorată când sunt verificate parole noi pentru a vedea dacă sunt formate corect.

Tabela 38. 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 Restricţie de caractere repetate pentru parole (QPWDLMTREP) limitează folosirea de caractere care se repetă 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’.

Observaţii:

1. Această valoare de sistem este o valoare restricţionată. Consultaţi Valori de sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorile de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.
2. Dacă valoarea de sistem QPWDRULES specifică orice altă valoare decât *PWDSYSVAL, această valoare de sistem nu poate fi modificată şi valoarea sa va fi ignorată când sunt verificate parolele noi pentru a vedea dacă sunt formate corect.

Tabela 39. Valorile posibile pentru valoarea de sistem QPWDLMTREP:

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

Tabela 40 arată exemple de parole permise în funcţie de valoarea de sistem QPWDLMTREP.

Tabela 40. Parole cu caractere care se repetă pentru QPWDLVL 0 sau 1

Exemplu de parolă	QPWDLMTREP cu valoarea 0	QPWDLMTREP cu valoarea 1	QPWDLMTREP cu valoarea 2
A11111	Permisă	Nepermisă	Nepermisă

Tabela 40. Parole cu caractere care se repetă pentru QPWDLVL 0 sau 1 (continuare)

Exemplu de parolă	QPWDLMTREP cu valoarea 0	QPWDLMTREP cu valoarea 1	QPWDLMTREP cu valoarea 2
BOBBY	Permisă	Nepermisă	Nepermisă
AIRPLANE	Permisă	Nepermisă	Permisă
N707UK	Permisă	Nepermisă	Permisă

Tabela 41. Parole cu caractere care se repetă pentru QPWDLVL 2 sau 3

Exemplu de parolă	QPWDLMTREP cu valoarea 0	QPWDLMTREP cu valoarea 1	QPWDLMTREP cu valoarea 2
j222222	Permisă	Nepermisă	Nepermisă
ReallyFast	Permisă	Nepermisă	Nepermisă
Mom'sApPlePie	Permisă	Nepermisă	Permisă
AaBbCcDdEe	Permisă	Permisă	Permisă

Diferenţa poziţiei caracterelor pentru parole (QPWDPOSDIF)

Valoarea de sistem Diferenţă poziţie caractere pentru parole (QPWDPOSDIF) controlează fiecare poziţie dintr-o parolă nouă.

Această valoare de sistem furnizează securitate suplimentară împiedicând utilizatorii să folosească acelaşi caracter (alfabetic sau numeric) într-o poziţie corespunzătoare cu aceeaşi poziţie 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'.

Observaţii:

1. Această valoare de sistem este o valoare restricţionată. Consultaţi Valori de sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorile de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.
2. Dacă valoarea de sistem QPWDRULES specifică orice valoare diferită de *PWDSYSVAL, această valoare de sistem nu poate fi modificată şi valoarea sa va fi ignorată când sunt verificate parole noi pentru a vedea dacă sunt formate corect.

Tabela 42. Valorile posibile pentru valoarea de sistem QPWDPOSDIF:

0	Pot fi folosite aceleaşi caractere într-o poziţie corespunzătoare aceleaşi poziţii din parola anterioară.
1	Nu poate fi folosit acelaşi caracter într-o poziţie corespunzătoare aceleaşi poziţii din parola anterioară.

Necesitatea caracterelor numerice în parole (QPWDRQDDGT)

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

Observaţii:

1. Această valoare de sistem este o valoare restricţionată. Consultaţi Valori de sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorile de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

2. Dacă valoarea de sistem QPWDRULES specifică orice valoare diferită de *PWDSYSVAL, această valoare de sistem nu poate fi modificată şi valoarea sa va fi ignorată când sunt verificate parole noi pentru a vedea dacă sunt formate corect.

Tabela 43. Valorile 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

Reguli parole (QPWDRULES)

Valoarea de sistem Reguli parole (QPWDRULES) specifică regulile folosite pentru a verifica dacă o parolă este formată corect. Puteţi specifica mai multe valori pentru valoarea de sistem QPWDRULES, dacă nu specificaţi *PWDSYSVAL.

Modificările făcute asupra acestei valori de sistem au efect următoarea dată când este modificată o parolă.

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi subiectul Valori sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 44. Valorile posibile pentru valoarea de sistem QPWDRULES:

***PWDSYSVAL**	Această valoare specifică faptul că QPWDRULES este ignorată şi sunt folosite celelalte valori de sistem parolă pentru a verifica dacă o parolă este formată corect. Aceste alte valori de sistem parolă includ QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDMAXLEN, QPWDMINLEN, QPWDPOSDIF şi QPWDQDDGT. **Notă:** Dacă orice altă valoare înafară de *PWDSYSVAL este specificată pentru QPWDRULES, valorile de sistem QPWDLMTAJC, QPWDLMTCHR, QPWDLMTREP, QPWDMAXLEN, QPWDMINLEN, QPWDPOSDIF şi QPWDRQDDGT sunt ignorate când o nouă parolă este verificată pentru a vedea dacă este formată corect. În plus, orice încercare de a modifica aceste valori de sistem va fi refuzată atâta timp cât valoarea de sistem QPWDRULES conţine altă valoare decât *PWDSYSVAL.

***CHRLMTAJC**	Valoarea specifică faptul că o parolă nu poate conţine 2 sau mai multe apariţii ale aceluiaşi caracter poziţionate adiacent. Această valoare realizează aceeaşi funcţie ca specificarea valorii 2 pentru QPWDLMTREP. Dacă s-a specificat *CHRLMTREP, această valoare nu poate fi specificată.
	Exemple:
	`Better.test nevalidă - tt`
	`fix11bugs nevalidă - 11`
	`@12/A78 validă`
	`A1234A1234 validă`

Tabela 44. Valorile posibile pentru valoarea de sistem QPWDRULES: (continuare)

***CHRLMTREP**	Valoarea specifică faptul că o parolă nu poate conţine 2 sau mai multe apariţii ale aceluiaşi caracter. Această valoare realizează aceeaşi funcţie ca specificarea valorii 1 pentru QPWDLMTREP. Dacă s-a specificat *CHRLMTAJC, această valoare nu poate fi specificată.
	Exemple:
	`John.Jones nevalidă - J o n`
	`THISONEOK nevalidă - O`
	`@12/A78 validă`
	`AaCcEeFfGg validă`

***DGTLMTAJC**	Valoarea specifică faptul că o parolă nu poate conţine 2 sau mai multe caractere cifră adiacente.
	Exemple:
	`@12/A78 nevalidă`
	`!@#$%a1234. nevalidă`
	`THISONEOK validă`
	`A1B2C3DE5 validă`

***DGTLMTFST**	Valoarea specifică faptul că primul caracter al unei parole nu poate fi un caracter cifră. Dacă au fost specificate *LTRLMTFST şi *SPCCHRLMTFST, această valoare nu poate fi specificată. Dacă sistemul operează la nivel de parolă 0 sau 1, funcţionează ca şi cum ar fi specificată *DGTLMTFST.
	Exemple:
	`16ST-SW-Roch nevalidă - 1`
	`99BottlesOfBeer nevalidă - 9`
	`@12/A78 validă`
	`Allow-this.1 validă`

***DGTLMTLST**	Valoarea specifică faptul că ultimul caracter al parolei nu poate fi un caracter cifră. Dacă au fost specificate *LTRLMTLST şi *SPCCHRLMTLFST, această valoare nu poate fi specificată.
	Exemple:
	`John.doe12 nevalidă - 2`
	`@12/A78 nevalidă - 8`
	`THISONEOK validă`
	`A1234b123. validă`

***DGTMAXn**	Valoarea specifică numărul maxim de caractere cifră care pot apărea în parolă. **n** este un număr între 0 şi 9.
	
	Doar o valoare *DGTMAXn poate fi specificată. Dacă o valoare *DGTMINn este de asemenea specificată, valoarea n specificată pentru *DGTMAXn trebuie să fie mai mare sau egală cu valoarea n specificată pentru *DGTMINn.
	Exemple: pentru *DGTMAX2
	`Q12345678 nevalidă - 6 cifre în plus`
	`3-2-1->Go nevalidă - 1 cifră în plus`
	`Rick1 validă`
	`Ed1-Jeff3 validă`

Tabela 44. Valorile posibile pentru valoarea de sistem QPWDRULES: (continuare)

***DGTMINn**	Valoarea specifică numărul minim de caractere cifră care trebuie să apară în parolă. **n** este un număr între 0 şi 9.
	
	Doar o valoare *DGTMINn poate fi specificată. Dacă o valoare *DGTMAXn este de asemenea specificată, valoarea n specificată pentru *DGTMAXn trebuie să fie mai mare sau egală cu valoarea n specificată pentru *DGTMINn.
	Exemple: pentru *DGTMIN3
	`Rick1 nevalidă - doar 1 cifră`
	`Ed1-Jeff3 nevalidă - doar 2 cifre`
	`3-2-1->Go validă`
	`Q12345678 validă`

***LMTSAMPOS**	Nu poate fi folosit acelaşi caracter într-o poziţie corespunzătoare aceleaşi poziţii din parola anterioară. Această valoare realizează aceeaşi funcţie ca valoarea de sistem QPWDPOSDIF.
	
	Când parola este setată de comanda Modificare profil de utilizator (CHGUSRPRF) sau Creare profil de utilizator (CRTUSRPRF), această regulă de parolă nu poate fi verificată deoarece valoare anterioară a parolei nu este livrată.
	Exemple: pentru *LMTSAMPOS când Vote4Me a fost parola anterioară:
	`Victory1 nevalidă - V în poziţia 1`
	`Mine2love nevalidă - e în poziţia 4`
	`vOTE-mE validă (literele sunt diferite)`
	`Allisgood validă`

***LMTPRFNAME**	Valoare parolei în litere mari nu poate conţine numele complet de profil de utilizator în poziţii consecutive.
	Exemple: pentru *LMTPRFNAME cu numele de profil JOHNB:
	`bigJOHNB9 nevalidă - poziţiile 4-8`
	`JohnB78 nevalidă - poziţiile 1-5`
	`J_ohn_B234 validă`
	`john_b validă`

***LTRLMTAJC**	Valoarea specifică faptul că o parolă nu poate conţine 2 sau mai multe caractere literă adiacente.
	Exemple:
	`John.Smith nevalidă`
	`THISONEOK nevalidă`
	`@12/A78 validă`
	`A1234b1234 validă`

***LTRLMTFST**	Valoarea specifică faptul că primul caracter al unei parole nu poate fi un caracter literă. Dacă au fost specificate *DGTLMTFST şi *SPCCHRLMTFST această valoare nu poate fi specificată. Dacă sistemul operează cu QPWDLVL 0 sau 1, *LTRLMTFST şi *SPCCHRLMTFST nu pot fi specificate ambele.
	Exemple:
	`John.Smith nevalidă - J`
	`THISONEOK nevalidă - T`
	`@12/A78 validă`
	`16ST-SW-Roch validă`

Tabela 44. Valorile posibile pentru valoarea de sistem QPWDRULES: (continuare)

***LTRLMTLST**	Valoarea specifică faptul că ultimul caracter al parolei nu poate fi un caracter literă. Dacă au fost specificate *DGTLMTLST şi *SPCCHRLMTLST, această valoare nu poate fi specificată.
	Exemple:
	`John.Smith nevalidă - h`
	`1Allow.It nevalidă - t`
	`@12/A78 validă`
	`(pay*rate) validă`

***LTRMAXn**	Valoarea specifică numărul maxim de caractere literă care pot apărea în parolă. **n** este un număr între 0 şi 9.
	
	Doar o valoare *LTRMAXn poate fi specificată. Dacă o valoare *LTRMINn este de asemenea specificată, valoarea n specificată pentru *LTRMAXn trebuie să fie mai mare sau egală cu valoarea n specificată pentru *LTRMINn.
	
	Dacă o valoare *MIXCASEn este de asemenea specificată, valoarea n specificată pentru *LTRMAXn trebuie să fie mai mare sau egală cu de 2 ori valoarea n specificată pentru *MIXCASEn.
	Exemple: pentru *LTRMAX4
	`THISONEOK nevalidă - 5 litere în plus`
	`John.Smith1 nevalidă - 5 litere în plus`
	`John1423 validă`
	`A1b2.#456 validă`

***LTRMINn**	Valoarea specifică numărul minim de caractere literă care trebuie să apară în parolă. **n** este un număr între 0 şi 9.
	
	Doar o valoare *LTRMINn poate fi specificată. Dacă o valoare *LTRMAXn a fost specificată, valoarea n specificată pentru *LTRMAXn trebuie să fie mai mare sau egală cu valoarea n specificată pentru *LTRMINn.
	Exemple: pentru *LTRMIN2
	`@12/A78 nevalidă - doar 1 literă`
	`!@#$%a1234 nevalidă - doar 1 literă`
	`THISONEOK validă`
	`A1234b1234 validă`

Tabela 44. Valorile posibile pentru valoarea de sistem QPWDRULES: (continuare)

***MAXLENnnn**	Valoarea specifică numărul maxim de caractere dintr-o parolă. **nnn** este un număr între 1 şi 128 (fără zerouri la început). Această valoare realizează aceeaşi funcţie ca valoarea de sistem QPWDMAXLEN. Dacă sistemul operează la QPWDLVL 0 sau 1, intervalul valid este între 1 şi 10. Dacă sistemul operează la QPWDLVL 2 sau 3, intervalul valide este între 1 şi 128. Valoarea nnn specificată trebuie să fie suficient de mare pentru a respecta toate cerinţele *MIXCASEn, *DGTMAXn, *LTRMAXn, *SPCCHRMAXn, restricţiile de prim şi ultim caracter şi cerinţele de caractere neadiacente. Dacă *MINLENnnn este de asemenea specificat, valoarea nnn specificată pentru *MAXLENnnn trebuie să fie mai mare sau egală cu valoarea nnn specificată pentru *MINLENnnn. Dacă nu este specificată nicio valoare *MAXLENnnn, o valoare *MAXLEN10 este presupusă dacă sistemul operează cu o valoare QPWDLVL de 0 sau 1 sau o valoare de *MAXLEN128 este presupusă dacă sistemul operează cu o valoare QPWDLVL de 2 sau 3.
***MINLENnnn**	Valoarea specifică numărul minim de caractere dintr-o parolă. **nnn** este un număr între 1 şi 128 (fără zerouri la început). Dacă sistemul operează la QPWDLVL 0 sau 1, intervalul valid este între 1 şi 10. Dacă sistemul operează la QPWDLVL 2 sau 3, intervalul valid este între 1 şi 128. Dacă *MAXLENnnn este de asemenea specificat, valoarea nnn specificată pentru *MAXLENnnn trebuie să fie mai mare sau egală cu valoarea nnn specificată pentru *MINLENnnn. Dacă nicio valoare *MINLENnnn nu este specificată, o valoare *MINLEN1 este presupusă.

***MIXCASEn**	Valoarea specifică faptul că o parolă trebuie să conţină cel puţin n litere mari şi n litere mici. **n** este un număr între 0 şi 9.Această valoare este refuzată dacă sistemul operează cu o valoare QPWDLVL de 0 sau 1 deoarece parolele trebuie să fie în litere mari.
	
	Doar o valoare*MIXCASEn poate fi specificată.
	
	Dacă o valoare *LTRMAXn a fost specificată, valoarea n specificată pentru *LTRMAXn trebuie să fie mai mare sau egală cu de două ori valoarea n specificată pentru *MIXCASEn.
	Exemple: pentru *MIXCASE2
	`@12/A78bC nevalidă - lipseşte 1 literă mică`
	`THISONEOK nevalidă - lipseşte 2 litere mici`
	`ThisIsOkay validă`
	`Allow-It validă`

Tabela 44. Valorile posibile pentru valoarea de sistem QPWDRULES: (continuare)

***REQANY3**	Valoarea specifică faptul că o parolă trebuie să conţină caractere din cel puţin trei dintre următoarele tipuri.
	• Litere mari
	• Litere mici
	• Cifre
	• Caractere speciale
	
	Când sistemul operează cu QPWDLVL 0 sau 1, *REQANY3 are acelaşi efect ca şi cum s-ar fi specificat *DGTMIN1, *LTRMIN1 şi *SPCCHRMIN1.
	Exemple:
	`THISONEOK nevalidă - doar 1 tip`
	`@12/-78 nevalidă - doar 2 tipuri`
	`A1234b1234 validă - mare, mică, cifră`
	`John.Smith validă - mare, mică, special`
	`peter(21) validă - mică, special, cifră`

***SPCCHRLMTAJC**	Valoarea specifică faptul că o parolă nu poate conţine 2 sau mai multe caractere speciale adiacente (consecutive). Un caracter este considerat special când caracterul echivalent unicode nu este o literă sau o cifră.
	Exemple:
	`Big//Box nevalidă`
	`this->way nevalidă`
	`@12/A78 validă`
	`John.Smith validă`

***SPCCHRLMTFST**	Valoarea specifică faptul că primul caracter al unei parole nu poate fi un caracter special. Un caracter este considerat special când caracterul echivalent unicode nu este o literă sau o cifră.
	
	Dacă valorile *DGTLMTFST şi *LTRLMTFST au fost specificate, această valoare nu poate fi specificată. Dacă sistemul operează cu o valoare QPWDLVL de 0 sau 1, *LTRLMTFST şi *SPCCHRLMTFST nu pot fi ambele specificate.
	Exemple:
	`(2+2equals4) nevalidă - (`
	`#fred/#charlie nevalidă - #`
	`1Good->one12 validă`
	`A1234b1234 validă`

***SPCCHRLMTLST**	Valoarea specifică faptul că ultimul caracter al parolei nu poate fi un caracter special. Un caracter este considerat special când caracterul echivalent unicode nu este o literă sau o cifră.
	
	Dacă au fost specificate valorile *DGTLMTLST şi *LTRLMTLST, această valoare nu poate fi specificată.
	Exemple:
	`A1234b123. nevalidă - .`
	`>John.Doe< nevalidă - <`
	`THISONEOK validă`
	`@12/A78 validă`

Tabela 44. Valorile posibile pentru valoarea de sistem QPWDRULES: (continuare)

***SPCCHRMAXn**	Valoarea specifică numărul maxim de caractere speciale care ar putea apărea în parolă. **n** este un număr între 0 şi 9. Un caracter este considerat caracter special când caracterul unicode echivalent nu este literă sau cifră.
	
	Poate fi specificată o singură valoare *SPCCHRMAXn. Dacă a fost specificată o valoare *SPCCHRMINn, valoarea n specificată pentru *SPCCHRMAXn trebuie să fie mai mare sau egală cu valoarea n specificată pentru *SPCCHRMINn.
	Exemple: pentru *SPCCHRMAX3
	`@12/A78.b#  nevalidă - cu 1 prea multe`
	`!@#$%a1234  not valid - cu 2 prea multe`
	`THISONEOK  validă`
	`A1234b-234  validă`

***SPCCHRMINn**	Valoarea specifică numărul minim de caractere speciale care trebuie să apară în parolă. **n** este un număr între 0 şi 9. Un caracter este considerat caracter special dacă caracterul unicode echivalent are proprietatea de a nu fi literă sau cifră.
	
	Doar o valoare *SPCCHRMINn poate fi specificată.Dacă o valoare *SPCCHRMAXn a fost specificată, valoare n specificată pentru *SPCCHRMAXn trebuie să fie mai mare sau egală cu valoarea n specificată pentru *SPCCHRMINn.
	Exemple: pentru *SPCCHRMIN4
	`Su@us.ibm.com  nevalidă - cu 1 prea puţine`
	`123+45=168  nevalidă - cu 2 prea puţine`
	`A.B@us.ibm.com validă`
	`(24/8=3)  validă`

Programul de aprobare a parolei (QPWDVLDPGM)

Puteţi specifica Program aprobare parolă (QPWDVLDPGM) pentru a controla validarea noilor parole.

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.

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. Consultaţi Valori de sistem securitate pentru detalii despre cum să restricţionaţi modificările asupra valorile de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 45. 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.

Tabela 45. Valorile posibile pentru valoarea de sistem QPWDVLDPGM: (continuare)

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 parole

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 a trecut toate celelalte teste specificate în valoare de sistem de control parolă.

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 46. Parametrii pentru program de aprobare parole

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 mesaj escape şi un cod de retur 0. Deoarece codul de retur este setat iniţial pentru parole care nu sunt valide (diferit de zero), programul de aprobare trebuie să seteze codul de retur la 0 înainte ca parolă să poată fi 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 responsabilul cu securitatea şi că modificările aduse programului 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 QPWDVLDPGM. 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:

Notă: Folosind exemplele de cod, sunteţi de acord cu termenii din Capitolul 10, “Informaţii referitoare la licenţa de cod şi declinarea responsabilităţii”, la pagina 307.

```
/************************************************/
/* 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 de utilizator. 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.                                 */
/*********************************************************/

PGM   PARM(&EXINPUT &RTN)
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(EXINPUT 61 4))
CHGVAR &NPOFF VALUE(EXINPUT 57 4) + 1)
CHGVAR &UNAME VALUE(EXINPUT 33 10))
CHGVAR &NEWPW VALUE(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(EXINPUT 65 4) = 13488) THEN(DO)
    CHGVAR &INDX2 VALUE(1)
    CHGVAR &INDX3 VALUE(1)
   CVT1:
    CHGVAR &XLTCHR VALUE(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 NEWPW &INDX3 1) VALUE(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 EXINPUT 65 4) VALUE(X'00000025')
ENDDO

/* Check the CCSID of the new password value - must be 37     */
IF COND(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 XLTCHR2 2 1) VALUE(NEWPW &INDX2 1))
  CHGVAR &XLTCHR VALUE(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(XLATEC &XLTCHR 1) *NE '.') +
  THEN(CHGVAR NEWPW &INDX3 1) VALUE(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(NEWPW &NPLEN 1) = '0') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '1') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '2') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '3') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '4') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '5') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '6') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '7') THEN(GOTO ERROR1)
IF COND(NEWPW &NPLEN 1) = '8') THEN(GOTO ERROR1)
IF COND(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(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(NEWPW &INDX &UNLEN) = 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 de auditarerii

Auditarea activităţii sistemului este o parte importantă a securităţii sistemului, deoarece poate ajuta la detectarea folosirii greşite a sistemului şia intruziunilor. Puteţi folosi valori de sistem specifice pentru a controla auditarea pe sistemul de operare i5/OS.

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

Controlul auditării (QAUDCTL)

Valoarea de sistem Control auditare (QAUDCTL) determină dacă este realizată auditare.

Această valoare de sistem funcţionează precum un comutator deschis sau închis pentru următoarele operaţii:

- Valorile de sistem QAUDLVL şi QAUDLVL2
- Auditarea definită pentru obiecte folosind comenzile Modificare auditare obiecte (CHGOBJAUD), Modificare valoare auditare (CHGAUD) şi Modificare DLO auditare (CHGDLOAUD)
- Auditarea definită pentru utilizatori folosind comanda Modificare auditare utilizatori (CHGUSRAUD)

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi 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 47. Valorile posibile pentru valoarea de sistem QAUDCTL

***NONE**	Nici o auditare nu este realizată pentru acţiuni utilizator şi obiecte.
***NOTAVL**	Această valoare indică faptul că valoarea de sistem nu este disponibilă utilizatorului deoarece acesta nu are autorizarea specială *AUDIT sau *ALLOBJ. Nu puteţi seta valoarea de sistem la această valoare.
***OBJAUD**	Auditare este realizată 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 Modificare auditare utilizator (CHGUSRAUD).
***NOQTEMP**	Pentru majoritatea acţiunilor auditarea nu este realizată dacă obiectul este în biblioteca QTEMP. Consultaţi Capitolul 9, “Auditarea securităţii pe System i”, la pagina 257 pentru mai multe detalii. Trebuie să specificaţi această valoare cu *OBJAUD sau *AUDLVL.
	Vedeţi “Planificarea auditării securităţii” la pagina 263 pentru o descriere completă a procesului pentru controlarea auditării pe sistemul dumneavoastră.

Acţiunea pentru oprirea auditării (QAUDENDACN)

Valoarea de sistem Auditare terminare acţiune (QAUDENDACN) determină ce acţiune face sistemul dacă auditarea este activă şi sistemul nu poate scrie intrări în jurnalul de auditare.

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 48. Valorile posibile pentru valoarea de sistem QAUDENDACN:

***NOTAVL**	Această valoare este afişată pentru a indica faptul că valoarea de sistem nu este disponibilă utilizatorului deoarece utilizatorul nu are nici autoritate specială *AUDIT nici *ALLOBJ. Valoarea sistemului nu poate fi setată la această valoare.
***NOTIFY**	Mesajul CPI2283 este trimis cozii de mesaje QSYSOPR şi cozii de mesaje QSYSMSG (dacă aceasta există) la fiecare 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.

Tabela 48. Valorile posibile pentru valoarea de sistem QAUDENDACN: (continuare)

***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, *NOTIFY este valoarea recomandată. 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 Nivel forţă auditare (QAUDFRCLVL) determină cât de des sunt forţate intrări nou de jurnal de auditare din memorie în spaţiu 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. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 49. Valorile posibile pentru valoarea de sistem QAUDFRCLVL

***NOTAVL**	Această valoare este afişată pentru a indica faptul că valoarea de sistem nu este disponibilă utilizatorului deoarece utilizatorul nu are nici autoritate specială *AUDIT nici *ALLOBJ. Valoarea sistemului nu poate fi setată la această valoare.
***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 necesită să nu fie pierdute intrări de auditare când sistemul se termină anormal, trebuie să specificaţi 1. Specificarea valorii 1 ar putea afecta performanţa.

Nivelul de auditare (QAUDLVL)

Valoarea de sistem Nivel de auditare (QAUDLVL) împreună cu valoarea de sistem QAUDLVL2 determină ce evenimente legate de securitate sunt înregistrate în jurnalul de auditare securitate (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. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 50. Valorile 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.
***NOTAVL**	Această valoare este afişată pentru a indica faptul că valoarea de sistem nu este disponibilă utilizatorului deoarece utilizatorul nu are nici autoritate specială *AUDIT nici *ALLOBJ. Valoarea sistemului nu poate fi setată la această valoare.
***AUDLVL2**	Ambele valori de sistem, QAUDLVL şi QAUDLVL2, vor fi folosite pentru a determina acţiunile de securitate care vor fi auditate.
***ATNEVT**	Sunt înregistrate evenimentele de atenţionare
***AUTFAIL**	Sunt înregistrate evenimentele de eşuare a autorizării.
***CREATE**	Operaţiile de creare obiect sunt înregistrate în istoric.
***DELETE**	Operaţiile de ştergere obiect sunt înregistrate în istoric.
***JOBBAS**	Funcţii de bază job sunt auditate.
***JOBCHGUSR**	Modifică la profilul de utilizator activ al unui fir de execuţie sau profilurile de grup sunt auditate.
***JOBDTA**	Sunt înregistrate acţiunile care afectează un job. *JOBDTA este compus din două valori, care sunt *JOBBAS şi *JOBCHGUSR, pentru a vă permite să personalizaţi mai bine auditarea.Dacă sunt specificate ambele valori, veţi obţine aceeaşi auditarea ca şi acum ar fi specificat doar *JOBDTA.
***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 mai multe valori pentru a vă permite să personalizaţi mai bine auditarea. Următoarele valori compun *NETCMN: *NETBAS *NETCLU *NETFAIL *NETSCK
***NETFAIL**	Sunt auditate eşuările de reţea.
***NETSCK**	Sunt auditate taskurile de socket.
***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.
***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**	Operaţiile de salvare şi restaurare sunt înregistrate în istoric.
***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.

Tabela 50. Valorile posibile pentru valoarea de sistem QAUDLVL (continuare)

***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 mai multe valori pentru a vă permite să personalizaţi mai bine auditarea. Următoarele valori compun *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**	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.

Referinţe înrudite

"Planificarea acţiunilor de auditare" la pagina 263
Valoarea de sistem QAUDCTL (control auditare), valoarea de sistem QAUDLVL (nivel auditare), valoarea de sistem QAUDLVL2 (extensie nivel auditare) şi parametrul AUDLVL (auditare acţiune) din profilurile de utilizator lucrează împreună pentru a controla auditarea acţiunilor.

Extensia nivelului de auditare (QAUDLVL2)

Valoarea de sistem Extensie nivel auditare (QAUDLVL2) este necesară când mai mult de şaisprezece valori de auditare sunt necesare.

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. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 51. Valorile posibile pentru valoarea de sistem QAUDLVL2

***NONE**	În această valoare de sistem nu este conţinută nici o valoare de auditare.
***NOTAVL**	Această valoare este afişată pentru a indica faptul că valoarea de sistem nu este disponibilă utilizatorului deoarece utilizatorul nu are nici autoritate specială *AUDIT nici *ALLOBJ. Valoarea sistemului nu poate fi setată la această valoare.
***ATNEVT**	Sunt înregistrate evenimentele de atenţionare
***AUTFAIL**	Sunt înregistrate evenimentele de eşuare a autorizării.
***CREATE**	Operaţiile de creare obiect sunt înregistrate în istoric.
***DELETE**	Operaţiile de ştergere obiect sunt înregistrate în istoric.
***JOBBAS**	Funcţii de bază job sunt auditate.

Tabela 51. Valorile posibile pentru valoarea de sistem QAUDLVL2 (continuare)

***JOBCHGUSR**	Modifică la profilul de utilizator activ al unui fir de execuţie sau profilurile de grup sunt auditate.
***JOBDTA**	Sunt înregistrate acţiunile care afectează un job. *JOBDTA este compus din două valori, care sunt *JOBBAS şi *JOBCHGUSR, pentru a vă permite să personalizaţi mai bine auditarea.Dacă sunt specificate ambele valori, veţi obţine aceeaşi auditarea ca şi acum ar fi specificat doar *JOBDTA.
***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 personalizaţi mai bine auditarea dumneavoastră. Următoarele valori compun *NETCMN: *NETBAS *NETCLU *NETFAIL *NETSCK
***NETFAIL**	Sunt auditate eşuările de reţea.
***NETSCK**	Sunt auditate taskurile de socket.
***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.
***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 compun *SECURITY: *SECCFG *SECDIRSRV *SECIPC *SECNAS *SECRUN *SECSCKD *SECVFY *SECVLDL
***SECVFY**	Este auditată folosirea funcţiilor de verificare.

Tabela 51. Valorile posibile pentru valoarea de sistem QAUDLVL2 (continuare)

***SECVLDL**	Sunt auditate modificările aduse obiectelor din lista de validare.
***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.

Referinţe înrudite

"Planificarea acţiunilor de auditare" la pagina 263
Valoarea de sistem QAUDCTL (control auditare), valoarea de sistem QAUDLVL (nivel auditare), valoarea de sistem QAUDLVL2 (extensie nivel auditare) şi parametrul AUDLVL (auditare acţiune) din profilurile de utilizator lucrează împreună pentru a controla auditarea acţiunilor.

Auditarea noilor obiecte (QCRTOBJAUD)

Valoarea de sistem Auditare pentru obiecte noi (QCRTOBJAUD) este folosită pentru a determina valoarea de auditare pentru un obiect nou, dacă valoarea implicită creare auditare obiect pentru biblioteca sau directorul noului obiect 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 obiect folosind comanda CHGOBJAUD sau CHGAUD.

Notă: Această valoare de sistem este o valoare restricţionată. Consultaţi Valorile de sistem de securitate pentru detalii despre cum să restricţionaţi modificarea valorilor de sistem de securitate şi o listă completă a valorilor de sistem restricţionate.

Tabela 52. Valorile posibile pentru valoarea de sistem QCRTOBJAUD:

***NONE**	Nu este realizată nici o auditare pentru obiect.
***NOTAVL**	Această valoare este afişată pentru a indica faptul că valoarea de sistem nu este disponibilă utilizatorului deoarece utilizatorul nu are nici autoritate specială *AUDIT nici *ALLOBJ. Valoarea sistemului nu poate fi setată la această valoare.
***USRPRF**	Auditarea obiectului este bazată pe valoarea din profilul de utilizator 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. 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. "Planificarea auditării accesului la obiecte" la pagina 286 vă oferă informaţii suplimentare despre metodele de a seta auditarea obiectelor în sistem. Puteţi control valoarea de auditare la nivel de director cu parametrul CRTOBJAUD în comanda Creare director (CRTDIR) şi valoarea *CRTOBJAUD în comanda Modificare atribut (CHGATR). Puteţi de asemenea control valoarea de auditare la nivel de bibliotecă cu parametrul CRTOBJAUD cu comanda CRTLIB şi comanda CHGLIB.

Capitolul 4. Profilurile de utilizator

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 Lucru cu profiluri de utilizator (WRKUSRPRF)

Comanda Modificare auditare utilizator (CHGUSRAUD)

Autorizare:

Autorizarea specială *SECADM

Autorizarea specială *AUDIT pentru modificarea auditării de utilizator

Intrare jurnal:

AD pentru modificări asupra auditării de utilizator

CO pentru crearea unui profil de utilizator

CP pentru modificări asupra profilurilor de utilizator

DO pentru ştergerea unui profil de utilizator

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

Concepte înrudite

"Profilurile de utilizator" la pagina 4
Pe sistemul de operare i5/OS, fiecare utilizator al sistemului are un profil de utilizator.

Roluri ale profilurilor de utilizator

Un profil de utilizator conţine parolele unui utilizator, lista de autorizări speciale asignate unui utilizator şi obiectele pe care le posedă utilizatorul.

Un profil de 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. "Valorile implicite pentru profilurile de utilizator" la pagina 317 din Anexa B, "profiluri de utilizator furnizate de IBM", la pagina 317 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, care furnizează aceeaşi autorizare unui grup de utilizatori.

Folosirea unui profil de grup pe sistem are două scopuri:

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 membru în maxim 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 desemna un profil ca profil de grup când îl creaţi, specificând o valoare în parametrul GID. “Planificarea profilurilor de utilizator” la pagina 238 arată un exemplu de setare a unui profil de grup.

Câmpuri parametru profil de utilizator

Acest subiect descrie informaţii detaliate despre câmpurile parametru pentru profilurile de utilizator arătate în prompt-ul Creare profil de utilizator.

Când creaţi un profil de utilizator, sistemul acordă aceste autorizări profilului: *OBJMGT, *CHANGE. Aceste autorizări sunt necesare pentru funcţiile sistemului şi nu trebuie înlăturate.

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

- Nivelul de asistenţă elementar, care conţine informaţii mai puţine şi nu foloseşte terminologie tehnică.
- Nivelul de asistenţă intermediar, care arată mai multe informaţii şi foloseşte termeni tehnici.
- Nivelul de asistenţă 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 asistenţă elementar, cât şi în cele la nivel de asistenţă intermediar.

Titlu câmp
Titlul secţiunii arată cum apare numele de câmp în prompt-ul de comandă Creare profil de utilizator. Titlul este afişat când crea un profil de utilizator cu nivel de ajutor mediu sau comanda Creare profil de utilizator (CRTUSRPRF).

Promptul Adăugare utilizator:
Acesta arată cum apare numele de câmp în ecranul Adăugare utilizator şi alte ecrane de profil de utilizator care folosesc nivelul de asistenţă elementar. Ecranele la nivel de asistenţă elementar afişează un subset al câmpurilor din profilul de utilizator. *Neafişat* înseamnă că acel câmp nu apare în ecranul la nivel de asistenţă elementar. Când folosiţi ecranul Adăugare utilizator pentru a crea un profil de 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 de utilizator (RTVUSRPRF) într-un program CL, aceasta este lungimea pe care ar trebui să o folosiţi pentru a defini câmpul asociat cu parametrul.

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, aveţi nevoie de autorizarea corespunzătoare listată. 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 de utilizator

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.

Promptul Adăugare utilizator:

Utilizator

Parametru CL:

USRPRF

Lungime:

10

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 (_), arond (@).

Numele profilului de utilizator nu poate începe cu o cifră.

Observaţii:

- Ecranul Adăugare utilizator permite numai un nume de utilizator de opt caractere.
- 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 de nume în sistem, consultaţi subiectul CL programming.

Recomandări pentru denumirea profilurilor de utilizator: Luaţi în considerare aceste lucru când decideţi cum să denumiţi profiluri 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 pe care le folosiţi pentru a gestiona profiluri de utilizator arată profilurile de utilizator în ordine alfabetică după numele de profil.

- Evitaţi folosirea caracterelor speciale în numele de profiluri de utilizator. Caracterele speciale ar putea cauza probleme cu maparea pe tastatură pentru anumite staţii de lucru sau cu versiunile de limbă naţională ale programului licenţiat i5/OS.

O tehnică pentru asignarea de nume de profiluri de utilizator este de a folosi primele şapte caractere ale numelui familiei urmat de primul caracter al numelui. De exemplu:

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

Recomandări pentru denumirea profilurilor de grup: Pentru a identifica uşor profilurile de grup în sistem, folosiţi o convenţie de numire. Începeţi toate numele de profiluri de grup cu aceleaşi caractere, precum GRP (pentru grup) sau DPT (pentru departament).

Parolă

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).

Promptul Adăugare utilizator:
Parolă

Parametru CL:
PAROLĂ

Lungime:
128

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 Nivel parolă (QPWDLVL) este 0 sau 1, regulile pentru specificarea parolelor sunt aceleaşi ca cele folosite pentru nume 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 Q12345 ca parolă în ecranul Modificare parolă, utilizatorul poate specifica 12345 sau Q12345 ca parolă în ecranul de semnare. Când QPWDLVL este 2 sau 3, utilizatorul trebuie să specifice parola ca Q12345 în ecranul de semnare dacă profilul de utilizator a fost creat cu o parolă de 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 Nivel parolă (QPWDLVL) este 2 sau 3, parola este sensibilă la majuscule şi poate conţine orice caracter inclusiv caractere blanc. Totuşi, parola nu poate începe cu un caracter asterisc (’*’) 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 semnarea prin ecranul de semnare al sistemului. 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 de 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. Un utilizator nu poate seta parola egală cu numele profilului de utilizator folosind comanda CHGPWD, meniul ASSIST sau API-ul QSYCHGPW în oricare din următoarele condiţii.

- Valoarea de sistem QPWDRULES este *PWDSYSVAL şi valoarea de sistem Lungime minimă parolă (QPWDMINLEN) nu este 1.
- Valoarea de sistem QPWDRULES este *PWDSYSVAL şi valoarea de sistem Lungime maximă parolă (QPWDMAXLEN) nu este 10.
- Valoarea de sistem QPWDRULES este *PWDSYSVAL şi oricare altă valoare de sistem de compunere parolă a fost modificată de la valoarea implicită.

Consultaţi subiectul “Valorile de sistem pentru parole” la pagina 46 pentru informaţii despre setarea valorilor de sistem compoziţie parolă.

Tabela 53. Valorile posibile pentru PASSWORD:

***USRPRF**	Parola pentru acest utilizator este numele profilului de utilizator. Când valoarea de sistem Nivel parolă (QPWDLVL) este 2 sau 3, parola este valoarea cu litere mari a numelui profilului de utilizator. 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 comunică cu alte sisteme, folosiţi valoarea de sistem QPWDMAXLEN sau QPWDRULES 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 expirată

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.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
PWDEXP

Lungime:
4

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 “Interval expirare parolă” la pagina 91). 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 expirare parolă

Tabela 54. Valorile 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

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.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
STATUS

Lungime:
10

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. “Activarea unui profil de utilizator” la pagina 123 arată un exemplu de program cu autorizare adoptată pentru a permite operatorului sistemului să activeze un profil.

Sistemul poate dezactiva un profil după un anumit număr de încercări incorecte de verificări de parolă 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 55. Valorile 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

Clasa utilizator este folosită pentru a controla ce opţiuni de meniu sunt arătate utilizatorului în meniurile i5/OS. Aceasta ajută controlarea accesului utilizatorului la unele funcţii de sistem.

Promptul Adăugare utilizator:
Tip de utilizator

Parametru CL:
USRCLS

Lungime:
10

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 meniurile 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).

Valori posibile pentru USRCLS: Tabela 56 arată clasele posibile de utilizatori şi ce autorizări speciale implicite sunt pentru fiecare clasă de utilizatori. 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 56. Autorizările speciale implicite după clasa de utilizator

Autorizare specială	**Clase de utilizatori**				
	***SECOFR**	***SECADM**	***PGMR**	***SYSOPR**	***USER**
*ALLOBJ	All	10 sau 20	10 sau 20	10 sau 20	10 sau 20
*SECADM	All	All			
*JOBCTL	All	10 sau 20	10 sau 20	All	
*SPLCTL	All				
*SAVSYS	All	10 sau 20	10 sau 20	All	10 sau 20
*SERVICE	All				
*AUDIT	All				
*IOSYSCFG	All				

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 asistenţă

Câmpul *Nivel de asistenţă* din profilul de utilizator specifică nivelul de asistenţă implicit pentru utilizator când profilul este creat. Platforma System i furnizează trei nivel de asistenţă: de bază, intermediar şi avansat.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
ASTLVL

Lungime:
10

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

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

Dacă nivelul de asistenţă din profilul de utilizator este modificat folosind comanda CHGUSRPRF sau comanda Modificare profil (CHGPRF), nivelurile de asistenţă 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 asistenţă implicit (de bază). Tabela 57 ne arată dacă USERA vede ecranul Gestionare profiluri de 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 57. Cu sunt stocate şi modificate nivelurile de asistenţă

Acţiune luată	**Versiune de ecran afişată**	**Versiune de ecran stocată**
Folosire comandă WRKUSRPRF	Ecranul Gestionare înrolare utilizator	Nicio modificare (nivel de asistenţă de bază)
Din ecranul Lucru cu înrolare utilizator, apăsaţi F21 şi selectaţi nivelul de asistenţă intermediar.	Ecranul Gestionare profiluri de utilizator	Modificat la nivel de asistenţă intermediar
Folosire comandă WRKUSRPRF	Ecranul Gestionare profiluri de utilizator	Nici o modificare (intermediară)
Selectaţi opţiunea gestionare înrolare utilizator de la meniul SETUP.	Ecranul Gestionare profiluri de utilizator	Nici o modificare (intermediară)
Tastaţi CHGUSRPRF USERA ASTLVL(*BASIC)		Modificat la nivel de asistenţă de bază
Folosire comandă WRKUSRPRF	Ecranul Gestionare înrolare utilizator	Nici o modificare (elementară)
Tastare WRKUSRPRF ASTLVL(*INTERMED)	Ecranul Gestionare profiluri de utilizator	Nici o modificare (elementară)

Notă: Câmpul *Opţiune utilizator* din profilul de utilizator de asemenea afectează afişarea ecranelor de sistem. Acest câmp este descris la pagina “Opţiuni utilizator” la pagina 108.

Tabela 58. Valorile posibile pentru ASTLVL

***SYSVAL**	Este folosit nivelul de asistenţă specificat în valoarea de sistem QASTLVL.
***BASIC**	Este folosită interfaţa de utilizator Asistent operaţional.

Tabela 58. Valorile posibile pentru ASTLVL (continuare)

***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

Biblioteca curentă este biblioteca specificată pentru a fi prima bibliotecă căutată pentru obiecte cerute de un utilizator. Dacă utilizatorul creează obiecte şi specifică *CURLIB, obiectele sunt puse în biblioteca curentă.

Promptul Adăugare utilizator:
Bibliotecă implicită

Parametru CL:
CURLIB

Lungime:
10

specială
*USE

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 “Listele de biblioteci” la pagina 207 furnizează informaţii suplimentare despre folosirea listelor de biblioteci şi a bibliotecii curente.

Tabela 59. Valorile 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 care utilizatori au voie să pună obiecte noi, cum ar fi programe Query. Folosiţi câmpul *Limitare capabilităţi* pentru a împiedica utilizatorii să modifice biblioteca curentă.

Program iniţial

Puteţi specifica numele unui program de apelat când un utilizator se loghează. Un asemenea program este numit un program iniţial. Un program iniţial rulează înainte de afişarea meniului iniţial, dacă aceste există.

Promptul Adăugare utilizator:
Program de semnare

Parametru CL:
INLPGM

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

Autorizare:
*USE pentru program *EXECUTE pentru bibliotecă

Dacă în câmpul *Limitare capabilităţi* din profilul de utilizator este *YES sau *PARTIAL, utilizatorul nu poate specifica un program iniţial în ecranul Semnare.

Programul iniţial este apelat doar dacă programul de rutare al utilizatorului este QCMD sau QCL. Consultaţi “Pornirea unui job interactiv” la pagina 199 pentru informaţii suplimentare despre secvenţa 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 60. Valorile 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 61. Valorile 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.

Meniul iniţial

Puteţi specifica numele meniului arătat când utilizatorul se loghează. Meniul iniţial este afişat după rularea programului iniţial al utilizatorului. Meniul iniţial este apelat doar dacă programul de rutare al utilizatorului este QCMD sau QCL.

Promptul Adăugare utilizator:
Primul meniu

Parametru CL:
INLMNU

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

Autorizare
*USE pentru meniu *EXECUTE pentru bibliotecă

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

Dacă opţiunea din câmpul Limitare capabilităţi din profilul de utilizator 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 de utilizator.

Tabela 62. Valorile posibile pentru MENU:

MAIN	Este afişat meniul principal System i.

Tabela 62. Valorile posibile pentru MENU: (continuare)

***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 63. Valorile 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.

Limitarea capabilităţilor

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 în sistem.

Promptul Adăugare utilizator:
Restricţionare folosire linie de comandă

Parametru CL:
LMTCPB

Lungime:
10

Un utilizator cu capabilităţi limitate poate doar rula comenzi care sunt definite ca fiind permise să fie folosite de utilizatori limitaţi. 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, FTP, REXEC, folosirea API-ului QCAPCMD sau o opţiune dintr-un meniu de grupare comandă. Utilizatorii nu sunt restricţionaţi să realizeze următoarele acţiuni:

- Să ruleze comenzi în programe CL care rulează o comandă ca rezultat al selectării unei opţiuni dintr-un meniu
- Rulare comenzi 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 propriile comenzi, puteţi specifica parametrul ALWLMTUSR din comanda Creare comandă (CRTCMD).

Valori posibile: Tabela 64 la pagina 84 arată valorile posibile pentru câmpul Limitare capabilităţi şi ce funcţii sunt permise pentru fiecare valoare.

Tabela 64. Funcţiile permise pentru valori de limitare capabilitate

Funcţia	***YES**	***PARTIAL**	***NO**
Modificare programul iniţial	Nu	Nu	Da
Modificare meniu iniţial	Nu	Da	Da
Modificare bibliotecă curentă	Nu	Nu	Da
Modificare program Attention	Nu	Nu	Da
Introducere comenzi	Câteva[1]	Da	Da

[1] Acest comenzi sunt permise implicit: 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.

Concepte înrudite

"Planificarea meniurilor" la pagina 227
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 capabilităţi limitate şi un meniu iniţial în profilul de utilizator.

Text

Textul din profilul de utilizator este folosit ca să descrie profilul de utilizator sau la ce este folosit.

Promptul Adăugare utilizator:
Descriere utilizator

Parametru CL:
TEXT

Lungime:
50

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 65. Valorile 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.

Autorizarea specială

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

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
SPCAUT

Lungime:
100 (10 caractere pentru autorizare specială)

Autorizare:

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

Tabela 66. Valorile 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 56 la pagina 79 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.

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.
- Acordaţi şi înlăturaţi autorizarea de cod de acces a unui utilizator.
- 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 Control job (*JOBCTL) permite unui utilizator să modifice prioritatea joburilor şi a tipăririi, opri un job înainte să se fi terminat sau şterge ieşierea înainte să fie tipărită. Autorizarea specială *JOBCTL poate de asemenea acorda unui utilizator acces la ieşire spooled confidenţială, dacă cozile de ieşire sunt specificate OPRCTL(*YES).

Autorizarea specială Control job (*JOBCTL) permite utilizatorului să realizeze următoarele acţiuni:

- 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 “Tipărirea” la pagina 211.

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 de utilizator care face modificările.

Riscuri: Un utilizator care abuzează de autorizarea specială *JOBCTL poate cauza un efect negativ asupra joburilor individuale şi a 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 Salvare sistem (*SAVSYS) acordă utilizatorului autorizarea de a salva, restaura şi elibera spaţiu de stocare pentru toate obiectele din sistem, indiferent dacă utilizatorul are autorizare existenţă obiect asupra obiectelor

Riscuri: Un utilizator cu autorizare specială *SAVSYS poate:

- Salvaţi un obiect şi duceţi-l în alt sistem 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. Această autorizare specială permite utilizatorului să depaneze un program doar cu autorizare *USE asupra programului şi să realizeze funcţii de service afişare şi modificare. Permite de asemenea utilizatorului să realizeze funcţii de urmărire.

Funcţia dump poate fi realizată fără autorizare *SERVICE.

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 le poate fi acordată autorizare pentru a realiza urmărirea serivicilor fără autorizare specială *SERVICE. În acest mod, doar anumiţi utilizatori au abilitatea de a realiza o comandă de urmărire, care le poate acorda acces la date sensibile. Utilizatorul trebuie să fie autorizat asupra comenzii şi să aibă ori autorizare specială *SERVICE sau să fie autorizaţi asupra funcţiei Urmărire servicii a i5/OS prin Application Administration în System i Navigator. 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:

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 de acces la urmăriri”)
TRCINT	Urmărire internă
STRTRC	Pornire job de urmărire
ENDTRC	Oprire job de urmărire
PRTTRC	Tipărire job de urmărire
DLTTRC	Ştergere job de urmărire
TRCTCPAPP	Urmărire aplicaţie TCP/IP (Trace TCP/IP Application)
WRKTRC	Gestionarea urmăririlor (Work with Traces)

Notă: Aveţi nevoie de *ALLOBJ pentru a modifica date folosind funcţii de service.

Acordarea de acces la urmăriri:

Comenzile de urmărire, cum ar fi TRCCNN (Urmărire conexiune) sunt comenzi puternice care nu ar trebui acordate tuturor utilizatorilor care au nevoie de acces la alte unelte de service şi depanare.

Finalizaţi următorii paşi pentru a limita cine poate accesa aceste comenzi de urmărire fără a avea autorizare *SERVICE:

1. În System i Navigator, deschideţi Utilizatori şi grupuri.
2. Selectaţi **Toţi utilizatorii** pentru a vizualiza o listă de profiluri de utilizator.
3. Faceţi clic dreapta pe profilul de utilizator pe care doriţi să-l modificaţi.
4. Selectaţi **Proprietăţi**.

5. Apăsaţi **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.

Alternativ, comanda Modificare folosire funcţie (CHGFCNUSG) poate fi folosită pentru a acorda utilizatorilor acces la comenzi de urmărire. Introduceţi CHGFCNUSG FCNID(QIBM_SERVICE_TRACE) USER(profil de utilizator) USAGE(*ALLOWED).

Autorizarea specială *AUDIT

Autorizarea specială de auditare (*AUDIT) oferă utilizatorului posibilitatea să vizualizeze şi să modifice caracteristicilor de auditare.

Un utilizator poate realiza următoarele taskuri cu autorizarea specială *AUDIT:

- Să modifice valorile de sistem care controlează auditarea.
- Să utilizeze comenzile CHGOBJAUT, CHGDLOAUD şi CHGAUD ca să modifice auditarea pentru obiecte.
- Să utilizeze comanda CHGUSRAUD ca să modifice auditarea pentru un utilizator.
- Să afişeze valorile de auditare ale unui obiect.
- Să afişeze valorile de auditare ale unui profil de utilizator.
- Rulaţi unele dintre comenzile unelte de securitate, cum ar fi PRTADPOBJ.

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.

Pentru a împiedica utilizatorii generali să vizualizeze informaţii de auditare, restricţionaţi accesul utilizatorilor generali la următoarele informaţii:

- Jurnal auditare de securitate (QAUDJRN)
- Alte jurnale care conţin date de auditare
- Fişiere de salvare, fişiere de ieşire, fişiere spool şi tipărituri care conţin informaţia de auditare

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

Autorizarea specială *IOSYSCFG

Autorizarea specială configurare sistem (*IOSYSCFG) acordă utilizatorului abilitatea de a modifica cum este configurat sistemul. Utilizatorii cu această autorizare specială pot adăuga sau înlătura informaţii de configuraţie comunicaţii, lucra cu servere TCP/IP şi configura serverul de conexiune la internet (ICS). Majoritatea comenzilor pentru configurarea comunicaţiilor necesită autorizare specială *IOSYSCFG.

Recomandări pentru autorizări speciale: Acordarea de autorări speciale utilizatorilor reprezintă o vulnerabilitate. 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 de utilizator şi programe:

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

Programele adoptă autorizarea specială *ALLOBJ a proprietarului dacă:

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

Mediu special

Utilizatorul poate opera în mediul System i5, System/36 sau System/38. Când utilizatorul semnează, sistemul foloseşte programul de rutare şi mediul special din profilul de utilizator pentru a determina mediul utilizatorului.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
SPCENV

Lungime:
10

Tabela 67. Valorile 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 System i5 .
***S36**	Utilizatorul operează în mediul System/36 dacă programul de rutare al utilizatorului este QCMD.

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

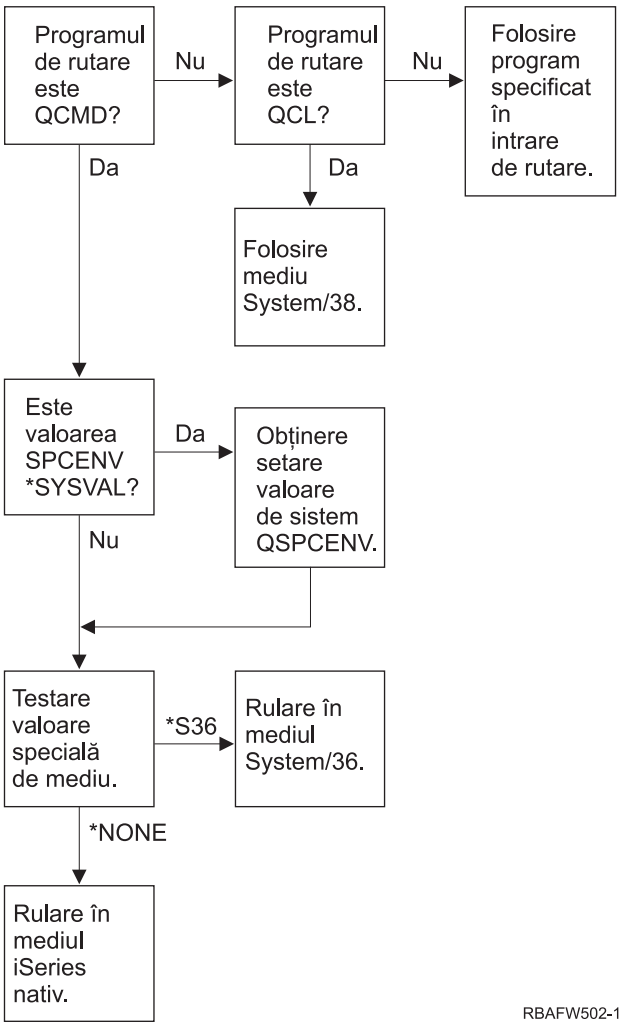


Figura 2. Descrierea mediului special

Descrierea mediului special în 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 valoare de mediu specială este setată la *NONE, atunci sistemul rulează mediul integrat System i.

Afişare informaţii de semnare

Ecranul Informaţii semnare este o unealtă cu care utilizatorii pot să-şi monitorizeze profilurile şi pot detecta încercarea de folosire greşită. Câmpul Afişare informaţii semnare specifică dacă ecranul Informaţii semnare este arătat când utilizatorul semnează.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
DSPSGNINF

Lungime:
7

Figura 3 arată ecranul. Informaţii despre expirarea parolei sunt arătate doar dacă parola expiră în zilele de avertisment expirare parolă.

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

Password verifications not valid . . . . . :   3

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

Figura 3. Ecranul Informaţii de semnare

Tabela 68. Valorile 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: Arătarea acestui ecran tuturor utilizatorilor este recomandată. 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 expirare parolă

Intervalul de expirare parolă controlează numărul de zile în care o parolă validă poate fi folosită înainte de a fi schimbată.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
PWDEXPITV

Lungime:
5,0

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. “Interval expirare parolă” arată un exemplu de mesaj de expirare parolă.

Tabela 69. Valorile 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 expirare parolă din profilul de utilizator pentru a cere utilizatorilor cu autorizări speciale *SERVICE, *SAVSYS, *SECADM sau *ALLOBJ să îşi modifice parolele mai frecvent decât alţi utilizatori.

Blocare modificare parolă

Parametrul blocare modificare parolă specifică perioada de timp în care o parolă este blocată la modificare după o operaţie de modificare parolă anterioară reuşită.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
PWDCHGBLK

Lungime:
10

Valoarea parametrului nu restricţionează modificările de parolă făcute de comanda Modificare profil de utilizator (CHGUSRPRF). În plus, această valoare de parametru nu este fortaţă adacă câmpul setare parolă expirată (PWDEXP) din profilul de utilizator are o valoare *YES. Aceasta permite unui administrator de securitate să creeze un profil de utilizator cu o parolă expirată şi să permită încă utilizatorului să se logheze şi să modifice parola (o dată) fără a fi restricţionat de valoarea de sistem blocare modificare parolă.

Tabela 70. Valorile posibile pentru PWDCHGBLK:

***SYSVAL**	Valoarea de sistem QPWDCHGBLK este folosită.
***NONE**	Parola poate fi modificată oricând.
1 - 99	O parolă nu poate fi modificată în numărul specificat de ore după o operaţie de modificare de parolă anterioară reuşită.

Recomandare: Setaţi parametrul la *SYSVAL dacă nu observaţi vreo activitate neobişnuită de modificare parolă pentru un anumit utilizator. În acest caz, puteţi folosi o valoare, cum ar fi 2, pentru a limita frecvenţa modificării parolei utilizatorului.

Gestionarea locală a parolei

Parametrul Gestionare locală parole (LCLPWDMGT) controlează dacă parola profilului de utilizator este gestionată local. Când parola nu este gestionată local, utilizatorii nu pot accesa sistemul prin semnarea directă, ci prin alte platforme.

Dacă parola este gestionată local, atunci parola este memorată local cu profilul de utilizator. Aceasta este metoda tradiţională de memorare a parolei.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
LCLPWDMGT

Lungime:
10

Dacă parola nu este gestionată local, atunci parola locală i5/OS este setată la *NONE. Valoarea parolei specificată în parametrul parolă va fi trimisă altor produse IBM care efectuează sincronizarede parole, cum ar fi IBM i5/OS Integration pentruWindows Server. Utilizatorii nu îşi vor putea modifica parolele folosind comanda Modificare parolă (CHGPWD). În plus, utilizatorii nu se vor putea loga în sistem direct. Specificarea acestei valori va afecta alte produse IBM care fac sincronizare de parolă, cum ar fi serverul IBM i5/OS Integration for Windows.

Acest parametru nu ar trebui setat la *NO dacă utilizatorul nu vrea doar să acceseze sistemul prin altă platformă, cum ar fi Windows Server.

Tabela 71. Valorile posibile pentru LCLPWDMGT:

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

Limitare sesiuni dispozitiv

Câmpul Limitare sesiuni dispozitiv controlează dacă numărul de sesiuni dispozitiv permise pentru un utilizator este limitat. Valoarea nu restricţionează folosirea meniului Cerere sistem sau a unei a doua semnări de la acelaşi dispozitiv.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
LMTDEVSSN

Lungime:
7

Tabela 72. Valorile 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.
0	Utilizatorul nu este limitat la un anumit număr de sesiuni dispozitiv. Această valoarea are aceeaşi semnificaţi ca *NO.
1	Utilizatorul este limitat la un singură sesiune dispozitiv. Această valoarea are aceeaşi semnificaţie ca *YES.
2 - 9	Utilizatorul este limitat la numărul specificat de sesiuni dispozitiv.

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 a tastaturii

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

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
KBDBUF

Lungime:
10

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 73. Valorile 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 de utilizator.
***TYPEAHEAD**	Caracteristica tastare înainte este activă pentru acest profil de utilizator.
***YES**	Caracteristica tastare înainte şi opţiunea de punere în buffer tastă Attn sunt active pentru acest profil de utilizator.

Spaţiu de stocare maxim

Puteţi să specificaţi cantitatea maximă de spaţiu de stocare auxiliar pe care o foloseşte sistemul pentru a stoca obiecte permanente pe care le posedă un profil de utilizator. Aceasta include obiectele pe care le plasează sistemul în biblioteca temporară (QTEMP) în timpul unui job.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
MAXSTG

Lungime:
11,0

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 dimensiuni de stocare auxiliară:

- 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 considerare 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 de 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 de 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 de 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.
- Sistemul asignează spaţiu de stocare pentru descrieri de obiecte care sunt plasate într-o bibliotecă proprietarului acelei biblioteci. Aceasta este adevărat chiar dacă obiectele sunt posedate de alt profil de utilizator. Exemple ale unor asemenea descrieri sunt referinţele text şi de program.
- Sistemul asignează spaţiu de stocare profilului de utilizator pentru obiectele temporare care sunt folosite în timpul procesării jobului. Exemple ale unor asemenea obiecte sunt blocurile de control comitere, spaţiile de editare fişier şi documentele.

Tabela 74. Valorile posibile pentru MAXSTG:

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

Limită prioritate

Limita de prioritate din profilul de utilizator determină priorităţile maxime de planificare (prioritate job şi prioritate de ieşire) care sunt permise pentru orice joburi lansate de utilizator. Limia de prioritate controlează prioritatea jobului când este lansat. Controlează de asemenea orice modificări făcute priorităţii jobului în timp ce jobul aşteaptă în coadă sau când jobul rulează.

Promptul 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. Puteţi seta prioritatea jobului în descrierea jobului sau folosind comanda de lansare.

Prioritate ieşire:
Determină prioritatea de planificare pentru o ieşire creată de job în coada de ieşire. Puteţi seta prioritatea de ieşire în descrierea de job sau când folosiţi comanda de lansare.

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 de 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 de utilizator, prioritatea jobului este redusă la nivelul permis de profilul de utilizator.

Tabela 75. Valorile posibile pentru PTYLMT:

3	Limita de prioritate implicită pentru profiluri de 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 de utilizator la 3 dă utilizatorului abilitatea de a muta unele joburi înaintea altora în cozi.
limită- 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 job

O descriere de job conţine un set specific de atributele legate de job, cum ar fi coada de joburi de folosit, prioritatea planificării, rutarea datelor, severitatea cozii de mesaje, lista de biblioteci şi informaţii de ieşire. Atributele determină cum este rulat fiecare job în sistem.

Promptul 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.

Vedeţi subiectul Control funcţionare pentru informaţii suplimentare despre descrierile de joburi şi folosirea lor.

Tabela 76. Valorile 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- job	Specificaţi numele descrierii de job, 10 caractere sau mai puţin.

Tabela 77. Valorile 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 de folosirea valorii de sistem QUSRLIBL (listă de biblioteci utilizator).

Profil de grup

Parametrul Profil de grup (GRPPRF) specifică dacă utilizatorul este membru al unui profil de grup. Profilul de grup poate furniza utilizatorului autorizarea de folosire a obiectelor pentru care utilizatorul nu are autorizare specifică. Puteţi specifica maxim 15 grupuri suplimentare pentru utilizator în parametrul Profil de grup suplimentar (SUPGRPPRF).

Promptul 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 149.

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. Sistemul generează de asemenea un gidpentru profilul de grup, dacă nu are deja unul.

Când este modificată valoarea GRPPRF, modificarea intră în vigoare următoarea dată când utilizatorul se înscrie sau următoarea dată când un job trece la profilul de utilizator folosind un mâner sau un jeton de profil care a fost obţinut după ce a avut loc modificarea.

Consultaţi “Planificarea profilurilor de utilizator” la pagina 238 pentru informaţii suplimentare despre folosirea profilurilor de grup.

Tabela 78. Valorile 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

Dacă utilizatorul este membru al unui grup, puteţi folosi parametrul proprietar din profilul de utilizator pentru a specifica cine posedă orice obiecte noi create de utilizator. Obiectele pot fi deţinute fie de utilizator, fie de primul grup al utilizatorului (valoarea parametrului GRPPRF). Puteţi specifica câmpul Proprietar doar dacă aţi specificat altă valoare decât *NONE pentru câmpul Profil de grup.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
OWNER

Lungime:
10

Când valoarea Proprietar este modificată, modificarea are efect următoarea dată când utilizatorul se loghează sau următoarea dată când un job schimbă profilul de utilizator folosind un mâner de profil sau un jeton de profil obţinut după ce a avut loc modificarea.

Tabela 79. Valorile posibile pentru Proprietar:

***USRPRF**	Acest profil de utilizator este proprietarul oricăror obiecte noi create.

Tabela 79. Valorile posibile pentru Proprietar: (continuare)

***GRPPRF**	Profilul de grup este făcut proprietarul oricăror obiecte create de utilizator şi îi este acordată autorizare tot (*ALL) asupra obiectelor. 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. **Observaţii:** 1. Dacă daţi drept de proprietate 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

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.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
GRPAUT

Lungime:
10

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.

Când valoarea GRPAUT este modificată, modificarea are efect următoarea dată când utilizatorul se loghează sau următoarea dată când un job schimbă profilul de utilizator folosind un mâner de profil sau un jeton de profil obţinut după ce a avut loc modificarea.

Tabela 80. Valorile 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.

Referinţe înrudite

"Definirea modului în care pot fi accesate informaţii" la pagina 132
Puteţi defini ce operaţii pot fi realizate asupra obiectelor, datelor şi câmpurilor.

Tip autorizare grup

Când un utilizator creează un obiect nou, parametrul Tip autorizare de grup din profilul de utilizator determină ce tip de autorizare primeşte grupul utilizatorului pentru noul obiect.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
GRPAUTTYP

Lungime:
10

Parametrul GRPAUTTYP lucrează împreună cu parametrii OWNER, GRPPRF şi GRPAUT la determinarea autorizării grupului pentru un obiect nou.

Când valoarea GRPAUTTYP este modificată, modificarea are efect următoarea dată când utilizatorul se loghează sau următoarea dată când un job schimbă profilul de utilizator folosind un mâner de profil sau un jeton de profil obţinut după ce a avut loc modificarea.

Tabela 81. Valorile 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. Această valoarea poate fi specificată doar când GRPAUT nu este *NONE.

[1] Autorizarea privată şi autorizarea de grup primar furnizează acelaşi acces obiectului pentru membrii grupului ,dar ele au caracteristici de performanţă diferite. “Grupul primar pentru un obiect” la pagina 144 explică cum lucrează autorizarea de grup primar.

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

Grupuri suplimentare

Puteţi specifica grupuri suplimentare la crearea sau modificarea unui profil de utilizator. Utilizatorul nu poate avea profiluri de grup suplimentare dacă parametrul GRPPRF este *NONE.

Promptul 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 informaţii suplimentare, vedeţi “Obiecte care adoptă autorizarea proprietarului” la pagina 149.

Puteţi specifica numele a maxim 15 profiluri din care acest utilizator va primi autorizare. Utilizatorul devine un membru al fiecărui profil de grup suplimentar.

Când profilurile de grup suplimentare sunt specificate într-un profil de 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 îl marchează ca profil de grup. Sistemul generează de asemenea un număr de identificare grup (gid) pentru profilul de grup, dacă nu are deja unul.

Când valoarea SUPGRPPRF este modificată, modificarea are efect următoarea dată când utilizatorul se loghează sau următoarea dată când un job schimbă profilul de utilizator folosind un mâner de profil sau un jeton de profil obţinut după ce a avut loc modificarea.

Consultaţi “Planificarea profilurilor de utilizator” la pagina 238 pentru informaţii suplimentare despre folosirea profilurilor de grup.

Tabela 82. Valorile posibile pentru SUPGRPPRF

***NONE**	Nici un grup suplimentar nu este folosit cu acest profil de 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. Nume de profil specificat pentru GRPPRF poate de asemenea fi specificat ca unul dintre cele 15 profiluri de grup suplimentare.

Cod de contabilizare

Specificarea codului de contabilitate vă permite să adunaţi informaţii despre resursele sistem folosite de un job.

Promptul 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).

Când valoarea *cod contabilitate* este modificată, modificarea are efect următoarea următoarea dată când utilizatorul se loghează sau următoarea dată când un job, care rulează folosind valoarea cod contabilitate a unui profil de utilizator, este pornit.

Vedeţi subiectul Control funcţionare pentru informaţii suplimentare despre contabilitatea joburilor.

Tabela 83. Valorile posibile pentru ACGCDE:

***BLANK**	Un cod de contabilizare de 15 spaţii este alocat acestui profil de utilizator.
cod-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

O parolă de document controlează accesibilitatea şi distribuirea de mail personal când este vizualizat de persoane care lucrează în numele utilizatorului. Parola documentului este suportată de unele produse DIA, cum ar fi Displaywriter.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
DOCPWD

Tabela 84. Valorile posibile pentru DOCPWD:

***NONE**	Nici o parolă de document nu este folosită de acest utilizator.

Tabela 84. Valorile posibile pentru DOCPWD: (continuare)

parolă- document	Specificaţi o parolă document pentru acest utilizator. Parola trebuie să aibă 1-8 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.

Coada de mesaje

O *coadă de mesaje* este un obiect în care sunt plasate mesaje când sunt trimise unei persoane sau unui program. O coadă de mesaje este folosită când un utilizator trimite sau primeşte mesaje.

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

Tabela 85. Valorile posibile pentru MSGQ:

***USRPRF**	O coadă de mesaje cu acelaşi nume cu numele de profil de 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-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 86. Valorile 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:** Acordaţi fiecărui profil de utilizator o coadă unică de mesaje, preferabil cu acelaşi nume ca profilul de
| utilizator.

Livrare

Modul de livrare al unei cozi de mesaje determină dacă utilizatorul este întrerupt când ajunge un nou mesaj în coadă.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
DLVRY

Lungime:
10

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 87. Valorile posibile pentru DLVRY:

***NOTIFY**	Jobul la care este asignată coada de mesaje este notificat când un mesaj ajunge în coada de mesaje. Pentru joburi interactive la o staţie de lucru, alarma sună şi lumina de aşteptare mesaj se aprinde. 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 un job interactiv, alarma sună (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

Dacă o coadă de mesaje este în mod *BREAK sau *NOTIFY, codul de severitate determină mesajele de nivel minim care sunt livrate utilizatorului. Mesajele a căror severitate este mai mică decât codul de severitate specificat sunt păstrate în coada de mesaje fără ca utilizatorul să fie notificat.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
SEV

Lungime:
2,0

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 88. Valorile 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.
cod- gravitate	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

Puteţi specifica imprimanta folosită pentru a tipări ieşirea de la acest utilizator. Fişiere spooled sunt plasate într-o coadă de ieşire cu acelaşi nume ca imprimata când coada de ieşire (OUTQ) este specificată ca dispozitiv de tipărire (*DEV).

Promptul Adăugare utilizator:
Imprimantă implicită

Parametru CL:
PRTDEV

Lungime:
10

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 direcţionarea ieşirii imprimantei, consultaţi subiectul Tipărire de bază.

Tabela 89. Valorile 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

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.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
OUTQ

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

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

O coadă de ieşire nu trebuie neapărat 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 direcţionarea ieşirii imprimantă, consultaţi subiectul Prezenzare avansată funcţie.

Tabela 90. Valorile 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 91. Valorile 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 manipulare-tastă-atenţionare

Programul manipulare-tastă-atenţionare (ATNPGM) este programul care este apelat când utilizatorul apasă tasta Atenţionare (ATTN) în timpul unui job interactiv.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
ATNPGM

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

Autorizare:
*USE pentru program

*EXECUTE pentru bibliotecă

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 se rulează comanda Setare program tratare tastă Atenţie (SETATNPGM) dintr-o linie de comandă sau dintr-o aplicaţie, noul ATNPGM specificat înlocuieşte ATNPGM din profilul de utilizator.

Notă: Consultaţi “Pornirea unui job interactiv” la pagina 199 pentru informaţii suplimentare despre secvenţa 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 92. Valorile 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 93. Valorile 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

Secvenţa de sortare este folosită pentru ieşirea acestui utilizator. Puteţi să folosiţi tabela de sortare furnizată de sistem sau să vă creaţi una proprie. O tabelă de sortare poate fi asociată cu un anumit identificator de limbă din sistem.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
SRTSEQ

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

Autorizare:
*USE pentru tabelă *EXECUTE pentru bibliotecă

Tabela 94. Valorile 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 95. Valorile 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 limbă

Puteţi specifica identificatorul de limbă pentru a fi folosit de sistem pentru utilizator.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
LANGID

Lungime:
10

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

Tabela 96. Valorile posibile pentru LANGID:

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

Identificator de ţară sau regiune

Puteţi specifica identificatorul de regiune sau ţară pentru a fi folosit de sistem pentru utilizator.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
CNTRYID

Lungime:
10

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 de utilizator sau din ecranul Modificare profil de utilizator.

Tabela 97. Valorile 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 codificat

Puteţi specifica identificatorul setului de caractere codate care va fi folosit de sistem pentru utilizator.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
CCSID

Lungime:
5,0

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 de utilizator sau în ecranul Modificare profil de utilizator.

Tabela 98. Valorile 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 caractere

Atributele *CHRIDCTL* controlează tipul de conversie a setului de caractere codate care apare pentru fişierele de afişare, fişierele de imprimantă şi grupurile de panouri.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
CHRIDCTL

Lungime:
10

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 99. Valorile 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

Câmpul SETJOBATR specifică ce fel de atribute de job urmează să fie luate la iniţierea jobului din Locale-ul specificat în parametrul LOCALE.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
SETJOBATR

Lungime:
160

Tabela 100. Valorile 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.
***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.

Orice combinaţie a următoarelor valori poate fi specificată:

- *CCSID
- *DATFMT
- *DATSEP
- *DECFMT
- *SRTSEQ
- *TIMSEP

Locale-ul

Câmpul Locale specifică numele de cale pentru Locale-ul care este alocat variabilei de mediu LANG pentru acest utilizator.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
LOCALE

Tabela 101. Valorile 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

Câmpul Opţiuni utilizator vă permite să personalizaţi anumite ecrane de sistem şi funcţii pentru utilizator. Puteţi specifica mai multe valori pentru parametrul opţiune utilizator.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
USROPT

Lungime:
240 (10 caractere fiecare)

Tabela 102. Valorile 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 vede ecrane care arată autorizare obiect, cum ar fi ecranul Editare autorizare obiect sau ecaranul Editare listă de autorizare, sunt arătate informaţii detaliate de autorizare fără ca utilizatorul să trebuiască să apese F11 (Afişare detalii). “Ecranele de autorizare” la pagina 154 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.

Număr identificare grup

Sistemul de fişiere integrat foloseşte numărul de identificare utilizator (uid) pentru a identifica un utilizator şi pentru a verifica autorizarea utilizatorului. Fiecare utilizator din sistem trebuie să aibă un uid unic.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
UID

Lungime:
10,0

Tabela 103. Valorile posibile pentru UID:

***GEN**	Sistemul generează un uid unic pentru acest utilizator. Uid-ul generat va fi mai mare decât 100.
uid	O valoare între 1 şi 4294967294 care să fie asignată ca uid pentru acest utilizator. Uid-ul nu poate fi deja asignat altui utilizator.

Recomandări: Pentru majoritatea instalărilor, lăsaţi sistemul să genereze un uid pentru profiluri de utilizator noi specificând UID(*GEN). Totuşi, dacă sistemul face parte dintr-o reţea, ar putea trebui să asignaţi uid-uri care să se potrivească cu cele asignate de alte sisteme din reţea. Consultaţi administratorul de reţea.

Număr identificare grup

Sistemul de fişier integrat foloseşte numărul de identificare grup (gid) pentru a identifica acest profil ca profil de grup. Un profiluri care este folosit ca un profil de grup trebuie să aibă un gid.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
GID

Lungime:
10,0

Tabela 104. Valorile posibile pentru GID:

***NONE**	Acest profil nu are un gid. Această valoarea trebuie specificată dacă profilul de utilizator este un membru al unui grup (GRPPRF nu este *NONE).
***GEN**	Sistemul generează un gid unic pentru acest profil. gid-ul generat va fi mai mare decât 100.
gid	O valoarea între 1 şi 4294967294 care să fie asignată ca gid pentru acest profil. gid-ul trebuie să nu fie deja asignat altui profil.

Recomandări: Pentru majoritatea instalărilor, lăsaţi sistemul să genereze un gid pentru profiluri noi de grup specificând GID(*GEN). Totuşi, dacă sistemul face parte dintr-o reţea, ar putea trebui să asignaţi gid-uri care să se potrivească cu cele asignate de alte sisteme din reţea. Consultaţi administratorul de reţea.

Nu asignaţi un gid unui profil de utilizator pe care nu aveţi de gând să îl folosiţi ca profil de grup. În unele medii, un utilizator care este logat şi are un gid este restricţionat la realizarea anumitor funcţii.

Director de bază

Directorul de bază este directorul de lucru iniţial al utilizatorului pentru sistemul de fişiere integrat. Directorul de bază este directorul curent al utilizatorului dacă un director curent diferit nu a fost specificat.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
HOMEDIR

Dacă directorul de bază specificat în profil nu există când utilizatorul semnează, directorul de bază al utilizatorului este directorul rădăcină (/).

Tabela 105. Valorile posibile pentru HOMEDIR:

***USRPRF**	Directorul de bază asignat utilizatorului este /home/xxxxx, unde xxxxx este numele profilului de utilizator.
director de bază	Numele directorului de bază de alocat acestui utilizator.

Asociere EIM

Asocierea EIM specifică dacă o asociare EIM ar trebui adăugată la un identificator EIM pentru acest utilizator. Opţional, identificatorul EIM poate fi creat dacă nu există deja.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
EIMASSOC

Observaţii:

1. Informaţiile asociere EIM 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 106. Valorile posibile pentru EIMASSOC, valori singulare:

Valori singulare	
***NOCHG**	Asocierea EIM nu va fi adăugată.

Tabela 107. Valorile posibile pentru EIMASSOC, elementul 1:

Elementul 1: identificatorul EIM Specificaţi identificatorul EIM pentru această asociere.	
***USRPRF**	Numele identificatorului EIM este acelaşi cu numele profilului de utilizator.
valoare caracter	Specificaţi numele indentificatorului EIM.

Tabela 108. Valorile 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 i5/OS. 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 109. Valorile posibile pentru EIMASSOC, elementul 3:

Elementul 3: Acţiune asociere	
***REPLACE**	Asocierile de tipul specificat vor fi înlăturate din identificatoarele EIM care au o asociere pentru acest profil de utilizator şi registru EIM local. O nouă asociere va fi adăugată la identificatorul EIM specificat.
***ADD**	Adăugaţi o asociere.
***REMOVE**	Înlăturaţi o asociere.

Tabela 110. Valorile 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

Câmpul Autorizare specifică autorizarea publică pentru profilul de utilizator.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
AUT

Autorizarea pentru un profil controlează multe funcţii asociate cu profilul, precum:

- Modificarea profilului
- Afişarea profilului
- Ştergerea profilului
- Lansarea unui job folosind profilul
- Specificarea profilului într-o descriere de job
- Transferarea posesiei obiectelor profilului
- Adăugarea de membrii, dacă profilul este un profil de grup

Tabela 111. Valorile 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 informaţii” la pagina 132 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 obiecte

Valoarea de auditare obiect pentru un profil de utilizator lucrează împreună cu valoarea de auditare obiect pentru un obiect pentru a determina dacă accesul utilizatorului la un obiect este auditat.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
OBJAUD

Lungime:
10

Auditarea de obiecte pentru un profil de utilizator nu poate fi specificată pe niciuna din comenzile profil de utilizator. Folosiţi comanda CHGUSRAUD pentru a specifica auditarea de obiect pentru un utilizator. Doar un utilizator cu autorizarea specială *AUDIT poate folosi comanda CHGUSRAUD.

Tabela 112. Valorile posibile pentru OBJAUD:

***NONE**	Valoarea OBJAUD pentru obiecte determină dacă auditarea de obiect este efectuată pentru acest utilizator.

Tabela 112. Valorile posibile pentru OBJAUD: (continuare)

***ALL**	Dacă valoarea OBJAUD pentru un obiect specifică *USRPRF, este scrisă o înregistrare de auditare când acest utilizator modifică sau citeşte obiectul.
***CHANGE**	Dacă valoarea OBJAUD pentru un obiect specifică *USRPRF, este scrisă o înregistrare de auditare când acest utilizator modifică obiectul.
***NOTAVL**	Această valoare indică faptul că valoarea parametrului nu este disponibilă utilizatorului deoarece acesta nu are autorizarea specială *AUDIT sau *ALLOBJ. Valoarea parametrului nu poate fi setată la această valoare.

Tabela 113 arată cum lucrează împreună valorile OBJAUD pentru utilizator şi obiecte:

Tabela 113. Auditarea realizată pentru accesul la obiecte

valoare OBJAUD pentru obiect	**valoare OBJAUD pentru utilizator**		
	***NONE**	***CHANGE**	***ALL**
*ALL	Modificare şi utilizare	Modificare şi utilizare	Modificare şi utilizare
*CHANGE	Modificare	Modificare	Modificare
*NONE	Fără	Fără	Fără
*USRPRF	Fără	Modificare	Modificare şi utilizare

Operaţii înrudite

“Planificarea auditării accesului la obiecte” la pagina 286
Sistemul de operare i5/OS furnizează abilitatea de a înregistra în istoric accesele la un obiect din jurnal de auditare de securitate folosind valori de sistem şi valorile de auditare obiecte pentru utilizatori şi obiecte. Aceasta este numită *auditare obiecte*.

Auditarea acţiunilor

Pentru un utilizator individual, puteţi să specificaţi ce 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.

Promptul Adăugare utilizator:
Neafişat

Parametru CL:
AUDLVL

Lungime:
640

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 poate folosi comanda CHGUSRAUD.

Tabela 114. Valorile posibile pentru AUDLVL:

***NONE**	Valoarea de sistem QAUDLVL controlează acţiunea de auditare pentru acest utilizator. Nu este terminată nici o auditare suplimentară.
***NOTAVL**	Această valoare indică faptul că valoarea parametrului nu este disponibilă utilizatorului deoarece nu are autorizarea specială *AUDIT sau *ALLOBJ. Valoarea parametrului nu poate fi setată la această valoare.
***AUTFAIL**	Eşuările de autorizare sunt auditate.

Tabela 114. Valorile posibile pentru AUDLVL: (continuare)

***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.
***JOBBAS**	Funcţii de bază job sunt auditate.
***JOBCHGUSR**	Modifică la profilul de utilizator activ al unui fir de execuţie sau profilurile de grup sunt auditate.
***JOBDTA**[1]	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.
***NETBAS**	Funcţii de bază de reţea sunt auditate.
***NETCLU**	Operaţiile cluster sau grup resurse cluster sunt auditate.
***NETCMN** [3]	Funcţiile de reţelistică şi comunicaţii sunt auditate.
***NETFAIL**	Eşuările de reţea sunt auditate.
***NETSCK**	Taskurile socket sunt auditate.
***OPTICAL**	Toate funcţiile optice sunt auditate.
***PGMADP**	Obţinerea autorizării la un obiect printr-un program care adoptă autorizare este înregistrată în istoric.
***PGMFAIL**	Eşuările de program sunt auditate.
***PRTDTA**	Funcţiile de tipărire cu parametrul SPOOL(*NO) sunt auditate.
***SAVRST**	Operaţiile de restaurare şi salvare sunt înregistrate în istoric.
***SECCFG**	Configuraţia de securitate este auditată.
***SECDIRSRV**	Modificările sau actualizările la efectuarea de funcţii de service director sunt auditate.
***SECIPC**	Modificările comunicaţiilor interprocese sunt auditate.
***SECNAS**	Acţiunile de servicii autentificare reţea sunt auditate.
***SECRUN**	Funcţiile runtime de securitate sunt auditate.
***SECSCKD**	Descriptorii de socket sunt auditaţi.
***SECURITY**[2]	Sunt înregistrate funcţiile referitoare la securitate.
***SECVFY**	Folosirea funcţiilor de verificare este auditată.
***SECVLDL**	Modificarea obiectelor din lista de validare este auditată.
***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.

Tabela 114. Valorile posibile pentru AUDLVL: (continuare)

[1]	*JOBDTA include două valori care sunt *JOBBAS şi *JOBCHGUSR, care vă permit să personalizaţi mai bine auditarea. Dacă sunt specificate ambele valori, veţi obţine aceeaşi auditarea ca şi acum ar fi specificat doar *JOBDTA.
[2]	*SECURITY este compus din mai multe valori pentru a vă permite să personalizaţi mai bine auditarea. Dacă sunt specificate toate valorile, veţi obţine aceeaşi auditarea ca şi cum doar *SECURITY este specificat. Aceste valori sunt după cum urmează. • *SECCFG • *SECDIRSRV • *SECIPC • *SECNAS • *SECRUN • *SECSCKD • *SECVFY • *SECVLDL
[3]	*NETCMN este compus din mai multe valori pentru a vă permite să personalizaţi mai bine auditarea. Dacă sunt specificate toate valorile, veţi obţine aceeaşi auditare ca şi cum doar *NETCMN este specificat. Aceste valori sunt după cum urmează. • *NETBAS • *NETCLU • *NETFAIL • *NETSCK

Referinţe înrudite

"Planificarea acţiunilor de auditare" la pagina 263
Valoarea de sistem QAUDCTL (control auditare), valoarea de sistem QAUDLVL (nivel auditare), valoarea de sistem QAUDLVL2 (extensie nivel auditare) şi parametrul AUDLVL (auditare acţiune) din profilurile de utilizator lucrează împreună pentru a controla auditarea acţiunilor.

Informaţii suplimentare asociate cu un profil de utilizator

Acest subiect discută autorizările private, informaţiile obiect posedat şi informaţii obiect grup primar care sunt asociate cu un profil de utilizator.

Referinţe înrudite

"Cum sunt stocate informaţiile de securitate" la pagina 246
Planificarea de proceduri adecvante de salvare de rezervă şi recuperare pentru informaţii de securitate necesită înţelegerea cum să stocate şi salvate informaţiile.

Autorizări private

Toate autorizările private pe care le are utilizatorul asupra obiectelor sunt stocate cu profilul de utilizator. Când un utilizator are nevoie de autorizare asupra unui obiect, autorizările privale ale utilizatorului ar putea fi căutate.

"Diagrama de flux 3: Cum este verificată autorizarea unui utilizator asupra unui obiect" la pagina 174 furnizează detalii suplimentare despre verificarea autorizării.

Puteţi afişa autorizările private ale unui utilizator asupra obiectelor bazate pe bibliotecă folosind comanda Afişare profil de utilizator:

```
DSPUSRPRF user-profile-name TYPE(*OBJAUT)
```

Puteţi lucra cu autorizările private ale utilizatorului asupra obiectelor bazate pe bibliotecă şi directory folosind comanda Work with Objects by Private Authority (WRKOBJPVT). 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 dintr-un profil de utilizator în altul folosind comanda Acordare autorizare utilizator (GRTUSRAUT). Consultaţi “Copierea autorizării de la un utilizator” la pagina 165 pentru mai multe informaţii.

Autorizări grup primar

Numele tuturor obiectelor pentru care profilul este grup primar sunt stocate cu profilul de grup.

Puteţi afişa obiectele bazate pe bibliotecă pentru care profilul este grupul primar folosind comanda DSPUSRPRF:

```
DSPUSRPRF group-profile-name TYPE(*OBJPGP)
```

De asemenea puteţi folosi şi comanda Gestionare obiecte după grup primar (WRKOBJPGP).

Informaţii obiect deţinut

Deoarece dimensiunea unui profil de utilizator poate afecta performanţa, este sugerat să nu asignaţi toate obiectele (sau aproape toate) unui singur profil.

Informaţiile de autorizare privată pentru un obiect sunt memorate cu profilul de 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. Operaţiile sistem pot fi afectate de asemenea. Pentru a preveni afectarea fie a performanţei, fie a operaţiilor de sistem, distribuiţi dreptul de proprietate a obiectelor la mai multe profiluri.

Autentificare ID digital

Certificatele digitale permit utilizatorilor să securizeze comunicaţiile şi să menţină integritatea mesajelor. Infrastructura de securitate System i permite certificatelor digitale x.509 să fie folosite pentru identificare.

API-urile pentru ID digital creează, distribuie şi gestionează certificate digitale asociate cu profiluri de utilizator. Consultaţi API-uri gestionare certificate digitale pentru detalii 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)

Lucru cu profiluri de utilizator

Acest subiect descrie comenzile şi ecranele pe care le folosiţi pentru a crea, modifica şi şterge profiluri de utilizator pe sistemul de operare i5/OS.

Trebuie să aveţi autorizarea specială *SECADM ca să creaţi, modificaţi sau ştergeţi profiluri de utilizator.

Crearea de profiluri de utilizator

Puteţi crea un profil de utilizator folosind ecranul listă Lucru cu profiluri de utilizator (WRKUSRPRF), folosind comanda Creare profil de utilizator (CRTUSRPRF), folosind opţiunea Lucru cu înrolare utilizator din meniul SETUP sau folosind Navigator System i .

Utilizatorul care creează profilul de 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: Nu puteţi folosi comanda Creare profil de utilizator (CRTUSRPRF) pentru a crea un profil de utilizator într-un pool de discuir 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 Lucru cu profiluri de utilizator

Puteţi introduce numelui unui anumit program, un set generic de profiluri sau *ALL în comanda Lucru cu profiluri de utilizator (WRKUSRPRF).

Nivelul de asistenţă determină ce listă de afişare vedeţi. Când folosiţi comanda WRKUSRPRF cu nivelul de asistenţă *BASIC, veţi accesa ecranul Gestionare înrolare utilizator. Dacă este specificat nivelul de asistenţă *INTERMED, veţi accesa ecranul Gestionare profiluri de utilizator.

Puteţi specifica parametrul ASTLVL (nivel de asistenţă) în comandă. Dacă nu specificaţi ASTLVL, sistemul va folosi nivelul de asistenţă memorat cu profilul dumneavoastră de utilizator.

În ecranul Gestionare profiluri de 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
```

Apare ecranul Creare profil de utilizator:

```
                      Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . . .   NEWUSER       Name
User password  . . . . . .   *NONE         Character value, *USRPRF...
Set password to expired  . . . .   *YES          *NO, *YES
Status . . . . . .   *ENABLED      *ENABLED, *DISABLED
User class . . . . . .   *USER         *USER, *SYSOPR, *PGMR...
Assistance level . . . . . .   *SYSVAL       *SYSVAL, *BASIC, *INTERMED...
Current library . . . . . .   *CRTDFT       Name, *CRTDFT
Initial program to call  . . . .   *NONE         Name, *NONE
  Library . . . . . .                 Name, *LIBL, *CURLIB
Initial menu . . . . . .   MAIN          Name, *SIGNOFF
  Library . . . . . .   QSYS          Name, *LIBL, *CURLIB
Limit capabilities . . . . . .   *NO           *NO, *PARTIAL, *YES
Text 'description' . . . . . .   *BLANK
```

Ecranul Creare profil de utilizator arată toate câmpurile din profilul de 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 de utilizator nu adaugă utilizatorul la directorul de sistem.

Folosirea comenzii Creare profil de utilizator

Puteţi folosi comanda (Creare profil de utilizator) CRTUSRPRF pentru a crea un profil de utilizator. Puteţi introduce parametrii cu comanda sau puteţi cere prompt-are (F4) şi vedea ecranul Creare profil de utilizator.

Folosirea opţiunii Lucru cu înrolare utilizatori

Puteţi folosi opţiunea Lucru cu înrolare utilizatori pentru a adăuga utilizatori în sistem.

Selectaţi opţiunea Gestionare înrolare utilizator din meniul SETUP. Nivelul de asistenţă memorat cu profilul dumneavoastră determină dacă veţi vedea ecranul Gestionare profiluri de utilizator sau ecranul Gestionare înrolare utilizator. Puteţi folosi F21 (Selectare nivel de asistenţă) 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        Name
User description  . . . .
Password  . . . . . .   NEWUSER
Type of user  . . . . .   *USER          Type, F4 for list
User group  . . . . . .   *NONE          Name, F4 for list

Restrict command line use   N             Y=Yes, N=No

Default library . . . . .                 Nume
Default printer . . . . .   *WRKSTN        Name, *WRKSTN, F4 for list
Sign on program . . . . .   *NONE          Name, *NONE
  Library . . . . . .                     Nume

First menu  . . . . . .                   Nume
  Library . . . . . .                     Nume

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 de 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 . . . . . .
```

Ecranul Adăugare utilizator adaugă în mod automat o intrare în directorul de sistem cu acelaşi ID utilizator ca şi numele de profil de utilizator (primele opt caractere) şi o adresă a numelui sistem.

Copierea profilurilor de utilizator

Puteţi crea un profil de utilizator copiind alt profil de utilizator sau profil de grup.

Aţi putea vrea să setaţi un profil într-un grup ca şablon. 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 de utilizator. Nici o comandă nu există pentru a copia un profil de utilizator.

Concepte înrudite

“Profiluri de grup” la pagina 4
Un *profil de grup* este un tip special de profil de utilizator. În loc să acordaţi autorizarea fiecărui utilizator individual, puteţi folosi un profil de grup ca să definiţi autorizarea pentru un grup de utilizatori.

Copierea din ecranul Lucru cu profiluri de utilizator

Puteţi copia informaţiile unui profil de utilizator din ecranul Lucru cu profiluri de utilizator.

În ecranul Gestionare profiluri de utilizator, tastaţi 3 în faţa profilului pe care doriţi să îl copiaţi. Apare ecranul Creare profil de utilizator:

```
                      Create User Profile (CRTUSRPRF)

Type choices, press Enter.

User profile . . . . . .                  Nume
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 copiere-din sunt arătate în ecranul Creare profil de utilizator, cu excepţia următoarelor câmpuri:

Profil de utilizator
Spaţiu liber. Trebuie completat.

| **Parolă** Valoare implicită comandă CRTUSRPRF

Parolă document
*NONE

Coada de mesaje
*USRPRF

Atribute de job locale
| *SYSVAL

Locale-ul
| *SYSVAL

Numărul de identificare utilizator
*GEN

Numărul de identificare grup
*NONE

Director de bază
*USRPRF

Asociere EIM
*NOCHG

Autorizare
*EXCLUDE

Puteţi modifica orice câmpuri în ecranul Creare profil de utilizator. Autorizările private ale profilului de copiere nu sunt copiate. În plus, obiecte interne care conţin preferinţe utilizator şi alte informaţii despre utilizator nu sunt copiate.

Copierea din ecranul Lucru cu înrolare utilizatori

Puteţi de asemenea copia profiluri de utilizator din ecranul Lucru cu înrolare utilizatori.

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

Default library . . . . .   DPTWH
Default printer . . . . .   PRT04
Sign on program . . . . .   *NONE
  Library . . . . . . . .
```

Toate valorile din profilul copiere-din apar în ecranul Adăugare utilizator, cu excepţia următoarelor valori:

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 de utilizator care nu apar în versiunea nivel de ajutor de bază sunt încă copiate din profilul copiere-din, cu următoarele excepţii:

Coada de mesaje
*USRPRF

Parolă document
*NONE

Numărul de identificare utilizator
*GEN

Numărul de identificare grup
*NONE

Asociere EIM
*NOCHG

Autorizare
*EXCLUDE

Autorizările private ale profilului de copiere nu sunt copiate.

Copiere autorizări private

Puteţi copia autorizările private de la un profil de utilizator la altul folosind comanda Acordare autorizare utilizator (GRTUSRAUT).

Aceasta nu ar trebui folosită în locul profilurilor de grup sau listelor de autorizare. Copierea autorizărilor nu ajută la gestionarea autorizărilor similare în viitor şi poate cauza probleme de performanţă în sistem.

Concepte înrudite

"Copierea autorizării de la un utilizator" la pagina 165
Puteţi copia toate autorizările private dintr-un profil de utilizator la altul prin folosirea comenzii Grant User Authority (GRTUSRAUT).

Modificarea profilurilor de utilizator

Puteţi modifica un profil de utilizator folosind opţiunea 2 (Modificare) din ecranul Gestionare înrolare utilizator sau Gestionare profiluri de utilizator. Puteţi de asemenea folosi comanda Modificare profil utilizator (CHGUSRPRF).

Utilizatorii cărora le este permis să introducă comenzi pot modifica unii parametrii ai profilurilor proprii 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 de profiluri de utilizator

Nu puteţi şterge un profil de utilizator care deţine obiecte. Înainte să puteţi ştergeasemenea profiluri de utilizator, trebuie să ştergeţi orice obiecte posedate de profil sau să transferaţi dreptul de proprietate asupra acelor obiect altui profil.

Nu puteţi şterge un profil de utilizator dacă este grupul primar pentru vreun obiect. Când folosiţi nivelul de ajutor intermediar pentru a şterge un profil de utilizator, puteţi modifica sau înlătura grupul primar pentru obiecte. Puteţi folosi comanda WRKOBJPGP cu opţiunea *OBJPGP (grup primar obiect) pentru a lista orice obiecte pentru care un profil este grupul primar.

Când ştergeţi un profil de 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 de membru înainte de a şterge profilul de grup.

Folosirea comenzii Ştergere profil de utilizator

Pentru a şterge un profil de utilizator, puteţi introduce comanda Ştergere profil de utilizator (DLTUSRPRF) direct sau puteţi folosi opţiunea 4 (Ştergere) din ecranul Lucru cu profiluri de 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  .
EIM association  . . . . . .   *DLT          *DLT, *NODLT
```

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 Utilizator la distanţă

Puteţi folosi opţiunea Înlăturare utilizator în ecranul Lucru de înrolare utilizatorpentru a şterge un profil de 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.

Observaţii:

1. Puteţi folosi F13 pentru a şterge toate obiectele deţinute de profilul de utilizator.
2. Fişierele spool nu apar în ecranul Gestionare obiecte după proprietar. Puteţi şterge un profil de 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.

Lucrul cu obiecte după autorizare privată

Puteţi folosi comanda Gestionare obiecte după autorizări private (WRKOBJPVT) pentru a lista şi gestiona orice obiecte pentru care un profil are autorizare primară.

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 din sistem sunt setate pentru a dezactiva un profil de utilizator după prea multe încercări de verificare parolă, se poate să fie nevoie să activaţi profilul modificând starea profilului la *ENABLED.

Pentru a activa un profil de utilizator, trebuie să aveţi autorizare specială *SECADM, autorizare *OBJMGT şi autorizare *USE asupra profilului de 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 posedat de un utilizator care are autorizare specială *SECADM, autorizare *OBJMGT şi autorizare *USE asupra profilurilor de utilizator din sistem. Adoptaţi autorizarea proprietarului când programul este creat specificând USRPRF(*OWNER).
2. Folosiţi comanda EDTOBJAUT pentru a face autorizarea publică a programului *EXCLUDE şi a acorda operatorilor de sistem autorizare *USE.
3. Operatorul activează profilul introducând CALL ENABLEPGM *profile-name*.
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 de utilizator într-o varietate de formate.

Afişarea unui profil individual

Pentru a afişa valorile pentru profil de utilizator individual, folosiţi opţiunea 5 (Afişare) din ecranul Lucru cu înrolare utilizatori sau ecranul Lucru cu profiluri de utilizator. Sau, aţi putea folosi comanda Afişare profil de utilizator (DSPUSRPRF).

Listarea tuturor profilurilor

Puteţi folosi comanda Afişare utilizatori autorizaţi (DSPAUTUSR) pentru a tipări sau afişa toate profilurile de utilizator în 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 de utilizator au parole definite pentru folosire la diferite niveluri de parolă.

```
                    Display Authorized Users

                   Password  Level      Level                  Local
User      Group    Last      0 or 1     2 or 3      Netserver  Pwd
Profile   Profile  Changed   Password   Password    Password   Mgt
ANGELA             04/21/0x    *YES       *NO        *YES      *YES
ARTHUR             07/07/0x    *YES       *YES       *YES      *YES
CAROL1             05/15/0x    *YES       *YES       *YES      *YES
CAROL2             05/15/0x    *NO        *NO        *NO       *NO
CHUCKE             05/18/0x    *YES       *NO        *YES      *YES
DENNISS            04/20/0x    *YES       *NO        *YES      *YES
DPORTER            03/30/0x    *YES       *NO        *YES      *YES
GARRY              08/04/0x    *YES       *YES       *YES      *YES
JANNY              03/16/0x    *YES       *NO        *YES      *YES
```

Tipuri de de afişări de profiluri de utilizator

Comanda Afişare profil de utilizator (DSPUSRPRF) furnizează mai multe tipuri de afişări şi listări.

- Unele ecrane şi listări sunt disponibile doar pentru profiluri individuale. Altele pot fi tipărite pentru toate profilurile sau un set generic de profiluri.
- 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. “Analizarea profilurilor de utilizator” la pagina 301 dă sugestii pentru rapoarte.

Tipuri de rapoarte profil de utilizator

Puteţi genera rapoarte profil de utilizator folosind comanda Tipărire profil de utilizator (PRTUSRPRF) sau comanda Analizare program implicit (ANZDFTPWD).

- Tipărire profil de utilizator (PRTUSRPRF)

  Această comandă generează rapoarte care conţin informaţii despre profilurile de utilizator din sistem. Pot fi tipărite patru variaţiuni diferite ale acestui raport. 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 generează un raport despre toate profilurile de utilizator din sistem care au o parolă implicită şi vă permite să efectuaţi o acţiune pe profiluri. Un profil are o parolă implicită când numele profil de utilizator se potriveşte parolei profilului.

  Profilurile de 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 de 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.
- Certificatele digitale care conţin numele utilizator nu vor fi validate.
- Informaţiile uid şi gid reţinute de sistemul de fişiere integrat nu pot fi modificate.
- Se poate să nu puteţi modifica informaţiile care sunt stocate de aplicaţii care conţin numele utilizatorului.

Aplicaţiile care sunt rulate de utilizator pot avea profiluri de utilizator. Crearea unui nou profil de utilizator i5/OS pentru a redenumi un utilizator nu redenumeşte orice profiluri aplicaţie pe care le poate avea utilizatorul. 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. Numele de profil vechi este SMITHM, în timp ce numele de profil de utilizator este JONESM:

1. Copiaţi vechiul profil (SMITHM) la un nou profil (JONESM) folosind opţiunea de copiere de la ecranul Gestionare înrolare utilizator.
2. Acoraţi lui JONESM toate autorizările private ale lui SMITHM folosind comanda Acoradare autorizare utilizator (GRTUSRAUT):

   ```
   GRTUSRAUT JONESM REFUSER(SMITHM)
   ```

3. Modificaţi grupul primar al tuturor obiectelor pentru care SMITHM este grupul primar pentru folosirea comenzii Lucru cu obiecte după grup primar (WRKOBJPGP):

   ```
   WRKOBJPGP PGP(SMITHM)
   ```

   Introduceţi opţiunea 9 pentru toate obiectele care au nevoie de modificarea grupului primar şi introduceţi din linia de comandă NEWPGP (JONESM).

   Notă: JONESM ar putea avea un gid asignat folosind parametrul GID în comanda Creare profil de utilizator (CRTUSRPRF sau CHGUSRPRF).
4. Afişaţi profilul de utilizator SMITHM folosind comanda Afişare profil de utilizator (DSPUSRPRF):

   ```
   DSPUSRPRF USRPRF(SMITHM)
   ```

   Notaţi uid-ul şi gid-ul pentru SMITHM.
5. Transferaţi dreptul de proprietate asupra tuturor celorlalte obiecte deţinute la JONESM şi înlăturaţi profilul de utilizator SMITHM, folosind opţiunea 4 (Înlăturare) din ecranul Gestionare înrolare utilizator.
6. Modificaţi uid-ul şi gid-ul lui JONESM la uid-ul şi gid-ul care au aparţinut lui SMITHM folosind comanda Modificare profil de utilizator (CHGUSRPRF):

   ```
   CHGUSRPRF USRPRF(JONESM) UID(uid-ul din
   SMITHM)
             GID(gid-ul din SMITHM)
   ```

   Dacă JONESM posedă obiectele dintr-un director, comanda CHGUSRPRF nu poate fi folosităpentru a modifica uid-ul şi gid-ul. Folosiţi API-ul QSYCHGID pentru modificarea uid-ul şi gid-ul profilului de utilizator JONESM.

Lucru cu auditare utilizatori

Puteţi folosi comanda Modificare auditare utilizatori (CHGUSRAUD) pentru a seta 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
              + for more values   JONESS
Object auditing value  . . . . .   *SAME
User action auditing . . . . . .   *CMD
              + for more values   *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. Valorile pe care le specificaţi nu sunt adăugate la valorile curente AUDLVL pentru utilizatori ci înlocuiesc valorile curente AUDLVL.

Dacă aveţi autorizarea specială *ALLOBJ sau *AUDIT, puteţi folosi comanda Afişare profil de utilizator (DSPUSRPRF) ca să vedeţi caracteristicile de auditare pentru un utilizator.

Lucru cu profiluri în programe CL

Puteţi lucra cu profiluri de utilizator într-un program CL.

Veţi dori să extrageţi informaţii despre profilul de utilizator de la un program CL. Puteţi folosi comanda Extragere profil de utilizator (RTVUSRPRF) în programul dumneavoastră CL. Comanda întoarce atributele cerute ale profilului la variabilele pe care le-aţi asociat cu numele de câmp profil de utilizator. Descrierile câmpurilor de profil de utilizator din această secţiune arată lungimile de câmpuri aşteptate 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 parole” la pagina 61 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 de 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.

Puncte de ieşire profil de utilizator

Puteţi scrie propriile programe de ieşire pentru a realiza funcţii specifice profil de utilizator. Când înregistraţi programele de ieşire cu oricare din punctele de ieşire profil de utilizator, sunteţi notificat când un profil de 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 de utilizator.

Informaţii înrudite

Programele de ieşire

Profiluri de utilizator furnizate de IBM

Împreună cu software-ul de sistem primiţi şi câteva profiluri de utilizator. Aceste profiluri de utilizator furnizate de IBM sunt folosite ca şi obiecte deţinute pentru funcţii de sistem variate. Unele funcţii sistem de asemenea rulează sub anumite profiluri de utilizator furnizate de IBM.

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, “profiluri de utilizator furnizate de IBM”, la pagina 317 conţine o listă completă a tuturor profilurilor de utilizator livrate de IBM şi valorile de câmp pentru fiecare profil.

Notă: Toate profilurile de utilizator livrate de IBM cu excepţia QSECOFR sunt livrate cu o parolă *NONE şi nu sunt intenţionate pentru semnare. Aceste profiluri sunt folosite de sistemul de operare IBM i5/OS. Ca urmare, nu este recomandată semnarea cu aceste profiluri sau folosirea profilurilor pentru posesia obiectelor de utilizator (nelivrate de IBM).

Concepte înrudite

"Profilurile de utilizator furnizate de IBM" la pagina 258
Puteţi realiza taskuri de auditare pe profiluri de utilizator livrate de IBM verificându-le parolele.

Modificarea parolelor pentru profiluri de utilizator livrate de IBM

Dacă trebuie să vă logaţi cu unul din profilurile livrate 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) . . . . . .
```

Lucrul cu ID-uri 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 principal. 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. **Note**:Informaţiile privind Uneltele de service au fost mutate la Centrul de informare.
- **Îmbunătăţiri gestionare parole**

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 utilizator 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 de utilizator DST, ID-uri utilizator, profiluri de utilizator unelte de service, sau variaţii ale acestor nume.

  Concepte înrudite

  “Profilurile de utilizator furnizate de IBM” la pagina 258
  Puteţi realiza taskuri de auditare pe profiluri de utilizator livrate de IBM verificându-le parolele.

  Informaţii înrudite

  Gestionarea ID-urile utilizator unelte de service

Parola 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

Această secţiune descrie fiecare dintre componentele securităţii resurselor şi cum funcţionează împreună pentru a proteja informaţiile despre sistem. Explică de asemenea cum să se utilizeze comanda CL şi afişează organizarea de securitate resursă pe sistemul dvs.

Securitate resursă defineşte căror utilizatori le este permis să utilizeze obiecte din sistem şi care operaţie le este permis să realizeze pe aceste obiecte.

Capitolul 7, “Proiectarea securităţii”, la pagina 219 discuţii tehnice pentru a proiecta securitatea resursă, inclusiv cum afectează aceasta şi design aplicaţiile şi performanţa sistemului.

Capitolul “Cum verifică sistemul autorizarea” la pagina 169 furnizează diagrame de flux detaliate şi descrie cum sistemul verifică autorizarea. Puteţi găsi util să consultaţi aceste informaţii pe măsură ce citiţi explicaţiile următoare.

Concepte înrudite

“Securitatea resurselor” la pagina 5
Capacitatea de a accesa un obiect este numită *autorizare*. Securitatea resurselor în sistemul de operare i5/OS vă permite să controlaţi autorizările obiectelor, care definesc cine poate folosi ce obiecte şi cum pot fi folosite acele obiecte.

“Recomandări generale pentru proiectarea securităţii” la pagina 220
Păstrarea proiectării securităţii cât mai simple face mai uşoară gestionarea şi auditarea ei. De asemenea îmbunătăţeşte performanţele aplicaţiei şi ale copiei de rezervă.

Definirea celor care pot avea acces la informaţii

Puteţi autoriza utilizatori individuali, grupuri de utilizatori şi publicul.

Notă: În unele medii, autorizarea acordată unui utilizator este numită **privilegiu**.

Definiţi cum puteţi utiliza un obiect în mai multe modalităţi:

Autorizare publică:
Autorizarea publică a alcătuită din oricine este autorizat să se logheze în sistem. 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 privată:
Puteţi defini autorizare specifică pentru a utiliza un (sau pentru a nu utiliza) obiect. Puteţi acorda autorizare unui profil de 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 de utilizator individuale le poate fi acordată autorizare să utilizeze obiecte în sistem. Acesta este un tip de autorizare privată.

Autorizare grup:
Unor profiluri de utilizator individuale le poate fi acordată autorizare să utilizeze 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 de 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 informaţii

Puteţi defini ce operaţii pot fi realizate asupra obiectelor, datelor şi câmpurilor.

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 ce operaţii pot fi realizate asupra obiectului ca un întreg.
2. **Autorizare date** defineşte ce operaţii pot fi realizate asupra conţinutului obiectului.
3. **Autorizare câmp** defineşte ce operaţii pot fi realizate asupra câmpurilor de date.

Tabela 115descrie 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, “Autorizare necesară pentru obiecte folosite de comenzi”, la pagina 337 furnizează informaţii despre autorizarea necesară pentru a realiza o funcţie specifică.

Tabela 115. Descrierea tipurilor de autorizări

specială	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 - Gestionare listă de autorizare	Adăugaţi şi eliminaţi utilizatori şi autorizările lor din lista de autorizare [2].
Autorizări asupra datelor:		

Tabela 115. Descrierea tipurilor de autorizări (continuare)

specială	Nume	Funcţii permise
*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:		
*MGT	Management - Gestionare	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 subiectul “Gestionarea listei de autorizare” la pagina 138 pentru informaţii suplimentare.

Operaţii înrudite

“Modificarea la nivel 30 de la un nivel mai mic” la pagina 13
Când treceţi la nivelul de securitate 30 de la un nivel de securitate mai mic, sistemul modifică toate profilurile de utilizator pentru a actualiza autorizările speciale următoarea dată când realizaţi un IPL.

Referinţe înrudite

“Autorizare de grup” la pagina 98
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.

Autorizări folosite în general

Puteţi specifica anumite seturi de obiecte şi autorizări de date.

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 116 la pagina 134 arată autorizările definite de sistem disponibile la folosirea comenzilor şi ecranelor de autorizare obiect.

Tabela 116. 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 117 arată autorizări suplimentare definite de sistem care sunt disponibile la folosirea comenzilor WRKAUT şi CHGAUT:

Tabela 117. 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 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

Programul cu licenţă LAN Server foloseşte liste de control al accesului pentru a gestiona autorizările. Autorizările unui utilizator sunt numite **permisiuni**. Tabela 118 arată cum sunt mapate permisiunile LAN Server către autorizările de obiect şi de date:

Tabela 118. Permisiune server LAN

Autorizare	Permisiuni server LAN
*EXCLUDE	Fără
Autorizări obiect	
*OBJOPR	Vedeţi nota 1
*OBJMGT	Permisiune
*OBJEXIST	Creare, Ştergere

Tabela 118. Permisiune server LAN (continuare)

Autorizare	Permisiuni server LAN
*OBJALTER	Atribut
*OBJREF	Fără echivalent
Autorizări pentru date	
*READ	Citire
*ADD	Creare
*UPD	Scriere
*DLT	Ştergere
*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. Puteţi de asemenea defini securitatea pentru grupuri de obiecte folosind securitatea bibliotecii sau o listă de autorizare.

Securitatea bibliotecii

Puteţi folosi securitatea bibliotecii pentru a proteja informaţii.

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, “Autorizare necesară pentru obiecte folosite de comenzi”, la pagina 337 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.

Concepte înrudite

“Planificarea bibliotecilor” la pagina 224
O bibliotecă este ca un director folosit pentru a localiza obiectele din ea. Mulţi factori afectează modul în care alegeţi să grupaţi informaţiile aplicaţiilor dumneavoastră în biblioteci şi să le gestionaţi.

Securitatea bibliotecilor şi liste 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 accesul la un obiect este cerut şi *LIBL este specificat pentru obiect, informaţiile listă 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 o potenţială expunere de 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.

Referinţe înrudite

“Listele de biblioteci” la pagina 207

Lista de biblioteci pentru un job indică bibliotecile în care se caută şi ordinea în care ele vor fi căutate.

Autorizări de câmp

Puteţi specifica autorizări de câmp pentru fişiere bază de date.

Autorizările de câmp sunt acum suportate pentru fişierele bază de date. Autorizările suportate sunt gestionare, modificare, referinţă, citire, adăugare şi actualizare. 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.

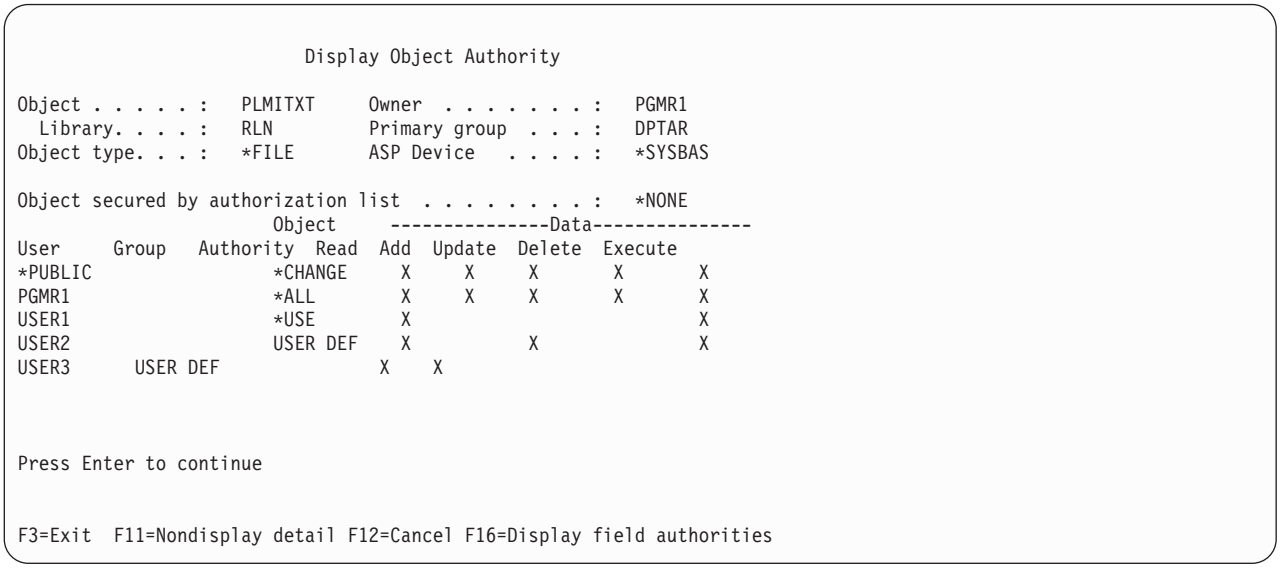


Figura 4. Ecranul Display Object Authority care arată F16=Display field authorities. Această tastă funcţională va fi afişată când un fişier bază de date are autorizări de câmp.

```
                          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.

Autorizările de câmp includ următoarele opţiuni:

- 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

Această secţiune furnizează informaţii despre securitate în 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.

Informaţii înrudite

System/38 Environment Programming

Recomandări pentru mediul System/38
Acest subiect include o listă de recomandări 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.

Securitate director
Puteţi folosi securitatea de director pentru a proteja informaţii.

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 performanţa procesului de verificare autorizare.

Securitate listă 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 autorizările pe care utilizatorii le au pentru obiectele securizate 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 folosi o listă de autorizări pentru a defini autorizarea publică pentru obiectele din listă. Dacă autorizarea publică pentru un obiect este setată la *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 de 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 “Avantajele folosirii unei liste de autorizare” la pagina 166 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 securiza obiecte livrate de IBM

Puteţi folosi liste de autorizare pentru a securiza obiecte livrate 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.

Autorizare pentru obiectele noi dintr-o bibliotecă

Puteţi specifica 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 bibliotecă. Când creaţi un obiect, parametrul AUT din comanda de creare determină autorizarea publică pentru obiect. Dacă valoarea AUT din comanda de creare este *LIBCRTAUT, care este valoarea implicită pentru majoritatea comenzilor, 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, presupuneţi 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)
```

“Alocarea autorizării şi a dreptului de proprietate obiectelor noi” la pagina 145 arată mai multe exemple de moduri în care sistemul asignează drept de proprietate şi autorizare noilor obiecte.

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 pe care le implică CRTAUT

Trebuie să luaţi în considerare riscurile când modificaţi CRTAUT (Creare autorizare) pentru o bibliotecă de aplicaţii.

Dacă aplicaţiile dumneavoastră folosesc autorizarea implicită pentru obiectele noi create în timpul procesării aplicaţiei, ar trebui să controlaţi cine are autorizarea să schimbe descrierile bibliotecii. Schimbarea valorii CRTAUT pentru o bibliotecă de aplicaţie poate permite accesul neautorizat la obiectele noi create în bibliotecă.

Autorizare pentru obiecte noi dintr-un director

Puteţi specifica autorizarea pentru 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 noul director. Dacă folosiţi opţiunea *INDIR, autorizarea pentru directorul creat este determinată de directorul în care este creat. Altfel, puteţi specifica autorizarea specifică necesară.

Când creaţi un nou director folosind API-ul mkdir()--Make Directory, proprietarul, grup primar şi autorizările publice de obiect pentru directorul creat sunt determinate din directorul în care este creat dar proprietarul, grup primar şi autorizările publice de obiect sunt determinate de modul specificat în apelul API-ului.

Următoarele 2 exemple arată diferite rezultate când creaţi un nou director cu diferite opţiuni.

Primul exemplu creează un nou director în sistemul de fişiere ″root″(/) folosind comanda CRTDIR şi autorizare specifică *PUBLIC.

Condiţii iniţiale: Autorizările directorului părinte:

```
                                  Display Authority

Object . . . . . . . . . . . . . :   /sanders/mytest
Owner  . . . . . . . . . . . . . :   SANDERS
Primary group  . . . . . . . . . :   SANDERSGP3
Authorization list . . . . . . . :   *NONE

             Data      -----Object Authorities-----
User         Authority  Exist    Mgt    Alter    Ref
*PUBLIC      *RWX        X        X      X        X
SANDERS      *RW
SANDERSGP3   *RX
QPGMR        *RWX
QTCM         *RWX        X        X      X        X
```

Utilizatorul SANDERS emite următoarea comandă:

CRTDIR DIR('/sanders/mytest/deletemepub') DTAAUT(*R) OBJAUT(*NONE)

Rezultate: Autorizările pentru directorul creat:

```
                                  Display Authority

Object . . . . . . . . . . . . . :   /sanders/mytest/deletemepub
Owner  . . . . . . . . . . . . . :   SANDERS
Primary group  . . . . . . . . . :   SANDERSGP3
Authorization list . . . . . . . :   *NONE

             Data      -----Object Authorities-----
User         Authority  Exist    Mgt    Alter    Ref
*PUBLIC      *R
SANDERS      *RWX
SANDERSGP3   *RX
```

Observaţii:

1. Autorizările date *PUBLIC şi obiect sunt bazate pe parametrii DTAAUT şi OBJAUT.
2. Autorizările de date ale proprietarului (SANDERS) sunt setate la *RWX dar autorizările de obiect sunt moştenite de la proprietarul directorului părinte. Asta înseamnă că proprietarul acestui director nu are autorizări de obiect asupra noului director deoarece proprietarul directorului părinte nu are autorizări de obiect asupra directorului părinte.
3. Noul director are un profil grup primar de SANDERSGP3 deoarece directorul părinte are SANDERSGP3 ca profilul primar de grup.

Al doilea exemplu arată cu toate autorizările sunt moştenite de la directorul părinte când creaţi un director nou în sistemul de fişiere ″root″ (/) folosind comanda CRTDIR.

Condiţii iniţiale: Autorizările directorului părinte:

```
                                  Display Authority

Object . . . . . . . . . . . . . :   /sanders/mytest
Owner  . . . . . . . . . . . . . :   SANDERS
Primary group  . . . . . . . . . :   SANDERSGP3
Authorization list . . . . . . . :   *NONE

             Data      -----Object Authorities-----
User         Authority  Exist    Mgt    Alter    Ref
*PUBLIC      *RWX        X        X      X        X
SANDERS      *RW
SANDERSGP3   *RX
QPGMR        *RWX
QTCM         *RWX        X        X      X        X
```

Utilizatorul SANDERSUSR emite următoarea comandă:

CRTDIR DIR('/sanders/mytest/deletemepub')

Rezultate: Autorizările pentru directorul creat:

```
                                  Display Authority

Object . . . . . . . . . . . . . :   /sanders/mytest/deletemepub
Owner  . . . . . . . . . . . . . :   SANDERSUSR
Grup primar  . . . . . . . . . . :   SANDERSGP3
Authorization list . . . . . . . :   *NONE

             Data      -----Object Authorities-----
User         Authority  Exist    Mgt    Alter    Ref
*PUBLIC      *RWX        X        X      X        X
SANDERSUSR   *RWX
SANDERSGP3   *RX
QPGMR        *RWX
QTCM         *RWX        X        X      X        X
SANDERS      *RW
```

Observaţii:

1. Autorizările *PUBLIC pentru date şi obiecte sunt moştenite de la directorul părinte; prin urmare, autorizarea de date este setată la *RWX cu toate autorizările de obiect.
2. Autorizările de date ale proprietarului (SANDERSUSR) sunt setate la *RWX dar autorizările de obiect sunt moştenite de la proprietarul directorului părinte. Asta înseamnă că proprietarul acestui director nu are autorizări de obiect asupra noului director deoarece proprietarul directorului părinte nu are autorizări de obiect asupra directorului părinte.
3. Noul director are un profil grup primar de SANDERSGP3 deoarece directorul părinte are SANDERSGP3 ca profilul primar de grup.
4. Tuturor utilizatorilor care sunt autorizaţi privat părintelui director (QPGMR, QTCM) şi proprietarului directorului părinte (SANDERS) li se acordă autorizare privată noului director.

Drept de proprietate obiect

Acest subiect descrie dreptul de proprietate al obiectelor şi funcţiile sale în sistem.

Fiecărui obiect îi este asignat un proprietar când este creat. Proprietarul este fie utilizatorul care creează obiectul, fie profilul de grup dacă profilul de 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. “Alocarea autorizării şi a dreptului de proprietate obiectelor noi” la pagina 145 arată exemple de moduri în care sistemul asignează drept de proprietate noilor obiecte.

Proprietarul unui obiect are întotdeauna toate autorizările pentru obiect dacă oricare sau toate autorizările nu sunt înlăturate specific. Ca proprietar de obiect, aţi putea alege să înlăturaţi unele autorizări specifice ca măsură de precauţie dacă nu aveţi autorizare specială *ALLOBJ. 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. Proprietarul unui obiect sistem de fişiere integrat nou creat are aceleaşi autorizări obiect pentru acel obiect sistem de fişiere integrat ca proprietarul directorului părinte asupra directorului părinte. Verificaţi subiectul Planificarea şi setarea securităţii sistemului pentru a vedea dacă regulile pentru autorizările de obiect se aplică tuturor sistemelor de fişier sau doar la unele.

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.

Următoarele paragrafe se aplică şi obiectelor bazate pe biblioteci şi directoare.

Când schimbaţi proprietarul unui obiect, aveţi opţiunea să păstraţi sau să revocaţi autorizarea proprietarului anterior.

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 de 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 împiedicaimpacturile asupra performaţei sau operaţiilor de sistem, nu asignaţi obiecte decât unui profil proprietar pentru întregul mediu System i5. Fiecare aplicaţie şi obiectele aplicaţiei ar trebui deţinute de un profil separat. De asemenea, profilurile de 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. Consultaţi “Spaţiu de stocare maxim” la pagina 94 pentru mai multe informaţii.

Dreptul de proprietate al grupului asupra obiectelor

Acest subiect furnizează informaţii detaliate despre dreptul de proprietate al grupului asupra obiectelor.

Când este creat un obiect, sistemul verifică profilul de utilizator care a creat obiectul pentru a determina dreptul de proprietate asupra obiectului. Dacă utilizatorul este un membru al unui profil de grup, câmpul OWNER din profilul de 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 de utilizator. Obiectele create în directoare nu folosesc valorile OWNER şi GRPAUT pentru a determina deptul de proprietate sau autorizarea de grup. Obiectul va fi întotdeauna posedat de creatorul obiectului.

Câmpul *tip autorizare grup* (GRPAUTTYP) din profilul de utilizator determină dacă grupul 1) devine grupul primar pentru obiect sau 2) îi este dată autorizare privată la obiect. “Alocarea autorizării şi a dreptului de proprietate obiectelor noi” la pagina 145arată 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 de 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 de 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 departament 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 de utilizator creator. Intrarea este scrisă doar dacă valoarea de sistem QAUDLVL specifică *CREATE şi valoarea de sistem QAUDCTL include *AUDLVL.

  Concepte înrudite

  “Profiluri de grup” la pagina 4
  Un *profil de grup* este un tip special de profil de utilizator. În loc să acordaţi autorizarea fiecărui utilizator individual, puteţi folosi un profil de grup ca să definiţi autorizarea pentru un grup de utilizatori.

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 de utilizator controlează dacă grupul utilizatorului are autorizare la obiect şi tipul autorizării este dat. Parametrul *Tip autorizare grup* (GRPAUTTYP) dintr-un profil de utilizator poate fi folosit pentru a face grupul utilizatorului grupul primar pentru obiect. “Alocarea autorizării şi a dreptului de proprietate obiectelor noi” la pagina 145 arată exemple de cum este asignată autorizare când sunt create obiecte noi. Pentru un obiect bazat pe director în unele sisteme de fişiere, obiectul moşteneşte grupul primar al directorului său părinte. De exemplu, dacă directorul părinte are un grup primar de FRED, atunci FRED va avea probleme încercând să creeze orice în acel director părinte. Asta e din cauză că acelaşi profil nu poate fi în acelaşi timp profil proprietar şi grup primar pentru acelaşi obiect.

Puteţi modifica grupul primar pentru un obiect bazat pe bibliotecă sau bazat direct folosind oricare din următoarele comenzi:

- Comanda Modificare grup primar obiect (CHGOBJPGP)
- Comanda Modificare grup primar (CHGPGP)
- Opţiunea 9 din comanda Lucru cu obiecte după grup primar (WRKOBJPGP)

Puteţi modifica autorizarea unui grup primar folosind comada Editare autorizare obiect (EDTOBJAUT) sau comenzile de acordarea şi revocare autorizare. Puteţi modifica autorizarea grupului primar pentru un obiect bazat pe bibliotecă sau bazat pe director folosind comanda Modificare autorizare (CHGAUT) sau comanda Lucru cu autorizare (WRKAUT).

Concepte înrudite

"Profiluri de grup" la pagina 4
Un *profil de grup* este un tip special de profil de utilizator. În loc să acordaţi autorizarea fiecărui utilizator individual, puteţi folosi un profil de grup ca să definiţi autorizarea pentru un grup de utilizatori.

Profilul de utilizator QDFTOWN

Profilul de utilizator QDFTOWN (Default Owner - Proprietar implicit) este un profil de utilizator livrat de IBM, folosit când un obiect nu are proprietar sau când dreptul de proprietate asupra unui obiect poate reprezenta un risc 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 de 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 17 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 de utilizator care deţine un păstrător de autorizare care are acelaşi nume ca fişierul care este mutat, redenumit sau a cărui bibliotecă este redenumită.

Sistemul furnizează profilul de 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 de utilizator şi transfera dreptul de proprietate al obiectelor asociate cu profilul de utilizator QDFTOWN. Puteţi acorda alte autorizări utilizator profilului QDFTOWN. Profilul de utilizator QDFTOWN este destinat folosirii doar de către sistem. Nu ar trebui să proiectaţi securitatea dvs. astfel încât QDFTOWN să deţină normal obiectul.

Alocarea autorizării şi a dreptului de proprietate obiectelor noi

Puteţi aloca autorizarea şi dreptul de proprietate obiectelor noi din sistem.

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 de utilizator al creatorului

Figura 6 la pagina 146 până la Figura 9 la pagina 149 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:
Fără

Autorizare privată:
DPT806 *CHANGE

Notă:

*LIBCRTAUT este valoarea implicită pentru parametrul AUT în majoritatea comenzilor CRTxxx.

Figura 6. Exemplu de obiect nou: Autorizare publică de la bibliotecă, autorizare privată dată de grup

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:
Fără

Autorizare privată:
DPT806 *CHANGE

Figura 7. Exemplu de obiect nou: Autorizare publică de la valoare de sistem, autorizare privată dată de grup

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:
Fără

Figura 8. Exemplu de obiect nou: Autorizare publică de la bibliotecă, autorizare primară de grup dată de grup

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:
Fără

Autorizare privată:
Fără

Figura 9. Exemplu de obiect nou: Autorizare publică specificată, grupul posedă obiectul

Obiecte care adoptă autorizarea proprietarului

Puteţi asigna autorizare adoptată unui program utilizator pentru a permite utilizatorului să modifice un fişier client.

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 întreţinere 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 de utilizator (USRPRF) în comanda CRTxxxPGM. Acest parametru determină dacă programul foloseşte autorizarea proprietarului programului în plus faţă de autorizarea utilizatorului care rulează programul.

Consultaţi subiectul Limitaţi folosirea autorizării adoptate cu privire la considerente de securitate şi autorizare adoptată la folosirea de pachete SQL.

Următoarele descrieri se aplică autorizărilor adoptate:

- 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 de utilizator nu este adoptat. De exemplu, atributele cu capabilităţi limitate nu sunt adoptate.
- Autorizarea adoptată este activă cât timp programul care foloseşte autorizarea adoptată rămâne în stica de apeluri. De exemplu, presupuneţi că PGMA foloseşte autorizare adoptată:
  - Dacă PGMA porneşte PGMB folosind comanda CALL, acestea sunt stivele de apeluri înainte şi după comanda CALL:

Tabela 119. Autorizare adoptată şi comanda CALL

Stiva de apeluri înainte de comanda CALL:	**Stiva de apeluri după comanda CALL:**
QCMD • • • PGMA	QCMD • • • PGMA PGMB

Deoarece PGMA rămâne în stiva de apeluri după ce PGMB este apelat, PGMB foloseşte autorizarea adoptată a PGMA. (Parametrul Folosire autorizare adoptată (USEADPAUT) poate înlocui aceasta. Vedeţi “Programe care ignoră autorizare adoptată” la pagina 152 pentru mai multe informaţii despre parametrul USEADPAUT.)

  - Dacă PGMA porneşte PGMB folosind comanda Transfer control (TFRCTL), stiva de apeluri arată aşa:

Tabela 120. Autorizare adoptată şi comanda TFRCTL

Stiva de apeluri înainte de comanda TFRCTL:	**Stiva de apeluri după comanda TFRCTL:**
QCMD • • • PGMA	QCMD • • • PGMB

PGMB nu foloseşte autorizarea adoptată a PGMA, deoarece PGMA nu mai este în stiva de apeluri.

- 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.
- Autorizarea adoptată nu este folosită de către sistemele de fişiere integrate, incluzând rădăcina, QOpenSzs, QDLS şi sisteme de fişiere definite de utilizator.
- Funcţie de adoptare program nu este folosită când folosiţi comanda Schimbare job (CHGJOB) pentru a schimba coada de ieşire pentru un job. Profilul de 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 private 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 *Profiluri de utilizator*) şi dacă foloseşte autorizare adoptată de la programe anterioare din stiva de apeluri (prompt *Folosire autorzare 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 au fost modificate de la ultima rulare a comenzii.

“Diagrama de flux 8: Cum este verificată autorizarea adoptată” la pagina 182 furnizează mai multe informaţii despre autorizarea adoptată. Subiectul “Folosirea autorizării adoptate în proiectarea meniurilor” la pagina 229 arată un exemplu de cum să folosiţi autorizarea adoptată într-o aplicaţie.

Autorzare 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 care se află mai sus în stiva de apeluri, autorizarea adoptată este folosită pentru a verifica autorizarea tuturor programelor de service la care este legat programul ILE. Dacă programul ILE adoptă autorizare, autorizarea adoptată nu va fi verificată când sistemul verifică autorizarea utilizatorului la programele service la momentul activării programului.

Riscuri şi recomandări autorizare adoptată

Ar trebui să folosiţi autorizări adoptate cu grijă pentru a preveni posibile riscuri de securitate.

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.
- Asiguraţi-vă că programele care adoptă autorizarea şi apelează alte programe trebuie să efectueze apeluri calificate de bibliotecă. 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 autorizare adoptată

Puteţi specifica parametrul folosire autorizare adoptată (USEADPAUT) pentru a controla dacă un program foloseşte autorizarea adoptată.

Aţi putea vrea ca unele programe să nu folosească autorizarea adoptată a programelor anterioare din stiva de apeluri. 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 231 arată un exemplu a modului de folosire a acestui parametru în proiectarea meniului. Vedeţi “Folosirea autorizării adoptate (QUSEADPAUT)” la pagina 35 pentru informaţii despre valoarea de sistem QUSEADPAUT.

Atenţie: În unele situaţii, puteţi folosi instrucţiunea MODINVAU MI pentru a împiedica pasarea autorizării adoptate funcţiilor 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.

Concepte înrudite

"Ignorarea autorizării adoptate" la pagina 231
Tehnica folosirii autorizării adoptate în proiectarea meniurilor necesită ca utilizatorul să revină 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.

Păstrătorii de autorizare

Un păstrător de autorizare este o unealtă de păstrare a autorizărilor pentru un fişier de bază de date descris prin program, dar care nu există pe sistem.

Folosirea primară a unui păstrător de autorizare este pentru aplicaţii mediu System/36, care şterg adesea fişiere descrise de sistem şi le creează din nou.

Un păstrător 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 păstrătorilor de autorizare:

- Păstrătorii 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.
- Păstrătorul de autorizare este asociat cu un anumit fişier şi bibliotecă. El are acelaşi nume ca şi fişierul.
- Păstrătorii de autorizare pot fi folosiţi doar pentru fişiere bază de date descrise prin program şi fişiere logice.
- O dată ce păstrătorul 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 păstrător de autorizare nu poate fi deosebit de fişierul propriu-zis. Ecranele nu indică dacă fişierul există şi nici nu arată dacă fişierul are un păstrător de autorizare.
- Dacă un fişier este asociat cu un păstrător de autorizare, autorizările definite pentru păstrătorul 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 păstrătorii de autorizare din sistem. O puteţi de asemenea folosi pentru a crea un fişier de ieşire (output file - OUTFILE) pentru procesare.
- Dacă creaţi un păstrător de autorizare pentru un fişier care există:
  - Utilizatorul care creează păstrătorul de autorizare trebuie să aibă autorizarea *ALL pentru fişier.
  - Proprietarul fişierului devine proprietarul păstrătorului de autorizare indiferent de utilizatorul care creează păstrătorul de autorizare.
  - Autorizarea publică pentru păstrătorul de autorizare provine de la fişier. Parametrul public authority (AUT) din comanda CRTAUTHLR este ignorat.
  - Autorizarea fişierului existent este copiată la păstrătorul de autorizare.
- Dacă creaţi un fişier şi există deja un păstrător de autorizare pentru acel fişier:
  - Utilizatorul care creează fişierul trebuie să aibă autorizarea *ALL pentru păstrătorul de autorizare.
  - Proprietarul păstrătorului de autorizare devine proprietarul fişierului indiferent de utilizatorul care creează fişierului.
  - Autorizarea publică pentru fişier provine de la păstrătorul de autorizare. Parametrul public authority (AUT) din comanda CRTPF sau CRTLF este ignorat.
  - Păstrătorul de autorizare este legat de fişier. Autorizarea specificată pentru păstrătorul de autorizare este folosită pentru a securiza fişierul.
- Dacă un păstrător 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 păstrător de autorizare existent, autorizarea şi dreptul de proprietate asupra fişierului sunt schimbate pentru a corespunde cu păstrătorul de autorizare. Utilizatorul care redenumeşte fişierul trebuie să aibă autorizarea *ALL pentru păstrătorul de autorizare.
- Dacă un fişier este mutat în altă bibliotecă şi un păstrător 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 păstrătorul de autorizare. Utilizatorul care mută fişierul trebuie să aibă autorizarea *ALL pentru păstrătorul de autorizare.

- Dreptul de proprietate al păstrătorului de autorizare şi asupra fişierului corespund întotdeauna. Dacă schimbaţi dreptul de proprietate asupra fişierului, atunci se schimbă şi dreptul de proprietate al păstrătorului de autorizare.
- Când un fişier este restaurat, dacă există un păstrător de autorizare pentru acel nume de fişier şi biblioteca în care este restaurat, el este legat de păstrătorul de autorizare.
- Păstrătorii de autorizare nu pot fi creaţi pentru fişierele din bibliotecile: QSYS, QRCL, QRECOVERY, QSPL, QTEMP şi QSPL0002 – QSPL0032.

Păstrătorii de autorizare şi migrarea System/36

System/36 Migration Aid creează un autorizare păstrător de autorizare pentru fiecare fişier care este migrat. El creează de asemenea un păstrător de autorizare pentru intrările din fişierul de securitate resurse System/36 dacă nu există un fişier corespunzător în System/36.

Aveţi nevoie de păstrători de autorizare doar pentru fişierele care sunt şterse şi re-create de aplicaţiile dumneavoastră. Folosiţi comanda Delete Authority Holder (DLTAUTHLR) pentru a şterge orice păstrători de autorizare de care nu aveţi nevoie.

Riscurile privind păstrătorul de autorizare

Ar trebui să luaţi în calcul securitatea când folosiţi un păstrător de autorizare.

Un păstrător 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 păstrător de autorizare pentru noul fişier. Utilizatorul astfel primeşte acces 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.

Lucru cu autorizare

Acest subiect descrie metodele folosite comun pentru setarea, întreţinerea şi afişarea de informaţii de autorizare despre sistem.

Anexa A, “Comenzi securitate”, la pagina 309 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.

Ecranele de autorizare

Această secţiune descrie unele caracteristici ale ecranelor care arată autorizările pentru obiecte.

Patru ecrane arată autorizările de obiect:

- Ecranul Afişare autorizare obiect
- Ecranul Editare autorizare obiect
- Ecranul Afişare autorizare
- Ecranul Gestionare autorizări

Figura 10 la pagina 155 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 10. 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                  *EXCLUDE
PGMR1                    *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 de utilizator 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 de 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)

Informaţii înrudite

Unelte securitate sistem

Lucru cu biblioteci

Puteţi specifica autorizarea pentru biblioteci şi obiecte noi create în biblioteci.

Doi parametri ai comenzii CRTLIB (Create Library) afectează autorizarea:

Autorizare (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 de utilizator 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 . . . . . . . . . . . . . . . . . :   TESTLIB

Type  . . . . . . . . . . . . . . . . . . :   PROD
ASP number . . . . . . . . . . . . . . . :   1
ASP device . . . . . . . . . . . . . . . :   *SYSBAS
Create authority . . . . . . . . . . . . :   OBJLST
Create object auditing . . . . . . . . . :   *SYSVAL
Text description . . . . . . . . . . . . :   Customer Rec
```

Crearea de obiecte

Puteţi specifica autorizarea unui obiect nou.

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  . . . . . . . :   PGMR1
  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  . . . . . . . :   PGMR1
  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
```

Lucru cu autorizare individuală obiect

Puteţi modifica autorizarea pentru un obiect.

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 EDTOBJAUT (Edit Object Authority) sau poate fi selectat ca o opţiune din ecranul WRKOBJOWN (Work with Objects by Owner), Work with Objects by Private Authority, Work with Objects by Primary Group sau Work with Objects.

```
                          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 autorizării definite de utilizator

Acest subiect furnizează informaţii despre specificarea autorizărilor 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 autorizare noilor utilizatori

Puteţi acorda autorizare 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
```

Înlăturarea autorizării unui utilizator

Puteţi de asemenea înlătura autorizarea unui utilizator pentru un obiect.

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.

Notă: Autorizarea *EXCLUDE pentru un profil de grup poate fi suprascrisă dacă utilizatorul are un alt profil de grup cu autorizare privată asupra obiectului.

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  Opr  Mgt  Exist  Alter  Ref
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

Object secured by authorization list  . . . . . .   *NONE

                       Object     ---------------Data---------------
User     Group   Authority  Read  Add  Update  Delete  Execute
USERB                   USER DEF
```

Lucrul cu autorizare pentru mai multe obiecte

Aflaţi cum să faceţi modificări de autorizare mai multor obiecte simultan.

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

Introduceţi opţiunile, apăsaţi 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
```

Lucru cu dreptul de proprietate obiect

Puteţi modifica dreptul de proprietate al unui obiect în mai multe moduri.

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 de profiluri de utilizator” la pagina 121 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 de cale este mai mung de 18 caractere, un simbol de mai mare (>) apare la sfârşitul numelui de cale. Pentru a vedea numele de cale absolut, plasaţi cursorul oriunde în numele de cale şi apăsaţi tasta F22.

Lucrul cu autorizarea grupului primar

Puteţi modifica grupul primar sau autorizarea grupului primar asupra unui obiect.

Pentru a schimba grupul primar sau autorizarea grupului primar pentru un obiect, folosiţi una dintre următoarele comenzi:

- Modificare grup primar obiect (CHGOBJPGP)
- Lucru cu obiecte după grup primar (WRKOBJPGP)
- Modificare grup primar (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

Ecranul Editare autorizare obiect şi comanda GRTOBJAUT vă permit să acordaţi autorizare unui obiect (sau unui grup de obiecte) pe baza autorizării obiectului 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 “Avantajele folosirii unei liste de autorizare” la pagina 166 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 125 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 gestionarea 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.

Operaţii înrudite

“Copiere autorizări private” la pagina 120
Puteţi copia autorizările private de la un profil de utilizator la altul folosind comanda Acordare autorizare utilizator (GRTUSRAUT).

Lucrul cu liste de autorizare

Această secţiune prezintă paşii pentru crearea unei liste 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 şi3 pot fi făcuţi în orice ordine.

Avantajele folosirii unei liste de autorizare

Puteţi proteja obiectele din sistem folosind liste de autorizare.

O listă de autorizare are următoarele avantaje:

- Listele de autorizare simplifică gestionarea autorizărilor. Autorizarea utilizatorului e definită pentru lista de autorizare, nu pentru obiectele individuale din listă. Dacă un obiect nou e securizat de lista de autorizare, 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 autorizare reduc numărul autorizărilor private din sistem. Fiecare utilizator are o autorizare privată pentru un obiect, lista de autorizare. Aceasta îi dă utilizatorului autorizare pentru toate obiectele din listă. Reducerea numărului de autorizări private din sistem are următoarele avantaje:
  - Reduce dimensiunea profilului de utilizator.
  - Îmbunătăţeşte performanţele la salvarea sistemului (SAVSYS) sau salvarea datelor de securitate (SAVSECDTA).
- Listele de autorizare 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 autorizare, 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 autorizare, puteţi modifica autorizările, chiar când fişierul e deschis.
- Listele de autorizare furnizează o cale de a memora autorizările când este salvat un obiect. Când este salvat un obiect care e securizat de o listă de autorizare, numele listei e salvat cu obiectul. Dacă obiectul este şters şi restaurat pe acelaşi sistem, este legat automat la lista de autorizare din nou. Dacă obiectul e restaurat pe un sistem diferit, lista de autorizare nu e legată, decât dacă se specifică ALWOBJDIF(*ALL) în comanda de restaurare.
- Din punctul de vedere al gestionării securităţii, o listă de autorizare este metoda preferată pentru a gestiona obiectele care au aceleaşi cerinţe de securitate. Chiar când există puţine obiecte care sunt securizate de listă, există încă un avantaj al folosirii unei liste de autorizare faţă de folosirea autorizărilor private asupra obiectului. Deoarece autorizările sunt într-un loc (lista de autorizare), 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.

Crearea unei liste de autorizare

Folosiţi comanda Creare listă de autorizare (CRTAUTL) pentru a crea o listă de autorizare.

Nu vă trebuie nici o autorizare pentru biblioteca QSYS pentru a crea o listă de autorizare în acea bibliotecă. Folosiţi comanda Creare listă de autorizare (CRTAUTL):

```
                    Create Authorization List (CRTAUTL)

Type choices, press Enter.

Authorization list . . . . . .   custlst1       Name
Text 'description' . . . . . .   Files cleared at month-end

                          Additional Parameters

Authority  . . . . . . . . . .   *use           *CHANGE, *ALL, *USE, *EXCLUDE
```

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 autorizării utilizatorilor la o listă de autorizare

Folosiţi ecranul Editare listă de autorizare (EDTAUTL) pentru a acorda utilizatorilor autorizare asupra listei de autorizare pe care a-ţi creat-o.

Pentru a lucra cu autorizarea pe care o au utilizatorii asupra listei de autorizare, trebuie să aveţi autorizarea *AUTLMGT (authorization list management - gestionare listă de autorizare), precum şi autorizările specifice pe care le acordaţi. Vedeţi subiectul “Gestionarea listei de autorizare” la pagina 138 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.
- 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.
- Work with Authority (WRKAUT) pentru a arăta lista utilizatorilor autorizaţi ai unui obiect.
- Change Authority (CHGAUT) pentru a modifica autorizarea unui utilizator asupra unui obiect.

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 Editare autorizare obiect, comanda GRTOBJAUT, comanda WRKAUT sau comanda CHGAUT 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 (Afişare obiecte listă de autorizare) pentru a lista toate obiectele securizate de 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 de asemenea folosi comanda Afişare obiecte listă de autorizare (DSPAUTLOBJ) pentru a vizualiza sau tipări o listă a obiectelor securizate de listă.

Setarea unei liste de autorizare

Setarea unei liste de autorizare face mai uşoară modificarea cine este autorizat asupra obiectelor şi mai uşor a securiza orice obiecte noi cu aceleaşi autorizări ca obiectele exitente.

La JKL Toy Company, este folosită o listă de autorizare pentru a securiza toate fişierele de lucru folosite în procesarea inventarului de la sfârşitul lunii. 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 autorizare face mai simplă gestionarea acestor modificări.

Urmaţi aceşti paşi pentru a seta lista de autorizare.

1. Creaţi lista de autorizare:
   ```
   CRTAUTL ICLIST1
   ```
2. Securizaţi toate fişierele de lucru cu lista de autorizare:
   ```
   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)
   ```

Dacă folosiţi liste de autorizare, 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 autorizare. Prima căutare este pentru autorizările private pentru obiect; cea de-a doua e pentru autorizările private din lista de autorizare. Două căutări necesită utilizarea resurselor sistemului; aşadar, performanţele pot fi alterate. Dacă folosiţi doar lista de autorizare, se realizează doar o căutare. De asemenea, din cauza folosirii cache-ului pentru autorizarea cu lista de autorizare, performanţa pentru verificarea autorizării va fi identică cu cea pentru verificarea doar a autorizărilor private pentru obiect.

Ştergerea unei liste de autorizare

Aţi putea de asemenea vrea să ştergeţi lista de autorizare pe care aţi creat-o.

Nu puteţi şterge o listă de autorizare dacă este folosită pentru a securiza obiecte. Folosiţi comanda DSPAUTLOBJ pentru a lista toate obiectele securizate de listă. Folosiţi ecranul Editare autorizare obiect, comanda Modificare autorizare (CHGAUT) sau Revocare autorizare obiect (RVKOBJAUT) pentru a modifica autorizarea pentru fiecare obiect. Când lista de autorizare nu mai securizează obiecte, folosiţi comanda Ştergere listă de autorizare (DLTAUTL) 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 149 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

Această secţiune prezintă diagrame de flux, descrieri şi exemple de verificare a autorizării.

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.

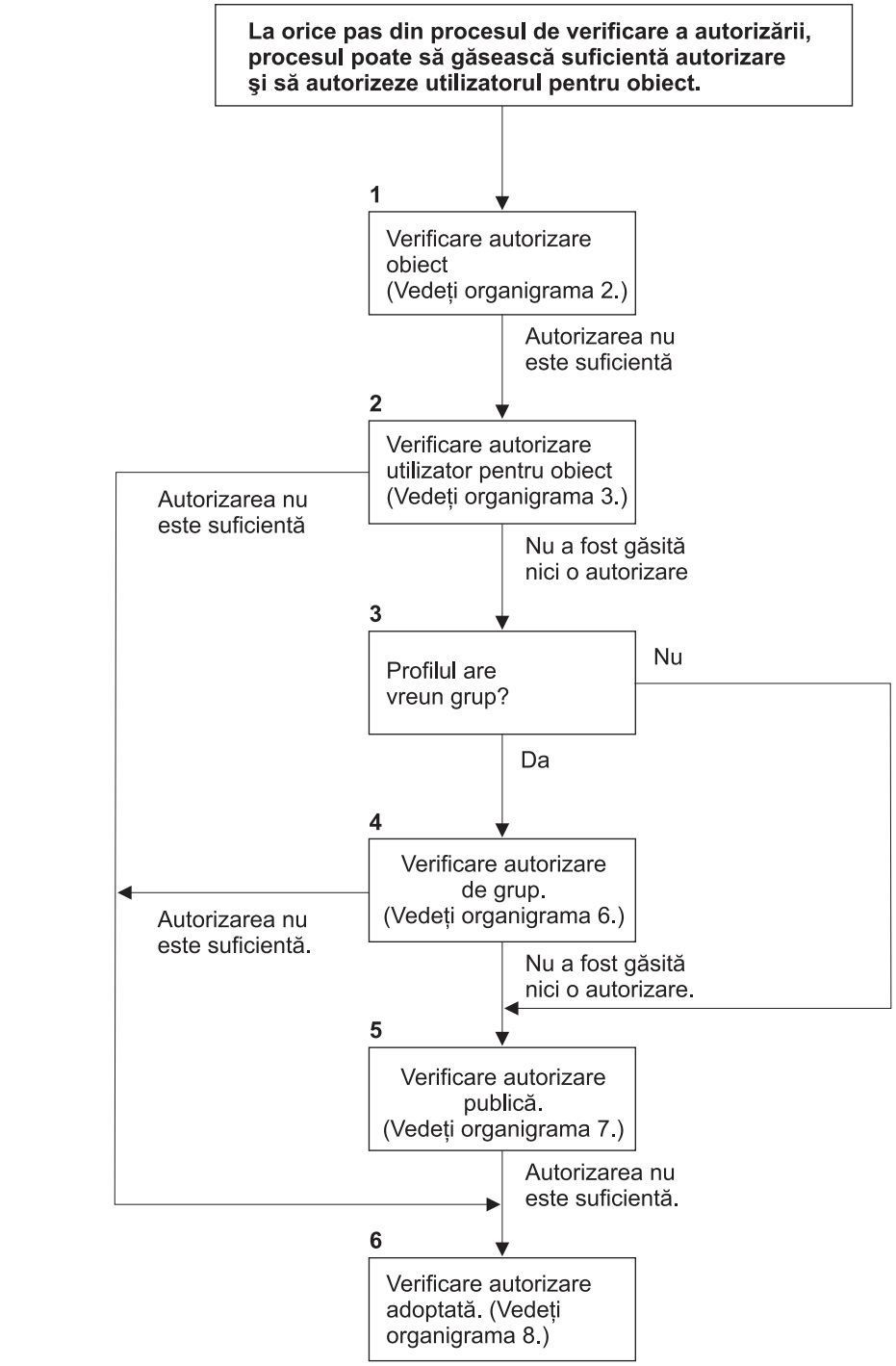
Paşii care reprezintă căutarea autorizărilor private ale unui profil sunt evidenţiaţi:

- Pasul 6 din Figura 13 la pagina 174
- Pasul 6 din Figura 16 la pagina 180
- Pasul 2 din Figura 19 la pagina 185

Repetarea acestor paşi este probabil să cauzeze probleme de performanţă în procesul de verificare a autorizării.

Diagrama de flux 1: Procesul principal de verificare a autorizării

Paşii din diagrama de flux 1 arată procesul principal pe care îl urmează sistemul la verificarea autorizării pentru un obiect.



Dacă utilizatorul nu este autorizat, se realizează una sau mai multe dintre următoarele:
1) Este trimis un mesaj utilizatorului sau porogramului;
2) Programul eşuează;
3) Este scrisă o intrare AF jurnalul de auditare.

RBAFW508-0

Figura 11. Diagrama de flux 1: Procesul principal de verificare a autorizării

Descrierea diagramei de flux 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 determină că nu există autorizare de grup asupra obiectului, continuă cu pasul 5. Dacă sistemul determină că autorizarea de grup asupra obiectului nu este suficientă, 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.)

Diagrama de flux 2: Cale rapidă de verificarea autorizării obiectelor

Paşii din diagrama de flux 2 sunt realizaţi folosind informaţiile stocate cu obiectul. Aceasta este cea mai rapidă metodă de autorizare a unui utilizator pentru un obiect.

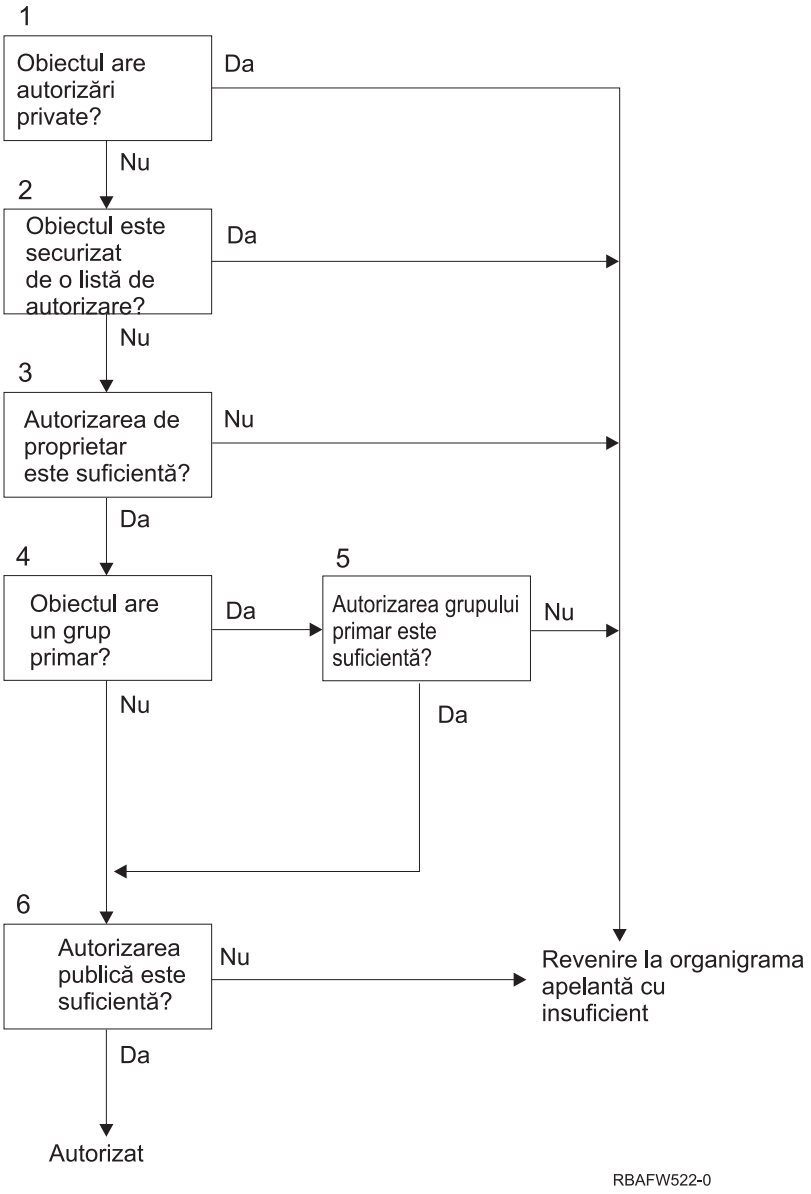


Figura 12. Diagrama de flux 2: Cale rapidă pentru autorizare obiecte

Descrierea diagramei de flux 2: Cale rapidă pentru autorizare obiecte

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 are, sistemul se întoarce la diagrama de flux apelantă cu insuficientă autorizare. 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 insuficientă autorizare. Dacă da, sistemul continua la 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 autorizarea publică este suficientă. Dacă este, atunci obiectul este autorizat. Dacă nu are, sistemul se întoarce la diagrama de flux apelantă cu insuficientă autorizare.

Diagrama de flux 3: Cum este verificată autorizarea unui utilizator asupra unui obiect

Paşii din diagrama de flux 3 sunt realizaţi pentru profilul de utilizator individual.

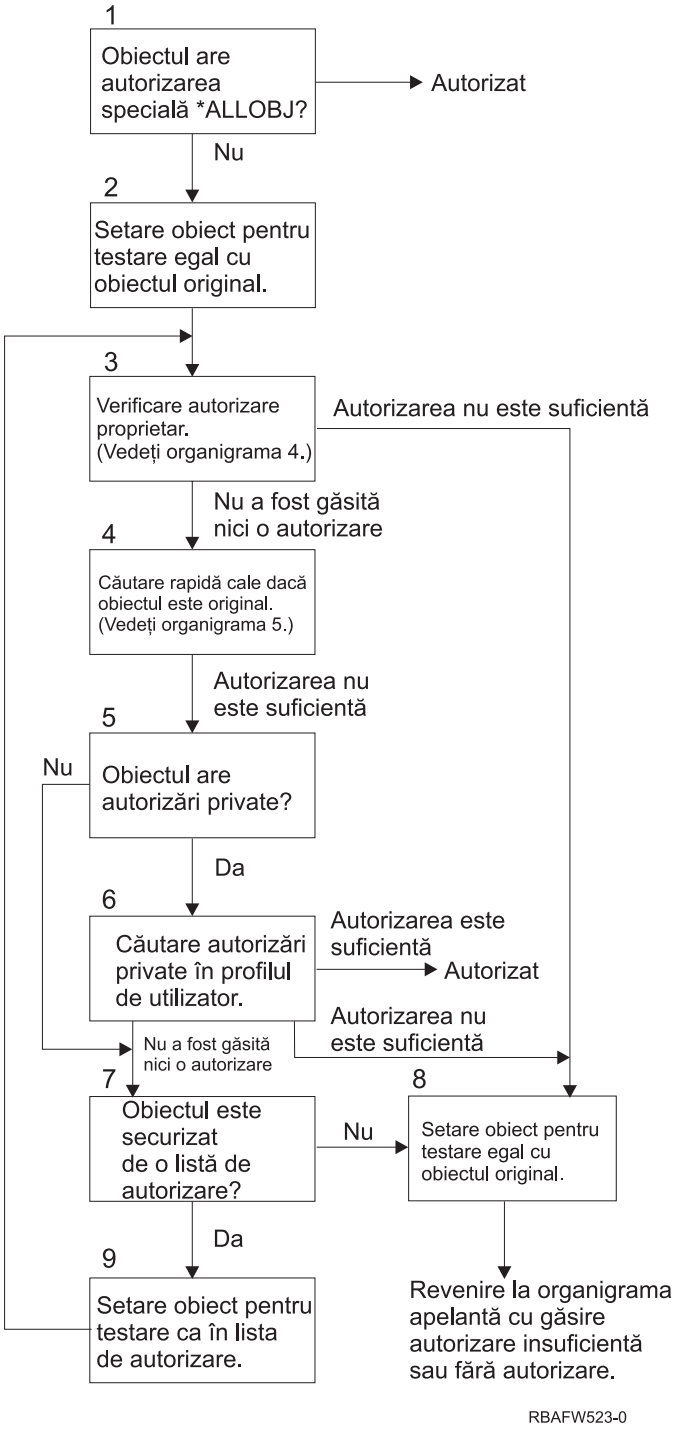


Figura 13. Diagrama de flux 3: Verificare autorizare utilizator

Descrierea diagramei de flux 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 continuă la pasul 8. Dacă nu este găsită nicio autorizare, atunci 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 verifică autorizările private cu 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.

Diagrama de flux 4: Cum este verificată autorizarea

Diagrama de flux 4 arată procesul de verificare a 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.

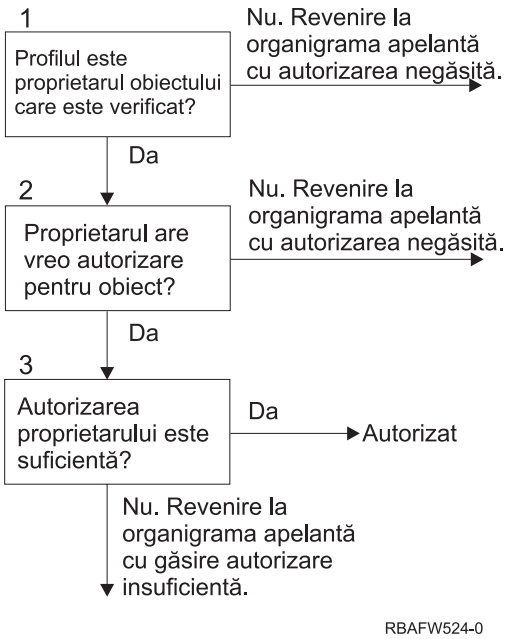


Figura 14. Diagrama de flux 4: Verificare autorizare proprietar

Descrierea diagramei de flux 4: Verificare autorizare proprietar

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 utilizatorul nu are autorizare asupra obiectului, atunci verificarea autorizării continuă cu pasul 3. Dacă sistemul determină că utilizatorul nu are autorizare asupra obiectului, atunci sistemul revine la diagrama de flux apelantă fără nicio 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.

Diagrama de flux 5: Cale rapidă de verificarea autorizării utilizatorilor

Diagrama de flux 5 arată calea rapidă pentru testarea autorizării utilizatorilor fără a căuta autorizări private.

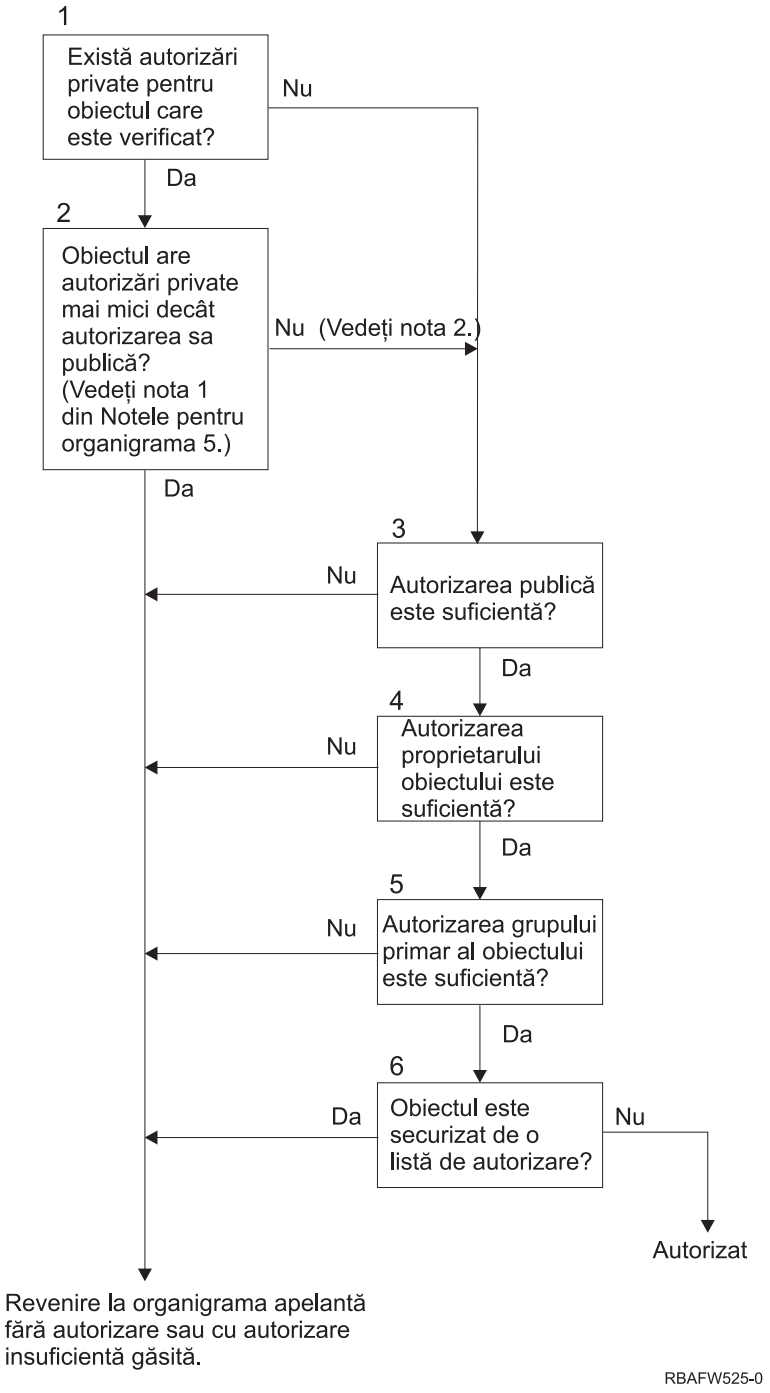


Figura 15. Diagrama de flux 5: Cale rapidă pentru autorizare utilizatori

Note diagrama de flux 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 121 la pagina 178, 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 121. Autorizarea publică şi cea privată

Autorizare	Utilizatori			
	OWNAR	**DPTMG**	**WILSONJ**	***PUBLIC**
Autorizări obiect:				
*OBJOPR		X		X
*OBJMGT	X			
*OBJEXIST				
*OBJALTER				
*OBJREF				
Autorizări pentru 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: Cale rapidă pentru autorizare utilizatori

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 sau obiectul nu are autorizări private care sunt mai mici decât autorizarea sa 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.

Diagrama de flux 6: Cum este verificată autorizarea de grup

Un utilizator poate fi membrul a cel mult 16 profiluri de grup. 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 122 arată autorizările pentru fişierul CRLIM:

Tabela 122. 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 pentru 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.

Diagrama de flux 6 de la pagina Figura 16 la pagina 180 arată paşii pentru verificarea autorizării de grup.

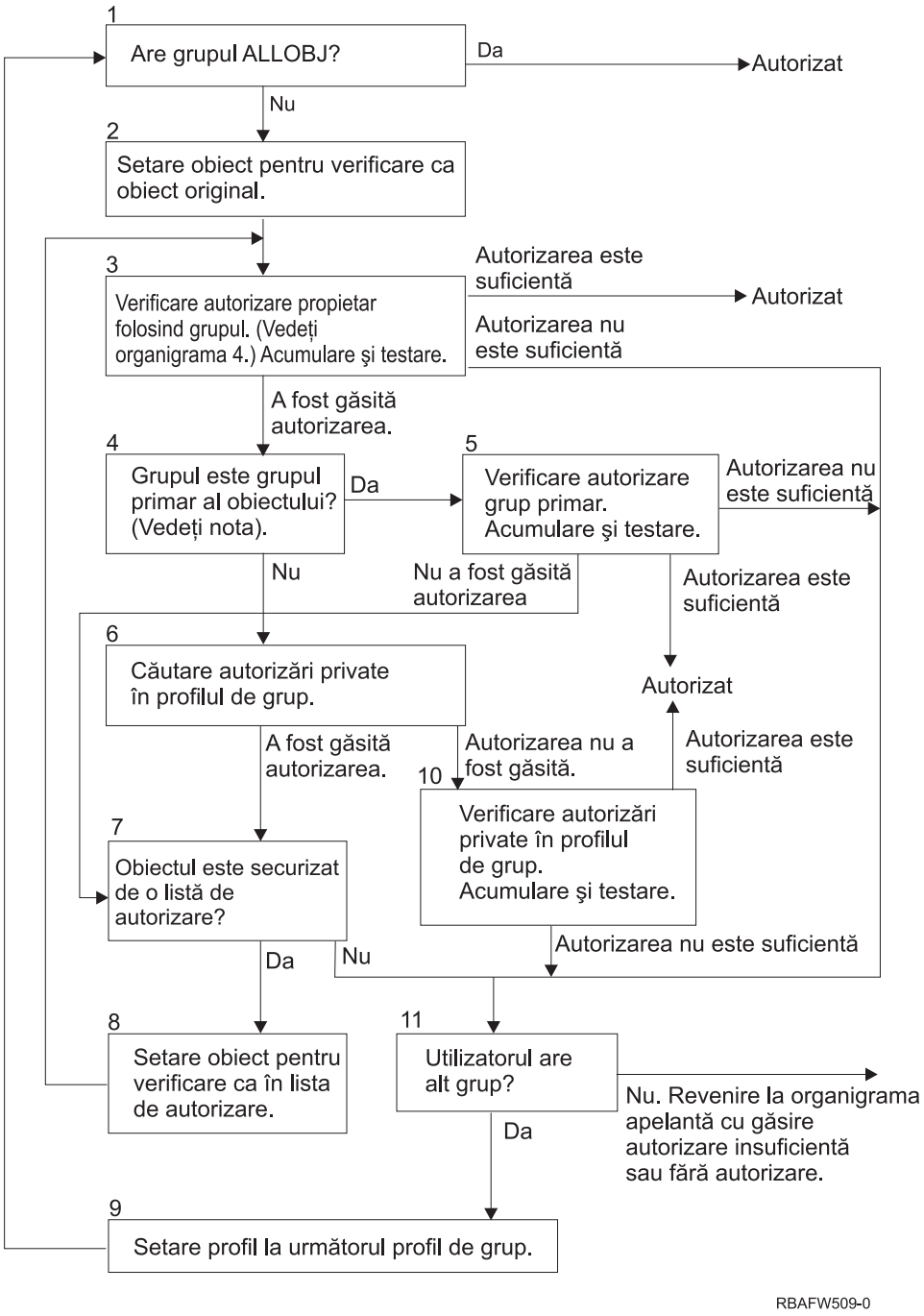


Figura 16. Diagrama de flux 6: Verificare autorizare de grup

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: Verificare autorizare grup

1. Sistemul determină dacă grupul are autorizare *ALLOBJ. Dacă are, atunci grupul este autorizat. Dacă nu are, atunci verificarea autorizării continuă cu Pasul 2.
2. Grupul nu are autorizare *ALLOBJ deci 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 în pasul 11. Dacă autorizarea nu este găsită, atunci verificarea autorizării continuă cu pasul 4.
4. Autorizarea proprietarului nu este găsită deci 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. Grupul este grupul primar al obiectului deci sistemul verifică şi testează autorizarea grupului primar. Dacă autorizarea grupului primar este suficientă, atunci grupul este autorizat. Dacă nu este găsită nicio autorizare primară, atunci verificarea de autorizare trece în pasul 7. Dacă autorizarea grupului primar este insuficientă, atunci verificarea de autorizare trece în pasul 11
6. Grupul nu este grupul primar al obiectului deci sistemul caută 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. Nu este găsită nicio autorizare pentru autorizările private pentru profilul de grup deci sistemul verifică să vadă 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.
8. Obiectul este securizat de o listă de autorizare deci sistemul setează obiectul să fie verificat egal cu lista de autorizare şi verificarea autorizării se întoarce la pasul 3.
9. Utilizatorul aparţine altui profil de grup deci sistemul setează profilul la următorul profil de grup şi revine la pasul 1 şi începe procesul de verificare a autorizării din nou.
10. Autorizarea este găsită pentru autorizările private din profilul de grup deci autorizările private sunt verificate şi testate în profilul de grup. Dacă autorizările sunt suficiente, atunci profilul de grup este autorizat. Dacă nu este suficient, atunci verificarea autorizării trece la pasul 11.
11. Autorizarea nu este găsită sau este insuficientă deci sistemul verifică pentru a vedea dacă utilizatorul este asociat cu alt profil de grup. Dacă utilizatorul nu aparţine altui profil de grup, atunci sistemul trece la pasul 9. Dacă utilizatorul nu aparţine altui profil de grup, atunci sistemul revine la diagrama de flux de apelare cu autorizare insuficientă sau fără nicio autorizare găsită.

Diagrama de flux 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.

Diagrama de flux 7 arată procesul:

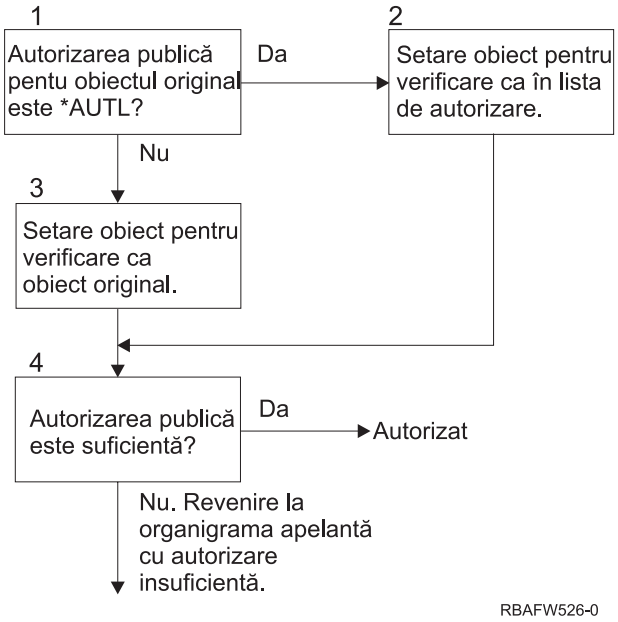


Figura 17. Diagrama de flux 7: Verificare autorizare publică

Descrierea diagramei de flux 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.

Diagrama de flux 8: Cum este verificată autorizarea adoptată

Dacă este găsită o autorizare insuficientă la verificarea autorizării utilizatorului, atunci sistemul verifică autorizarea adoptată.

Sistemul ar putea folosi autorizare adoptată de la programul original apelat de utilizator sau de la programe anterioare din stiva de apeluri. 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 18 la pagina 183 şi Figura 19 la pagina 185 arată procesul pentru verificarea autorizării adoptate.

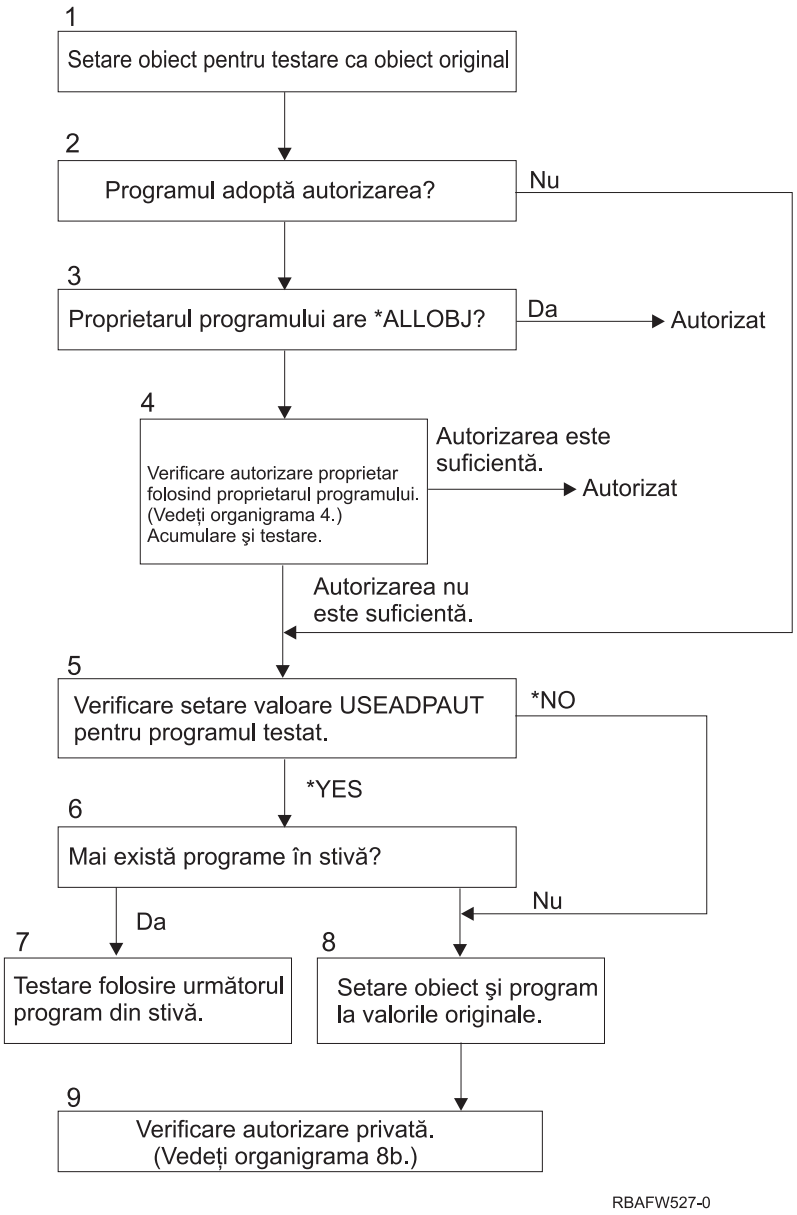


*Figura 18. Diagrama de flux 8A: Verificare autorizării adoptate utilizator *ALLOBJ şi proprietar*

Descrierea diagramei de flux 8A: Verificarea autorizării adoptate utilizator *ALLOBJ şi proprietar

Diagrama de flux 8A descrie cum verifică sistemul autorizarea adoptată când a fost găsită autorizare insuficientă verificând autorizarea utilizator.

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. Testaţi folosind următorul program din stivă şi porniţi de la pasul 2.
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 autorizare privată. Aceasta este descrisă în Diagrama de flux 8B: Verificarea autorizării adoptate folosind autorizări private.

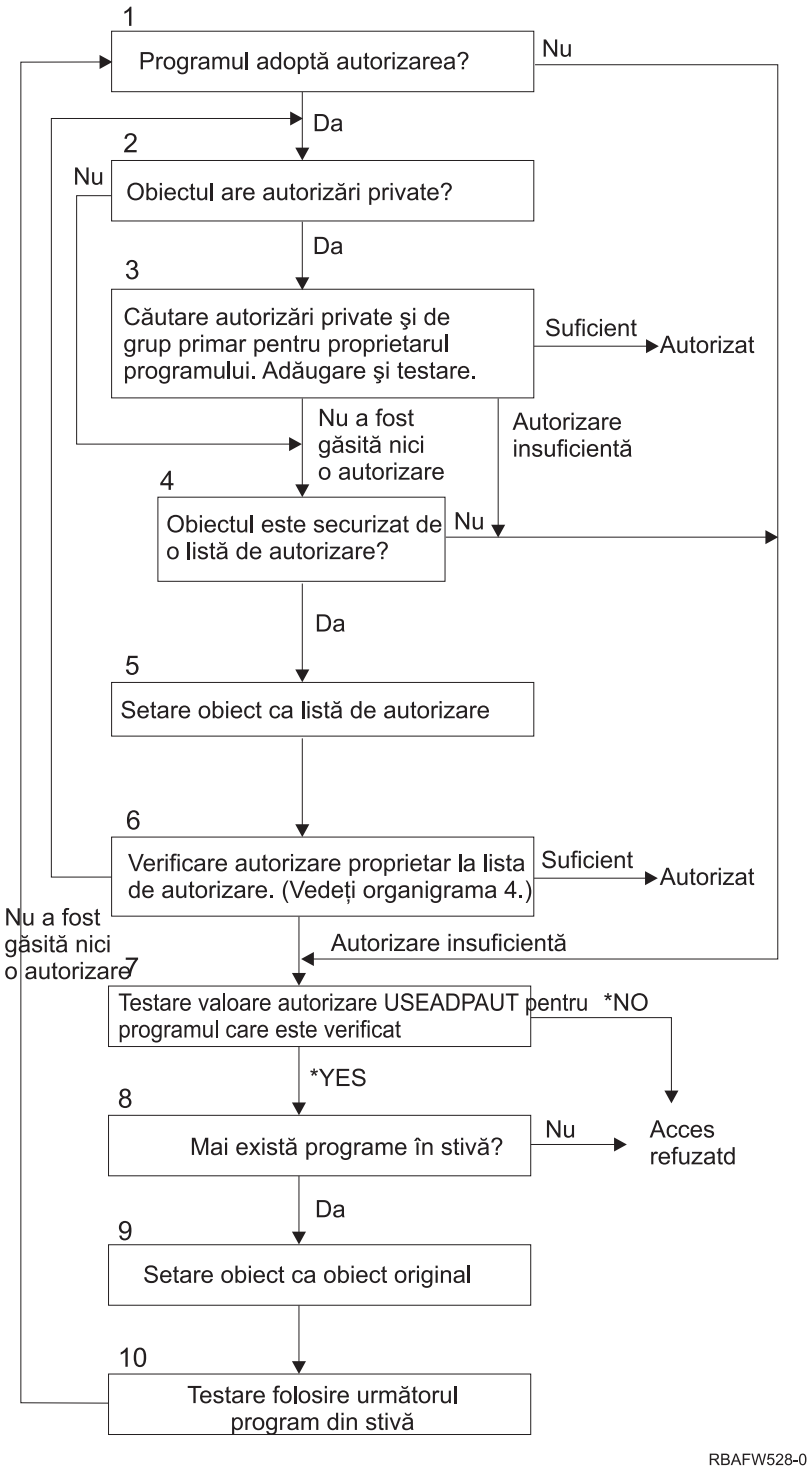


Figura 19. Diagrama de flux 8B: Verificarea autorizării adoptate folosind autorizări private

Descrierea diagramei de flux 8B: 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. Testaţi folosind următorul program din stivă şi începeţi de la pasul 1.

Concepte înrudite

"Ignorarea autorizării adoptate" la pagina 231
Tehnica folosirii autorizării adoptate în proiectarea meniurilor necesită ca utilizatorul să revină 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.

Exemple de verificare autorizare

Această secţiune include 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 20 arată autorizările pentru fişierul PRICES. După figură urmează mai multe exemple de acces cerut la acest fişier şi procesul de verificare a autorizării. În aceste exemple, căutarea de autorizări private (diagrama de flux 4, pasul 6) este evidenţiată deoarece aceasta este partea procesului de verificare a autorizării care poate cauza 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 20. Autorizarea pentru fişierul PRICES

Cazul 1: Folosirea autorizării private de grup

Acest caz vă arată cum să folosiţi autorizarea privată 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. Diagrama de flux 1, pasul 1.
   a. Diagrama de flux 2, pasul 1.
2. Diagrama de flux 1, pasul 2.
   a. Diagrama de flux 3, paşii 1 şi 2. Obiect de verificat = CONTRACTS/PRICES *FILE.
   b. Diagrama de flux 3, pasul 3.
      1) Diagrama de flux 4, pasul 1. Reveniţi la diagrama de flux 3 fără nicio autorizare găsită.ROSSM nu deţine fişierul PRICES.
   c. Diagrama de flux 3, pasul 4.
      1) Diagrama de flux 5, paşii 1, 2 şi 3. Public nu este suficient.
   d. Diagrama de flux 3, pasul 5.
   e. Diagrama de flux 3, pasul 6. ROSSM nu are autorizare privată asupra fişierului PRICES.
   f. Diagrama de flux 3, paşii 7 şi 8. Fişierul PRICES nu este securizat de o listă de autorizare. Reveniţi la diagrama de flux 1 fără nicio autorizare găsită.
3. Diagrama de flux 1, paşii 3 şi 4. DPTSM este profilul de grup pentru ROSSM.
   a. Diagrama de flux 6, paşii 1, 2 şi 3.
      1) Diagrama de flux 4, pasul 1. DPTSM nu posedă fişierul PRICES.
   b. Diagrama de flux 6, pasul 4. DPTSM nu este grupul primar pentru fişierul PRICES.
   c. Diagrama de flux 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 gestionarea 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

Acest caz demonstrează cum să folosiţi autorizarea 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 21 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 21. Autorizarea pentru fişierul CREDIT

Sistemul efectuează aceşti paşi pentru a determina dacă să îi permită lui ANDERSJ accesul *CHANGE la fişierul CREDIT:

1. Diagrama de flux 1, pasul 1.
   a. Diagrama de flux 2, pasul 1. Autorizarea lui DPTAR este autorizarea grupului primar, nu autorizarea privată.
   b. Diagrama de flux 2, paşii 2, 3, 4, 5 şi 6. Autorizarea publică nu este suficientă.
2. Diagrama de flux 1, pasul 2.
   a. Diagrama de flux 3, paşii 1 şi 2. Obiectul de verificat = ACCTSRCV/CREDIT *FILE.
   b. Diagrama de flux 3, pasul 3.
      1) Diagrama de flux 4, pasul 1. ANDERSJ nu posedă fişierul CREDIT. Reveniţi la diagrama de flux 3 fără nicio autorizare găsită.
   c. Diagrama de flux 3, pasul 4.
      1) Diagrama de flux 5, pasul 1. Fişierul CREDIT nu are autorizări private.
      2) Diagrama de flux 5, pasul 3. Autorizarea publică nu este suficientă. Reveniţi la diagrama de flux 3 fără nicio autorizare găsită.
   d. Diagrama de flux 3, paşii 5, 7 şi 8. Fişierul CREDIT nu este securizat de o listă de autorizare. Reveniţi la diagrama de flux 1 fără nicio autorizare găsită.
3. Diagrama de flux 1, paşii 3 şi 4. ANDERSJ este un membru al profilului de grup DPTAR.
   a. Diagrama de flux 6, paşii 1 şi 2. Obiectul de verificat = ACCTSRCV/CREDIT *FILE.
   b. Diagrama de flux 6, pasul 3.
      1) Diagrama de flux 4, pasul 1. DPTAR nu posedă fişierul CREDIT. Reveniţi la diagrama de flux 6 fără nicio autorizare găsită.
   c. Diagrama de flux 6, paşii 4 şi 5. 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.

Concepte înrudite

“Considerente pentru grupuri primare pentru obiecte” la pagina 239
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.

Cazul 3: Folosirea autorizării publice

Acest caz descrie paşii folosirii 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:

Diagrama de flux 1, pasul 1.

1. Diagrama de flux 2, pasul 1. Fişierul CREDIT nu are autorizări private. Autorizarea lui DPTAR este autorizarea grupului primar, nu autorizarea privată.
2. Diagrama de flux 2, paşii 2 şi 3. Autorizarea proprietarului (OWNAR) este suficientă.
3. Diagrama de flux 2, paşii 4 şi 5. Autorizarea grupului primar (DPTAR) este suficientă.
4. Diagrama de flux 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

Acest caz descrie cum să folosiţi autorizare publică fără a căuta autorizare privată.

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. Diagrama de flux 1, pasul 1.
   a. Diagrama de flux 2, pasul 1. Fişierul PRICES are autorizări private.
2. Diagrama de flux 1, pasul 2.
   a. Diagrama de flux 3, paşii 1 şi 2. Obiectul de verificat = CONTRACTS/PRICES *FILE.
   b. Diagrama de flux 3, pasul 3.
      1) Diagrama de flux 4, pasul 1. JONESP nu deţine fişierul PRICES. Reveniţi la diagrama de flux 3 fără nicio autorizare găsită.
   c. Diagrama de flux 3, pasul 4.
      1) Diagrama de flux 5, paşii 1, 2 şi 3. Autorizarea publică nu este suficientă.
      2) Diagrama de flux 5, pasul 4. Autorizarea proprietarului este suficientă. (OWNCP are *ALL.)
      3) Diagrama de flux 5, pasul 5. Fişierul PRICES nu are un grup primar.
      4) Diagrama de flux 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 securităţii adoptate

Acest caz demonstrează avantajul de performanţă la 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. Diagrama de flux 1, pasul 1.
   a. Diagrama de flux 2, pasul 1.
2. Diagrama de flux 1, pasul 2.
   a. Diagrama de flux 3, paşii 1 şi 2. Obiectul de verificat = CONTRACTS/PRICES *FILE.
   b. Diagrama de flux 3, pasul 3.
      1) Diagrama de flux 4, pasul 1. SMITHG nu deţine fişierul PRICES. Reveniţi la diagrama de flux 3 fără nicio autorizare găsită.
   c. Diagrama de flux 3, pasul 4.
      1) Diagrama de flux 5, paşii 1, 2 şi 3. Public nu este suficient.
   d. Diagrama de flux 3, pasul 5.
   e. **Diagrama de flux 3, pasul 6**. SMITHG nu are autorizare privată.
   f. Diagrama de flux 3, paşii 7 şi 8. Fişierul PRICES nu este securizat de o listă de autorizare. Reveniţi la diagrama de flux 1 fără nicio autorizare găsită.
3. Diagrama de flux 1, pasul 3. SMITHG nu are un grup.
4. Diagrama de flux 1, pasul 5.
   a. Diagrama de flux 7, pasul 1. Autorizarea publică nu este *AUTL.

b. Diagrama de flux 7, pasul 3. Obiectul de verificat = CONTRACTS/PRICES *FILE.
c. Diagrama de flux 7, pasul 4. Autorizarea publică nu este suficientă.

5. Diagrama de flux 1, pasul 6.
   a. Diagrama de flux 8A, pasul 1. Obiectul de verificat = CONTRACTS/PRICES *FILE.
   b. Diagrama de flux 8A, paşii 2 şi 3. OWNCP nu are autorizarea *ALLOBJ.
   c. Diagrama de flux 8A, pasul 4.
      1) Diagrama de flux 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 186.

- 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 utilizatorului şi grupului

Acest caz demonstrează că unui utilizator îi poate fi refuzat accesul la un obiect chiar dacă grupul utilizatorului are autorizare suficientă.

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. Diagrama de flux 1, pasul 1.
   a. Diagrama de flux 2, pasul 1. PRICES are autorizări private.
2. Diagrama de flux 1, pasul 2.
   a. Diagrama de flux 3, paşii 1 şi 2. Obiectul de verificat = CONTRACTS/PRICES *FILE.
   b. Diagrama de flux 3, pasul 3.
      1) Diagrama de flux 4, pasul 1. WILSONJ nu deţine fişierul PRICES. Reveniţi la diagrama de flux 3 fără nicio autorizare găsită.
   c. Diagrama de flux 3, pasul 4.
      1) Diagrama de flux 5, paşii 1, 2 şi 3. Public nu este suficient.
   d. Diagrama de flux 3, pasul 5.
   e. **Diagrama de flux 3, pasul 6**. WILSONJ are autorizarea *USE, care nu este suficientă.
   f. Diagrama de flux 3, pasul 8. Obiectul de testat = CONTRACTS/PRICES *FILE. Reveniţi la diagrama de flux 1 cu autorizare insuficientă.
3. Diagrama de flux 1, pasul 6.
   a. Diagrama de flux 8A, pasul 1. Obiect de verificat = CONTRACTS/PRICES *FILE.
   b. Diagrama de flux 8A, pasul 2. Programul CPPGM01 nu adoptă autorizare.

c. Diagrama de flux 8A, pasul 5. Parametrul *USEADPAUT pentru programul CPPGM01 este *NO.
d. Diagrama de flux 8A, paşii 8 şi 9.
   1) Diagrama de flux 8B, pasul 1. Programul CPPGM01 nu adoptă autorizare.
   2) Diagrama de flux 8B, pasul 7. Parametrul *USEADPAUT pentru programul CPPGM01 este *NO. Accesul este interzis.

Analiză:

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

Acest caz demonstrează avantajul de performanţă la folosirea autorizării publice 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 22. Afişarea autorizării obiectului

ROSSM are nevoie de autorizarea *USE pentru fişierul ITEM. ROSSM este membru al profilului de grup DPTSM. Aceştia sunt paşii verificării autorizării:

Diagrama de flux 1, pasul 1.

1. Diagrama de flux 2, paşii 1, 2 şi 3. Autorizarea lui OWNIC este suficientă.
2. Diagrama de flux 2, pasul 4. Fişierul ITEM nu are un grup primar.
3. Diagrama de flux 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: Autorizare adoptată fără autorizare privată

Acest caz vă arată avantajul folosirii autorizării adoptate 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. Diagrama de flux 1, pasul 1.

a. Diagrama de flux 2, paşii 1, 2, 3, 4 şi 6. Autorizarea publică nu este suficientă.

2. Diagrama de flux 1, pasul 2.
   a. Diagrama de flux 3, paşii 1 şi 2. Obiectul de verificat = ITEMLIB/ITEM *FILE.
   b. Diagrama de flux 3, pasul 3.
      1) Diagrama de flux 4, pasul 1. WILSONJ nu deţine fişierul ITEM. Reveniţi la diagrama de flux 3 fără nicio autorizare găsită.
   c. Diagrama de flux 3, pasul 4.
      1) Diagrama de flux 5, paşii 1 şi 3. Autorizarea publică nu este suficientă. Reveniţi la diagrama de flux 3 fără nicio autorizare găsită.
   d. Diagrama de flux 3, paşii 5, 7 şi 8. Fişierul ITEM nu este securizat de o listă de autentificare. Reveniţi la diagrama de flux 1 fără nicio autorizare găsită.
3. Diagrama de flux 1, paşii 3 şi 5. (WILSONJ nu are un profil de grup.)
   a. Diagrama de flux 7, paşii 1, 3 şi 4. Publicul are autorizarea *USE, care nu este suficientă.
4. Diagrama de flux 1, pasul 6.
   a. Diagrama de flux 8A, pasul 1. Obiectul de verificat = ITEMLIB/ITEM *FILE.
   b. Diagrama de flux 8A, paşii 2, 3 şi 4. Profilul OWNIC nu are autorizarea *ALLOBJ.
      1) Diagrama de flux 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

Acest caz demonstrează avantajul folosirii listelor de autorizare.

Fişierul ARWKR01 din biblioteca CUSTLIB este securizat de lista de autorizare ARLST1. Figura 23 şi Figura 24 la pagina 193 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 23. 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 24. 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. Diagrama de flux 1, pasul 1.
   a. Diagrama de flux 2, paşii 1 şi 2. Fişierul ARWRK01 este securizat de o listă de autorizare.
2. Diagrama de flux 1, pasul 2.
   a. Diagrama de flux 3, paşii 1 şi 2. Obiectul de verificat = CUSTLIB/ARWRK01 *FILE.
   b. Diagrama de flux 3, pasul 3.
      1) Diagrama de flux 4, pasul 1. AMESJ nu posedă fişierul ARWRK01. Reveniţi la diagrama de flux 2 fără nicio autorizare găsită.
   c. Diagrama de flux 3, pasul 4.
      1) Diagrama de flux 5, paşii 1 şi 3. Autorizarea publică nu este suficientă. Reveniţi la diagrama de flux 3 fără nicio autorizare găsită.
   d. Diagrama de flux 3, paşii 5, 7 şi 9. Obiect de verificat = ARLST1 *AUTL.
   e. Diagrama de flux 3, pasul 3.
      1) Diagrama de flux 4, pasul 1. AMESJ nu deţine lista de autorizare ARLST1. Reveniţi la diagrama de flux 3 fără nicio autorizare găsită.
   f. Diagrama de flux 3, paşii 4 şi 5.
   g. Diagrama de flux 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 194.

Cazul 10: Folosirea mai multor grupuri

Acesta este un exemplu de folosire a 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 25 la pagina 194 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 25. Autorizarea pentru fişierul CRLIM

Aceştia sunt paşii verificării autorizării:

1. Diagrama de flux 1, pasul 1.
   a. Diagrama de flux 2, pasul 1. Revenire la diagrama de flux apelantă cu autorizare insuficientă.
2. Diagrama de flux 1, pasul 2.
   a. Diagrama de flux 3, paşii 1 şi 2. Obiectul de verificat = CUSTLIB/CRLIM *FILE.
   b. Diagrama de flux 3, pasul 3.
      1) Diagrama de flux 4, pasul 1. WOODBC nu deţine fişierul CRLIM. Reveniţi la diagrama de flux 3 fără nicio autorizare găsită.
   c. Diagrama de flux 3, pasul 4.
      1) Diagrama de flux 5, paşii 1, 2 şi 3. Autorizarea publică nu este suficientă.
   d. Diagrama de flux 3, pasul 5.
   e. Diagrama de flux 3, pasul 6. WOODBC nu are nici o autorizare pentru fişierul CRLIM.
   f. Diagrama de flux 3, paşii 7 şi 8. Fişierul CRLIM nu este securizat de o listă de autorizare. Reveniţi la diagrama de flux 1 fără nicio autorizare găsită.
3. Diagrama de flux 1, paşii 3 şi 4. Primul grup pentru WOODBC este DPTAR.
   a. Diagrama de flux 6, paşii 1 şi 2. Obiect de verificat = CUSTLIB/CRLIM *FILE.
   b. Diagrama de flux 6, pasul 3.
      1) Diagrama de flux 4, pasul 1. DPTAR nu deţine fişierul CRLIM. Reveniţi la diagrama de flux 6 fără nicio autorizare găsită.
   c. Diagrama de flux 6, paşii 4 şi 5. Autorizat. DPTAR este grupul primar şi are autorizare suficientă.

Cazul 11: Combinarea metodelor de autorizare

Acest caz arată o proiectare slabă 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 26 la pagina 195 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 26. Autorizarea pentru fişierul CRLIMWRK

Fişierul CRLIMWRK este securizat de lista de autorizare CRLST1. Figura 27 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 27. Autorizarea pentru lista de autorizare CRLST1

Acest exemplu arată multe dintre posibilităţile 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. Diagrama de flux 1, pasul 1.
   a. Diagrama de flux 2, pasul 1.
2. Diagrama de flux 1, pasul 2.
   a. Diagrama de flux 3, paşii 1 şi 2. Obiect de verificat = CUSTLIB/CRLIMWRK *FILE.
   b. Diagrama de flux 3, pasul 3.
      1) Diagrama de flux 4, pasul 1. WAGNERB nu deţine fişierul CRLIMWRK. Reveniţi la diagrama de flux 3 fără nicio autorizare găsită.
   c. Diagrama de flux 3, pasul 4.
      1) Diagrama de flux 5, paşii 1 şi 2. WILSONJ are autorizarea *EXCLUDE, care este mai mică decât autorizarea publică *USE.
   d. Diagrama de flux 3, paşii 5 şi 6 (**prima căutare de autorizări private**). WAGNERB nu are autorizare privată.
   e. Diagrama de flux 3, paşii 7 şi 9. Obiect de verificat = CRLST1 *AUTL.
   f. Diagrama de flux 3, pasul 3.
      1) Diagrama de flux 4, pasul 1. WILSONJ nu deţine CRLST1. Reveniţi la diagrama de flux 3 fără nicio autorizare găsită.
   g. Diagrama de flux 3, paşii 4 şi 5.
   h. Diagrama de flux 3, pasul 6 (**a doua căutare de autorizări private**). WAGNERB nu are autorizare privată pentru CRLST1.
   i. Diagrama de flux 3, paşii 7 şi 8. Obiect de verificat = CUSTLIB/CRLIMWRK *FILE.

3. Diagrama de flux 1, paşii 3 şi 4. Primul profil de grup al lui WAGNERB este DPTSM.
   a. Diagrama de flux 6, paşii 1 şi 2. Obiect de verificat = CUSTLIB/CRLIMWRK *FILE.
   b. Diagrama de flux 6, pasul 3.
      1) Diagrama de flux 4, pasul 1. DPTSM nu deţine fişierul CRLIMWRK. Reveniţi la diagrama de flux 6 fără nicio autorizare găsită.
   c. Diagrama de flux 6, pasul 4. DPTSM nu este grupul primar pentru fişierul CRLIMWRK.
   d. Diagrama de flux 6, pasul 6 (**a treia căutare de autorizări private**). DPTSM are autorizarea *USE pentru fişierul CRLIMWRK, care nu este suficientă.
   e. Diagrama de flux 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. Diagrama de flux 6, paşii 9 şi 10. Următorul grup al lui WAGNERB este DPT702.
   g. Diagrama de flux 6, paşii 1 şi 2. Obiect de verificat = CUSTLIB/CRLIMWRK *FILE.
   h. Diagrama de flux 6, pasul 3.
      1) Diagrama de flux 4, pasul 1. DPT702 nu deţine fişierul CRLIMWRK. Reveniţi la diagrama de flux 6 fără nicio autorizare găsită.
   i. Diagrama de flux 6, pasul 4. DPT702 nu este grupul primar pentru fişierul CRLIMWRK.
   j. Diagrama de flux 6, pasul 6 (**a patra căutare de autorizări private**). DPT702 nu are autorizare pentru fişierul CRLIMWRK.
   k. Diagrama de flux 6, paşii 7 şi 8. Obiect de verificat = CRLST1 *AUTL.
   l. Diagrama de flux 6, pasul 3.
      1) Diagrama de flux 5, pasul 1. DPT702 nu deţine lista de autorizare CRLST1. Reveniţi la diagrama de flux 6 fără nicio autorizare găsită.
   m. Diagrama de flux 6, paşii 4 şi 6 (**a cincea căutare de autorizări private**). DPT702 nu are autorizare pentru lista de autorizare CRLST1.
   n. Diagrama de flux 6, paşii 7, 9 şi 10. DPTAR este următorul profil de grup al lui WAGNERB.
   o. Diagrama de flux 6, paşii 1 şi 2. Obiect de verificat = CUSTLIB/CRLIMWRK *FILE.
   p. Diagrama de flux 6, pasul 3.
      1) Diagrama de flux 4, pasul 1. DPTAR nu deţine fişierul CRLIMWRK. Reveniţi la diagrama de flux 6 fără nicio autorizare găsită.
   q. Diagrama de flux 6, paşii 4 şi 6 (**a şasea căutare de autorizări private**). DPTAR nu are autorizare pentru fişierul CRLIMWRK.
   r. Diagrama de flux 6, paşii 7 şi 8. Obiect de verificat = CRLST1 *AUTL.
   s. Diagrama de flux 6, pasul 3.
      1) Diagrama de flux 4, pasul 1. DPTAR nu deţine lista de autorizare CRLST1. Reveniţi la diagrama de flux 6 fără nicio autorizare găsită.
   t. Diagrama de flux 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 autorizare

Sistemul creează cache-uri de autorizare pentru utilizatori, îmbunătăţind flexibilitatea şi performanţa.

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 de utilizator. 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. Securitatea controlului funcţionării

Această secţiune discută problemele de securitate asociate cu controlul funcţionării sistemului.

În această secţiune sunt tratate următoarele probleme.

Informaţii înrudite

Controlul funcţionării

Iniţierea jobului

Sistemul verifică autorizarea unor obiecte când este pornit un 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 asupra unora din aceste obiecte este verificată înainte ca jobului să îi fie permis să pornească, în timp ce autorizarea asupra altor obiecte este verificată după pornirea jobului. Autorizarea necorespunzătoare poate cauza erori sau oprirea jobului.

Obiectele care sunt parte a structurii jobului pot fi specificate în descrierea de job, profilul de utilizator şi în comanda SBMJOB (Submit Job - Lansare job) pentru un job batch.

Pornirea unui job interactiv

Acest subiect este o descriere a activităţii de securitate 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 de 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 de utilizator şi parola. Starea profilului de utilizator trebuie să fie *ENABLED. Profilul de 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 201 pentru detalii.
3. Sistemul verifică autorizarea pentru valorile din profilul de utilizator şi din descrierea de job utilizator care sunt folosite pentru a construi structura jobului, cum este:
   - Descriere 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 autorizării este făcută pentru programul procesor QCMD, biblioteca de program şi orice obiecte folosite, după cum este descris în 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 de 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 de 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

Acest subiect include 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 de utilizator în comanda SBMJOB, trebuie să aveţi autorizarea *USE pentru profilul de utilizator.
2. Autorizarea este verificată pentru obiectele specificate ca parametrii în comanda SBMJOB şi în descrierea de job. Autorizarea este verificată pentru profilul de utilizator sub care rulează jobul.
3. Dacă nivelul de securitate este 40 sau 50 şi comanda SBMJOB specifică USER(*JOBD), utilizatorul care lansează jobul trebuie să aibă autorizare *USE asupra profilul de utilizator din descrierea jobului.
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.

Autorizare adoptată şi joburi batch

Puteţi modifica parametrii pentru un job batch când rulează sub autorizare adoptată.

Când este pornit un job nou, este creată o nouă stivă de apeluri pentru job. Autorizarea adoptată nu poate avea efect până când primul program nu este adăugat la stiva de apeluri. 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 să modificaţi caracteristicile unui job batch când aşteaptă să ruleze, folosind comanda Modificare job (CHGJOB). Vedeţi Comenzijob pentru autorizarea care este necesară pentru a modifica paramerii pentru un job.

Staţii de lucru

Sistemul realizează verificarea autorizării pentru o staţie de lucru când vă logaţi.

O *descriere de dispozitiv* conţine informaţii despre un dispozitiv particular sau o unitate logică 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 28 la pagina 202 arată logica pentru a determina dacă unui utilizator îi este permis să se semneze la un dispozitiv:

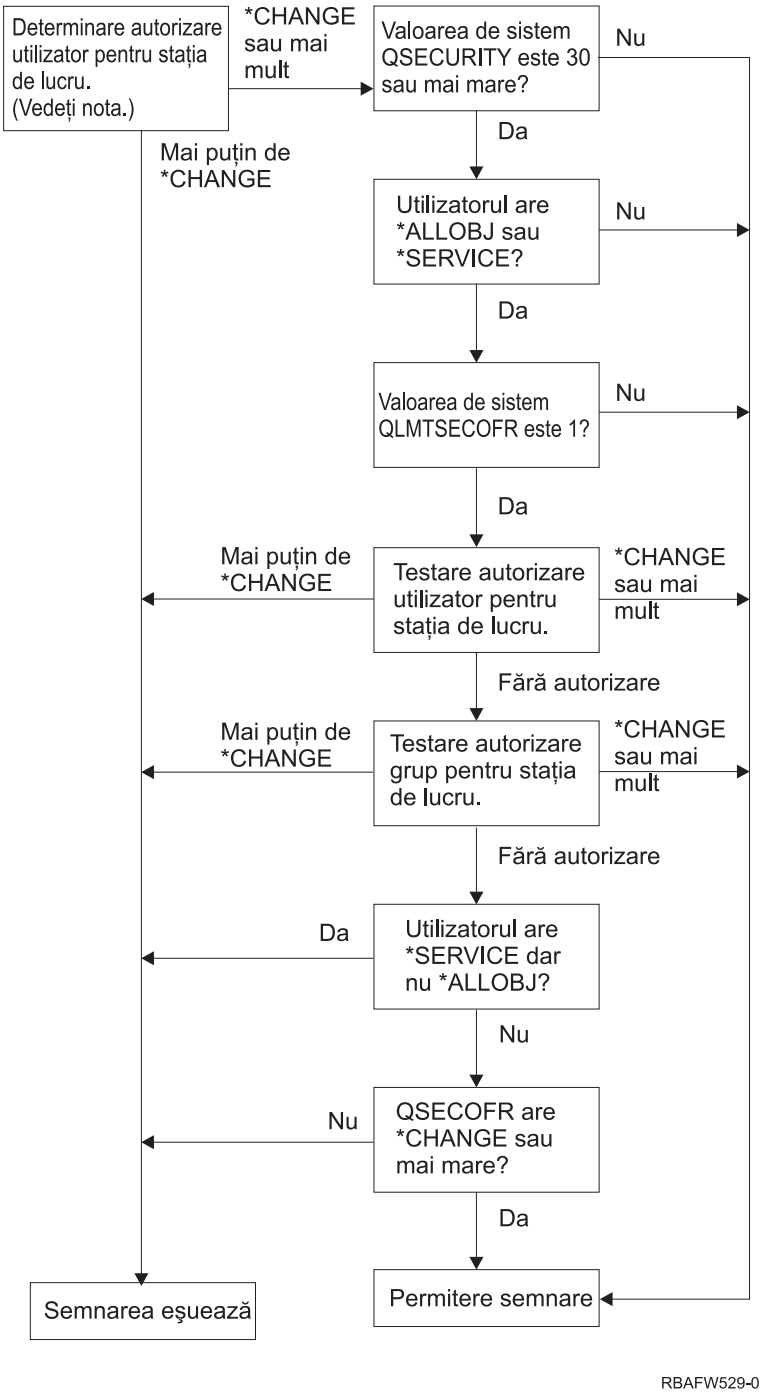


Figura 28. Verificarea autorizării pentru staţii de lucru

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 de utilizator, profilul de grup sau profilurile de grup suplimentare.
- Autorizarea privată pentru descrierea de dispozitiv din profilul de utilizator, profilul de grup sau profilurile de grup suplimentare.
- Autorizarea pentru o listă de autorizări folosită pentru a securiza descrierea de dispozitiv.
- Autorizarea pentru o listă de autorizări folosită pentru a securiza autorizarea publică.

Verificarea autorizării pentru descrierea de dispozitiv este făcută înainte de orice programe să fie în stiva de apeluri pentru job; de aceea, autorizarea adoptată nu se aplică.

Descrierea verificării autorizării pentru staţii 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 grupul utilizatorului nu are nicio autorizare asuora staţiei de lucru, sistemul verifică dacă utilizatorul are autorizare specială *SERVICE dar nu *ALLOBJ.

Dacă utilizatorul are autorizarea specială *SERVICE, dar nu are autorizarea specială *ALLOBJ atunci semnarea eşuează. Dacă utilizatorul are autorizare specială *ALLOBJ, atunci sistemul verifică dacă QSECOFR are *CHANGE sau mai mare.

Dacă QSECOFR nu are *CHANGE sau mai înaltă, semnarea eşuează. Dacă QSECOFR are *CHANGE sau mai înaltă, atunci semnarea este permisă.

Profilurilor de 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.

Dreptul de proprietate al descrierilor de dispozitiv

Puteţi specifica dreptul de proprietate al descrierilor de dispozitiv pentru a controla autorizarea asupra dispozitivelor.

Autorizarea publică implicită pentru comenzile CRTDEVxxx este *CHANGE. Dispozitivele sunt create în biblioteca QSYS, care este livrată cu o valoare CRTAUT a *SYSVAL. Valoarea 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 comanda 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 al ecranului de semnare

Administratorul de sistem poate modifica ecranul de semnare sistem pentru a adăuga text sau logo-ul companiei.

La modificarea fişierului de afişare al ecranului de semnare, administratorul sistemului trebuie să se asigure că nu modifică numele de câmpuri sau lungimea buffer-elor fişierului de afişare la adăugarea textului în fişier. Modificarea numelor câmpului sau a lungimilor buffer-ului poate cauza eşecul semnării.

Modificarea ecranului de semnare

Puteţi modifica codul sursă pentru ca fişierul de afişare la semnare să modifice ecranul.

Codul sursă pentru fişierul de afişare la 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 de buffer trebuie să rămână nemodificate.

Sursa fişierului de afişare pentru ecranul de semnare

Trebuie să copiaţi fişierul sursă corespunzător pentru a vă crea propriul ecran de semnare.

Sursa fişierului de afişare pentru 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 i5/OS 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 dumneavoastră sursă şi să faceţi modificări în copia din fişierul dumneavoastră sursă.

Modificarea fişierului de afişare pentru semnare

Acest subiect include paşii pentru modificarea fişierului de afişare pentru semnare.

Pentru a modifica formatul ecranului Semnare, realizaţi următorii paşi:

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 să modificaţi câmpul UBUFFER pentru a conţine atâtea câmpuri mai mici câte aveţi nevoie, dacă sunt îndeplinite următoarele cerinţe:

   - Noile câmpuri trebuie să urmeze toate celelalte câmpuri din fişierul de afişare. Locaţia câmpurilor pe ecran nu contează atât timp cât ordinea în care sunt puse în specificaţiile de descriere a datelor (DDS) întruneşte această cerinţă.
   - Lungimea trebuie să fie în total 128. Dacă lungimea câmpurilor este mai mare de 128, unele din date nu vor fi pasate aplicaţiei.
   - 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 subsistemului, realizaţi următorii paşi:
   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.

Observaţii:

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

Descrierile de subsisteme realizează mai multe funcţii în sistem.

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.

Concepte înrudite

“Semnarea fără ID şi parolă de utilizator” la pagina 16
Nivelul de securitate determină cum controlează sistemul semnarea fără ID şi parolă de utilizator.

Controlarea modului de intrare a joburilor în sistem

Puteţi folosi descrierile de subsisteme pentru a controla cum intră în sistemul joburile.

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 de 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. Consultaţi “Semnarea fără ID şi parolă de utilizator” la pagina 16 pentru mai multe informaţii.

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 indică spre un profil de 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. “Atribute reţea” la pagina 214 discutaţi atributele de reţea care sunt importante pentru securitate.

Descrierile 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 ieşire 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 modului de intrare a joburilor în sistem” la pagina 205 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 de 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 de 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("Call 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 de utilizator.

Uneori, un nume de profil de 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 de utilizator programator (QPGMR), indiferent dacă utilizatorul are sau nu autorizarea pentru profilul de utilizator QPGMR. La nivelul de securitate 40 sau mai înalt, autorizarea *USE pentru profilul QPGMR este de asemenea necesară.

Coada de mesaje pentru operatorul de sistem

Puteţi specifica autorizările pentru a controla accesul la coada de mesaje pentru operatorul de sistem

Meniul i5/OS 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 şi *ADD pentru coada de mesaje. Înlăturarea mesajelor necesită autorizările *USE şi *DLT (consultaţi Comenzile pentru mesaje.) 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 joburile au nevoie de abilitatea de a adăuga mesaje noi la coada de mesaje QSYSOPR. Nu faceţi autorizarea publică pentru QSYSOPR *EXCLUDE.

Listele de biblioteci

Lista de biblioteci pentru un job indică bibliotecile în care se caută 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 123 rezumă părţile 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 123. Părţile componente ale listei de biblioteci. Lista de biblioteci este căutată în această ordine:

Parte	Cum este construit
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.
Bibliotecă curentă - 1 intrare	Specificată în profilul de 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.

Concepte înrudite

“Securitatea bibliotecilor şi liste de biblioteci” la pagina 136
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.

“Planificarea bibliotecilor” la pagina 224
O bibliotecă este ca un director folosit pentru a localiza obiectele din ea. Mulţi factori afectează modul în care alegeţi să grupaţi informaţiile aplicaţiilor dumneavoastră în biblioteci şi să le gestionaţi.

Riscuri de securitate ale listelor de biblioteci

Acest subiect oferă exemple specifice ale expunerilor posibile de securitate ale listelor de bibliotecişi cum să le evitaţi.

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 bibliotecilor şi liste de biblioteci” la pagina 136 furnizează unele informaţii generale despre problemele asociate cu listele de biblioteci.

Această secţiune furnizează două exemple despre cum modificările asupra unei liste de biblioteci ar putea încălca cerinţele de securitate.

Modificarea funcţionării

Acest exemplu arată riscul posibil de modificare a funcţionării la apelarea unui program din bibliotecă.

Figura 29 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, căutându-se în lista de biblioteci până când este găsit programul B.

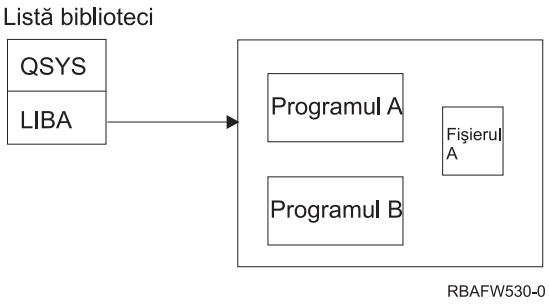


Figura 29. Mediul aşteptat al listei de biblioteci

Un programator sau alt utilizator cu cunoştinţe de specialitate poate pune alt Program B în biblioteca LIBB. Programul înlocuit poate realiza funcţii diferite, cum ar fi copierea informaţiilor confidenţiale sau actualizarea incorectă a fişierelor. Dacă LIBB este plasată înainte de LIBA în lista de biblioteci, este rulat Programul B înlocuitor în locul Programului B original, deoarece programul este apelat fără un nume calificat:

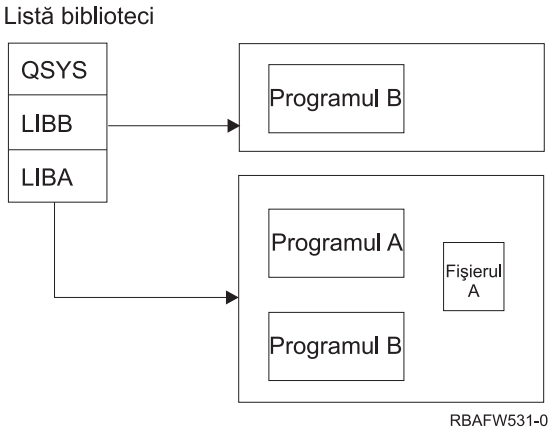


Figura 30. Mediul real al listei de biblioteci

Accesul neautorizat la informaţii

Exemplul demonstrează riscul de acces neautorizat la informaţiile din bibliotecă.

Să presupunem că programul A din Figura 29 la pagina 208 adoptă autorizarea lui USER1, care are autorizare *ALL asupra fişierului A. Să presupunem că programul B este apelat de programul A (autrizarea adoptată rămâne efectivă). Un utilizator cu cunoştinţele necesare poate crea un program de înlocuire B care apelează procesorul de comenzi. Utilizatorul va avea o linie de comandă şi acces total la Fişierul A.

Recomandări pentru porţiunea de sistem a listei de biblioteci

Acest subiect furnizează recomandările 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 sistem 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 a sistemului” la pagina 226.

Recomandări pentru bibliotecă produs

În acest subiect veţi găsi recomandările pentru protejarea bibliotecii produsului.

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 - Creare comandă), CHGCMD (Change Command - Modificare comandă), CRTMNU (Create Menu - Creare meniu) şi CHGMNU (Change Menu - Modificare meniu).
- Când creaţi comenzi şi meniuri, specificaţi PRDLIB(*NONE), ceea ce 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 dumneavoastră 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

Acest subiect furnizează recomandări pentru a asigura securitatea sistemului la folosirea bibliotecii curente.

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 biblioteci. 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 de 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 - Creare meniu), CHGMNU (Change Menu - Modificare meniu), CRTCMD (Create Command - Creare comandă) şi CHGCMD (Change Command - Modificare comandă).
- Folosiţi tehnica descrisă în “Controlarea listei de biblioteci utilizator” la pagina 225 pentru a seta biblioteca curentă în timpul procesării aplicaţiei.

Recomandări pentru porţiunea utilizator a listei de biblioteci

În acest subiect veţi găsi recomandările pentru controlarea porţiunii 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 de utilizator la *YES pentru a restricţiona abilitatea lor de a introduce comenzi. “Planificarea meniurilor” la pagina 227 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 Adăugare intrare în lista de biblioteci (ADDLIBLE) la începutul programului pentru a vă asigura că obiectele necesare sunt la începutul poţiunii 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 necesară aplicaţiei. Când se termină aplicaţia, întoarceţi lista de biblioteci la setarea originală. Vedeţi “Controlarea listei de biblioteci utilizator” la pagina 225 pentru un exemplu al acestei tehnici.

Tipărirea

Puteţi controla securitatea cozilor de ieşire din sistem.

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 de 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. Subiectul Prezentare avansată funcţie furnizează exemple despre cum să direcţionaţi ieşirea într-o anumită coadă de ieşire.

Securizarea fişierelor spooled

Puteţi specifica mai mulţi parametrii pentru a controla securitatea unui fişier spooled.

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 - Gestionare descriere coadă de ieşire).

Atenţie: Un utilizator cu autorizare specială *SPLCTL poate realiza toate funcţiile asupra tuturor intrărilor, indiferent de 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

Puteţi specifica parametrul Afişare date (DSPDTA) pentru a proteja conţinutul unui fişier spooled.

Parametrul DSPDTA determină ce autorizare este necesară pentru a realiza următoarele funcţii asupra fişierelor spooled posedate 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 de verificare (AUTCHK) al cozii de ieşire

Puteţi folosi parametrul Autorizare de verificat (AUTCHK) pentru a controla autorizarea unui utilizator pentru a modifica sau şterge un fişier spooled din sistem.

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 Control operator (OPRCTL) determină dacă un utilizator cu autorizare 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 autorizări de parametrii necesari pentru tipărire

Acest subiect include informaţiile de referinţă despre parametrii cozii de ieşire şi autorizările necesare pentru realiza funcţiilor de gestionare tipărire.

Tabela 124 la pagina 213 arată ce combinaţie între parametrii cozii de ieşire şi autorizarea pentru coada de ieşire este necesară pentru a realiza funcţiile de gestionare 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 consultaţi “Comenzi scriitor” la pagina 493.

Autorizarea şi parametrii cozii de ieşire pentru toate comenzile asociate cu fişiere spool sunt listate pe “Comenzi fişier spooled” la pagina 478. Comenzile cozii de ieşire sunt listate pe “Comenzi coadă ieşire” la pagina 451.

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 124. Autorizarea necesară pentru a realiza funcţii de tipărire

Funcţie tipărire	Parametri coadă ieşire			Autorizare coadă de ieşire	Autorizare specială
	DSPDTA	AUTCHK	OPRCTL		
Adăugare fişiere spool în coadă [1]				*READ	Fără
			*YES		*JOBCTL
Vizualizaţi lista de fişiere spool (comanda WRKOUTQ [2])				*READ	Fără
			*YES		*JOBCTL
Afişare, copiere sau trimitere fişiere spool (DSPSPLF, CPYSPLF, SNDNETSPLF, SNDTCPSP[2])	*YES			*READ	Fără
	*NO	*DTAAUT		*READ, *ADD, *DLT	Fără
	*NO	*OWNER		Proprietar [3]	Fără
	*YES		*YES		*JOBCTL
	*NO		*YES		*JOBCTL
	*OWNER				
Modificare, ştergere, reţinere şi eliberare fişier spool (CHGSPLFA, DLTSPLF, HLDSPLF, RLSSPLF [2])		*DTAAUT		*READ, *ADD, *DLT	Fără
		*OWNER		Proprietar [3]	Fără
			*YES		*JOBCTL
Modificare, curăţare, reţinere şi eliberare coadă de ieşire (CHGOUTQ, CLROUTQ, HLDOUTQ, RLSOUTQ [2])		*DTAAUT		*READ, *ADD, *DLT	Fără
		*OWNER		Proprietar [3]	Fără
			*YES		*JOBCTL
Pornire scriitor pentru coadă ieşire (STRPRTWTR, STRRMTWTR [2])		*DTAAUT		*CHANGE	Fără
			*YES		*JOBCTL

[1] Aceasta este autorizarea necesară pentru a direcţiona ieşirea dumneavoastră spre o coadă de ieşire.

[2] Folosind aceste comenzi sau opţiunile echivalente dintr-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: Coadă de ieşire

Aceste exemple demonstrează cum să setaţi parametrii de securitate pentru cozi de ieşire pentru a îndeplini diverse cerinţe.

- 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 fişiere 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)
```

Atribute 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)
- Acces cerere client (PCSACC)
- Acess cerere DDM (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).

Atribut 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.

Informaţii înrudite

SNA Distribution Services

Atributul de reţea Acces cerere client (PCSACC)

Atributul de reţea PCSACC determină cum programul licenţiatSystem i Access pentru Windows procesează cereri de la calculatoare personale ataşate pentru obiecte accesate.

Atributul de reţea PCSACC controlează dacă joburile calculatorului personal pot accesa obiecte de pe platforma System i, dar nu controlează dacă PC-ul poate folosi emularea de staţie de lucru.

Notă: Atributul de reţea PCSACC controlează doar clienţii DOS şi OS/2. Acest atribut nu are efect asupra altor clienţi System i Access.

Valorile posibile pentru PCSACC:	
***REJECT**	System i Access refuză fiecare cerere de la calculatorul personal pentru a accesa obiecte de pe platforma System i. Un mesaj de eroare este trimis aplicaţiei PC.
***OBJAUT**	Programele System i Access de pe sistem verifică autorizările normale pentru orice 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 System i Access apelează acest program de ieşire scris de utilizator pentru a determina dacă cererea PC ar trebui refuzată. Programul de ieşire este apelat doar dacă verificarea de autorizare normală pentru obiect are succes. Programul System i Access transmite informaţii despre utilizator şi funcţia cerută programului de ieşire. Programul întoarce un cod care indică dacă cererea trebuie permisă sau refuzată. În cazul în care codul retur indică faptul că cererea trebuie refuzată sau dacă apare o eroare, este trimis un mesaj de eroare calculatorului personal.

Riscuri şi recomandări

Folosiţi instrucţiunile din acest subiect pentru a proteja fişierele din sistem.

Măsurile normale de securitate din sistem se poate să nu fie protecţii suficiente dacă programul System i Access este instalat în sistem. De exemplu, dacă un utilizator are autorizare *USE asupra un fişier şi atributul de reţea PCSACC este *OBJAUT, utilizatorul poate folosi programul System i Access şi un program de pe calculatorul personal pentru a transfra fişierul întreg pe calculatorul personal. Utilizatorul poate copia datele pe o dischetă sau o bandă PC şi le poate înlătura din punctul de plecare.

Mai multe metode sunt disponibile pentru a împiedica un utilizator System i cu autorizare *USE asupra unui fişier să copieze fişierul:

- Setare LMTCPB(*YES) în profilul de utilizator.
- Restricţionaţi autorizarea pentru comenzile care copiază fişiere.
- Restricţionarea autorizării asupra comenzilor folosite de System i 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.

Niciuna din aceste metode nu funcţionează pentru utilizator PC al programului licenţiat System i Access. Folosirea unui program de ieşire pentru a verifica toate cererile este singura măsură de protecţie adecvată.

Programul System i Access transmite informaţii pentru următoarele tipuri de acces asupra programului de ieşire utilizator apelate de atributul de reţea PCSACC:

- Transfer fişier
- Tipărire virtuală

- Mesaj
- Folder partajat

Informaţii înrudite

Programare: iSeries Access

Atribut de reţea Acces cerere DDM (DDMACC)

Atributul de reţea Acces cerere DDM (DDMACC) determină cum sistemul procesează cereri de la alte sisteme pentru a accesa date folosind 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.

Informaţii înrudite

Cosiderente parametru DDMACC

Operaţii 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 programare, 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 restricţiona operaţiile de salvare şi restaurare pentru a vă proteja sistemul.

Puteţi controla abilitatea de a salva şi restaura obiecte în mai multe căi:

- Restricţionaţi accesele fizice la dispozitivele de salvare şi restaurare, cum ar fi unităţile de bandă şi unităţile optice.
- 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 dumneavoastră şi restaurat în sistemul dumneavoastră prin toate interfeţele - prin includerea fişierelor de salvare. Vedeţi “Exemplu: Restricţionarea comenzile de salvare şi restaurare” la pagina 217 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 comenzile de salvare şi restaurare

Acest subiect arată un exemplu de restricţionare a comenzilor de salvare şi restaurare.

Puteţi urma aceşti paşi pentru a restricţiona salvarea şi restaurarea comenzilor pe sistemul dumneavoastră:

1. Pentru a crea o listă de autorizare 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 autorizare 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 autorizare, tastaţi următoarele:

   ```
   GRTOBJAUT OBJ(SAV*) OBJTYPE(*CMD) USER(*PUBLIC)
      AUT(*AUTL)
   ```

4. Pentru a folosi lista de autorizare 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 autorizare, 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 autorizare:

   ```
   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 autorizare separate.

7. Pentru a restricţiona API-urile de salvare şi restaurare şi a le securiza cu lista de autorizare, 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)
   GRTOBJAUT OBJ(QSRRSTO) OBJTYPE(*PGM) AUTL(SRLIST)
   GRTOBJAUT OBJ(QSRRSTO) OBJTYPE(*PGM) USER(*PUBLIC)
      AUT(*AUTL)
   ```

Ajustarea performanţei

Monitorizarea şi ajustarea performanţei nu fac parte din atribuţiile unui responsabil cu securitatea. Însă 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 - Gestionare 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 de utilizator. Alocaţi cu grijă autorizarea specială *JOBCTL şi PTYLMT în profilurile de 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 să creaţi sau să modificaţi comenzi pentru a restricţiona anumite joburi, astfel încât să fie rulate doar într-un mediu batch.

De exemplu, s-ar putea să vreţi să rulaţi anumite rapoarte sau compilări de program în batch. Un job care rulează în batch afectează de obicei performanţa sistemului mai puţin decât dacă ar rula interactiv.

De exemplu, pentru a restricţiona la batch comanda care rulează programul RPTA, 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

Această secţiune conţine indicaţii pentru dezvoltatorii de aplicaţii şi managerii de sistem să includă securitate ca parte a proiectării generale. Conţine de asemenea exemple de tehnici pe care le puteţi folosi pentru a realiza obiective de securitate în sistem.

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.

Unele din exemplele din această secţiune 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.

Planificaţi şi setaţi securitatea sistemului din centrul de informaţii este pentru administratorul de securitate. El conţine formulare, exemple şi linii de ghidare pentru planificarea securităţii pentru aplicaţii care au fost deja dezvoltate. Dacă aveţi responsibilitatea pentru proiectarea unei aplicaţii, aţi putea considera util să examinaţi formularele şi exemplele din subiectul Planificarea şi setarea securităţii sistemului 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 Planificarea şi setarea securităţii sistemului din centrul de informaţii foloseşte de asemenea un set de aplicaţii exemplu pentru o companie fictivă numită JKL Toy Company. Această secţiune discută considerente de proiectare pentru acelaşi set de aplicaţii exemplu. Figura 31 arată relaţia între grupuri utilizatori, aplicaţii şi biblioteci pentru JKL Toy Company:

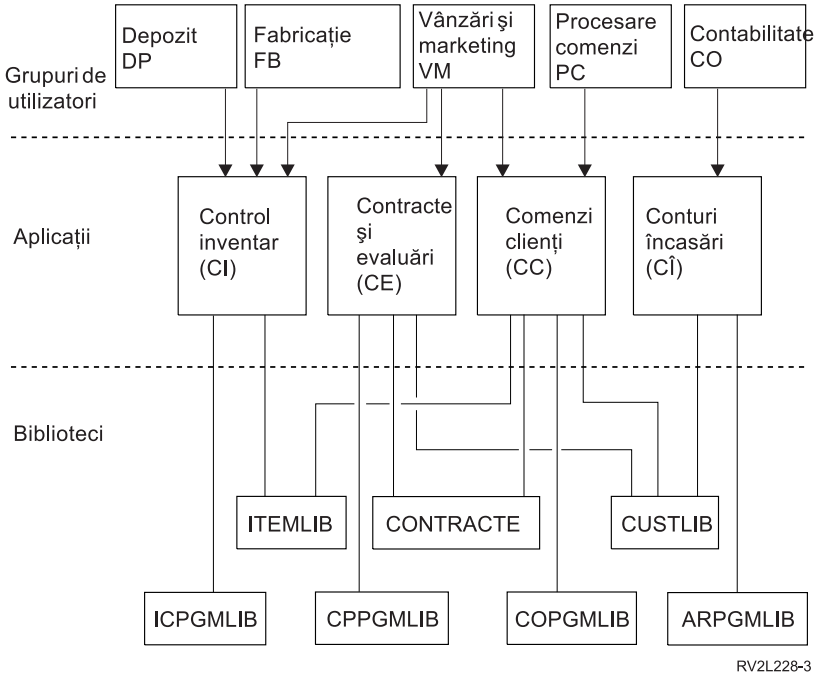


Figura 31. Aplicaţii exemplu

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. Aceste grupuri de utilizatori au accese diferite la aplicaţii diferite, care sunt în următoarea listă.

- 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 are acces doar la aplicaţii Conturi primite.

Informaţii înrudite

Scenarii pentru HTTP Server

Recomandări generale pentru proiectarea securităţii

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 de utilizator şi restricţionarea utilizatorilor la un set de meniuri, pentru a proteja informaţiile.

  Attn: Dacă folosiţi un produs precum System i Access sau dacă aveţi linii de comunicaţii ataşate la sistem, nu vă bazaţi doar pe limitarea capabilităţilor din profilul de utilizator şi controlul accesului la meniu. Trebuie să folosiţi securitatea resurselor pentru a securiza orice obiecte care nu vreţi să fie accesibile prin 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) aceeaşi 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 autorizare pentru a grupa obiecte cu aceleaşi cerinţe de securitate. Listele de autorizare sunt mai simplu de gestionat decât autorizările individuale şi ajută la recuperarea informaţiilor de securitate.

Concepte înrudite

Capitolul 5, “Securitatea resurselor”, la pagina 131
Această secţiune descrie fiecare dintre componentele securităţii resurselor şi cum funcţionează împreună pentru a proteja informaţiile despre sistem. Explică de asemenea cum să se utilizeze comanda CL şi afişează organizarea de securitate resursă pe sistemul dvs.

Planificarea modificărilor nivelurilor 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 modificarea valorii de sistem QPWDLVL, asiguraţi-vă că aţi salvat datele de securitate folosind comanda SAVSECDTA sau SAVSYS. Dacă aveţi o copie de rezervă curentă, veţi putea reseta parolele pentru toate profilurile de utilizator, chiar dacă trebuie să reveniţi la un nivel de parolă mai mic.

Produsele pe care le folosiţi în sistem şi clienţii cu care interfaţează sistemul ar putea avea probleme când valoarea de sistem nivel parolă (QPWDLVL) este setată la 2 sau 3. Orice produs sau client care trimite parole sistemului într-o formă criptată, în loc de text clar pe care un utilizator îl introduce într-un ecran de semnare, trebuie modernizat pentru a lucra cu regulile de criptare parolă pentru QPWDLVL 2 sau 3. Trimiterea parolei criptate este cunoscută ca substituirea parolei. Sustituireaa parolei este folosită pentru a preveni capturarea parolei în timpul transmisiei prin reţea. Nu vor fi acceptaţi înlocuitorii de parolă generaţi de clienţi mai vechi ce nu suportă algoritmul pentru QPWDLVL 2 sau 3, chiar dacă sunt corecte caracterele specifice tastate. Aceasta se aplică de asemenea tuturor acceselor punct System i laSystem i care utilizează valorile criptate pentru a se autentificare de pe un sistem pe altul.

Problema este generată de faptul că anumite produse afectate (cum ar fi IBM Toolbox pentru 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

Parola de nivel 1 permite unui sistem, care nu trebuie să comunice cu System i Support pentruWindows Network Neighborhood (NetServer), pentru a elimina parolele NetServer. Eliminarea parolelor criptate nenecesare din sistem creşte securitatea generală a sistemului.

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.

Considerente pentru modificarea QPWDLVL de la 0 sau 1 la 2

Nivelul de parolă 2 introduce folosirea parolelor sensibile la majuscule de maxim 128 caractere 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 sistemului ar trebui să folosească comanda PRTUSRPRF TYPE(*PWDLVL) pentru a localiza toate profilurile de utilizator care nu au o parolă care este folosibilă la nivelul de parolă 2. În funcţie de profilurile localizate, administratorul poate folosi unul din următoarele mecanisme pentru a avea o parolă nivel de parolă 2 şi 3 adăugată la profiluri.

- Modificaţi parola pentru profilul de utilizator folosind comanda CHGUSRPRF sau CHGPWD CL sau API-ul QSYCHGPW API. Aceasta 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 de 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 de 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 îndeplineşte descrierea următoare, sistemul validează utilizatorul cu o parolă nivel de parolă 0 şi creează două parole nivel de parolă 2 (după cum este descris mai sus) pentru profilul de utilizator.

- Profilul de utilizator nu are o parolă care este folosibilă la nivelurile de parolă 2 şi 3.

- Profilul de utilizator are o parolă care este folosibilă la nivelurile de parolă 0 şi 1.
- Utilizatorul se loghează printr-un produs care trimite parole în clar.

Următoarele semnări vor fi validate cu parolele din nivelul 2.

Orice client care foloseşte înlocuirea de parole nu va funcţiona corect la QPWDLVL 2 dacă clientul nu a fost actualizat să folosească noua schemă de substituţie parolă. Administratorul ar trebui să verifice dacă un client care nu a fost actualizat la noua schemă de substituţie parolă este necesar.

Clienţii care folosesc substituirea parolei includ:
- TELNET
- System i Access
- System i Host Servers
- QFileSrv.400
- System i NetServer Print support
- 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.

| Evitaţi schimbarea valorilor de sistem pentru parolă, cum ar fi QPWDMINLEN, QPWDMAXLEN şi QPWDRULES,
| până după ce aţi testat QPWDLVL 2. Aceasta face mai uşoară tranziţia înapoi la QPWDLVL 1 sau 0, dacă este necesar.
| Însă valoarea de sistem QPWDVLDPGM trebuie să specifice *REGFAC sau *NONE înainte ca sistemul să permite
| modificarea QPWDLVL la 2. Deci, dacă folosiţi un program de validare a parolei, ar putea fi necesar să scrieţi unul
| nou, care să poată 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 sunt comfortabil cu rularea sistemului la QPWDLVL 2, puteţi modifica valorile de sistem pentru parolă pentru a folosi parole mai lungi. Totuşi, trebuie să fiţi conştienţi că parolele mai lungi au aceste efecte:
- Dacă sunt specificate parole mai mari de 10 caractere, nivelurile de parolă 0 şi 1 sunt curăţate. Acest profil de utilizator nu se va putea loga dacă sistemul este întors 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 rularea sistemului la QPWDLVL 2 o perioadă de timp, puteţi lua în considerare mutarea la QPWDLVL 3 pentru a maximiza protecţia de securitate parolă.

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 comanda DSPAUTUSR sau PRTUSRPRF pentru a localiza profilurile de utilizator care nu au parole nivel de parolă 2 sau 3 asociate cu ele.

Modificarea QPWDLVL la un nivel mai mic de parolă

Revenirea la i valoare mai mică QPWDLVL, chiar dacă este posibilă, nu se aşteaptă să fie o operaţie complet lipsită de probleme. În general, ar trebui să fie un singur sens de la valori QPWDLVL mai mici la valori QPWDLVL mai mari. Totuşi, ar putea exista cazuri unde o valoare mai mică QPWDLVL trebuie setată.

Considerente pentru modificarea de la QPWDLVL 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 de la QPWDLVL 3 la 1 sau 0

Datorită unui potenţial foarte mare de a cauza probleme pentru sistem (cum ar fi că nimeni nu se poate loga deoarece parolele de nivel 0 şi 1 au fost curăţate), această modificare nu este 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 de la QPWDLVL 2 la 1

Înainte de a modifica QPWDLVL la 1, ar trebui să folosiţi comanda DSPAUTUSR sau PRTUSRPRF TYPE(*PWDINFO) pentru a localiza orice profiluri de utilizator care nu au nivel de parolă 0 sau 1. Dacă profilul de utilizator necesită o parolă după ce QPWDLVL este modificat, asiguraţi-vă că o parolă de nivel 0 şi 1 este creată pe profil folosind unul din următoarele mecanisme:

- Modificaţi parola pentru profilul de utilizator folosind comanda CHGUSRPRF sau CHGPWD CL sau API-ul QSYCHGPW API. Aceasta face ca sistemul să modifice parola care este folosibilă la nivelurile de parolă 2 şi 3; şi sistemul creează de asemenea o parolă în majuscule echivalentă care este folosibilă la nivelurile de parolă 0 şi 1. Sistemul poate crea parola de nivel 0 şi 1 dacă următoarele condiţii sunt îndeplinite:
  - Parola are o lungime de 10 caractere sau mai puţin.
  - Parola poate fi convertită la caractere 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 poate face ca sistemul să genereze o parolă de nivel 0 şi 1 de RAINYDAY. Dar modificarea valorii parolei la Rainy Days In April poate face ca sistemul să cureţe parola de nivel 0 sau 1 (deoarece parola este prea lungă şi conţine blancuri).

  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 de 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.

Administratorul poate apoi modifica QPWDLVL la 1. Toate parolele NetServer sunt curăţate când modificarea la QPWDLVL 1 devine efectivă (la următorul IPL).

Considerente pentru modificarea de la QPWDLVL 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 de la QPWDLVL 1 la 0

După modificarea QPWDLVL la 0, ar trebui să folosiţi comanda DSPAUTUSR sau PRTUSRPRF pentru a localiza orice profiluri 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.

Puteţi apoi modifica QPWDLVL la 0.

Planificarea bibliotecilor

O bibliotecă este ca un director folosit pentru a localiza obiectele din ea. Mulţi factori afectează modul în care alegeţi să grupaţi informaţiile aplicaţiilor dumneavoastră în biblioteci şi să le gestionaţi.

Securitatea bibliotecilor este eficientă doar dacă regulile de mai jos sunt urmate:

- 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.

Pentru a accesa un obiect, aveţi nevoie de autorizare pentru obiectul respectiv şi pentru biblioteca în care se află. Puteţi restricţiona accesul la un obiect restricţionând obiectul propriu-zis, biblioteca în care se află sau ambele.

Autorizarea *USE asupra unei biblioteci vă permite să găsiţi obiecte în bibliotecă. 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.

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 asemenea 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.

Aici sunt două exemple de folosire a securităţii bibliotecii pentru aplicaţii JKL Toy Company. (Vedeţi Figura 31 la pagina 219 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.
- JKL Toy Company este o companie mică cu o abordare nerestrictivă asupra securităţii, cu excepţia informaţiilor de contracte şi evaloare a preţului. Toţi utilizatorii sistemului au dreptul să vadă informaţii client şi inventar, chiar dacă doar utilizatorii autorizaţi pot modifica aceste informaţii. Bibliotecile CUSTLIB şi ITEMLIB şi obiectele din biblioteci, au autorizarea publică *USE. Utilizatorii pot vizualiza informaţiile din aceste biblioteci prin aplicaţia lor primară sau folosind o interogare SQL. 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.

  Concepte înrudite

  “Securitatea bibliotecii” la pagina 135
  Puteţi folosi securitatea bibliotecii pentru a proteja informaţii.

  Referinţe înrudite

  “Listele de biblioteci” la pagina 207
  Lista de biblioteci pentru un job indică bibliotecile în care se caută şi ordinea în care ele vor fi căutate.

Informaţii înrudite

Scenarii pentru HTTP Server

Planificarea aplicaţiilor pentru a împiedica profiluri mari

Pentru a reduce impacturile asupra performanţei şi securităţii sistemului, trebuie să planificaţi aplicaţiile cu grijă pentru a evita profiluri mari.

Datorită impacturilor potenţiale asupra performanţei şi securităţii, realizaţi următoarele acţiuni pentru a împiedica profilurile să devină prea pline:

- Să nu aveţi un profil care să deţină totul pe sistemul dumneavoastră.

  Creaţi profiluri de 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 dispersate în mai multe profiluri, ceea ce îmbunătăţeşte performanţa. Folosind mai multe profiluri proprietar, puteţi împiedica un profil să devină prea mare deoarece posedă prea multe obiecte. Profilurile de 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 de 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 de utilizator livrate de IBM poate cauza de asemenea şi probleme de securitate atunci când sunt mutate aplicaţiile de pe un sistem pe altul. Aplicaţiile posedate de profiluri de utilizator livrate de IBM pot de asemenea afecta performanţa pentru comenzi, cum ar fi CHKOBJITG şiWRKOBJOWN.
- Folosiţi liste de autorizare 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 autorizări vor cauza o intrare de autorizare privată pentru lista de autorizări din profilul de utilizator, nu o intrare de autorizare privată pentru fiecare obiect. În profilul proprietarului obiectului, listele de autorizări creează o intrare de obiect autorizat pentru fiecare utilizator cu autorizare asupra listei de autorizări.

Listele de biblioteci

Lista de biblioteci pentru un job reprezintă a expunere de securitate, chiar dacă furnizează flexibilitate. 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.

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, următoarele tehnici pot reduce expunerea de securitate.

Notă: Folosind exemplele de cod, sunteţi de acord cu termenii din Capitolul 10, “Informaţii referitoare la licenţa de cod şi declinarea responsabilităţii”, la pagina 307.

Controlarea listei de biblioteci utilizator

Ca o precauţie de securitate, poate vreţi să vă asiguraţi că porţiunea utilizator a listei de biblioteci are intrările corecte în secvenţa aşteptată înainte de rularea unui job. O metodă pentru a face aceasta este de a folosi un program CL pentru a salva lista de biblioteci a utilizatorului, a o înlocui cu lista pe care vreţi şi a o restaura la finalul aplicaţiei.

Urmează un program exemplu pentru a face asta:

Notă: Folosind exemplele de cod, sunteţi de acord cu termenii din Capitolul 10, “Informaţii referitoare la licenţa de cod şi declinarea responsabilităţii”, la pagina 307.

```
          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 32. Program pentru înlocuirea listei de biblioteci de restaurare

Observaţii:

1. Indiferent cum se termină programul (normal sau anormal), lista de biblioteci este întoarsă la versiunea pe care o avea când a fost apelat programul. Aceasta se întâmplă deoarece manipularea erorilor include restaurarea listei de biblioteci.
2. Deoarece comanda CHGLIBL necesită o listă de nume de biblioteci, nu poate fi rulată direct. Comanda RTVJOBA, deci, 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 a sistemului

Se poate să fie nevoie să modificaţi de asemenea poţiunea de sistem a listei de biblioteci pentru a vă proteja sistemul.

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 32, cu următoarele modificări:

- În loc de a folosi comanda RTVJOBA, folosiţi comanda Extragere valori de sistem (RTVSYSVAL) pentru a obţine valoarea valorii de sistem QSYSLIBL.
- Folosiţi comanda Modificare listă de biblioteci sistem (CHGSYSLIBL) pentru a modifica poţiunea de sistem a listei de biblioteci la valoarea pe care o vreţi.
- La finalului programului, folosiţi comanda CHGSYSLIBL din nou pentru a restaura poţiunea de sistem a listei de biblioteci la valoarea sa originală.
- Comanda CHGSYSLIBL este livrată cu autorizare publică *EXCLUDE. Pentru a folosi această comandă în programul dumneavoastră, faceţi una din următoarele:

– Acordaţi proprietarului programului autorizare *USE asupra comenzii CHGSYSLIBL şi folosiţi autorizare adoptată.
– Acordaţi utilizatorilor care rulează programul autorizare *USE asupra comenzii 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 biblioteca şi obiectele ei.

Informaţiile tipice necesare sunt:

- Orice funcţii aplicaţie care adaugă obiecte la 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 33 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 33. 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 capabilităţi limitate şi un meniu iniţial în profilul de 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 de utilizator ca programul Attention-key-handling program. Dacă profilul de 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 meniurilor" la pagina 229 dă un exemplu cum să faceţi asta.
- Consideraţi controlarea accesului la Meniul System Request sau la unele din opţiunile acestui meniu.
- Pentru utilizatorii cărora le e permis să ruleze doar o singură funcţie, evitaţi complet meniurile şi specificaţi un program iniţial în profilul de utilizator. Specificaţi *SIGNOFF ca meniu iniţial.

De exemplu, la JKL Toy Company, toţi utilizatorii văd un meniu de interogare care permite accesarea majorităţii 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 34. Meniu de interogare exemplu

Notă: Folosind exemplele de cod, sunteţi de acord cu termenii din Capitolul 10, "Informaţii referitoare la licenţa de cod şi declinarea responsabilităţii", la pagina 307.

Concepte înrudite

"Meniul Cerere sistem" la pagina 233
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 transfere la un al doilea job sau să oprească jobul curent. Aceasta ar putea reprezenta o expunere de securitate deoarece autorizarea publică la meniul cerere sistem este *USE când este livrat un sistem.

Referinţe înrudite

"Limitarea capabilităţilor" la pagina 83
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 în sistem.

Informaţii înrudite

Scenarii pentru HTTP Server

Descrierea securităţii meniului

Ca 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.

Exemple de tipuri de informaţii de care are nevoie un administrator de securitate 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 35 arată un format exemplu pentru furnizarea acestor informaţii.

Nume meniu: MENU1 Bibliotecă: QGPL Număr opţiune: 3 Description: Query

Program apelat: QRYSTART Bibliotecă: QGPL

Autorizare adoptată: QRYUSR

Autorizare specială necesară: Fără

Autorizări obiect necesare: Utilizatorul trebuie să aibă autorizarea *USE pentru programul QRYSTART. QRYUSR trebuie să aibă autorizare *USE pentru bibliotecile cu fişierele interogate. Utilizatorul, QRYUSR sau public trebuie să aibă autorizare *USE pentru fişierele care sunt interogate.

Figura 35. Format pentru cerinţe securitate meniu

Folosirea autorizării adoptate în proiectarea meniurilor

Disponibilitatea uneltelor de suport decizie, cum ar fi Query/400, creează probleme la proiectarea securităţii. 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.

De exemplu, aţi putea vrea ca utilizatorii să poată vizualiza informaţiile din fişier folosind o unealtă de interogare, dar probabil vreţi să vă asiguraţi că fişierele sunt modificate doar de programe de aplicaţii testate.

Notă: “Obiecte care adoptă autorizarea proprietarului” la pagina 149 descrie cum funcţionează autorizare adoptată. “Diagrama de flux 8: Cum este verificată autorizarea adoptată” la pagina 182 descrie cum verifică sistemul autorizarea adoptată.

Figura 36 arată un exemplu de meniu iniţial care foloseşte autorizare adoptată pentru a furniza 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 36. Exemplu de meniu 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 control inventar (ICSTART).

Notă: Folosind exemplele de cod, sunteţi de acord cu termenii din Capitolul 10, “Informaţii referitoare la licenţa de cod şi declinarea responsabilităţii”, la pagina 307.

```
PGM
ADDLIBLE ITEMLIB
ADDLIBLE ICPGMLIB
GO ICMENU
RMVLIBLE ITEMLIB
RMVLIBLE ICPGMLIB
ENDPGM
```

Figura 37. Exemplu de program aplicaţie iniţial

Programul care porneşte Query (QRYSTART) adoptă autorizarea unui profil (QRYUSR) furnizat pentru a permite acces la fişiere pentru interogări. Figura 38 arată programul QRYSTART:

```
PGM
ADDLIBLE ITEMLIB
ADDLIBLE CUSTLIB
STRQRY
RMVLIBLE ITEMLIB
RMVLIBLE CUSTLIB
ENDPGM
```

Figura 38. Exemplu de program pentru interogare cu autorizare adoptată

Sistemul meniu foloseşte trei tipuri de profiluri de utilizator, arătate în Tabela 125. Tabela 126 descrie obiectele folosite de sistemul meniu.

Tabela 125. Profilurile de utilizator pentru sistemul de meniuri

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	Neaplicabilă	Aşa cum e necesar aplicaţiei	Neaplicabilă
Utilizator aplicaţie [1]	Profil exemplu pentru oricine care foloseşte sistemul meniu	Da	*YES	Fără	MENU1
Profil interogare	Folosit pentru a furniza acces la biblioteci pentru interogare	*NONE	Neaplicabilă	Fără	Neaplicabilă

[1] Biblioteca curentă specificată în profilul de 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 126. Obiecte folosite de sistemul de meniuri

Nume obiect	Proprietar	Autorizare publică	Autorizări private	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		

Tabela 126. Obiecte folosite de sistemul de meniuri (continuare)

Nume obiect	Proprietar	Autorizare publică	Autorizări private	Informaţii suplimentare
Fişiere nedisponibile pentru Interogare în ITEMLIB	OWNIC	*EXCLUDE		
Programe din ICPGMLIB	OWNIC	*USE		
Notă: Poate fi creat un profil special de proprietar 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 revine la MENU1, bibliotecile ITEMLIB şi ICPGMLIB sunt înlăturate din lista de biblioteci USERA şi programul ICSTART este înlăturat din stiva de apeluri. 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: Autorizare adoptată fără autorizare privată” la pagina 191 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.

Concepte înrudite

“Planificarea securităţii fişierelor” la pagina 235
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.

Ignorarea autorizării adoptate

Tehnica folosirii autorizării adoptate în proiectarea meniurilor necesită ca utilizatorul să revină 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.

Figura 39 la pagina 232 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 39. Meniu aplicaţie exemplu cu interogare

Informaţiile de autorizare pentru programul QRYSTART sunt identice cu cele arătate în Tabela 126 la pagina 230. Programul este creat cu parametrul de autorizare adoptată de utilizare (USEADPAUT) setat pe *NO, pentru a ignora autorizarea adoptată a programelor anterioare din stivă.

Aici sunt comparaţiile stivelor de apeluri când USERA selectează interogare din MENU1 (consultaţi Figura 36 la pagina 229) şi din ICMENU:

Stivă de apeluri când interogare este selectat din MENU1

- MENU1 (fără autorizare adoptată)
- QRYSTART (autorizare adoptată QRYUSR)

Stivă de apeluri când interogare este selectat 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. Aceasta permite USERA să ruleze o interogare din ICMENU fără a avea abilitatea de a modifica şi şterge fişiere. Aceasta se întâmplă deoarece autorizarea OWNIC nu este folosită de programul QRYSTART.

Când USERA termină interogarea şi revine la ICMENU, autorizarea adoptată este activă din nou. 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 34 la pagina 228) de la JKL Toy Company foloseşte de asemenea această tehnică, deoarece poate fi apelat din meniuri din diverse biblioteci de aplicaţii. Adoptă autorizarea QRYUSR şi ignoră orice alte autorizări adoptate din stiva de apeluri.

Concepte înrudite

“Programe care ignoră autorizare adoptată” la pagina 152
Puteţi specifica parametrul folosire autorizare adoptată (USEADPAUT) pentru a controla dacă un program foloseşte autorizarea adoptată.

Referinţe înrudite

“Diagrama de flux 8: Cum este verificată autorizarea adoptată” la pagina 182
Dacă este găsită o autorizare insuficientă la verificarea autorizării utilizatorului, atunci sistemul verifică autorizarea adoptată.

Informaţii înrudite

Scenarii pentru HTTP Server

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 transfere la un al doilea job sau să oprească jobul curent. Aceasta ar putea reprezenta o expunere de securitate deoarece autorizarea publică la meniul cerere sistem este *USE când este livrat un sistem.

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. Comenzile sunt calificate cu un nume de bibliotecă din mesajul CPX2373. Valorile din mesajul CPX2373 pentru fiecare comandă sunt *NLVLIBL sau *SYSTEM. Cineva ar putea folosi comanda OVRMSGF (Override Message File - Înlocuire fişier de mesaje) ca să modifice comenzile pe care le folosesc opţiunile meniului cerere sistem.

De fiecare dată când este apăsată tasta System Request, sistemul în mod automat modifică profilul de utilizator curent al jobului la profilul de utilizator iniţial al jobului. Acest lucru se întâmplă pentru ca utilizatorul să nu aibă nici o autoritate adiţională în meniul System Request sau în programul de ieşire Presystem Request Program. De fiecare dată când este apăsată tasta System Request, sistemul în mod automat modifică profilul de utilizator curent al jobului la profilul de utilizator iniţial al jobului.

Puteţi împiedica utilizatorii să selecteze opţiuni specifice din Meniul cerere sistem restricţionând autorizarea pentru comenzile asociate. Tabela 127 arată comenzile asociate cu opţiunile meniului:

Tabela 127. 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.)

Tabela 127. Opţiuni şi comenzi pentru meniul cerere sistem (continuare)

Opţiune	Comandă
80	Deconectare job (DSCJOB)
90	Sign-Off (SIGNOFF)

Observaţii:

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. Unele din opţiuni au restricţii pentru mediul System/36.

De exemplu, pentru a împiedica utilizatorii să transfere la un job interactiv 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.

Concepte înrudite

“Planificarea meniurilor” la pagina 227
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 capabilităţi limitate şi un meniu iniţial în profilul de utilizator.

Planificarea securităţii comenzilor

Când sistemul ajunge, abilitatea de a folosi comenzi este setată pentru a îndeplini 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 comenzilor pentru a îndeplini cerinţele 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 de obiect pentru comenzile propriu-zise. 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 asupra acelei comenzi. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 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, puteţi restricţiona accesul la întreaga bibliotecă. Dacă folosiţi una sau mai multe versiuni de limbă naţională5/OS a programului licenţiat pe sistemul dumneavoastră, aveţi nevoie să restricţionaţi comenzile în bibliotecile QSYSxxx suplimentare din sistemul dumneavoastră de asemenea.

O altă măsură 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 fişierelor

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.

Pentru fişiere critice de pe sistemul dumneavoastră, 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 programele care adoptă autorizarea unui anumit utilizator folosind comanda Afişare adoptare program (DSPPGMADP).

Puteţi folosi de asemenea 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 Afişare jurnal (DSPJRN) pentru a vizualiza un exemplu de intrări jurnal periodic.

Referinţe înrudite

"Folosirea autorizării adoptate în proiectarea meniurilor" la pagina 229
Disponibilitatea uneltelor de suport decizie, cum ar fi Query/400, creează probleme la proiectarea securităţii. 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.

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 specifice sau înregistrări dintr-un fişier.

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 40 la pagina 236 arată un exemplu de fişier fizic şi trei fişiere logice diferite asociate cu el.

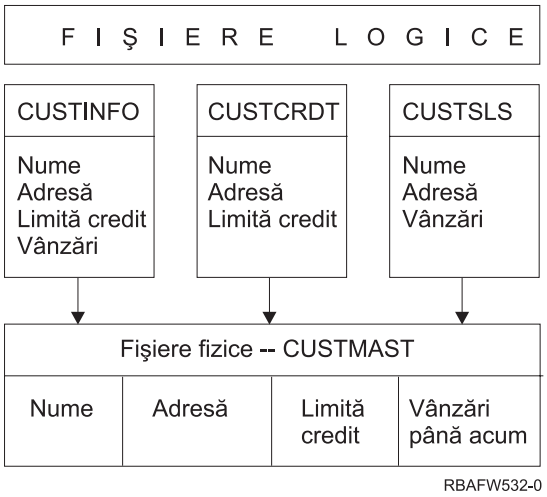


Figura 40. Folosirea unui fişier logic pentru securitate

Membrilor departamentului de vânzări (profilul de grup DPTSM) le e permis să vadă toate câmpurile, dar nu pot modifica limita de credit. Membrilor departamentului pentru conturi de încasări (profilul de grup DPTAR) le e permis să vadă toate câmpurile, dar nu pot să modifice câmpul vânzări. Autorizarea pentru fişierul fizic arată astfel:

Tabela 128. Exemplu de fişier fizic: Fişierul 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 187 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 i5/OS licenţiat. Când un fişier logic pre-V3R1 este restaurat pe un sistem V3R1 sau mai recent, sistemul converteşte fişierele logice prima dată când este accesat un fişier logic. Sistemul îi acordă autorizări pentru toate datele.

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.

Informaţii înrudite

Înlocuirea fişierelor

Puteţi folosi comenzile de înlocuire pentru a face ca un program să folosească un fişier diferit cu acelaşi format.

De exemplu, presupuneţi că un program din aplicaţia de contracte şi evaluarea preţului la JKL Toy Company scrie informaţii de evaluarea preţului într-un fişier de lucru înainte de a face modificări ale preţului. 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, deşi acele fişiere sunt protejate de efectele oricăror comenzi de înlocuire fişier care au fost apelate anterior. Dacă folosiţi SECURE(*NO), acele fişiere nu sunt protejate de alte înlocuiri de fişiere. Valorile lor pot fi suprascrise de efectele oricăror comenzi de înlocuire fişier care au fost apelate anterior.

Securitatea fişierelor şi SQL

Ar trebui să acordaţi atenţie securităţii fişierelor la folosirea unui 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, deci, accesa orice fişier la care are autorizare profilul adoptat.

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.

Planificarea profilurilor de utilizator

Un profil de grup este o unealtă folositoare când mai mulţi utilizatori au cerinţe de securitate similare. Puteţi crea direct fişiere grup sau puteţi face un profil existent un profil de grup. Când folosiţi profiluri de grup, puteţi gestiona autorizarea mai eficient şi reduce numărul de autorizări private individuale pentru obiecte.

Fişierele de grup sunt utile în special când cerinţele 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 intră 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 de utilizator.

Un profil de grup este doar un tip special de profiluri de 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.

Concepte înrudite

“Profiluri de grup” la pagina 4
Un *profil de grup* este un tip special de profil de utilizator. În loc să acordaţi autorizarea fiecărui utilizator individual, puteţi folosi un profil de grup ca să definiţi autorizarea pentru un grup de utilizatori.

Considerente pentru grupuri 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.

Operaţii înrudite

"Cazul 2: Folosirea autorizării grupului primar" la pagina 187
Acest caz demonstrează cum să folosiţi autorizarea grupului primar.

Considerende pentru mai multe profiluri de grup

Folosind profiluri de grup, puteţi gestiona autorizarea mai eficientşi reduce numărul de autorizări private individuale pentru obiecte. Însă folosirea greşită a profilurilor de grup poate avea un efect negativ asupra performanţelor verificării autorizării. Acest subiect furnizează unele sugestii despre folosirea mai multor profiluri de grup.

Un utilizator poate fi membru a până la 16 grupuri: primul grup (parametrul GRPPRF din profilul de utilizator) şi 15 grupuri suplimentare (parametrul SUPGRPPRF din profilul de utilizator).

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 169. Asiguraţi-vă că înţelegeţi cum folosirea grupurilor multiple în combinaţie cu alte tehnici de autorizare, cum ar fi liste de autorizare, vă poate afecta performanţa sistemului.

Acumularea de autorizări speciale pentru membrii profil grup

Autorizările speciale sunt cumulative pentru utilizatorii care sunt membri ale grupurilor multiple.

Autorizările speciale ale profilurilor de grup sunt disponibile membrilor acelui grup. Profilurile de 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 membru. 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 de utilizator care are toate cele trei profiluri ca profilurile sale de grup are autorizările speciale *JOBCTL, *AUDIT şi *IOSYSCFG.

Notă: Dacă un membru de grup deţine un program, acesta adoptă doar autorizarea proprietarului. Autorizările grupului proprietarului nu sunt 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.

Aţi putea observa că un anumit utilizator are toate autorizările necesare unui grup de utilizatori şi să fiţi tentat să faceţi acel profil de utilizator 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 membrii 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 acorda autorizări utilizator profilului de grup.
3. Înlăturaţi autorizările private din utilizator, deoarece ele nu mai sunt necesare. Folosiţi comanda RVKOBJAUT sau EDTOBJAUT.

Compararea profilurilor de grup şi a listelor de autorizare

Profilurile de grup sunt folosite pentru a simplifica gestionarea profilurilor de utilizator care au cerinţe de securitate similare. Listele de autorizare sunt folosite pentru a securiza obiecte cu cerinţe similare de securitate.

Tabela 129 arată caracteristicile celor două metode.

Tabela 129. Comparaţie listă de autorizare şi profil de grup

Element comparat	Listă de autorizări	Profil de grup
Folosit pentru a securiza obiecte multiple	Da	Da
Utilizatorul poate aparţine 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	Yes [2]

[1] Profilului de grup îi poate fi acordată autorizare când este crea un obiect folosind parametrul GRPAUT din profilul de utilizator care îl creează.

[2] Autorizarea de grup primar este salvată cu obiectul. Autorizările private de grup suntspecificate dacă PVTAUT(*YES) este specificat în comanda de salvare.

Pentru lista de autorizări a elementului ″Autorizarea poate fi specificată când este creat obiectul″:

- Pentru a asigna o listă de autorizări unui obiect bazat pe bibliotecă, specificaţi AUT (*LIBCRTAUT) în comanda CRTxxxx şi CRTAUT (authorization-list-name) pentru bibliotecă. Unele obiecte, cum ar fi listele de validare, nu pot folosi o valoare de *LIBCRTAUT în comanda CRT.
- Pentru a asigna o listă de autorizări unui obiect bazat pe bibliotecă, specificaţi valoarea *INDIR pentru parametrii DTAAUT şi OBJAUT ai comenzii MKDIR. În acest fel, lista de autorizări asigură şi directorul părinte şi pe cel nou. Sistemul nu permite ca o listă de autorizări arbitrară să fie specificată când este creat un obiect.

Planificarea securităţii pentru programatori

Programatorii reprezintă o problemă pentru responsabilul cu securitatea. Cunoştinţele lor îi pot face să ocolească procedurile de securitate care nu sunt proiectate cu atenţie.

Programatorii pot ocoli securitatea pentru a accesa datele 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 văzută de ei ca un obstacol pentru realizarea taskurilor 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 setaţi un mediu pentru programatorii de aplicaţii:

- Nu acordaţi autorizări speciale totale programatorilor. Dacă trebuie să daţi programatorilor autorizări speciale, daţi-le doar autorizarea specială care este necesară pentru a realiza joburile sau taskurile care sunt asignate programatorului.
- Nu folosiţi profilul de 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 să lucreze asupra membrilor aplicaţie ai grupului şi definiţi profilurile de utilizator programator pentru a face ca grupul să posede orice obiecte noi care sunt create (OWNER(*GRPPRF)). Când un programator se mută de la un proiect la altul, puteţi modifica informaţiile de grup din profilul său. Consultaţi “Dreptul de proprietate al grupului asupra obiectelor” la pagina 143 pentru mai multe informaţii.
- 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 programe, ar trebui posedate de profilul de utilizator care este proiectat pentru aplicaţie.

  Obiectele aplicaţie nu ar trebui posedate de un programator deoarece programatorul poate avea control 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 proprietar al aplicaţiei.

Gestionarea fişierelor sursă

Pentru a proteja informaţii din sistem, trebuie să planificaţi cu atenţie securitatea 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. Luaţi în considerare plasarea fişierelor sursă în biblioteci separate şi controlarea persoanelor care le pot actualiza şi cine le poate muta în producţie.

Când un fişier sursă este creat în sistem, autorizarea publică implicită este *CHANGE. Aceasta permite oricărui utilizator să actualizeze orice membru 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 autorizare *OBJMGT asupra fişierelor sursă pentru a adăuga membrii noi. Autorizarea publică ar trebui redusă la *USE sau *EXCLUDE, dacă fişierele sursă nu sunt într-o bibliotecă controlată.

Protejarea fişierelor clasă fişier fişierelor jarJava în sistemul de fişiere integrat

Pentru a rula un program Java, aveţi nevoie de autorizare de citire (*R) asupra fiecărui fişier clasă şi jar Java plus autorizare de execuţie (*X) asupra fiecărui director din calea spre fişierele clasă şi jar Java. Dacă folosiţi fişiere clasă şi jar Java în sistemul de fişiere integrat, trebuie să le protejaţi folosind autorizări normale de obiect.

Pentru a proteja fişiere Java,folosiţi comanda CHGAUT pentru a securiza directoarele din cale şi fişierele cu atribute autorizare obiect. Un utilizator poate avea nevoie de autorizare de citire (*R) pentru fişierele class şi jar Java pentru a rula un program Java. Pot primi acea autorizare de la autorizarea publică a fişierului sau de la autorizarea privată. O listă de autorizări este utilă în setarea autorizării private pentru un grup de utilizatori. Nu daţi oricui autorizare de scriere (*W) asupra fişierului decât dacă au permisiunea de a modifica fişierul.

Puteţi folosi parametrul Nivel verificare securitate cale de clase (CHKPATH) în comanda RUNJVA pentru a vă asigura că o aplicaţie în rulare Java foloseşte fişierele corecte din CLASSPATH. Puteţi folosi o valoare de CHKPATH(*SECURE) pentru a împiedica un program Java să ruleze dacă unul sau mai multe mesaje de avertisment sunt trimise pentru fiecare director din CLASSPATH care are autorizare publică de scriere.

Planificarea securităţii pentru programatorii de sistem sau pentru manageri

Puteţi limita autorizarea acordată programatorilor de sistem sau managerilor pentru a protejaţi fişierele din sistem.

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.

De exemplu, aţi putea vrea ca Sue şi Fred să fie două persoane care pot crea şi modifica profiluri de utilizator fără a le acorda autorizări speciale. Puteţi realiza aceasta făcând următorii paşi.

1. Scrieţi o comandă sau un program care este un front end pentru comanda CRT/CHGUSRPRF.
2. Faceţi ca comanda sau programul să adopte un profil care poate face creările şi modificările.
3. Autorizaţi pe Sue şi Fred pe acel program.

Atunci Sue şi Fred pot efectua doar taskul prin aplicaţie.

Folosirea listelor de validare

Obiectele listei de validare furnizează o metodă pentru aplicaţii de a stoca în siguranţă informaţii de autentificare utilizatori.

De exemplu, ICS foloseşte liste de validare pentru a realiza conceptul de utilizator internet. ICS poate realiza autentificare de bază înainte ca o pagină web să fie servită. 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-ul poate folosi informaţiile din lista de validare în loc de a cere ca toţi utilizatorii ICS-ul să aibă un id utilizator şi o parolă System i.

Unui utilizator internet îi poate fi permis sau refuzat accesul la sistem din serverul web. Utilizatorul, totuşi, nu are nici o autorizare pentru System i nici o resursă sau autorizare să semneze sau să ruleze joburi. Un profil de utilizator System i nu este creat niciodată pentru utilizatori internet.

Pentru a crea şi şterge liste de validare, puteţi folosi comenzile CL Creare listă de validare (CRTVLDL) şi Ştergere listă de validare(DLTVLDL). 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.

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 listă de validare pentru a verifica parola unui utilizator. Deoarece lista de validare este criptată, această metodă este mai sigură decât folosirea doar a aplicaţiei pentru a verifica parola utilizatorului.

Puteţi stoca informaţiile de autentificare într-o formă decriptabilă. Dacă un utilizator are securitatea corespunzătoare, informaţiile de autentificare pot fi descriptate şi returnate utilizatorului.

Referinţe înrudite

"Reţinerea informaţiilor de securitate server (QRETSVRSEC)" la pagina 31
Valoarea de sistem Păstrare securitate server (QRETSVRSEC) determină dacă informaţii de autentificare decriptibile asociate cu profiluri de utilizator sau intrări listă de validare (*VLDL) pot fi păstrate pe sistemul gazdă. Aceasta nu include parola profilului de utilizator System i.

Informaţii înrudite

Interfeţe de programare aplicaţii

Limitarea accesului la funcţii de program

Limitarea accesului la funcţia programuluivă permite să definiţi cine poate folosi o aplicaţie, părţi din ea sau funcţiile dintr-un program.

Acest suport nu este o înlocuire pentru securitatea resurselor. 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. Funcţia trece prin următoarele procese pentru a face verificarea.

- Înregistrarea unei funcţii
- Extragerea informaţiilor despre funcţie
- Definirea celor care pot sau nu să folosească funcţia
- Verifica dacă utilizatorului îi e permis să folosească funcţia

Funcţia de limitare acces la program permite API-urilor să realizeze următoarele taskuri: Să folosească această funcţie cu o aplicaţie, furnizorul aplicaţiei trebuie să înregistreze funcţiile când aplicaţia este instalată. Funcţia înregistrată corespunde unui bloc de cod pentru funcţii specifice din aplicaţie. Când utilizatorul rulează aplicaţia, înainte ca aplicaţia să invoce blocul de cod, apelează API-ul de verificare folosire pentru a verifica dacă utilizatorul are autorizarea de a folosi funcţia asociată cu blocul de cod. Dacă utilizatorului îi este permis să folosească funcţia înregistrată, blocul de cod rulează. 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 folosi comanda Lucru cu informaţii folosire funcţie (WRKFCNUSG) pentru a gestiona accesul la funcţia de program sau să folosească Application Administration în Navigator System i.

Informaţii înrudite

Administrare aplicaţii

Capitolul 8. Salvarea de rezervă şi recuperarea informaţiilor de securitate

Salvarea informaţiilor dumneavoastră de securitate este la fel de importantă ca salvarea datelor. În anumite situaţii, 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 de utilizator şi autorizările de obiecte. Aceasta poate fi o activitate consumatoare de timp şi poate duce la erori şi la probleme de securitate.

Acest subiect include informaţii despre următoarele subiecte:

- 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

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 130 arată comenzile care sunt folosite pentru a salva şi restaura informaţii de securitate. Această secţiune discută despre salvarea şi recuperarea datelor de securitate în detaliu.

Tabela 130. Modul în care informaţiile despre securitate sunt salvate şi restaurate

	Comenzi de salvare şi restaurare folosite					
Informaţii de securitate salvate sau restaurate	**SAVSECDTA SAVSYS**	**SAVCHGOBJ SAVOBJ SAVLIB SAVDLO SAVCFG**	**RSTUSRPRF**	**RSTOBJ RSTLIB RSTDLO RSTCFG**	**RSTAUT**	**RSTDFROBJ**
Profilurile de utilizator	X		X			
Dreptul de proprietate [1]		X		X		X
Grup primar [1]		X		X		X
Autorizări publice [1]		X		X		X
Autorizări private[3]	X	X	X	X	X	X
Listele de autorizare	X		X			
Păstrătorii de autorizare	X		X			
Legătura cu lista de autorizare şi păstrătorii de autorizare		X		X		
Valoare auditare obiect		X		X		
Informaţii înregistrare funcţie [2]		X		X		
Informaţii de folosire funcţie	X		X		X	
Liste de validare		X		X		
Intrări autentificare server	X		X			

Tabela 130. Modul în care informaţiile despre securitate sunt salvate şi restaurate (continuare)

Informaţii de securitate salvate sau restaurate	Comenzi de salvare şi restaurare folosite					
	SAVSECDTA SAVSYS	**SAVCHGOBJ SAVOBJ SAVLIB SAVDLO SAVCFG**	**RSTUSRPRF**	**RSTOBJ RSTLIB RSTDLO RSTCFG**	**RSTAUT**	**RSTDFROBJ**
[1] Comenzile SAVSECDTA, SAVSYS şi RSTUSRPRF salvează şi restaurează dreptul de proprietate, grupul primar, autorizare grup primar şi autorizarea publică pentru aceste tipuri de obiecte : profil de utilizator (*USRPRF), listă de autorizare (*AUTL) şi păstrător de autorizare (*AUTHLR).						
[2] Obiectul de salvat/restaurat este QUSEXRGOBJ, tip *EXITRG din biblioteca QUSRSYS.						
[3] Autorizările private pentru toate obiectele sunt salvate cu SAVSECDTA. RSTUSRPRF va restaura informaţiile de autorizare necesare pentru a restaura autorizările private. Autorizările private sunt restaurate cu RSTAUT. Autorizările private pentru obiecte individuale pot fi salvate cu comenzile SAV, SAVLIB, SAVOBJ şi SAVCHGOBJ. Autorizările private pentru obiecte individuale pot fi restaurate cu comenzile RST, RSTLIB şi RSTOBJ dacă acestea au fost salvate cu comanda de salvare.						

Informaţii înrudite

Salvarea de rezervă şi recuperarea

PDF Salvare de rezervă şi recuperare

Cum sunt stocate informaţiile de securitate

Planificarea de proceduri adecvante de salvare de rezervă şi recuperare pentru informaţii de securitate necesită înţelegerea cum să stocate şi salvate informaţiile.

Informaţiile de securitate sunt stocate cu obiecte, profiluri de utilizator şi liste de autorizare:

Informaţii de autorizare stocate cu obiectul:

- 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 de utilizator:

- *Informaţii antet*
  - Atributele profilului de utilizator afişate în ecranul Create User Profile - Creare profil de utilizator.
  - Uid-ul şi gid-ul.
- *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 autentificare server*:
  - Intrări autentificare server.

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.

Concepte înrudite

"Informaţii suplimentare asociate cu un profil de utilizator" la pagina 114
Acest subiect discută autorizările private, informaţiile obiect posedat şi informaţii obiect grup primar care sunt asociate cu un profil de utilizator.

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 de utilizator, informaţiile de autorizare privată stocate cu profilul de utilizator sunt formatate într-o tabelă de autorizare.

O tabelă de autorizare este construită şi salvată pentru fiecare profil de utilizator care are autorizări private. Această reformatare şi salvare a informaţiilor 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:

Informaţiile de autorizare salvate cu obiectul:

- 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
- Autorizările private pentru obiect, dacă PVTAUT(*YES) este specificat în comanda SAVxxx

Informaţii de autorizare salvate cu lista 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 de utilizator:

- Atributele profilului de utilizator afişate în ecranul Create User Profile - Creare profil de utilizator.
- Alte informaţii de aplicaţie asociate cu profilul de utilizator. De exemplu:

– Intrări autentificare server
– Intrările Informaţii aplicaţie utilizator care sunt adăugate folosind API-ul Actualizare informaţii aplicaţii utilizator (QsyUpdateUserApplicationInfo)

Tabela de autorozări salvată asociată cu profilul de utilizator:

- Câte o înregistrare pentru fiecare autorizare privată a profilului de 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.

Recuperarea informaţiilor de securitate

Recuperarea sistemului dumneavoastră înseamnă restaurarea datelor şi a informaţiilor de securitate asociate.

Secvenţa tipică pentru recuperare este:

1. Restaurare profiluri de utilizator şi liste de autorizare (RSTUSRPRF USRPRF(*ALL)).
2. Restaurare obiecte (RSTCFG, RSTLIB, RSTOBJ, RSTDLO sau RST).
3. Restaurare autorizări private la obiecte (RSTAUT).

Notă: Folosind exemplele de cod, sunteţi de acord cu termenii din Capitolul 10, “Informaţii referitoare la licenţa de cod şi declinarea responsabilităţii”, la pagina 307.

Informaţii înrudite

Salvare de rezervă şi recuperare

Restaurarea profilurilor de utilizator

Ar putea exista unele modificări care sunt făcute asupra unui profil de utilizator când este restaurat.

Se aplică următoarele reguli:

- Dacă profilurile sunt restaurate individual (RSTUSRPRF USRPRF(*ALL) nu este specificat), SECDTA(*PWDGRP) nu este cerut şi profilul care este restaurat nu există în sistem, aceste câmpuri sunt modificate la *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 de 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 de utilizator 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 de utilizator vor fi incorecte după restaurarea unui profil de utilizator individual care există pe sistem, doar dacă nu este specificat parametrul SECDTA(*PWDGRP) în comanda RSTUSRPRF.
- Dacă toate profilurile de utilizator sunt restaurate în sistem, toate câmpurile din oricare profiluri care există deja în sistem sunt restaurate de pe mediul de salvare, inclusiv parola.

Atenţie:

1. Profilurile de 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 de 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 va fi validă pe un sistem care rulează nivelul de parolă 0 sau 1.
2. Păstraţi o înregistrare a parolei responsabilului ce securitatea (QSECOFR) asociată cu fiecare versiune a informaţiilor de securitate care sunt salvate. Aceasta asigură că vă puteţi loga în sistem dacă trebuie să efectuaţi o operaţie completă de restaurare.

Puteţi folosi DST (Dedicated Service Tools - Instrumente dedicate de service) pentru a reseta parola pentru profilul QSECOFR.

- Dacă există un profil pe sistem, operaţia de restaurare nu modifică uid sau gid.
- Dacă un profil nu există în sistem, uid-ul şi gid-ul pentru un profil sunt restaurate de pe mediul de salvare. Dacă uid-ul sau gid-ul există deja în sistem, sistemul generează o nouă valoare şi emiterea unui mesaj (CPI3810).
- Autorizarea specială *ALLOBJ este înlăturată din profilurile de utilizator care sunt restaurate pe un sistem la nivelul de securitate 30 sau mai mare în oricare din aceste situaţii:
  - 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 serial al maşinii în sistem şi pe mediul de salvare pentru a determina dacă obiectele sunt restaurate pe acelaşi sistem sau pe un sistem diferit.

  Autorizarea specială *ALLOBJ nu este înlăturată din aceste profiluri livrate de IBM:
  - profil de utilizator QSYS (sistem)
  - profil de utilizator QSECOFR (responsabil de securitate)
  - profil de utilizator QLPAUTO (instalare automată a programului licenţiat)
  - profil de utilizator QLPINSTALL (instalare a programului licenţiat)

  Informaţii înrudite

  Resetarea parolei profilului de utilizator QSECOFR i5/OS

Restaurarea obiectelor

Când restauraţi un obiect pe un sistem, sistemul foloseşte informaţiile de autorizare stocate cu obiectul. Acest subiect descrie regulile care se aplică la informaţiile de autorizare la restaurarea obiectelor.

Următoarele se aplică securităţii obiectului restaurat:

Drept de proprietate a obiectului:

- Dacă profilul care posedă obiectul există în sistem, dreptul de proprietate este restaurat acelui profil.
- Dacă proprietarul profilului nu există pe sistem, dreptul de proprietate al obiectului este cedat profilului de 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 252 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 care este restaurat nu există în sistem, autorizarea publică este setată la autorizarea publică a obiectului salvat.
- Dacă obiectul care este restaurat nu există 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 existent 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 la lista de autorizare care este asociată cu obiectul existent.
- Dacă un document sau folder care există deja în sistem este restaurat, lista de autorizare care este asociată cu obiectul din 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) sau ALWOBJDIF(*AUTL), 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 profiluri de utilizator şi cu obiecte dacă PVTAUT(*YES) este specificat în comanda SAVxxx.
- Dacă profilurile de utilizator au autorizare privată asupra unui obiect care este restaurat, acele autorizări private nu sunt afectate tipic. Restaurarea anumitor tipuri de programe poate determina revocarea autorizărilor private.
- Dacă un obiect este şters din sistem, autorizarea privată pentru obiect nu mai există în sistem. Când este şters un obiect, toate autorizările private ale obiectului sunt înlăturate din profilul de utilizator. Dacă obiectul este apoi restaurat de la o versiune salvată, autorizările private pot fi restaurate dacă PVTAUT(*YES) a fost specificat când obiectul a fost salvat.
- Dacă autorizările private trebuie recuperate şi autorizările private nu au fost salvate cu obiectul, atunci trebuie folosită comanda Restaurare autorizare (RSTAUT). Secvenţa obişnuită este:
  1. Restaurare profiluri de utilizator
  2. Restaurare obiecte
  3. Restaurare autorizare

Auditare obiecte:

- Dacă obiectul care este restaurat nu există în sistem, valoarea de auditare obiect (OBJAUD) a obiectului salvat este restaurată.

- Dacă obiectul care este restaurat nu există şi este înlocuit, valoarea de auditare obiect nu este modificată. Valoarea OBJAUD de la versiunea salvată a obiectului nu este restaurată.
- Dacă o bibliotecă sau un director care este restaurat nu există în sistem, valoarea creare obiect sau auditare director (CRTOBJAUD) pentru bibliotecă sau director este restaurată.
- Dacă o bibliotecă sau un director care este restaurat există şi este înlocuit, valoarea CRTOBJAUD pentru bibliotecă sau director nu este restaurată.Variabila CRTOBJAUD pentru biblioteca existentă este folosită.

Păstrător de autorizare:
- Dacă un fişier este restaurat şi păstrătorul de autorizare există pentru acel nume de fişier precum şi biblioteca în care este restaurat, fişierul este legat la păstrătorul de autorizare.
- Informaţiile de autorizare asociate cu păstrătorul de autorizare înlocuiesc autorizarea publică şi informaţiile proprietarului salvate cu fişierul.

Obiecte domeniu utilizator:

Sistemul restricţionează obiecte domeniu utilizator (*USRSPC, *USRIDX şi *USRQ) la bibliotecile specificate în valoarea 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 de 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.

Concepte înrudite

“Restaurarea programelor” la pagina 252
Restaurarea programelor pe sistemul dumneavoastră ce sunt obţinute de la o sursă necunoscută pun o problemă de securitate. Acest subiect furnizează informaţii despre factorii care ar trebui luaţi în considerare la restaurarea programelor.

“Restaurarea listelor de autorizare” la pagina 253
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.

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) recontruieşte autorizarea privată din profilul de utilizator folosind informaţiile din tabela de autorizare. Operaţia acordare autorizare rulează pentru fiecare autorizare privată din tabela de autorizări. Acesta poate fi un proces lung dacă autorizarea este restaurată pentru multe profiluri şi dacă există multe autorizări private în tabela de autorizări.

Comenzile RSTUSRPRF şi RSTAUT poate fi rulat pentru un profil singular, o listă de profiluri, un nume generic de profil sau toate profilurile. Sistemul caută mediul de salvare sau fişierul de salvare care a fost creat de comanda SAVSECDTA, comanda SAVSYS sau API-ul QSRSAVO pentru a găsi profilurile pe care vreţi să le restauraţi.

| Dacă autorizările private sunt salvate cu obiectele, le puteţi restaura opţional cu obiectele. Este sugerat dacă salvaţi şi
| restauraţi un număr relativ mic de obiecte, în loc de tot sistemul.

Restaurarea autorizării de câmp:

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 de utilizator necesare.
- Restaurare fişiere.
- Rulaţi comanda Restaurare autorizare (RSTAUT).

Autorizările de câmp private nu sunt restaurate în totalitate decât după ce sunt din nou restabilite autorizările de obiect private pe care ele le restricţionează.

Restaurarea programelor

Restaurarea programelor pe sistemul dumneavoastră ce sunt obţinute de la o sursă necunoscută pun o problemă de securitate. Acest subiect furnizează informaţii despre factorii care ar trebui luaţi în considerare la restaurarea programelor.

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.

Sistemul foloseşte 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 în comanda şi valoarea de sistem Forţare conversie la restaurare (QFRCCVNRST).

Notă: Programele conţin informaţii care permit programului să fie recontruite la restaurare 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.

Restaurarea programelor care adoptă autorizarea proprietarului:

Când un program care adoptă autorizarea proprietarului este restaurat, dreptul de proprietate şi autorizarea programului ar putea fi modificate. Se aplică următoarele reguli:

- Profilul de utilizator ce realizează operaţiunea de restaurare trebuie fie să deţină programul, fie să aibă autorizările speciale *ALLOBJ şi *SECADM.
- Profilul de utilizator ce realizează operaţiunea de restaurare poate primi autorizarea de a restaura programul dacă
  - Este proprietarul 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 de utilizator QDFTOWN. Autorizarea publică este modificată în *EXCLUDE şi lista de autorizare este înlăturată.

Concepte înrudite

"Restaurarea obiectelor" la pagina 249
Când restauraţi un obiect pe un sistem, sistemul foloseşte informaţiile de autorizare stocate cu obiectul. Acest subiect descrie regulile care se aplică la informaţiile de autorizare la restaurarea obiectelor.

Referinţe înrudite

"Valorile de sistem pentru restaurare referitoare la securitate" la pagina 41
Acest subiect introduce valorile de sistem restaurare legate de securitate pe sistemul de operare i5/OS.

Restaurarea programelor licenţiate

Acest subiect introduce instrucţiunile despre restaurarea programelor licenţiate din sistem.

Comanda Restaurare programe licenţiate (RSTLICPGM) este folosită pentru a instala programe livrate de IBM din sistem. Poate fi de asemenea folosită pentru a instala programe care nu sunt de la IBM care au fost create folosind IBM System Manager pentru programe licenţiate i5/OS.

Când este livrat sistemul, 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. În loc ca un utilizator cu autorizare *ALLOBJ să ruleze comanda direct, folosiţi un program care adoptă autorizarea specială *ALLOBJ pentru a rula comanda RSTLICPGM.

Urmează un exemplu pentru această tehnică. Programul care va fi instalat folosind comanda RSTLICPGM este apelat CPAPP (Contracte şi evaluarea preţului).

1. Creaţi un profil de utilizator cu autorizare suficientă pentru a instala cu succes aplicaţia. Nu acordaţi acestui profil autorizarea specială *ALLOBJ. În acest exemplu, profilul de utilizator este numit OWNCP.
2. Scrieţi un program pentru a instala aplicaţia. În acest exemplu, programul este numit CPINST:

   Notă: Folosind exemplele de cod, sunteţi de acord cu termenii din Capitolul 10, "Informaţii referitoare la licenţa de cod şi declinarea responsabilităţii", la pagina 307.

   ```
   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

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. Autorizările private ale utilizatorilor asupra listei sunt restaurate folosind comanda RSTAUT.

Listele de autorizare sunt salvate de comanda SAVSECDTA sau comanda SAVSYS. Listele de autorizare sunt restaurate de comanda:

```
RSTUSRPRF USRPRF(*ALL)
```

Recuperarea dintr-o listă deteriorată de autorizare

Când o listă de autorizare care securizează un obiect devine deteriorată, accesul la obiect este limitat la utilizatorii care au autorizare specială toate obiectele (*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.

Concepte înrudite

"Restaurarea obiectelor" la pagina 249
Când restauraţi un obiect pe un sistem, sistemul foloseşte informaţiile de autorizare stocate cu obiectul. Acest subiect descrie regulile care se aplică la informaţiile de autorizare la restaurarea obiectelor.

Recuperarea listei de autorizare

Folosiţi instrucţiunile din acest subiect pentru a recupera lista de autorizare.

Dacă autorizările utilizatorului asupra listei de autorizare sunt cunoscute, puteţi restaura lista de autorizare urmând paşii de mai jos.

1. Ştergereţi lista de autorizare.
2. Creaţi lista de autorizare din nou.
3. Adăugaţi toţi utilizatorii cunoscuţi la ea.

Dacă nu cunoaşteţi toate autorizăţi utilizator, puteţi restaura lista de autorizare folosind ultimele banzi salvate SAVSYS sau SAVECDTA. 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 de utilizator:
   ```
   RSTUSRPRF USRPRF(*ALL)
   ```
3. Restauraţi autorizările private ale utilizatorilor asupra listei folosind comanda RSTAUT.

Această procedură restaurează valorile profil de utilizator de pe mediul de salvare. Consultaţi"Restaurarea profilurilor de utilizator" la pagina 248 pentru informaţii suplimentare despre restaurarea valorilor profil de utilizator de pe mediul de salvare.

Recuperarea asocierii obiectelor la lista de autorizare

Urmaţi paşii din acest subiect pentru a recupera asocierea obiectelor în lista de autorizare.

Când lista de autorizare deterioară este ştearsă, obiectele care au fost securizate de lista de autorizare trebuie să fie adăugate la noua listă de autorizare. Faceţi următoarele acţiuni:

1. Găsiţi obiectele care au fost asociate cu lista de autorizare deteriorată folosind comanda Pretindere spaţiu de stocare (RCLSTG). Reclamarea spaţiului de stocare asociază obiectele care erau asociate cu lista de autorizare la lista de autorizare QRCLAUTL.
2. Folosiţi comanda Afişare obiecte listă de autorizare (DSPAUTLOBJ) pentru a lista obiectele care sunt asociate cu lista de autorizare QRCLAUTL.
3. Folosiţi comanda Acordare autorizare obiect (GRTOBJAUT) pentru a securiza fiecare obiect cu lista corectă de autorizare:
   ```
   GRTOBJAUT OBJ(nume-bibliotecă/nume-obiect) +
             OBJTYPE(tip-obiect) +
             AUTL(nume-listă-autorizare)
   ```

Dacă un număr mare de obiecte sunt asociate cu lista de autorizare QRCLAUTL, creaţi un fişier bază de date specificând 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 dumneavoastră, 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.

Observaţii:

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

O înregistrare de auditare de securitate este scrisă pentru fiecare operaţie de restaurare dacă valoarea de auditare acţiune (valoarea de sistem QAUDLVL sau AUDLVL în 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 ar putea cauza probleme cu dimensiunea receptorului de jurnal de auditare, în special 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 System i

Această secţiune descrie tehnici pentru auditarea eficienţei securităţii de pe sistemul dumneavoastră.

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 această secţiune sunt corespunzătoare pentru toate aceste situaţii. Ce lucruri şi cât de des le auditaţi, depinde de dimensiunea şi nevoile de securitate ale organizaţiei dumneavoastră. Scopul acestei secţiuni este de a discuta că informaţiile sunt disponibile, cum să le obţineţi şi de ce sunt necesare, în loc de a da indicaţii pentru frecvenţa auditărilor.

Această secţiune 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 folosirea de comenzi în mediul System i şi accesarea informaţiilor istoric şi jurnal despre sistem. 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 din taskurile de auditare sugerate în această secţiune necesită un profil de utilizator cu autorizare specială *ALLOBJ şi *SECADM. Asiguraţi-vă că setaţi parola pentru profilul de auditare la *NONE, când s-a terminat perioada de auditare.

Concepte înrudite

“Jurnalul de auditare de securitate” la pagina 6
Puteţi folosi jurnalele de auditare de securitate pentru a audita eficienţa securităţii sistemului.

Listă de verificare pentru responsabili cu securitatea şi auditori

Puteţi folosi lista de verificare pentru a planifica şi audita securitatea sistemului.

Pe măsură ce planificaţi securitatea, alegeţi subiectele din această colecţie care se potrivesc cel mai bine cu cerinţele de securitate. Când auditaţi securitatea sistemului, folosiţi lista pentru a evalua elementele de control pe care le aveţi şi pentru a determina dacă sunt necesare elemente de control suplimentare.

Fiecare listă serveşte ca o trecere în revistă a informaţiilor din această colecţie de subiecte. Acestea conţine descrieri sumare a cum să faceţi fiecare element şi cum să verificaţi că elementul a fost făcut, inclusiv ce intrări din jurnalul QAUDJRN să căutaţi. Detalii despre elemente sunt găsite în această colecţie de subiecte.

Securitate fizică

Puteţi folosi lista de verificare securitate fizică pentru a planifica sau audita securitatea fizică din sistem.

Notă: Consultaţi Planning and setting up system security pentru o discuţie completă a securităţii fizice din produsul System i.

Aici este o listă de verificare pentru planificarea securităţii fizice a sistemului:

__ • 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. Cheile sunt înlăturate şi păstrate separat sub securitate fizică dură. Consultaţi Planificarea securităţii fizice pentru unitatea de sistem pentru informaţii suplimentare despre comutarea cheii IPL.

__ • 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.

__ • Semnarea pentru utilizatorii cu autorizarea specială *ALLOBJ sau *SERVICE este limitată la câteva staţii de lucru. Verificaţi că valoarea de sistem QLMTSECOFR este 1. Folosiţi comanda DSPOBJAUT pentru dispozitive, pentru a vedea dacă profilul QSECOFR are autorizarea *CHANGE.

Valorile de sistem

Setarea funcţiei de auditare pentru valori de sistem vă ajută să urmăriţi valorile modificate din 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.
- Folosiţi comanda Afişare atribute de securitate (DSPSECA) pentru a verifica valorile curente şi în aşteptare ale QSECURITY (nivel securitate) şi QPWDLVL (nivel parolă) şi setarea curentă a sistemul înrudit de securitate (dacă valorile pot fi modificate).
- Revedeţi deciziile despre valorile de sistem periodic. Aceasta este importantă în special când se modifică mediul sistemului, cum ar fi instalarea aplicaţiilor noi sau a unei reţele de comunicaţii.

Profilurile de utilizator furnizate de IBM

Puteţi realiza taskuri de auditare pe profiluri de utilizator livrate de IBM verificându-le parolele.

- 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 modificată prima dată când vă logaţi în sistemşi modificată 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.
- Parolele IBM pentru DST sunt modificate.

ID-urile utilizator pentru unelte service 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.

- Cu excepţia QSECOFR, nu semnaţi cu profilurile de utilizator livrate de IBM.

  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 profilurile de utilizator livrate de IBM listate în Anexa B, "profiluri de utilizator furnizate de IBM", la pagina 317, cu excepţia QSECOFR, au o parolă *NONE.

Concepte înrudite

"Profiluri de utilizator furnizate de IBM" la pagina 127
Împreună cu software-ul de sistem primiţi şi câteva profiluri de utilizator. Aceste profiluri de utilizator furnizate de IBM sunt folosite ca şi obiecte deţinute pentru funcţii de sistem variate. Unele funcţii sistem de asemenea rulează sub anumite profiluri de utilizator furnizate de IBM.

"Lucrul cu ID-uri utilizator unelte de service" la pagina 128
Sunt mai multe îmbunătăţiri adăugate la uneltele de service pentru această ediţie care le face mai uşor de folosit şi de înţeles.

Referinţe înrudite

Anexa B, "profiluri de utilizator furnizate de IBM", la pagina 317
Această secţiune conţine informaţii despre profilurile de 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 de utilizator furnizate de IBM.

Controlul parolei

Puteţi folosi mecanismul de control parolă pentru a audita securitatea sistemului dumneavoastră.

- 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 nivelul de parolă 3 şi utilizatorii îşi modifică parola, sistemul încearcă să creeze o parolă echivalentă care este folosibilă la alte niveluri de parolă. Puteţi utiliza comanda PRTUSRPRF TYPE(*PWDLVL) pentru a vedea ce profiluri de 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 parola BbAaA3x este specificat la nivelul de parolă 2, sistemul va crea o parolă echivalentă BBAAA3X de folosit la nivelurile de parolă 0 şi 1. Aceasta poate fi adevărat chiar dacă valoarea de sistem QPWDLMTCHR

include ’A’ ca unul din caracterele limitate (QPWDLMTCHR nu este forţat la nivelul de parolă 2) sau valoarea de sistem QPWDLMTREP a specificat că nu pot fi identice caracterele consecutive (deoarece verificarea este sensibilă la majuscule la nivelul de parolă 2 dar nu este sensibilă la majuscule la nivelurile de parolă 0 şi 1).

Profiluri de utilizator şi grup

Puteţi valida profilurile de utilizator şi grup şi autorizările lor pentru a audita eficienţa securităţii din sistem.

- Fiecărui utilizator îi este alocat un profil de utilizator unic.

  Setaţi valoarea de sistem QLMTDEVSSN la 1. Chiar dacă limitaţi fiecare utilizator la o singură sesiune dispozitiv o dată aceasta nu împiedică partajarea de profiluri de utilizator, ci o descurajează.
- Profilurile de utilizator cu autorizarea specială *ALLOBJ sunt limitate şi nu sunt utilizate ca profiluri de grup.

  Folosiţi comanda DSPUSRPRF pentru a verifica autoritările specialepentru profiluri de utilizator şi a determina ce profiluri sunt profiluri de grup. Subiectul “Tipărirea profilurilor de utilizator selectate” la pagina 301 arată cum se foloseşte un fişier de ieşire şi o interogare pentru a determina aceasta.
- Câmpul *Capabilităţi limită* este *YES în profilurile de utilizatorilor, care ar trebui să fie restricţionate la un set de meniuri.

  Subiectul “Tipărirea profilurilor de utilizator selectate” la pagina 301 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 241are 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 de utilizator mari” la pagina 302 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. Pentru a vă asigura cu profilurile de utilizator sunt şterse imediat după plecarea angajatului, revedeţi intrările DO (Ştergere obiect) din jurnalul de auditare.
- Gestionarea verifică în mod regulat utilizatorii autorizaţi pe sistem.

  Folosiţi comanda DSPAUTUSR pentru a vizualiza informaţiile de autorizare ale utilizatorilor.
- Parola pentru un angajat inactiv este setată la *NONE.

  Utilizaţi comanda DSPAUTUSR pentru a verifica faptul că profilurile de utilizatori inactivi nu au parole.
- Gestionarea verifică în mod regulat utilizatorii cu autorizări speciale, în particular, *ALLOBJ *SAVSYS şi autorizări speciale *AUDIT.

Subiectul “Tipărirea profilurilor de utilizator selectate” la pagina 301 oferă un exemplu despre modul în care se determină aceasta.

Controlul autorizării

Controlul autorizării vă permite să auditaţi securitatea informaţiilor stocate în sistem.

Puteţi folosi următoarea listă de verificare pentru a vă ajuta să auditaţi securitatea controluluiautorizării.

- 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 de utilizator.
- Date sensibile nu sunt publice. Verificare a autorizării pentru utilizator *PUBLIC pentru obiecte critice utilizând comanda DSPOBJAUT.
- Autorizarea pentru profilurile de utilizator este controlată.

  Autorizarea publică pentru profilurile de 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 parametrul *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 de 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 Enter în ecranul Semnare.

  Asiguraţi-vă că nicio intrare staţie de lucru din descrierile de subsisteme nu specifică o descriere de job care are specificat un nume de profil de utilizator pentru parametrul USER.

  Semnarea implicită este împiedicată 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 se încearcă semnarea implicită şi este definită o descriere de subsistem pentru a o permite.
- Lista de biblioteci din programele aplicaţie este controlată, pentru a împiedica adăugarea unei biblioteci ce conţine un program similar înainte de bibliotecile de producţie.

  Subiectul “Listele de biblioteci” la pagina 207 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 autorizare” la pagina 303 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.

Acces neautorizat

Folosiţi această listă de verificare împreună cu jurnal de auditare pentru a audita încercările neautorizate de a accesa informaţii.

- 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 semnare.

  Nivelurile de securitate 40 şi 50 impun aceasta. La nivelul 20 sau 30, trebuie să vă asiguraţi că nicio descriere de subsistem nu are vreo intrare staţie de lucru care foloseşte o descriere de job care are un nume de profil de utilizator.

Programe neautorizate

Comanda Verificare integritate obiecte (CHKOBJITG) vă permite să auditaţi modificările neautorizate ale programului de pe sistem.

- 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 care au fost modificate” la pagina 304

Comunicaţiile

Această listă de verificare poate fi folosită pentru a planifica şi audita elementele de control necesare peste diverse tipuri de comunicaţii din sistem.

- Folosiţi proceduri call-back pentru a proteja comunicaţiile telefonice.
- Folosiţi criptare la date importante.
- Controlaţi semnarea de la distanţă. Variabila de sistem QRMTSIGN este setată la *FRCSIGNON sau este folosit un program de validare passthrough.
- Folosiţi atributele de reţea JOBACN, PCSACC şi DDMACC pentru a control accesul la datele de pe alte sistem, inclusiv calculatoare personale. Atributul de reţea JOBACN trebuie să fie *FILE.

Folosirea jurnalului de auditare a securităţii

Jurnalul de auditare a securităţii este sursa primară de auditare a informaţiilor despre sistem. Această secţiune descrie cum să planificaţi, setaţi şi gestionaţi auditarea securităţii, ce informaţii sunt înregistrate şi cum să vizualizaţi acele informaţii.

Un auditor de securitate din interiorul sau exteriorul organizaţiei poate folosi funcţia de auditare care este furnizată de sistemul pentru a aduna informaţii despre evenimente legate de securitate care au loc în 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 de 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. Puteţi folosi un program de aplicaţii sau o unealtă de interogare pentru a analiza datele.

Referinţe înrudite

Anexa F, “Dispunerea intrărilor de jurnal de auditare”, la pagina 561
Această secţiune conţine informaţii de dispunere pentru toate tipurile de intrări cu codul de jurnal T în jurnalul de auditare (QAUDJRN). Aceste intrări sunt controlate de auditarea de acţiune şi de obiect pe care o definiţi dumneavoastră.

Anexa E, “Operaţii obiecte şi auditare”, la pagina 497
Această colecţie de subiecte listează operaţiile care pot fi realizate asupra obiectelor din sistem şi dacă acele operaţii sunt auditate.

Planificarea auditării securităţii

Funcţia de auditare a securităţii este opţională. Trebuie să efectuaţi anumiţi paşi pentru a seta auditarea securităţii.

Pentru a planifica folosirea auditării securităţii în sistem, urmaţi aceşti paşi:

- Determinaţi ce evenimente relevante de securitate doriţi să înregistraţi pentru toţi utilizatorii sistemului. Auditarea evenimentelor relevante pentru securitate este numită *auditare acţiuni*.
- 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 acţiunilor de auditare

Valoarea de sistem QAUDCTL (control auditare), valoarea de sistem QAUDLVL (nivel auditare), valoarea de sistem QAUDLVL2 (extensie nivel auditare) şi parametrul AUDLVL (auditare acţiune) din profilurile de utilizator lucrează împreună pentru a controla auditarea acţiunilor.

Funcţiile fiecărei valori de sistem sunt următoarele:

- 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 de 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 care alegeţi să le înregistraţi în istoric depind de obiectivele dumneavoastră de securitate şi de expunerile potenţiale. “Auditarea acţiunilor” la pagina 112 descrie valorile de nivel de auditare posibile şi cum le puteţi folosi. Arată dacă acestea sunt disponibile ca variabilă de sistem, parametru profil de utilizator sau ambele.

Referinţe înrudite

“Nivelul de auditare (QAUDLVL)” la pagina 67
Valoarea de sistem Nivel de auditare (QAUDLVL) împreună cu valoarea de sistem QAUDLVL2 determină ce evenimente legate de securitate sunt înregistrate în jurnalul de auditare securitate (QAUDJRN) pentru toţi utilizatorii sistemului.

“Extensia nivelului de auditare (QAUDLVL2)” la pagina 69
Valoarea de sistem Extensie nivel auditare (QAUDLVL2) este necesară când mai mult de şaisprezece valori de auditare sunt necesare.

“Auditarea acţiunilor” la pagina 112
Pentru un utilizator individual, puteţi să specificaţi ce 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.

Valorile de auditare acţiuni:

Această tabelă listează valorile posibile disponibile în valorile de sistem QAUDLVL şi QAUDLVL2 şi comanda CHGUSRAUD la auditarea de acţiuni ale sistemului.

Tabela 131. Valorile de auditare acţiuni

Valoare posibilă	Disponibilă în valorile de sistem QAUDLVL şi QAUDLVL2	Disponibilă în 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 de 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.
*ATNEVT	Da	Nu	**Evenimente atenţionare**: Sistemul scrie o intrare de jurnal pentru evenimente care necesită examinare ulterioară. Cu aceste informaţii, puteţi determina semnificaţia potenţială a evenimentului de atenţionare asupra sistemului.
*AUTFAIL	Da	Da	**Autorizare eşecuri**: Încercările eşuate de semnare pe 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.

Tabela 131. Valorile de auditare acţiuni (continuare)

Valoare posibilă	Disponibilă în valorile de sistem QAUDLVL şi QAUDLVL2	Disponibilă în comanda CHGUSRAUD	Descriere
*CMD	Nu	Da	**Comenzi**: Şirurile de comandă pentru înregistrare în istoric, ale sistemului, rulate de un utilizator. Dacă o comandă este rulatădintr-un program CL care este creat cu LOG(*NO) şi ALWRTVSRC(*NO), atunci doar numele comenzii şi numele bibliotecii sunt înregistrate în istoric. *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.
*JOBBAS	Yes	Yes	**Funcţii de bază job**: Acţiunile care afectează un job sunt înregistrate în istoric, cum ar fi pornirea sau oprirea unui job, blocarea, eliberarea, anularea sau modificarea jobului.
*JOBCHGUSR	Yes	Yes	**Utilizator modificare job**: Modificările asupra profilului de utilizator activ al unui fir de execuţie sau profilurilor de grup sunt înregistrate în istoric.
*JOBDTA	Da	Da	**Taskuri job**: Acţiunile care afectează un job sunt înregistrate în istoric, cum ar fi pornirea sau oprirea unui job, blocarea, eliberarea, anularea sau modificarea jobului, modificarea profilului de utilizator activ al firului de execuţie sau a profilului de grup. *JOBDTA poate fi folosit pentru a monitoriza cine rulează joburile batch. *JOBDTA este compus din două valori, care sunt *JOBBAS şi *JOBCHGUSR, pentru a vă permite să personalizaţi mai bine auditarea.
*NETBAS	Da	Yes	**Funcţii de bază reţea**: Acţiuni reguli IP, conexiuni socket-uri, filtru de căutare director APPN, filtru punct final APPN.
*NETCLU	Da	Yes	**Operaţii cluster sau grup resurse cluster**: O intrarea de jurnal de auditarea este scrisă când oricare din aceste evenimente are loc: • 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.

Tabela 131. Valorile de auditare acţiuni (continuare)

Valoare posibilă	Disponibilă în valorile de sistem QAUDLVL şi QAUDLVL2	Disponibilă în comanda CHGUSRAUD	Descriere
*NETCMN	Da	Yes	**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	Yes	**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	Yes	**Taskuri socket**: O intrare de jurnal de auditarea este scrisă când oricare din aceste evenimente are loc: • Este acceptată o conexiune de intrare socket TCP/IP. • Este stabilită 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 confidenţiale 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.
*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	Yes	**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.

Tabela 131. Valorile de auditare acţiuni (continuare)

Valoare posibilă	Disponibilă în valorile de sistem QAUDLVL şi QAUDLVL2	Disponibilă în comanda CHGUSRAUD	Descriere
*PRTDTA	Da	Yes	**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	**Operaţii restaurare** : *SAVRST poate fi folosit pentru a detecta încercările de restaurare a obiectelor neautorizate.
*SECCFG	Da	Yes	**Configuraţie securitate**: O intrare de jurnal de auditare este scrisă când oricare din aceste evenimente are loc: • Sunt create, modificate, şterse sau restaurate profiluri de 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	Yes	**Funcţii servicii director**: O intrare de jurnal de auditare este scrisă când oricare din aceste evenimente are loc: • Modificări sau actualizări se fac auditării, autorizării, parolelor şi dreptului de proprietate. • Legări şi dezlegări de succes. • Au fost făcute modificări asupra politicilor de securitate (de exemplu, politica de parolă)
*SECIPC	Da	Yes	**Comunicaţii interprocese**: O intrare de jurnal de auditare este scrisă când oricare din aceste evenimente are loc: • Se fac modificări dreptului de proprietate sau autorizării unui obiect IPC. • O creare, ştergere sau extragere a unui obiect IPC. • Ataşare de memorie partajată.

Tabela 131. Valorile de auditare acţiuni (continuare)

Valoare posibilă	Disponibilă în valorile de sistem QAUDLVL şi QAUDLVL2	Disponibilă în comanda CHGUSRAUD	Descriere
*SECNAS	Da	Yes	**Acţiuni servicii autentificare reţea**: O intrare de jurnal de auditare este scrisă când oricare din aceste evenimente are loc: • Tichet de serviciu invalid. • Principalii serviciului nu se potrivesc. • Principalii clientului nu se potrivesc. • Nepotrivire adresă IP tichet. • Decriptarea tichetului a eşuat. • Decriptarea autorizării a eşuat. • Regiunea 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 set de simboluri grafice acceptaţi: Acreditări expirate, eroare sumă de control sau legături de canal. • Pentru set de simboluri grafice unwrap sau set de simboluri grafice verificare: Context expirat, decriptare/decodificare, eroare sumă de control sau eroare de secvenţă.
*SECRUN	Da	Yes	**Funcţii de securitate la rulare**: Modificările privind dreptul de proprietate, autorizarea şi grupul primar al obiectului sunt scrise în jurnalul de auditare.
*SECSCKD	Da	Yes	**Descriptori socket**: O intrare de jurnal de auditare este scrisă când oricare din aceste evenimente are loc: • Un descriptor socket este acordat altui job. • Un descriptor socket este primit. • Un descriptor socket este inutilizabil.
*SECVFY	Da	Yes	**Funcţii de verificare**: O intrare de jurnal de auditare este scrisă când oricare din aceste evenimente are loc: • 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 de utilizator a fost autentificat. • Un profil destinaţie a fost modificat în timpul unei sesiuni passthrough.

Tabela 131. Valorile de auditare acţiuni (continuare)

Valoare posibilă	Disponibilă în valorile de sistem QAUDLVL şi QAUDLVL2	Disponibilă în comanda CHGUSRAUD	Descriere
*SECVLDL	Da	Yes	**Operaţii listă de validare**: O intrare de jurnal de auditare este scrisă când oricare din aceste evenimente are loc: • 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.

Intrări jurnal auditare securitate:

Acest subiect furnizează informaţii despre intrările de jurnal care sunt scrise pentru valorile de auditare acţiune specificate în valorile de sistem QAUDLVL şi QAUDLVL2 şi în profilul de utilizator.

Arată:

- Tipul intrării scrise pentru jurnalul QAUDJRN.

- Pentru a modela fişier bază de date de ieşire care poate fi folosit pentru a defini înregistrarea când creaţi un fişier de ieşire cu comanda DSPJRN. Machete complete pentru fişierele externe ale bazei de date model se găsesc în Anexa F, “Dispunerea intrărilor de jurnal de auditare”, la pagina 561.
- 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 132. Intrări jurnal auditare securitate

Valoare auditare acţiune sau obiect	Tip intrare jurnal	Fişier ieşire bază de date model	Intrare detaliată	Descriere
Auditare acţiune:				
*ATNEVT	IM	QASYIMJ5	P	O intruziune potenţială a fost detectată. Evaluări ulterioare sunt necesare pentru a determina dacă este vorba de o intruziune reală sau o acţiune aşteptată şi permisă.
*AUTFAIL	AF	QASYAFJE/J4/J5	A	A fost făcută o încercare de a accesa un obiect sau a realiza o operaţie la care utilizatorul nu a fost autorizat.
			B	Instrucţiune restricţionată
			C	Eşuare validare
			D	Folosirea unei interfeţe nesuportate, eşuare domeniu obiect
			E	Eroare protecţie spaţiu de stocare hardware, violare spaţiu constant program
			F	Eroare autorizare ICAPI.
			G	Eroare autentificare ICAPI.
			H	Final de scanare acţiune program.
			I	Moştenirea de sistem Java nu este permisă
			J	A fost făcută o încercare de a lansa sau planifica un job sub o descriere de job care are un profil de utilizator specificat. Lansatorul nu are autorizarea la profilul de utilizator.
			K	A fost făcută o încercare de a realiza o operaţie pentru care utilizatorul nu a avut autorizarea specială necesară.
			N	Jetonul de profil nu a fost un jeton de profil regenerabil.
			O	Eşuare autorizare obiect optic
			P	A fost făcută o încercare de a folosi un mâner de profil care nu este valid în API-ul QWTSETP.
			R	Eroare protecţie hardware
			S	Încercare de semnătură implicită
			T	Neautorizat pentru port TCP/IP.
			U	O cerere de permisiune utilizator nu a fost validă.
			V	Jetonul de profil nu a fost valid pentru generearea unui jeton de profil nou.

Tabela 132. Intrări jurnal auditare securitate (continuare)

Valoare auditare acţiune sau obiect	Tip intrare jurnal	Fişier ieşire bază de date model	Intrare detaliată	Descriere
			W	Jetonul de profil nu a fost valid pentru schimb.
			X	Violare sistem, vedeţi descrierea intrărilor de jurnal AF (eşuare autorizare) pentru detalii
			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.
	CV	QASYCVJ4/J5	E	Conexiune finalizată anormal.
			R	Conexiune refuzată.
	DI	QASYDIJ4/J5	AF	Eşuare autorizare.
			PW	Eşuare parolă.
	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.
			C	Eşuare CHKPWD.
			D	A fost introdus un nume utilizator DSTincorect.
			E	A fost introdus un nume utilizator DSTincorect.
			P	A fost introdusă o parolă incorectă.
			Q	Încercarea de autentificare utilizator a eşuat deoarece este dezactivat profilul de utilizator.
			R	Încercarea de autentificare utilizator a eşuat deoarece parola a fost expirată.
			S	SQL a decriptat o parolă care nu a fost validă.
			U	Numele utilizator nu este valid.
			X	Utilizatorul uneltelor de service este dezactivat.
			Y	Utilizatorul uneltelor de service nu este valid.
			Z	Parola uneltelor de service nu este validă.
	VC	QASYVCJE/J4/J5	R	O conexiune a fost refuzată din cauza parolei incorecte.
	VO	QASYVOJ4/J5	U	Verificare fără succes a unei intrări a listei de validare.
	VN	QASYVNJE/J4/J5	R	O logare în reţea a fost refuzată din cauza contului expirat, a orelor incorecte, a ID-ului de utilizator incorect sau a parolei incorecte.
	VP	QASYVPJE/J4/J5	P	A fost folosită parolă incorectă de reţea.

Tabela 132. Intrări jurnal auditare securitate (continuare)

Valoare auditare acţiune sau obiect	Tip intrare jurnal	Fişier ieşire bază de date model	Intrare detaliată	Descriere
	X1	QASYX1J5	F	Delegare jeton identitate eşuată.
			U	Obţinerea utilizatorului din jetonul identitate a eşuat.
	XD	QASYXDJ5	G	Nume de grup (asociat cu intrare DI)
*CMD [1]	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 [2]	CO	QASYCOJE/J4/J5	N	Creare de obiect nou, cu excepţia creării obiectelor din biblioteca QTTEMP.
			R	Înlocuirea obiectului existent.
	DI	QASYDIJ4/J5	CO	Obiect creat.
	XD	QASYXDJ5	G	Nume de grup (asociat cu intrare DI)
*DELETE [2]	DO	QASYDOJE/J4/J5	A	Obiect şters.
			C	Comitere ştergere în aşteptare.
			D	Creare în aşteptare dată înapoi.
			P	Ştergere în aşteptare.
			R	Ştergere în aşteptare dată înapoi.
	DI	QASYDIJ4/J5	DO	Obiect şters.
	XD	QASYXDJ5	G	Nume de grup (asociat cu intrare DI)
*JOBBAS	JS	QASYJSJ5	A	Comanda ENDJOBABN a fost folosită.
			B	A fost lansat un job.
			C	A fost modificat un job.
			E	A fost terminat un job.
			H	A fost reţinut un job.
			I	A fost deconectat un job.
			N	Comanda ENDJOB a fost folosită.
			P	O cerere de pornire program a fost ataşată la un job prepornit.
			Q	Atributele interogării au fost modificate.
			R	Un job reţinut a fost eliberat.
			S	A fost pornit un job.
			U	Comanda CHGUSRTRC.
*JOBCHGUSR	JS	QASYJSJ5	M	Modificare profil sau profil de grup.
			T	Modificare profil sau profil de grup folosind un jeton de profiluri.

Tabela 132. Intrări jurnal auditare securitate (continuare)

Valoare auditare acţiune sau obiect	Tip intrare jurnal	Fişier ieşire bază de date model	Intrare detaliată	Descriere
*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 i5/OS.
			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.
	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	Regulile IP au fost citite şi copiate într-un fişier.
			U	Au fost descărcate (înlăturate) reguli.
	IS	QASYISJ4/J5	1	Negociere faza 1.
			2	Negociere faza 2.
	ND	QASYNDJE/J4/J5	A	A fost detectată o violare la suportul de APPN Filter când a fost auditat filtrul de căutare director.

Tabela 132. Intrări jurnal auditare securitate (continuare)

Valoare auditare acţiune sau obiect	Tip intrare jurnal	Fişier ieşire bază de date model	Intrare detaliată	Descriere
	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 gestionare 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 gestionare 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	Negociere faza 1.
			2	Negociere faza 2.
	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
			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

Tabela 132. Intrări jurnal auditare securitate (continuare)

Valoare auditare acţiune sau obiect	Tip intrare jurnal	Fişier ieşire bază de date model	Intrare detaliată	Descriere
*OBJMGT [2]	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 distribuţie sistem.
*OPTICAL	O1	QASY01JE/J4/J5	R	Deschidere fişier sau director
			U	Schimbare 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	Copie de rezervă fişier sau director
			S	Salvare de fişier optic reţinut
			M	Mutare fişier
	O3	QASY03JE/J4/J5	I	Iniţializare volum
			B	Volum copie de rezervă
			N	Redenumire volum
			C	Convertire volum de copie de rezervă în 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 este folosită autorizarea adoptată pentru a obţine accesul la un obiect, nu când programul intră în stiva de apeluri.
			E	A fost oprit un program care adoptă autorizarea proprietarului. Intrarea de sfârşit este scrisă când programul iese din stiva de apeluri. Dacă acelaşi program are loc de mai multe ori în stiva de apeluri, intrarea de terminare este scrisă când cea mai înaltă apariţie (ultima) a programului părăseşte stiva.
			A	Autorizarea adoptată a fost folosită în timpul activării programului.
*PGMFAIL	AF	QASYAFJE/J4/J5	B	Un program rula o instrucţiune restricţionată de interfaţă de maşină.

Tabela 132. Intrări jurnal auditare securitate (continuare)

Valoare auditare acţiune sau obiect	Tip intrare jurnal	Fişier ieşire bază de date model	Intrare detaliată	Descriere
			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 înregistrării.
			D	Un program accesează un obiect printr-o interfaţă nesuportată sau programul apelabil nu este listat ca API apelabil.
			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	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 [2]	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. [3]
	RJ	QASYRJJE/J4/J5	A	O descriere de job ce conţine un nume de profil de utilizatore a fost restaurată.
	RO	QASYROJE/J4/J5	A	Proprietarul obiectului a fost modificat la QDFTOWN în timpul operaţiei de restaurare.[3]
	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 de 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.

Tabela 132. Intrări jurnal auditare securitate (continuare)

Valoare auditare acţiune sau obiect	Tip intrare jurnal	Fişier ieşire bază de date model	Intrare detaliată	Descriere
			O	Auditarea pentru un obiect a fost modificată cu comanda CHGOBJAUD sau CHGAUD.
			S	Atributul de scanare a fost modificat folosind comanda CHGATR sau API-ul Qp0lSetAttr sau când obiectul a fost creat.
			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 de 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 controlul comiterii
			C	A fost comisă ştergere în aşteptare a obiectului
			D	O creare în aşteptare a obiectului a fost rulată înapoi.
			P	Ştergerea obiectului este în curs (ştergerea a fost realizată sub controlul comiterii)
			R	O ştergere în curs de obiect 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.
			I	Iniţializare spaţiu variabilă de mediu.
	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.

Tabela 132. Intrări jurnal auditare securitate (continuare)

Valoare auditare acţiune sau obiect	Tip intrare jurnal	Fişier ieşire bază de date model	Intrare detaliată	Descriere
			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.
			E	Modificare opţiune
			F	Modifica atribut de jurnal 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.
			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 de utilizator a fost modificată.
			U	A fost modificată o înregistrare utilizator.
*SECDIRSRV	DI	QASYDIJE/J4/J5	AD	Modificare auditare.
			BN	Legătură reuşită.
			CA	Modificare autorizare
			CP	Modificare parolă
			OW	Modificare drept de proprietate
			PO	Modificare politică
			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	Decriptare a tichetului eşuat.

Tabela 132. Intrări jurnal auditare securitate (continuare)

Valoare auditare acţiune sau obiect	Tip intrare jurnal	Fişier ieşire bază de date model	Intrare detaliată	Descriere
			6	Decriptare a autentificatorului eşuat.
			7	Regiunea nu este în client şi regiunile locale.
			8	Tichetul este o încercare de repunere în funcţiune.
			9	Tichetul nu este încă valid.
			A	Decriptare eroare 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	Acceptare GSS - acreditare expirată
			L	Acceptare GSS - eroare sumă de control
			M	Acceptare GSS - legături canal
			N	Context expirat desfăşurare GSS sau verificare GSS
			O	Decriptare/decodificare desfăşurare GSS sau verificare GSS
			P	Eroare sumă de control desfăşurare GSS sau verificare GSS
			Q	Eroare secvenţială desfăşurare GSS sau verificare GSS
*SECRUN	CA	QASYCAJE/J4/J5	A	Modificări ale listei de autorizare sau ale autorizării obiectului.
	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 pentru un obiect a fost modificată cu comanda CHGOBJAUD sau CHGAUD.

Tabela 132. Intrări jurnal auditare securitate (continuare)

Valoare auditare acţiune sau obiect	Tip intrare jurnal	Fişier ieşire bază de date model	Intrare detaliată	Descriere
			S	Atributul de scanare a fost modificat de comanda CHGATR sau API-ul Qp01SetAttr
			U	Auditarea pentru un utilizator a fost modificată cu comanda CHGUSRAUD.
	X1	QASYADJE/J4/J5	D	Reuşire delegare jeton de identitate
			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 autorizării obiectului.
	CP	QASYCPJE/J4/J5	A	Operaţia de creare, modificare sau restaurare a unui profil de 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
			PO	Modificare politică
			UB	Dezlegare reuşită
	DO	QASYDOJE/J4/J5	A	Obiectul nu a fost şters sub controlul comiterii
			C	A fost comisă ştergere în aşteptare a obiectului
			D	O creare în aşteptare a obiectului a fost rulată înapoi.
			P	Ştergerea obiectului este în curs (ştergerea a fost realizată sub controlul comiterii)
			R	O ştergere în curs de obiect 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.

Tabela 132. Intrări jurnal auditare securitate (continuare)

Valoare auditare acţiune sau obiect	Tip intrare jurnal	Fişier ieşire bază de date model	Intrare detaliată	Descriere
	EV	QASYEVJ4/J5	A	Adăugare.
			C	Modificare.
			D	Ştergere.
			I	Iniţializare spaţiu variabilă de mediu.
	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 de utilizator destinaţie a fost modificat în timpul unei sesiuni passthrough.
			E	Un utilizator office a terminat lucrul în numele altui utilizator.
			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.

Tabela 132. Intrări jurnal auditare securitate (continuare)

Valoare auditare acţiune sau obiect	Tip intrare jurnal	Fişier ieşire bază de date model	Intrare detaliată	Descriere
			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 de utilizator autentificat.
	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.
			E	Modificare opţiune
			F	Modifica atribut de jurnal 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 de 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	Regiunea nu este în client şi regiunile locale.
			8	Tichetul este o încercare de repunere în funcţiune.
			9	Tichetul nu este încă valid.
			A	Decriptare eroare 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

Tabela 132. Intrări jurnal auditare securitate (continuare)

Valoare auditare acţiune sau obiect	Tip intrare jurnal	Fişier ieşire bază de date model	Intrare detaliată	Descriere
			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	Acceptare GSS - acreditare expirată
			L	Acceptare GSS - eroare sumă de control
			M	Acceptare GSS - legături canal
			N	Context expirat desfăşurare GSS sau verificare GSS
			O	Decriptare/decodificare desfăşurare GSS sau verificare GSS
			P	Eroare sumă de control desfăşurare GSS sau verificare GSS
			Q	Eroare secvenţială desfăşurare GSS sau verificare GSS
*SECVFY	PS	QASYPSJE/J4/J5	A	Un profil de utilizator destinaţie a fost modificat în timpul unei sesiuni passthrough.
	X1	QASYX1J5	D	Reuşire delegare jeton de identitate
			G	Primire utilizator de la jetonul identitate reuşit
			E	Un utilizator office a terminat lucrul în numele altui utilizator.
			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 de 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	A 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.

Tabela 132. Intrări jurnal auditare securitate (continuare)

Valoare auditare acţiune sau obiect	Tip intrare jurnal	Fişier ieşire bază de date model	Intrare detaliată	Descriere
			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 eliberat un fişier spool.
			S	A fost salvat un fişier spooled.
			T	A fost restaurat un fişier spooled.
			U	A fost modificat un fişier spool.
			V	Doar atributele fişierelor spooled care nu sunt relevante pentru securitate au fost modificate.
*SYSMGT	DI	QASYDIJ4/J5	CF	Modificări de configurare
			CI	Creare instanţă
			DI	Ştergere instanţă
			RM	Gestionarea replicărilor
	SM	QASYSMJE/J4/J5	B	Opţiunile de salvare de rezervă au fost modificate folosind xxxxxxxxxx.
			C	Opţiunile de curăţare automată au fost modificate folosind xxxxxxxxxx.
			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 salvare de rezervă a fost modificată folosind xxxxxxxxxx.
			P	Planificarea de 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
Auditare obiect:				
*CHANGE	DI	QASYDIJ4/J5	IM	Import director LDAP
			ZC	Modificare obiect
	ZC	QASYZCJ4/J5	C	Modificări obiect
			U	Modernizare a accesului deschis către un obiect

Tabela 132. Intrări jurnal auditare securitate (continuare)

Valoare auditare acţiune sau obiect	Tip intrare jurnal	Fişier ieşire bază de date model	Intrare detaliată	Descriere
	AD	QASYADJEJ4/J5	D	Auditarea unui obiect a fost modificată cu comanda CHGOBJAUD.
			O	Auditarea unui obiect a fost modificată cu comanda CHGOBJAUD.
			S	Atributul de scanare a fost modificat de comanda CHGATR sau API-ul 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 autorizării 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 înregistrare funcţie[5]
	LD	QASYLDJE/J4/J5	L	Legătură la un director.
			U	Dezlegare de la un 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.

Tabela 132. Intrări jurnal auditare securitate (continuare)

Valoare auditare acţiune sau obiect	Tip intrare jurnal	Fişier ieşire bază de date model	Intrare detaliată	Descriere
	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.
	ZC	QASYZCJE/J4/J5	C	Un obiect a fost modificat.
			U	Modernizare a accesului deschis către un obiect.
*ALL [4]	CD	QASYCDJ4/J5	C	Rulare comandă
	DI	QASYDIJ4/J5	EX	Export director LDAP
			ZR	Citire obiect
	GR	QASYGRJ4/J5	F	Operaţii înregistrare funcţie[5]
	LD	QASYLDJE/J4/J5	K	Căutaţi într-un director.
	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 parametrul AUDLVL al unui profil de utilizator. Nu este o valoare pentru variabila de sistem QAUDLVL,

[2] 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.

[3] Vedeţi acest subiect “Restaurarea obiectelor” la pagina 249 pentru informaţii despre modificările de autorizare care pot apărea când un obiect este restaurat.

[4] Când este specificat *ALL, intrările pentru *CHANGE şi *ALL sunt scrise.

[5] Când obiectul QUSRSYS/QUSEXRGOBJ *EXITRG este auditat.

Planificarea auditării accesului la obiecte

Sistemul de operare i5/OS furnizează abilitatea de a înregistra în istoric accesele la un obiect din jurnal de auditare de securitate folosind valori de sistem şi valorile de auditare obiecte pentru utilizatori şi obiecte. Aceasta este numită *auditare obiecte*.

Variabila de sistem QAUDCTL, valoarea OBJAUD pentru un obiect şi valoarea OBJAUD pentru un profil de 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 133 arată cum lucrează împreună valorile OBJAUD pentru obiect şi profilul de utilizator.

Tabela 133. Cum lucrează împreună auditarea de obiecte şi de utilizatori

	Valoare OBJAUD utilizator		
Valoare OBJAUD obiect	***NONE**	***CHANGE**	***ALL**
*NONE	Fără	Fără	Fără
*USRPRF	Fără	Modificare	Modificare şi utilizare
*CHANGE	Modificare	Modificare	Modificare
*ALL	Modificare şi utilizare	Modificare şi utilizare	Modificare şi utilizare

Puteţi folosi auditarea de obiecte pentru a urmării toţi utilizatorii care accesează un obiect critic din sistem. Puteţi de asemenea folosi auditarea de obiecte pentru a urmări toate obiectele care sunt accesate de un anumit utilizator. Auditarea de obiecte este o unealtă flexibilă care vă permite să monitorizaţi acele accese la obiecte care sunt importante pentru organizaţia dumneavoastră.

Folosirea capabilităţilor de auditare a obiectelor necesită o planificare atentă. O auditare proiectată slab ar putea genera mult mai multe înregistrări de auditare decât puteţi analiza. Aceasta poate avea un efect grav asupra performanţei 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.

Aici sunt câteva exemple despre cum să folosiţi auditarea de obiecte.

- 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 de utilizator la *NONE sau înlăturaţi *OBJAUD de la variabila de sistem QAUDCTL.
  5. Analizaţi intrările jurnalului de auditare folosind tehnicile descrise în “Analizarea intrărilor jurnalului de auditare cu o interogare sau cu un program” la pagina 296.
- Dacă vă interesează cine foloseşte un anumit fişier, puteţi colecta informaţii despre toate accesele la fişier într-o perioadă de timp:
  1. Setaţi auditarea obiectului pentru fişier, independent de valorile profilului de utilizator:

     ```
     CHGOBJAUD OBJECT(nume-bibliotecă/nume-fişier)
               OBJTYPE(*FILE)  OBJAUD(*CHANGE sau *ALL)
     ```

  2. Asiguraţi-vă că valoarea 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 jurnalului de auditare cu o interogare sau cu un program” la pagina 296
- 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 de utilizator specific la *CHANGE sau *ALL folosind comanda CHGUSRAUD.
3. Asiguraţi-vă că variabila de sistem QAUDCTL include *OBJAUD.
4. După ce aţi colectat un exemplu particular, setaţi valoarea OBJAUD pentru profilul de utilizator la *NONE.

Referinţe înrudite

“Auditare obiecte” la pagina 111
Valoarea de auditare obiect pentru un profil de utilizator lucrează împreună cu valoarea de auditare obiect pentru un obiect pentru a determina dacă accesul utilizatorului la un obiect este auditat.

Afişarea auditării obiectelor:

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 valoarea de sistem QCRTOBJAUD şi valoarea CRTOBJAUD pentru bibliotecile şi directoarele pentru a seta auditarea obiectelor pentru obiectele nou 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 de informaţii de auditare

Cele două variabile de sistem controlează ceea ce face sistemul când condiţiile de eroare pot determina pierderea intrărilor de jurnal de auditare.

Nivel forţă auditare

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 intrări pe spaţiu de stocare auxiliar, sistemul echilibrează efectul asupra performanţei cu pierderea potenţială de informaţii într-o pană de curent. *SYS este alegerea implicită.

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 terminarea auditării

Valoarea de sistem Acţiune terminare auditare (QAUDENDACN) determină ce acţiune execută sistemul dacă nu poate scrie intrări în jurnalul de auditare.

Valoarea implicită este *NOTIFY. Sistemul realizează următoarele taskuri dacă nu poate scrie intrări în jurnalul 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 cozii de 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 finaliza IPL-ul, logaţi-vă în consolă folosind un utilizator cu autorizare specială *ALLOBJ şi *AUDIT.

   Sistemul porneşte într-o stare restricţionată cu un mesaj ce indică faptul că eroarea de auditare a cauzat oprirea sistemului.
3. Variabila de sistem QAUDCTL este setată la *NONE.
4. Pentru a restaura sistemul la normal, setaţi valoarea de sistem QAUDCTL la o valore diferită de *NONE. 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 resetaţi valoarea QAUDCTL.

Alegerea de a nu audita obiecte QTEMP

Puteţi alege să nu auditaţi obiecte QTEMP specificând valoarea *NOQTEMP.

Valoarea, *NOQTEMP, poate fi specificată ca o valoare pentru valoarea de sistem QAUDCTL. Dacă folosiţi valoarea *NOQTEMP, trebuie de asemenea să specificaţi *OBJAUD sau *AUDLVL pentru QAUDCTL. 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 obiecte din QTEMP (tipuri de intrări jurnal CA, OW, PG).

Folosirea CHGSECAUD pentru a seta auditarea securităţii

Privire generală:

Folosind comanda CHGSECAUD, puteţi activa auditarea sistemului de securitate pentru acţiuni asigurându-vă că jurnalul de securitate există, setând valoarea de sistem QAUDCTL la *AUDLVL şi setând valoarea de sistem QAUDLVL la setul implicit de valori. Setul implicit include auditările de acţiune *AUTFAIL, *CREATE, *DELETE, *SECURITY şi *SAVRST.

```
CHGSECAUD QAUDCTL(*AUDLVL) QAUDLVL(*DFTSET)
```

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)

Notă: Comanda CHGSECAUD creează jurnalul şi receptorul jurnal, dacă acesta nu există. CHGSECAUD setează apoi variabilele de sistem QAUDCTL, QAUDLVL şi QAUDLVL2.

Referinţe înrudite

“Opţiuni din meniul Unelte de securitate” la pagina 699
Puteţi folosi meniul Unelte de securitate (SECTOOLS) pentru a simplifica gestionarea şi controlul securităţii sistemului cu multele opţiuni şi comenzi pe care le furnizează.

Setarea auditării securităţii

Cu auditarea securităţii, puteţi colecta informaţii despre evenimentele de securitate din jurnalul QAUDJRN.

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 poată fi modificat, altfel funcţia de auditare a sistemului nu cunoaşte numele jurnalului şi nu îl va găsi.

Pentru a seta auditarea securităţii, faceţi paşii următori. Aveţi nevoie de autorizare specială *AUDIT pentru a finaliza aceşti paşi.

1. Creaţi un receptor de jurnal într-o bibliotecă la alegere folosind comanda Creare receptor jurnal (CRTJRNRCV). Acest exemplu foloseşte o bibliotecă numită JRNLIB pentru receptori de jurnal.

```
CRTJRNRCV  JRNRCV(JRNLIB/AUDRCV0001) +
           THRESHOLD(100000) AUT(*EXCLUDE)   +
           TEXT('Auditare receptor jurnal')
```

   a. 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.
   b. 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.

      Este foarte util să folosiţi acest tip de convenţie de numire dacă alegeţi ca sistemul să gestioneze receptorii de jurnal.
   c. Specificaţi un prag de receptor adecvat mărimii şi activităţii sistemului dumneavoastră. Dimensiunea pe care o alegeţi ar trebui să fie bazată pe numărul de tranzacţii din sistem şi numărul de acţiuni pe care alegeţi să le auditaţi. Dacă folosiţi suport gestionare jurnal modificare sistem, pragurile recetorilor de jurnal trebuie să fie minim 100 000 KB. Pentru informaţii suplimentare despre pragul receptorului de jurnal, consultaţi Gestionarea jurnalului.
   d. Specificaţi *EXCLUDE în parametrul AUT pentru a limita accesul la informaţiile care sunt stocate în jurnal.
2. Creaţi jurnalul QSYS/QAUDJRN folosind comanda Creare jurnal (CRTJRN):

```
CRTJRN  JRN(QSYS/QAUDJRN) +
        JRNRCV(JRNLIB/AUDRCV0001) +
        MNGRCV(*SYSTEM) DLTRCV(*NO) +
        AUT(*EXCLUDE) TEXT('Auditare jurnal')
```

   - Trebuie folosit numele QSYS/QAUDJRN.
   - Specificaţi numele recetorului de jurnal pe care l-aţi creat în 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 a face ca sistemul să modifice receptorul de jurnal şi să ataşeze unul nou când receptorul ataşat depăşeşte pragul specificat în crearea receptorului de 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 şteargă receptorii detaşaţi. Specificaţi DLTRCV(*NO), care este implicit. Receptorii QAUDJRN reprezintă coada dumneavoastră de auditare a securităţii. Asiguraţi-vă că sunt salvate adecvat înainte de a le şterge din sistem.

   Subiectul Gestionare jurnal furnizează mai multe informaţii despre lucrul cu jurnale şi receptorii jurnal.

3. Setaţi valoarea de sistem nivel de auditare (QAUDLVL) sau valoarea de sistem 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 acţiunilor de auditare" la pagina 263.
4. Dacă este necesar, setaţi auditarea acţiunilor pentru utilizatori individuali folosind comanda CHGUSRAUD. Vedeţi"Planificarea acţiunilor de auditare" la pagina 263.
5. Dacă este necesar, setaţi auditarea obiectelor pentru anumite obiecte folosind comenzile CHGOBJAUD, CHGAUD şi CHGDLOAUD. Vedeţi"Planificarea auditării accesului la obiecte" la pagina 286.
6. Dacă este necesar, setaţi auditarea obiectelor pentru anumiţi utilizatori 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 terminarea auditării" la pagina 289.
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 de informaţii de auditare" la pagina 288.
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 jurnalelor de auditare şi receptorilor de jurnal

Sistemul furnizează un mecanism pentru gestionarea jurnalului de auditare şi a receptorilor de jurnal. Puteţi folosiţi metodele descrise în acest subiect pentru a audita securitatea din sistem.

Jurnalul de auditare QSYS/QAUDJRN este intenţionat doar pentru securitatea securităţii. Obiectele nu trebuie să fie jurnalizate în jurnalul de auditare. Controlul obligaţiilor nu trebuie să folosească jurnalul de auditare. Intrările utilizatornu ar trebui trimise în acest jurnal folosind comanda Trimitere intrare jurnal (SNDJRNE) sauAPI-ul Trimitere intrare jurnal (QJOSJRNE).

Sistemul foloseşte protecţie specială de blocare pentru a se asigura că 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
- Mutare a jurnalului
- Restaurare a jurnalului
- Comanda WRKJRN

Informaţiile înregistrate în intrările jurnal securitate sunt descrise în Anexa F, "Dispunerea intrărilor de jurnal de auditare", la pagina 561. 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 este numiăt *gestionare modificare jurnal sistem*.

Dacă specificaţi MNGRCV(*USER) pentru QAUDJRN, este trimis un mesaj cozii de mesaje prag care a fost specificată pentru jurnal când receptorul de jurnal atinge un prag de spaţiu de stocare. Mesajul indică faptul că receptorul a atins pragul său. Folosiţi comanda CHGJRN pentru a detaşa receptorul şi a ataşa un nou receptor de jurnal. Aceasta împiedică condiţiile eroare *Intare nejurnalizată* Dacă primiţi un mesaj, trebuie să folosiţi comanda CHGJRN pentru ca auditarea securităţii să continue.

Coada implicită de mesaje pentru un jurnal este QSYSOPR. Dacă instalarea are un volum mare de mesaje în coada de mesaje QSYSOPR, puteţi asocia o coadă de mesaje diferită, cum ar fi 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 gestionare modificare jurnal sistem, atunci mesajul CPF7020 este trimis cozii de mesaje jurnal când o modificare de jurnal sistem se termină. Puteţi monitirza acest mesaj astfel încât să ştiţi când să faceţi o salvare a receptorilor de jurnal detaşaţi.

Atenţie: Funcţia de curăţare automată care este furnizată la folosirea meniurilor Operational Assistant nu curăţă receptorii QAUDJRN. Pentru a evita probleme cu spaţiu pe disc, detaşaţi regulat, salvaţi şi ştergeţi receptori QAUDJRN.

Vedeţi subiectul Gestionarea jurnalului pentru informaţii complete despre gestionarea jurnalelor şi a receptorilor de jurnal.

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.

Informaţii înrudite

Gestionarea jurnalelor

Salvarea şi ştergerea receptorilor de jurnal de auditare

Ar trebui să detaşaţi regulat receptorul de jurnal de auditare curent şi să ataşaţi unul nou.

Privire generală:

Scop: Ataşaţi un nou receptor de jurnal de auditare; salvaţi şi ştergeţi receptorul vechi

Cum se face:

- CHGJRN QSYS/QAUDJRN JRNRCV(*GEN)
- 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 mari de jurnal pot afecta performanţa sistemul şi ocupa spaţiu preţios din spaţiul de stocare auxiliar.

Este sugerat ca sistemul să gestioneze receptorii automat. 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 în care se află receptorul de jurnal.

Puteţi folosi comanda CHGJRN pentru a detaşa un receptor şi a ataşa unul nou.

Receptori de jurnal gestionaţi de sistem:

Puteţi urma paşii descrişi în acest subiect pentru a salva sau şterge receptorii de jurnal.

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 corespunzătoare.
3. Folosiţi comanda SAVOBJ pentru a salva fiecare receptor. Nu primiţi receptorul ataşat momentan.
4. Folosiţi comanda DLTJRNRCV pentru a şterge fiecare receptor după ce este salvat.

O alternativă la procedura precedentă poate fi făcută folosind coada de mesaje jurnal şi monitorizarea pentru mesajul CPF7020 care indică că jurnalul de modificare sistem s-a terminat cu succes.

Informaţii înrudite

Salvare de rezervă şi recuperare

Receptori de jurnal gestionaţi de utilizator:

Puteţi urma paşii descrişi aici pentru a detaşa, salva sau şterge receptori de jurnal manual.

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, veţi primi un mesaj de avertisment.

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 valoarea de sistem QAUDCTL la *NONE. Aceasta opreşte sistemul de la înregistrarea în continuare a altor evenimente.
2. Detaşaţi receptorul curent de jurnal folosind comanda CHGJRN.
3. Salvaţi şi ştergeţi receptorul detaşat, folosind comenzile SAVOBJ şiDLTJRNRCV.

4. Puteţi şterge jurnalul QAUDJRN după ce l-aţi modificat pe QAUDCTL la *NONE. Dacă aveţi de gând să continuaţi auditarea securităţii în viitor, ar trebui să lăsaţi jurnalul QAUDJRN în sistem.

   Dacă jurnalul QAUDJRN este setat cu MNGRCV(*SYSTEM), sistemul detaşează receptorul şi ataşează unul nou oricând realizaţi un IPL, 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 de jurnal de auditare

După ce aţi setat funcţia de auditare securitate, puteţi folosi diverse metode pentru a analiza evenimentele care sunt înregistrate în istoric.

- Vizualizaţi intrările selectate la staţia de lucru folosind comanda Afişare jurnal (DSPJRN).
- Copiaţi intrările selectate în fişiere de ieşire folosind comanda Copiere intrări jurnal auditare (CPYAUDJRNE) sau DSPJRN şi apoi folosind o unealtă de interogare sau un program pentru a analiza intrările.
- Folosiţi comanda Afişare intrări jurnal auditare (DSPAUDJRNE).

  Notă: IBM a încetat să furnizeze îmbunătăţiri pentru comanda DSPAUDJRNE. Comanda nu suportă toate tipurile de înregistrări de auditare a securităţii şi nu listează toate câmpurile pentru înregistrările pe care ea le suportă.
- Folosiţi comanda Primire intrare jurnal (RCVJRNE) în jurnalul QAUDJRN pentru a primi intrările cum sunt scrise în jurnalul QAUDJRN.

Vizualizarea intrărilor de jurnal 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 semnare (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 . . . . . :                  Library  . . . . . :
Member . . . . . :
Incomplete data  . . :   No          Minimized entry data : *None
Sequence . . . . . :   1198
Code . . . . . :   T  - Audit trail entry
Type . . . . . :   CO - Create object

            Entry specific data
Column      *...+....1....+....2....+....3....+....4....+....5
00001      'NISAVLDCK  QSYS      *PGM    CLE                  '
00051      '                                                  '
00101      '                                                  '
00151      '                                                  '
00201      '                                                  '
00251      '                                                  '
00301      '                                                  '

                                                                More...
Press Enter to continue.

F3=Exit   F6=Display only entry specific data
F10=Display only entry details    F12=Cancel    F24=More keys
```

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, “Dispunerea intrărilor de jurnal de auditare”, la pagina 561 conţine modelul pentru fiecare tip al intrării jurnal QAUDJRN.

Analizarea intrărilor jurnalului de auditare cu o interogare sau cu un program

Privire generală:

Scop: Afişare sau printare a informaţiilor selectate din intrările jurnal.

Cum se face:

DSPJRN OUTPUT(*OUTFILE), Creaţi o interogare sau un program sau Rulaţi o interogare sau un program

Autorizare:

Autorizare *USE pentru autorizare QSYS/QAUDJRN, autorizare *USE pentru receptor jurnal, autorizare *ADD pentru biblioteca pentru fişier ieşire

Puteţi folosi comanda DSPJRN (Display Journal - Afişare jurnal) pentru a scrie intrările selectate din receptorii jurnalului de auditare într-un fişier de ieşire. Puteţi folosi programul sau interogarea pentru a vedea informaţiile din fişierul de 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 înregistrare QJORDJE5) este furnizat pentru a defini aceste câmpuri când specificaţi *TYPE5 ca parametru format ieşire. Consultaţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561 pentru mai multe informaţii.

Pentru informaţii suplimentare despre alte înregistrări şi formatele fişierelor de ieşire, consultaţi Anexa F, “Dispunerea intrărilor de jurnal de auditare”, la pagina 561.

Dacă doriţi să realizaţi o analiză detaliată a unui tip particular de intrare, folosiţi unul din fişierele bază de date model furnizate. Tabela 132 la pagina 270 arată numele fişierului bază de date model pentru fiecare tip de intrare. Anexa F, “Dispunerea intrărilor de jurnal de auditare”, la pagina 561 arată dispunerile de fişiere pentru fiecare fişier de ieşire de tip bază de date.

De exemplu, pentru a crea un fişier ieşire numit AUDJRNAF5 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 AUDJRNAF5.

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 Semnare. 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 despre 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 132 la pagina 270arată care intrare jurnal este scrisă pentru fiecare mesaj de încălcare a autorizării.

Relaţia Modificare dată/oră obiect cu înregistrările de auditare

Rapoartele scrise pentru a detecta modificări în programe sau alte obiecte sunt uneori bazate pe câmpul Change Date/Time al obiectului în loc de informaţii din jurnalul audit de securitate. Următoarea listă descrie motivele pentru care ar putea exista o diferenţă între date de pe obiect şi data sursei pentru obiect.

- Comanda CHGPGM este folosită pentru a forţa reconstruirea programului pentru a actualiza câmpul Modificare dată/oră a programului. Această operaţie scrie o înregistrare de auditare ZC (Modificare obiect)
- API-ul Semnare obiect (QYDOSGNO) este folosit pentru a semna digital un program sau o comandă pentru a actualiza câmpul Modificare dată/oră pentru program sau comandă. Această operaţie scrie o înregistrare de auditare ZC.

Sistemul de operare poate de asemenea actualiza automat câmpul Change Date/Time al unui obiect în următoarele situaţii:

- Când un profil de utilizator are autorizare privată asupra unui obiect şi acel obiect este apoi şters, sistemul actualizează câmpul Change Date/Time al acelui profil de utilizator pe măsură ce înlătură acea autorizare privată.
- Dacă auditarea de securitate este pornită când obiectul este şters, o înregistrare de auditare DO (Delete Operation) este scrisă pentru obiectul şters.
- Deoarece sistemul actualizează automat fiecare profil de utilizator care are autorizare privată asupra obiectului şters, nu sunt scrise înregistrări de auditare pentru acele profiluri de utilizator, chiar dacă câmpurile lor Change Date/Time sunt actualizate.

Pentru a urmări când utilizatorii au folosit interfeţe de sistem normale pentru a modifica obiecte, folosiţi jurnalului de auditare securitate. Rapoartele de detectare modificări asupra obiectelor care sunt bazate doar pe câmpul Change Date/Time al unui obiect pot produce rezultate parţiale.

De ce nu ar trebui să folosiţi câmpul Dată/oră pentru auditarea generală a securităţii

Indicaţia principală folosită pentru a decide ce să se auditeze pentru i5/OS este să auditeze acţiunile utilizatorilor care au relevanţă pentru securitate. A doua indicaţie este să nu se scrie înregistrări de auditare pentru operaţiile pe care sistemul de operare le face automat. În unele cazuri, operaţiile automate pot fi auditate dacă sistemul de operare realizează operaţia folosind o funcţie care este de asemenea proiectată să fie folosită de către utilizatori.

Obiectivele pentru menţinerea câmpului Change Date/Time al unui obiect sunt diferite faţă de obiectivele auditării. Scopul principal al câmpului Modificare dată/oră este de a indica când este modifica un obiect. Un câmp actualizat Change Date/Time nu indică ce a fost modificat la obiect sau cine a făcut modificarea. Una dintre utilizările principale ale acestui câmp este acela de a indica faptul că obiectul ar trebui salvat cu comanda Save Changed Objects (SAVCHGOBJ). Comanda SAVCHGOBJ nu trebuie să ştie când a fost făcută ultima modificare, doar că obiectul a fost modificat de când a fost salvat ultima oară. Această caracteristică permite optimizarea performanţelor pentru fişiere baze de date. Câmpul Change Date/Time este actualizat doar prima oară când fişierul este modificat după ce a fost salvat ultima oară. Performanţa poate fi afectată dacă câmpul Modificare dată/oră a fost actualizat de fiecare dată când o înregistrare din fişier a fost actualizată, adăugată sau ştearsă.

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 în Anexa G, “Comenzi şi meniuri pentru comenzi de securitate”, la pagina 699. Această secţiune include exemple pentru a folosi comenzile şi informaţiile despre meniurile pentru uneltele de securitate.

Monitorizarea mesajelor de securitate

Unele evenimente relevante de securitate, precum încercările de semnare 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.

Folosirea istoricului de sistem

Nu tate mesajele de eşuare autorizare şi violare integritate sunt găsite în istoricul QHST. Aceste mesaje sunt listate aici.

Unele evenimente în relaţie cu securitatea, precum depăşirea încercărilor de semnare 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 i5/OS, unele mesaje privind eşecul autorizării şi violarea integrităţii nu mai sunt trimise în istoricul (istoria) QHST. Toate informaţiile care au fost disponibile în istoricul 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 pot fi capturate în jurnalul audit prin specificarea *AUTFAIL pentru variabila de sistem QAUDLVL.
- CPF2240. Aceste evenimente pot fi capturate în jurnalul audit prin specificarea *AUTFAIL pentru variabila de sistem QAUDLVL.
- CPF2220. Aceste evenimente pot fi capturate în jurnalul audit prin specificarea *AUTFAIL pentru variabila de sistem QAUDLVL.
- CPF4AAE. Aceste evenimente pot fi capturate în jurnalul audit prin specificarea *AUTFAIL pentru variabila de sistem QAUDLVL.

- CPF2246. Aceste evenimente pot fi capturate în jurnalul audit prin specificarea *AUTFAIL pentru variabila de sistem QAUDLVL.

Folosirea jurnalelor pentru monitorizarea activităţii obiectelor

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. Consultaţi subiectul Gestionarea jurnalului pentru o listă de tipuri de obiecte care pot fi jurnalizate şi 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, utilizatorul şi timpul de acces
- Imagini înainte şi după modificările tuturor obiectelor
- Înregistrări când obiectul a fost deschis, închis, modificat, salvat, creat, şters şi aşa mai departe.

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 un fişier bază de date, zonă de date, coadă de date, bibliotecă sau obiect sistem de fişiere integrat, puteţi folosi comanda DSPJRN pentru a tipări toate modificările pentru acel obiect particular. Acestea sunt câteva exemple:

```
| Tastaţi următoarea comandă pentru un anumit  fişier bază de date.
| DSPJRN JRN(bibliotecă/jurnal) +
|        FILE(bibliotecă/fişier) OUTPUT(*PRINT)
|
| Tastaţi următoarea comandă pentru un anumit fişier zonă de date.
| DSPJRN JRN(bibliotecă/jurnal) +
|        OBJ((bibliotecă/nume obiect *DTAARA))  OUTPUT(*PRINT)
|
| Tastaţi următoarea comandă pentru un anumit fişier coadă de date.
| DSPJRN JRN(bibliotecă/jurnal) +
|        OBJ((bibliotecă/nume obiect *DTAQ)  OUTPUT(*PRINT)
|
| Tastaţi următoarea comandă pentru un anumit sistem integrat de fişiere.
| DSPJRN JRN(bibliotecă/jurnal) +
|        OBJPATH(('nume cale')) OUTPUT(*PRINT)
|
| Tastaţi următoarea comandă pentru o anumită bibliotecă.
| DSPJRN JRN(bibliotecă/jurnal) +
|        OBJ(*LIBL/nume-bibliotecă *LIB) OUTPUT(*PRINT)
```

De exemplu, dacă jurnalul JRNCUST din biblioteca CUSTLIB este folosit pentru a înregistra informaţii despre fişierul CUSTFILE (de asemenea din biblioteca CUSTLIB), comanda poate fi:

```
DSPJRN JRN(CUSTLIB/JRNCUST) +
       FILE(CUSTLIB/CUSTFILE) OUTPUT(*PRINT)
```

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.

Tastaţi următoarea comandă pentru a crea un fişier de ieşire pentru un anumit fişier bază de date.

```
DSPJRN JRN(bibliotecă/jurnal) +
                  FILE(bibliotecă/nume fişier) +
               OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(bibliotecă/fişier de ieşire) ENTDTALEN(*CALC)
```

Tastaţi următoarea comandă pentru a crea un fişier de ieşire pentru o anumită zonă de date.

```
DSPJRN JRN(bibliotecă/jurnal) +
                  OBJ((bibliotecă/nume obiect *DTAARA)) +
               OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(bibliotecă/fişier de ieşire) ENTDTALEN(*CALC)
```

Tastaţi următoarea comandă pentru a crea un fişier de ieşire pentru un anumit fişier coadă de date.

```
DSPJRN JRN(bibliotecă/jurnal) +
                  OBJ((bibliotecă/nume obiect *DTAQ)) +
               OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(bibliotecă/fişier de ieşire) ENTDTALEN(*CALC)
```

Tastaţi următoarea comandă pentru a crea un fişier de ieşire pentru un anumit obiect sistem de fişier integrat.

```
DSPJRN JRN(bibliotecă/jurnal) +
                  OBJPATH(('nume cale')) +
               OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(bibliotecă/fişier de ieşire) ENTDTALEN(*CALC)
```

Tastaţi următoarea comandă pentru a crea un fişier de ieşire pentru o anumită bibliotecă.

```
DSPJRN JRN(bibliotecă/jurnal) +
                  OBJ((*LIBL/nume-bibliotecă *LIB)) +
               OUTPUT(*OUTFILE) OUTFILEFMT(*TYPE5) OUTFILE(bibliotecă/fişier de ieşire) ENTDTALEN(*CALC)
```

Dacă vreţi să aflaţi care jurnale sunt în sistem, folosiţi comanda Lucru cu jurnale (WRKJRN). Dacă vreţi să aflaţi care obiecte sunt jurnalizate de un anumit jurnal, folosiţi comanda Lucru cu atribute jurnal (WRKJRNA).

Informaţii înrudite

Gestionarea jurnalelor

Analizarea profilurilor de utilizator

Puteţi afişa sau tipări o listă completă a tuturor utilizatorilor din sistem folosind comanda Afişare utilizatori autorizaţi (DSPAUTUSR).

Lista poate fi aranjată pe nume de profil sau nume de profil grup. Aici este un exemplu de secvenţă profil grup.

```
                          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 Afilare profil de utilizator (DSPUSRPRF) pentru a crea un fişier de ieşire, pe care îl puteţi procesa folosind o unelată 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 de 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 de 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 *Capabilităţi 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 căutarea câmpului cu ultima semnare.
- 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 de utilizator mari

Aţi putea vrea să evaluaţi eficienţa securităţii unor profiluri de utilizatori mariîn sistem. 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.

Aici este o metodă pentru localizarea profilurilor mari de utilizator şi evaluarea lor.

1. Folosiţi comanda DSPOBJD (Display Object Description - Afişare descriere de obiect) pentru a crea un fişier de ieşire conţinând informaţii despre toate profilurile de utilizator de pe sistem:
   ```
   DSPOBJD OBJ(*ALL) OBJTYPE(*USRPRF) +
           DETAIL(*BASIC) OUTPUT(*OUTFILE)
   ```
2. Creareaţi un program de interogare pentru a lista numele şi dimensiunea fiecărui profil de utilizator, în ordine descrescătoare, după dimensiune.
3. Tipăriţi 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)
   ```

   Notă: Directoarele şi obiectele bazate pe directoare nu sunt tipărite. Comenzile WRKOBJOWN şi WRKOBJPVT pot fi folosite pentru a afişa obiecte bazate pe director şi obiecte bazate pe bibliotecă, dar nu există o funcţie de tipărire asociată cu aceste comenzi.

   Unele profiluri de 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 de utilizator furnizate de IBM care au autorizare specială *ALLOBJ, precum QSECOFR şi QSYS. Vedeţi“Analizarea programelor care adoptă autorizare” la pagina 303.

   Referinţe înrudite

   Anexa B, “profiluri de utilizator furnizate de IBM”, la pagina 317
   Această secţiune conţine informaţii despre profilurile de 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 de utilizator furnizate de IBM.

Analizarea autorizărilor obiect şi bibliotecă

Puteţi audita autorizărilor obiect şi bibliotecă din sistem.

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 anumite biblioteci:

   ```
   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 autorizare

Programe care adoptă autorizarea unui utilizator cu autorizarea speială *ALLOBJ reprezintă o expunere de securitate. Puteţi analiza aceste programe pentru a audita securitatea sistemului.

Următoarea metodă poate fi folosită pentru a găsi şi inspecta acele programe care adoptă autorizare:

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(user-profile-name) +
             OUTPUT(*PRINT)
   ```

   Notă: Subiectul “Tipărirea profilurilor de utilizator selectate” la pagina 301 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)
   ```

   Notă: Parametrul tip obiect ar putea fi necesar să fie *PGM, *SQLPKG sau *SRVPGM după cum este indicat de raportul DSPPGMADP.

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 de 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 comanda DSPOBJD:

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

   Notă: Parametrul tip obiect ar putea trebui să fie *PGM, *SQLPKG sau *SRVPGM după cum este indicat de raportul DSPPGMADP.

Verificarea obiectelor care au fost modificate

Un obiect transformat este, de obicei, un indiciu că cineva încearcă să facă modificări pe sistemul dumneavoastră. Puteţi folosi comanda Verificarea integritate obiect (CHKOBJITG) pentru a verifica acele obiecte care au fost modificate.

Este posibil să doriţi să rulaţi această comandă după ce cineva:

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

Când rulaţi comanda, sistemul creează un fişier bază de date 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 de fişiere integrat sau verifica dacă obiectele au picat o scanare anterioară de sistem de fişiere integrat.

Rularea comenzii CHKOBJITG necesită autorizare specială *AUDIT. Comanda ar putea dura mult timp datorită 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 ar trebui şterse şi recontruite folosind comanda Creare obiecte duplicat (CRTDUPOBJ) de fiecare dată când este încărcată o ediţie nouă.

Informaţii înrudite

Suport scanare

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. Doar semnăturile de la un sistem de încredere 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.

Referinţe înrudite

API verificare sistem (QYDOCHKS)

Auditarea acţiunilor responsabilului cu securitatea

Puteţi păstra o înregistrare a tuturor acţiunilor realizate de utilizatorii cu autorizare specială *ALLOBJ şi *SECADM în scopuri de urmărire.

Pentru a face aceasta, puteţi folosi valoarea de auditare acţiune din profilul de utilizator:

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 de utilizator responsabilul cu securitatea:

```
CHGUSRAUD USER(SECUSER) +
          AUDLVL(*CMD *CREATE *DELETE +
                 *OBJMGT *OFCSRV *PGMADP +
                 *SAVRST *SERVICE, +
                 *SPLFDTA *SYSMGT)
```

"Auditarea acţiunilor" la pagina 112arată toate valorile posibile pentru auditarea acţiunii.

2. Înlătură autorizarea specială *AUDIT din profilul de utilizator cu autorizarea specială *ALLOBJ şi *SECADM. Aceasta îi împiedică pe aceşti utilizatori să modifice caracteristicile de auditare ale profilurilor lor.

   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 ca să modifice caracteristicile de auditare, în jurnalul de auditare este scris un tip de intrare AD.

   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 distribuită.

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 jurnalului de auditare cu o interogare sau cu un program" la pagina 296

Capitolul 10. Informaţii referitoare la licenţa de cod şi declinarea responsabilităţii

IBM vă acordă o o licenţă de copyright neexclusivă pentru utilizarea tuturor exemplelor de cod de programare din care puteţi genera funcţii similare, adaptate propriilor nevoi specifice.

CU EXCEPŢIA GARANŢIILOR LEGALE CARE NU POT FI EXCLUSE, IBM, DEZVOLTATORII SĂI DE PROGRAME ŞI FURNIZORII SĂI NU ACORDĂ NICI O GARANŢIE SAU CLAUZĂ, EXPLICITĂ SAU IMPLICITĂ, INCLUSIV DAR FĂRĂ A SE LIMITA LA GARANŢIILE SAU CLAUZELE IMPLICITE DE VANDABILITATE, DE CONCORDANŢĂ CU UN ANUMIT SCOP ŞI DE NEÎNCĂLCARE A LEGII, PRIVIND PROGRAMUL SAU SUPORTUL TEHNIC, DACĂ ESTE CAZUL.

IBM, DEZVOLTATORII SĂI DE PROGRAME SAU FURNIZORII SĂI NU VOR FI ÎN NICI O ÎMPREJURARE RĂSPUNZĂTORI PENTRU ORICARE DINTRE URMĂTOARELE, CHIAR DACĂ AU FOST INFORMAŢI CU PRIVIRE LA POSIBILITATEA PRODUCERII ACESTORA:

1. PIERDERE SAU DETERIORARE A DATELOR;
2. PAGUBE DIRECTE, SPECIFICE, ACCIDENTALE SAU INDIRECTE, SAU PENTRU ORICE PAGUBE ECONOMICE SURVENITE DREPT CONSECINŢĂ; SAU
3. PIERDERI DE PROFIT, DE VENITURI, PIERDERI COMERCIALE SAU PIERDERI PRIVIND REPUTAŢIA SAU ECONOMIILE SCONTATE.

ANUMITE JURISDICŢII NU PERMIT EXCLUDEREA SAU LIMITAREA PREJUDICIILOR DIRECTE, ACCIDENTALE SAU A CELOR SURVENITE DREPT CONSECINŢĂ, CAZ ÎN CARE ESTE POSIBIL CA UNELE SAU TOATE LIMITĂRILE SAU EXCLUDERILE DE MAI SUS SĂ NU SE APLICE ÎN CAZUL DUMNEAVOASTRĂ.

Anexa A. Comenzi securitate

Această secţiune conţine comenzile de sistem legate de securitate. Puteţi folosi aceste comenzi în locul meniurilor de sistem tastând aceste comenzi într-o linie de comandă. Comenzile sunt împărţite în grupuri orientate pe operaţii.

Subiectul Control language (CL) conţine informaţii mai detaliate despre aceste comenzi. Tabelele din Anexa D, “Autorizare necesară pentru obiecte folosite de comenzi”, la pagina 337 arată ce autorizări de obiect sunt necesare pentru a folosi aceste comenzi.

Pentru informaţii suplimentare despre uneltele şi sugestiile despre cum să folosiţi uneltele de securitate, consultaţi subiectul Configurarea sistemului să folosească unelte de securitate.

Comenzi păstrători autorizare

Această tabelă furnizează o listă de comenzi care vă permit să lucraţi cu păstrători de securitate.

Tabela 134. Comenzi păstrători autorizare

Nume comandă	Nume descriptiv	Funcţia
CRTAUTHLR	Creare păstrător de autorizare	Securizaţi un fişier înainte ca fişierul să existe. Păstrătorii de autorizare sunt valizi doar pentru fişiere bază de date descrise de program.
DLTAUTHLR	Ştergere păstrător de autorizare	Ştergeţi un păstrător de autorizare. Dacă fişierul asociat există, informaţiile păstrător autorizare sunt copiate în fişier.
DSPAUTHLR	Afişare păstrător de autorizare	Afişaţi păstrătorii de autorizare din sistem.

Comenzi liste de autorizare

Puteţi folosi aceste comenzi pentru a realiza diferite taskuri pe listele de autorizare.

Tabela 135. Comenzi liste de autorizare

Nume comandă	Nume descriptiv	Funcţia
ADDAUTLE	Adăugare intrare listă de autorizare	Adăugaţi un utilizator la o listă de autorizare. Dumneavoastră specificaţi ce autorizare are utilizatorul pentru toate obiectele din listă.
CHGAUTLE	Modificare intrare listă de autorizare	Modificaţi autorizările utilizatorilor asupra obiectelor din lista de autorizare.
CRTAUTL	Comanda Creare listă de autorizare	Creaţi o listă de autorizare.
DLTAUTL	Ştergere listă de autorizare	Ştergeţi o întreagă listă de autorizare.
DSPAUTL	Afişare listă de autorizare	Afişaţi o listă de utilizatori şi autorizările lor într-o listă de autorizare.
DSPAUTLOBJ	Afişare obiecte listă de autorizare	Afişaţi o listă de obiecte securizate de o listă de autorizare.
EDTAUTL	Editare listă de autorizare	Adăugaţi, modificaţi şi înlăturaţi utilizatori şi autorizările lor într-o listă de autorizare.
RMVAUTLE	Înlăturare intrare listă de autorizare	Înlăturaţi un utilizator dintr-o listă de autorizare.
RTVAUTLE	Extragere intrare de listă de autorizare	Folosită într-un program în limbaj de control (CL) pentru a obţine una sau mai multe valori asociate cu un utilizator din lista de autorizare. Comanda poate fi folosită împreună cu comanda CHGAUTLE pentru a acorda unui utilizator noi autorizări faţă de cele pe care le are deja.

Tabela 135. Comenzi liste de autorizare (continuare)

Nume comandă	Nume descriptiv	Funcţia
WRKAUTL	Lucru cu liste de autorizare	Lucraţi cu liste de autorizare dintr-o afişare de listă.

Autorizare obiecte şi comenzi de auditare

Puteţi consula această tabelă pentru comenzile pe care le puteţi folosipentru a lucra cu autorizări de obiecte şi auditare.

Tabela 136. Autorizare obiecte şi comenzi de auditare

Nume comandă	Nume descriptiv	Funcţia
CHGAUD	Modificare auditare	Modificarea valorii de auditare pentru un obiect.
CHGAUT	Modificare autorizare	Modificarea autorizării utilizatorilor asupra obiectelor.
CHGOBJAUD	Modificare auditare obiect	Specificaţi dacă accesul la un obiect este auditat.
CHGOBJOWN	Modificare proprietar obiect	Modificaţi dreptul de proprietate al unui obiect de la un utilizator la altul.
CHGOBJPGP	Modificare grup primar obiect	Modificaţi grupul primar pentru un obiect la alt utilizator sau la niciun grup primar.
CHGOWN	Modificare proprietar	Modificaţi dreptul de proprietate al unui obiect de la un utilizator la altul.
CHGPGP	Modificare grup primar	Modificaţi grupul primar pentru un obiect la alt utilizator sau la niciun grup primar.
DSPAUT	Afişare autorizare	Afişaţi autorizarea utilizatorilor pentru un obiect.
DSPLNK	Afişare legături	Arată o listă cu numele obiectelor specificat în directoare şi opţiuni pentru a afişa informaţii despre obiecte.
DSPOBJAUT	Display Object Authority - Afişare autorizare obiect	Afişează proprietarul obiectului, autorizare publică pentru obiect, toate autorizările private pentru obiect şi numele listei de autorizare folosite pentru a asigura obiectul.
DSPOBJD	Afişare descriere obiect	Afişează nivelul de auditare obiect pentru obiect.
EDTOBJAUT	Editare autorizare obiect	Adăugaţi, modificaţi sau înlăturaţi autorizarea unui utilizator pentru un obiect.
GRTOBJAUT	Acordare de autorizare obiect	Acordaţi specific autorizare utilizatorilor numiţi, tuturor utilizatorilor (*PUBLIC) sau utilizatorilor obiectului referit pentru obiectele numite în această comandă.
RVKOBJAUT	Revocare autorizare obiect	Înlăturaţi una sau mai multe (sau toate) din autorizările acordate specific unui utilizator pentru obiecte numite.
WRKAUT	Lucru cu autorizări	Lucraţi cu autorizare obiect selectând opţiuni într-o afişare de listă.
WRKLNK	Gestionare legături	Arată o listă cu numele obiectelor specificate în directoare şi opţiuni pentru a lucra cu obiecte.
WRKOBJ	Lucru cu obiecte	Lucraţi cu autorizare obiect selectând opţiuni într-o afişare de listă.
WRKOBJOWN	Lucru cu obiecte după proprietar	Lucraţi cu obiectele posedate de un profil de utilizator.
WRKOBJPGP	Lucru cu obiecte după grup primar	Lucraţi cu obiectele pentru care un profil este grupul primar folosind opţiunile dintr-o afişare de listă.
WRKOBJPVT	Lucru cu obiecte după Private Authorities	Lucraţi cu obiectele pentru care un profil este autorizat privat, folosind opţiunile dintr-o afişare de listă.

Comenzi parole

Aceste comenzi permit administratorului de securitate pentru a asigna, modifica, verifica sau reseta parola asociată cu un profil de utilizator.

Tabela 137. Comenzi parole

Nume comandă	Nume descriptiv	Funcţia
CHGDSTPWD	Modificare parolă Unelte de service dedicate	Resetaţi profilul de capabilităţi securitate DST la parola implicită livrată cu sistemul.
CHGPWD	Modificare parolă	Modificaţi parola proprie a utilizatorului.
CHGUSRPRF	Modificare profil de utilizator	Modificaţi valorile specificate în profilul unui utilizator, inclusiv parola utilizatorului.
CHKPWD	Verificare parolă	Verificaţi parola utilizatorului. 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 de utilizator	Când adăugaţi un utilizatorul în sistem, asignaţi o parolă utilizatorului.

[1] După ce se termină CRTUSRPRF, nu puteţi să specificaţi crearea *USRPRF într-un ASP. Totuşi, când un utilizator este autorizat privat asupra unui obiect sau asupra unui ASP, utilizatorul este proprietarul unui obiect de pe un ASP sau utilizatorul este grupul primar al unui obiect într-un ASP, numele profilului este stocat în ASP. 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 în sistemul destinaţie, este creat. Utilizatorul nu va avea nici o autorizare specială şi parola va fi setată la *NONE.

Comenzi profiluri de utilizator

Ca administrator de securitate, va trebui să folosiţi aceste comenzi pentru a lucra cu profiluri de utilizator.

Tabela 138. Comenzi profiluri de utilizator

Nume comandă	Nume descriptiv	Funcţia
CHGPRF	Modificare profil	Modificaţi unele din atributele unui profil propriu al utilizatorului.
CHGUSRAUD	Modificare auditare utilizator	Specificaţi auditarea de acţiuni şi obiecte pentru un profil de utilizator.
CHGUSRPRF	Modificare profil de utilizator	Modificaţi valorile specificate în profilul unui utilizator cum ar fi parola utilizatorului, autorizările speciale, meniul iniţial, programul iniţial, biblioteca curentă şi limita 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 de utilizator	Adăugaţi un utilizator în sistem specificaţi valori cum ar fi parola utilizatorului, autorizările speciale, meniul iniţial, programul iniţial, biblioteca curentă şi limita de prioritate.
DLTUSRPRF	Ştergere profil de utilizator	Ştergeţi un utilizator din sistem. Această comandă furnizează o opţiune de a şterge sau modifica dreptul de proprietate asupra obiectelor deţinute de profilul de utilizator.
DMPUSRPRF	Dump profil de utilizator	Vă permite să faceţi dump la profilul de utilizator şi la informaţiile înrudite.

Tabela 138. Comenzi profiluri de utilizator (continuare)

Nume comandă	Nume descriptiv	Funcţia
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.
DSPSSTUSR	Afişare ID utilizator unelte de service	Afişează o listă de identificatori utilizatori unelte de service. Poate fi de asemenea folosită pentru a arăta informaţii detaliate despre un anumit ID utilizator unelte de service, inclusiv starea şi privilegiile acelui utilizator.
DSPUSRPRF	Afişare profil de utilizator	Afişaţi un profil de utilizator în mai multe formate diferite.
GRTUSRAUT	Acordare autorizare utilizator	Copiaţi autorizările private dintr-un profil de utilizator în alt profil de utilizator.
PRTPRFINT	Tipărire valori interne profil	Tipăriţi un raport al informaţiilor interne despre numărul de intrări.
PRTUSRPRF	Tipărire profil de utilizator	Analizaţi profilurile de utilizator care îndeplinesc criteriile specificate.
RTVUSRPRF	Extragere profil de 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 de utilizator.
WRKUSRPRF	Lucru cu profiluri de utilizator	Lucraţi cu profiluri de utilizator introducând opţiuni într-un afişare de listă.

Comenzi înrudite profil de utilizator

Această tabelă listează alte comenzi care sunt înrudite de profiluri de utilizator. Aceste comenzi vă permit să restauraţi sau să salvaţi profilurile de utilizator şi atributele lor.

Tabela 139. Comenzi înrudite profil de utilizator

Nume comandă	Nume descriptiv	Funcţia
DSPPGMADP	Afişare programe care adoptă	Afilaţi o listă de programe şi pachetele SQL care adoptă un profil de utilizator specificat.
RSTAUT	Restaurare autorizare	Restauraţi autorizări pentru obiecte păstrate de un profil de utilizator când a fost salvat profilul de utilizator. Aceste autorizări pot fi restaurate doar ce un profil de utilizator este restaurat cu comanda Restaurare profil de utilizator (RSTUSRPRF).
RSTUSRPRF	Restaurare profil de utilizator	Restauraţi un profil de 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 păstrătorii de autorizări, dacă se specifică RSTUSRPRF(*ALL).
SAVSECDTA	Salvare date de securitate	Salvează toate profilurile de utilizator, liste de autorizare şi păstrători de autorizare fără a folosi un sistem care este într-o stare restrictivă.
SAVSYS	Salvare sistem	Salvează toate profilurile de utilizator, listele de autorizări şi păstrători de autorizare din sistem. Este necesar un sistem dedicat pentru a folosi această funcţie.

Comenzi auditare

Puteţi folosi aceste comenzi pentru a gestiona auditarea pe un obiect.

Tabela 140. Comenzi auditare

Nume comandă	Nume descriptiv	Funcţia
CHGAUD	Modificare auditare	Specificaţi auditarea pentru un obiect.
CHGDLOAUD	Modificare auditare obiect de bibliotecă de documente	Specificaţi dacă accesul este auditat pentru un obiect bibliotecă de documente.
CHGOBJAUD	Modificare auditare obiect	Specificaţi auditarea pentru un obiect.
CHGUSRAUD	Modificare auditare utilizator	Specificaţi acţiunea şi auditarea obiect pentru un profil de utilizator.

Comenzi obiect bibliotecă de documente

Această tabelă listează comenzile pe care le puteţi folosi pentru a lucra cu obiecte bibliotecă de documente.

Tabela 141. Comenzi obiecte bibliotecă de documente

Nume comandă	Nume descriptiv	Funcţia
ADDDLOAUT	Adăugare autorizare obiect de bibliotecă de documente	Acordaţi unui utilizator acces asupra unui document sau folder sau pentru a securiza un document sau folder cu o listă de autorizare sau un cod de acces.
CHGDLOAUD	Modificare auditare obiect de bibliotecă de documente	Specificaţi nivelul de auditare obiecte pentru un obiect bibliotecă de documente.
CHGDLOAUT	Modificare autorizare obiect de bibliotecă de documente	Modificaţi autorizarea pentru un document sau 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	Modificaţi grupul primar pentru un obiect bibliotecă de documente.
DSPAUTLDLO	Afişare obiecte de bibliotecă de documente pentru listă de autorizare	Afişaţi documentele şi folderele care sunt securizate de lista de autorizare 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	Afişaţi informaţii de autorizare pentru un document sau un folder.
EDTDLOAUT	Editare autorizare obiect de bibliotecă de documente	Adăugaţi, modificaţi sau înlăturaţi autorizările unui utilizator asupra unui document sau folder.
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	Înlăturaţi autorizarea unui utilizator asupra documentelor sau folderelor.
RVKUSRPMN	Revocare permisiune utilizator	Retrage de la un utilizator (sau toţi utilizatorii) autorizarea de a accesa documente în numele unui alt utilizator.

Comenzi intrări autenficare server

Aceste comenzi vă permit să afişaţi, adăugaţi, înlăturaţi sau să modificaţi intrările de autentificare server dintr-un profil de utilizator.

Tabela 142. Comenzi intrări autenficare server

Nume comandă	Nume descriptiv	Funcţia
ADDSVRAUTE	Adăugare intrare de autentificare server	Adăugaţi informaţii autentificare server pentru un profil de utilizator.
CHGSVRAUTE	Modificare intrare de autentificare server	Modificaţi intrări autentificare server existente pentru un profil de utilizator.
DSPSVRAUTE	Afişare intrări de autentificare server	Afişaţi intrări autentificare server pentru un profil de utilizator.
RMVSVRAUTE	Înlăturare intrare de autentificare server	Înlăturaţi intrări autentificare server din profilul de 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.		

Comenzi director distribuţie sistem

Puteţi folosi aceste comenzi pentru a adăuga, înlătura sau modifica intrările din directorul de distribuţie al sistemului.

Tabela 143. Comenzi director distribuţie sistem

Nume comandă	Nume descriptiv	Funcţia
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 de 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.

Comenzi liste de validare

Aceste două comenzi vă permit să creaţi şi să ştergeţi liste de validare dintr-o bibliotecă.

Tabela 144. Comenzi liste de validare

Nume comandă	Nume descriptiv	Funcţia
CRTVLDL	Creare liste de validare	Creaţi un obiect listă de validare care conţine intrări care sunt alcătuite dintr-un identificator, date care vor fi criptate de sistem când sunt stocate şi date formate liber.
DLTVLDL	Ştergere listă de validare	Ştergeţi lista de validare specificată dintr-o bibliotecă.

Comenzi informaţii folosire funcţie

Puteţi folosi aceste comenzi pentru a modifica sau afişa informaţii de folosire funcţii.

Tabela 145. Comenzi informaţii folosire funcţie

Nume comandă	Nume descriptiv	Funcţia
CHGFCNUSG	Modificare utilizare funcţie	Modificaţi informaţiile de folosire pentru o funcţie înregistrată.
DSPFCNUSG	Afişare utilizare funcţie	Afişaţi o listă de identificatori de funcţii şi informaţii detaliate de folosire pentru o anumită funcţie.
WRKFCNUSG	Gestionare utilizare funcţie	Afişaţi o listă de identificatori de funcţii şi modificaţi sau afişaţi informaţii de folosire funcţii.

Comenzi unelte de securitate auditare

Aceste comenzi vă permit să lucraţi cu auditarea securităţii, intrările din jurnalul de auditare sistem şi valorile de sistem care controlează auditarea securităţii.

Pentru informaţii suplimentare despre uneltele de securitate, vedeţi Anexa G, “Comenzi şi meniuri pentru comenzi de securitate”, la pagina 699.

Tabela 146. Comenzi unelte de securitate auditare

Nume comandă	Nume descriptiv	Funcţia
CHGSECAUD	Modificare auditare de securitate	Setaţi auditarea securităţii şi pentru a modifica valorile de sistem care controlează auditarea securităţii.
CPYAUDJRNE	Copiere intrări jurnal de auditare	Copiaţi intrările din jurnalul de auditare securitate în fişierele de ieşire pe care le puteţi interoga. Puteţi selecta tipuri de intrări specifice, utilizatori specifice, şi o perioadă de timp.
DSPAUDJRNE[1]	Afişare intrări jurnal de auditare	Afişaţi sau tipăriţi informaţii despre intrările din jurnalul de auditare securitate. Puteţi selecta tipuri de intrări specifice, utilizatori specifice, şi o perioadă de timp.
DSPSECAUD	Afişare valori auditare de securitate	Afişaţi informaţii despre jurnalul de auditare securitate şi valorile de sistem care controlează auditarea securităţii.

1 IBM a încetat să furnizeze îmbunătăţiri pentru comanda DSPAUDJRNE. Comanda nu suportă toate tipurile de înregistrări de auditare a securităţii şi nu listează toate câmpurile pentru înregistrările pe care ea le suportă.

Comenzi unelte de securitate autorizare

Puteţi folosi aceste comenzi pentru a realiza diferite taskuri de tipărire care sunt legate de setările de securitate.

Tabela 147. Comenzi unelte de securitate autorizare

Nume comandă	Nume descriptiv	Funcţia
PRTJOBDAUT	Tipărire autorizare descriere de job	Tipăriţi o listă de descriptori 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 de utilizator care poate fi accesat de toţi utilizatorii din sistem.
PRTPUBAUT	Tipărire obiecte autorizate public	Tipăriţi o listă de obiecte a căror autorizare publică nu este *EXCLUDE.
PRTPVTAUT	Tipărire autorizări private	Tipăriţi o listă de autorizări private pentru obiecte de un anumit tip.
PRTQAUT	Tipărire autorizare coadă	Tipăriţi setările de securitate pentru cozile de ieşire şi cozile de joburi din sistem. Aceste setări controlează cine poate vizualiza şi modifica intrări din coada de ieşire sau coada de joburi.
PRTSBSDAUT	Tipărire autorizare descriere subsistem	Tipăriţi o listă de descrieri de subsisteme într-o bibliotecă ce conţine un utilizator implicit într-o intrare subsistem.

Tabela 147. Comenzi unelte de securitate autorizare (continuare)

Nume comandă	Nume descriptiv	Funcţia
PRTTRGPGM	Tipărire programe de declanşare	Tipăriţi o listă de programe declanşatoare care sunt asociate cu fişierele bază de date din sistem.
PRTUSROBJ	Tipărire obiecte utilizator	Tipăriţi o listă de obiecte utilizator (obiecte care nu sunt livrate de IBM) care sunt într-o bibliotecă.

Comenzi unelte de securitate sistem

Puteţi folosi aceste comenzi pentru a lucra cu securitatea sistemului.

Tabela 148. Comenzi unelte de securitate sistem

Nume comandă	Nume descriptiv	Funcţia
CHGSECA [1]	Modificare atribute de securitate	Setaţi valori noi de pornire pentru generarea de numere ID utilizator sau numere ID grup. Utilizatorii pot specifica un ID utilizator de pornire şi un ID grup de pornire.
CFGSYSSEC	Configurare securitate sistem	Setaţi valori de sistem relevante pentru securitate la setările recomandate. Comanda setează de asemenea auditarea de securitate pe sistemul dumneavoastră.
CLRSVRSEC	Curăţare date de securitate server	Curăţaţi informaţiile de autentificare decriptabile care sunt asociate cu profiluri de utilizator şi intrări listă validare (*VLDL). **Notă:** Acestea sunt aceleaşi informaţii care au fost curăţate în ediţii anterioare V5R2 când valoarea sistem QRETSVRSEC se schimba de ’1’ la ’0’.
DSPSECA	Afişare atribute de securitate	Afişaţi valorile curente şi în aşteptare ale unor atribute de securitate sistem.
PRTCMNSEC	Tipărire securitate comunicaţii	Tipăriţi atributele de securitate ale obiectelor *DEVD, *CTL şi *LIND din sistem.
PRTSYSSECA	Tipărire atribute de securitate sistem	Tipăriţi o listă de valori de sistem relevante pentru securitate şi atribute de reţea. Raportul arată valoarea curentă şi valoarea recomandată.
RVKPUBAUT	Revocare autorizare publică	Setaţi autorizarea publică la *EXCLUDE pentru un set de comenzi sensibile la securitate din sistem.

[1] Pentru a folosi această comandă, trebuie să aveţi autorizare specială *SECADM.

Anexa B. profiluri de utilizator furnizate de IBM

Această secţiune conţine informaţii despre profilurile de 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 de utilizator furnizate de IBM.

Valorile implicite pentru profilurile de utilizator

Această tabelă arată valorile implicite care sunt folosite pentru toate profilurile de utilizator livrate de IBM şi în comanda Creare profil de utilizator (CRTUSRPRF). Parametrii sunt ordonaţi în funcţie de momentul apariţiei lor în ecranul Creare profil de utilizator.

Tabela 149. Valorile implicite pentru profilurile de utilizator

	Valori implicite	
Parametru profil de utilizator	**Profiluri de utilizator furnizate de IBM**	**Ecran Creare profil de 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 asistenţă (ASTLVL)	*SYSVAL	*SYSVAL
Bibliotecă curentă (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
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

Tabela 149. Valorile implicite pentru profilurile de utilizator (continuare)

Parametru profil de utilizator	Valori implicite	
	Profiluri de utilizator furnizate de IBM	**Ecran Creare profil de utilizator**
Parolă a documentului (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 de 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 privat asupra unui obiect în pool-ul de discuri independent, utilizatorul este proprietarul unui obiect dintr-un pool de discuri independent sau utilizatorul este grupul primar al unui obiect într-un pool de discuri independent, numele profilului este stocat 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.

Profilurile de utilizator furnizate de IBM

Această tabelă prezintă fiecare profil livrat de IBM, scopul său şi valorile pentru profil care sunt diferite de valorile implicite pentru profilurile de utilizator livrate de IBM.

Notă:

Profilurile de utilizator livrate de IBM includ acum profiluri de utilizator suplimentare, care sunt livrate cu produsele program licenţiat. Tabela nu conţine toate profilurile de utilizator pentru produse program licenţiat; deci lista nu este exhaustivă.

Atenţie:

- Parola pentru profilul QSECOFR

  Trebuie să modificaţi parola pentru profilul QSECOFR după ce instalaţi sistemul. Această parolă este aceeaşi pentru fiecare produs System i şi este o vulnerabilitate de securitate până când este schimbată. Totuşi, nu modificaţi alte valori pentru profiluri de utilizator livrate de IBM. Modificarea acestor profiluri poate cauza eşuarea funcţiilor sistemului.
- Autorizările pentru profilurile livrate de IBM

  Aveţi grijă la înlăturarea autorizărilor pe care profilurile livrate de IBM le au pentru obiectele care sunt livrate cu sistemul de operare. Unor profiluri livrate de IBM le sunt acordate autorizări private care sunt livrate cu sistemul de operare. Înlăturarea oricărei din aceste autorizări poate duce la eşuarea funcţiilor sistemului.

Tabela 150. profiluri de utilizator furnizate de IBM

Nume profil	Nume descriptiv	Parametrii diferiţi de valori implicite
QADSM	Profil de utilizator ADSM	• USERCLS: *SYSOPR • CURLIB: QADSM • TEXT: Profil ADSM folosit de serverul ADSM • SPCAUT: *JOBCTL, *SAVSYS • JOBD: QADSM/QADSM • OUTQ: QADSM/QADSM
QAFOWN	Profil de utilizator APD	• USRCLS: *PGMR • SPCAUT: *JOBCTL • JOBD: QADSM/QADSM • TEXT: Profil de utilizator intern APD
QAFUSR	Profil de utilizator APD	• TEXT: Profil de utilizator intern APD
QAFDFTUSR	Profil de utilizator APD	• INLPGM: *LIBL/QAFINLPG • LMTCPB: *YES • TEXT: Profil de utilizator intern APD
QAUTPROF	Profil de utilizator autorizare IBM	
QBRMS	Profil de utilizator BRM	
QCLUMGT	Profil gestionare cluster	• STARE: *DISABLED • MSGQ: *NONE • ATNPGM: *NONE
QCLUSTER	Profil cluster disponibilitate înaltă	• SPCAUT: *IOSYSCFG
QCOLSRV	Profil de utilizator servicii de colectare Administrare centrală	
QDBSHR	Profil partajare bază de date	• AUT: *ADD, *DELETE
QDBSHRDO	Profil partajare bază de date	• AUT: *ADD, *DELETE
QDFTOWN	Profil proprietar implicit	• PTYLMT: 3

Tabela 150. profiluri de utilizator furnizate de IBM (continuare)

Nume profil	Nume descriptiv	Parametrii diferiţi de valori implicite
QDIRSRV	Profilul de utilizator server i5/OS Directory Server	• LMTCPB: *YES • JOBD: QGPL/QBATCH • DSPSGNINF: *NO • LMTDEVSSN: *NO • DLVRY: *HOLD • SPCENV: *NONE • ATNPGM: *NONE
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 de utilizator WebSphere Application Server	
QEJB	Profil de 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 de utilizator MQSeries	• USRCLS: *SECADM • SPCAUT: *NONE • PRTDEV: *SYSVAL • TEXT: Utilizator MQM care deţine biblioteca QMQM
QNFSANON	Profil de utilizator NFS	
QNETSPLF	Profil de spool reţea	

Tabela 150. profiluri de utilizator furnizate de IBM (continuare)

Nume profil	Nume descriptiv	Parametrii diferiţi de valori implicite
QNTP	Profil timp reţea	• JOBD: QTOTNTP • JOBD LIBRARY: QSYS
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 de utilizator subsistem de comunicaţii intern OSI
QOSIFS	Profil de utilizator server fişiere OSI	• USRCLS: *SYSOPR • SPCAUT: *JOBCTL, *SAVSYS • OUTQ: *DEV • CURLIB: *QOSIFS • CCSID: *HEX • TEXT: Profil de utilizator servicii fişiere intern OSI
QPGMR	Profil programator	• USRCLS: *PGMR • SPCAUT: *ALLOBJ [1] *SAVSYS *JOBCTL • PTYLMT: 3 • ACGCDE: *BLANK
QPEX	Profil de utilizator Performance Explorer	• PTYLMT: 3 • ATNPGM: *SYSVAL • TEXT: Profil de utilizator livrat de IBM
QPM400	IBM Performance Management pentru System i(PM System i)	• SPCAUT: *IOSYSCFG, *JOBCTL
QPRJOWN	Profil de utilizator proprietar de proiecte şi părţi	• STARE: *DISABLED • CURLIB: QADM • TEXT: Profilul de utilizator al proprietarului de proiecte şi părţi
QRDARSADM	Profil de 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 150. profiluri de utilizator furnizate de IBM (continuare)

Nume profil	Nume descriptiv	Parametrii diferiţi de valori 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 de 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 de utilizator OptiConnect	• USRCLS: *SYSOPR • CURLIB: *QSOC • SPCAUT: *JOBCTL • MSGQ: QUSRSYS/QSOC
QSPL	Profil spool	
QSPLJOB	Profil job spool	• AUT: *EXCLUDE
QSRV	Profil service	• USRCLS: *PGMR • SPCAUT: *ALLOBJ [1], *SAVSYS [1], *JOBCTL, *SERVICE • ASTLVL: *INTERMED • ATNPGM: QSYS/QSCATTN
QSRVAGT	Profil de utilizator agent service	

Tabela 150. profiluri de utilizator furnizate de IBM (continuare)

Nume profil	Nume descriptiv	Parametrii diferiţi de valori implicite
QSRVBAS	Profil service de bază	• USRCLS: *PGMR • SPCAUT: *ALLOBJ [1] *SAVSYS [1] *JOBCTL • ASTLVL: *INTERMED • ATNPGM: QSYS/QSCATTN
QSVCCS	Profil de utilizator CC Server	• USRCLS: *SYSOPR • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: Profil de utilizator CC Server
QSVCM	Profil de utilizator Client Management Server	• TEXT: Profil de utilizator Client Management Server
QSVSM	Profil de utilizator ECS	• USRCLS: *SYSOPR • STARE: *DISABLED • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: Profil de utilizator Manager sistem SystemView
QSVSMSS	Profil de utilizator Managed System Service	• STARE: *DISABLED • USRCLS: *SYSOPR • SPCAUT: *JOBCTL • SPCENV: *SYSVAL • TEXT: Profil de 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 de utilizator LPR la distanţă	• JOBD: QGPL/QDFTJOBD • PWDEXPITV: *NOMAX • MSGQ: QTCP/QTMPLPD

Tabela 150. profiluri de utilizator furnizate de IBM (continuare)

Nume profil	Nume descriptiv	Parametrii diferiţi de valori implicite
QTMTWSG	Profil de utilizator HTML Workstation Gateway	• MSGQ: QUSRSYS/QTMTWSG • TEXT: Profil HTML Workstation Gateway
QTMHHTTP	Profil de utilizator HTML Workstation Gateway	• MSGQ: QUSRSYS/QTMHHTTP • TEXT: Profil server HTTP
QTMHHTP1	Profil de utilizator HTML Workstation Gateway	• MSGQ: QUSRSYS/QTMHHTTP • TEXT: Profil CGI server HTTP
QTSTRQS	Profil cerere test	
QUMB	Profil de utilizator Ultimedia System Facilities	
QUMVUSER	Profil de utilizator Ultimedia Business Conferencing	
QUSER	Profil de utilizator staţie de lucru	• PTYLMT: 3
QX400	Profil de 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 de utilizator servicii mesaje interne OSI
QYCMCIMOM	Profil de utilizator server	
QYPSJSVR	Profil server Administrare centrală Java	
QYPUOWN	Profil de utilizator intern APU	• TEXT: Profil de 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. Comenzi livrate cu autorizare publică *EXCLUDE

Această secţiune identifică ce comenzi au autorizare restricţionată (autorizarea publică este *EXCLUDE) când sistemul este livrat. Arată care profiluri de utilizator livrate de IBM sunt autorizate să folosească aceste comenzi restricţionate.

Pentru mai multe detalii despre profilurile de utilizator, vedeţi subiectul “Profiluri de utilizator furnizate de IBM” la pagina 127.

În Tabela 151, comenzile care sunt restricţionate pentru responsabilul cu securitatea şi pentru orice profil de utilizator cu autorizare *ALLOBJ au un **R** în profilul QSECOFR. Comenzile care sunt autorizate special unuia sau mai multor profiluri de 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, “Autorizare necesară pentru obiecte folosite de comenzi”, la pagina 337

Dacă alegeţi să acordaţi altor utilizatori sau publicului autorizarea *USE pentru aceste comenzi, actualizaţi această tabelă astfel încât să indice comenzile care nu mai sunt restricţionate în sistem. Folosirea unor comenzi ar putea necesita autorizarea pentru anumite obiecte din sistem, precum şi pentru comenzile respective. Vedeţi Anexa D, “Autorizare necesară pentru obiecte folosite de comenzi”, la pagina 337 pentru autorizările de obiect necesare pentru comenzi.

Tabela 151. Autorizările profilurilor de utilizator livrate de IBM pentru comenzi restricţionate

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ADDCLUNODE	R				
ADDCMDCRQA		S	S	S	S
ADDCRGDEVE	R				
ADDCRGNODE	R				
ADDCRSDMNK	R				
ADDDEVDMNE	R				
ADDDSTQ		S	S		
ADDDSTRTE		S	S		
ADDDSTSYSN		S	S		
ADDEXITPGM	R				
ADDDWDFN					
ADDJWDFN					
ADDMFS	R				
ADDMSTPART					
ADDNETJOBE	R				
ADDOBJCRQA		S	S	S	S
ADDOPTCTG	R				
ADDOPTSVR	R				
ADDPEXDFN		S		S	
ADDPEXFTR		S		S	

Tabela 151. Autorizările profilurilor de utilizator livrate de IBM pentru comenzi restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
ADDPRDCRQA		S	S	S	S
ADDPTFCRQA		S	S	S	S
ADDRPYLE		S			
ADDRSCCRQA		S	S	S	S
ADDTRCFTR	R				
ANSQST	R				
ANZBESTMDL	R				
ANZCMDPFR	R				
ANZDBF	R				
ANZDBFKEY	R				
ANZDFTPWD	R				
ANZJVM		S	S	S	S
ANZOBJCVN	R				
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				
CHGASPA	R				
CHGASPACT					
CHGCLUCFG	R				
CHGCLUNODE	R				
CHGCLURCY	R				
CHGCLUVER	R				
CHGCMDCRQA		S	S	S	S
CHGCRG	R				
CHGCRGDEVE	R				
CHGCRGPRI	R				
CHGCRSDMNK	R				
CHGDIRSRVA					
CHGDSTQ		S	S		
CHGDSTRTE		S	S		

Tabela 151. Autorizările profilurilor de utilizator livrate de IBM pentru comenzi restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CHGEXPSCDE	R				
CHGFCNARA	R				
CHGGPHFMT	R				
CHGGPHPKG	R				
CHGJOBTRC	R				
CHGJOBTYP	R				
CHGJRN		S	S	S	
CHGJRNA		S	S		
CHGLICINF	R				
CHGMGDSYSA		S	S	S	S
CHGMGRSRVA		S	S	S	S
CHGMSTK	R				
CHGNETA	R				
CHGNETJOBE	R				
CHGNFSEXP	R				
CHGNWSA	R				
CHGNWSCFG	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	
CHKMSTKVV					
CHKPRDOPT		S	S	S	S
CLRMSTKEY					
CPHDTA	R				
CPYFCNARA	R				
CPYFRMLDIF					
CPYGPHFMT	R				

Tabela 151. Autorizările profilurilor de utilizator livrate de IBM pentru comenzi restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
CPYGPHPKG	R				
CPYPFRCOL	R				
CPYPFRDTA	R				
CPYPTF		S	S	S	S
CPYPTFGRP		S	S	S	S
CPYTOLDIF					
CRTADMDMN	R				
CRTAUTHLR	R				
CRTBESTMDL	R				
CRTCLS	R				
CRTCLU	R				
CRTCRG	R				
CRTFCNARA	R				
CRTGPHFMT	R				
CRTGPHPKG	R				
CRTHSTDTA	R				
CRTJOBD	R				
CRTNWSCFG	R				
CRTPFRDTA	R				
CRTPFRSUM					
CRTLASREP		S			
CRTPEXDTA		S		S	
CRTQSTDB	R				
CRTQSTLOD	R				
CRTSBSD		S	S		
CRTUDFS	R				
CRTUDFS	R				
CRTVLDL	R				
CVTBASSTR	R				
CVTBASUNF	R				
CVTBGUDTA	R				
CVTDIR	R				
CVTPFRCOL	R				
CVTPFRDTA	R				
CVTPFRTHD	R				
CVTS36FCT	R				
CVTS36JOB	R				
CVTS38JOB	R				
CVTTCPCL		S	S	S	S
DB2LDIF					

Tabela 151. Autorizările profilurilor de utilizator livrate de IBM pentru comenzi restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
DLTADMDMN	R				
DLTAPARDTA		S	S	S	S
DLTBESTMDL	R				
DLTCLU	R				
DLTCMNTRC				S	
DLTCRGCLU	R				
DLTEXPSPLF	R				
DLTFCNARA	R				
DLTGPHFMT	R				
DLTGPHPKG	R				
DLTHSTDTA	R				
DLTLICPGM	R				
DLTNWSCFG	R				
DLTPEXDTA		S		S	
DLTPFRCOL	R				
DLTPFRDTA	R				
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				
DLTWNTSVR	R				
DMPDLO		S	S	S	S
DMPJOB		S	S	S	S
DMPJOBINT		S	S	S	S
DMPJVM		S	S	S	S
DMPMEMINF					
DMPOBJ				S	S
DMPSYSOBJ		S	S	S	S
DMPTRC	R	S		S	
DMPUSRPRF					
DSPDSTLOG	R				
DSPHSTGPH	R				
DSPMGDSYSA		S	S	S	S
DSPNWSCFG	R				
DSPPFRDTA	R				
DSPPFRGPH	R				

Tabela 151. Autorizările profilurilor de utilizator livrate de IBM pentru comenzi restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
DSPPTF		S	S	S	S
DSPSRVSTS		S	S	S	S
EDTCPCST			S		
EDTQST	R				
EDTRBDAP			S		
EDTRCYAP		S	S		
ENCCPHK	R				
ENCFRMMSTK	R				
ENCTOMSTK	R				
ENDASPBAL	R				
ENDCHTSVR	R				
ENDCLUNOD	R				
ENDCMNTRC	R			S	
ENDCRG	R				
ENDDBGSVR		S	S	S	S
ENDDW					
ENDHOSTSVR		S	S	S	S
ENDIDXMON	R				
ENDIPSIFC		S	S	S	S
ENDJOBABN		S	S	S	
ENDJOBTRC	R				
ENDJW					
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
ENDWCH	R				
GENCPHK	R				
GENCRSDMNK	R				
GENMAC	R				
GENPIN	R				
GENS36RPT	R				

Tabela 151. Autorizările profilurilor de utilizator livrate de IBM pentru comenzi restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
GENS38RPT	R				
GRTACCAUT	R				
HLDCMNDEV		S	S	S	S
HLDDSTQ		S	S		
INSPTF[2]				S	
INSRMTPRD		S	S	S	S
INSWNTSVR	R				
INZDSTQ		S	S		
INZNWSCFG	R				
INZSYS	R				
LDIF2DB					
LODOPTFMW	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				
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				

Tabela 151. Autorizările profilurilor de utilizator livrate de IBM pentru comenzi restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
PRTDSKINF	R				
PRTERRLOG		S	S	S	S
PRTINTDTA		S	S	S	S
PRTPRFINT	R				
PWRDWNSYS	R		S		
RCLDBXREF	R				
RCLOBJOWN	R				
RCLOPT	R				
RCLSPLSTG		S	S	S	S
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				
RMVCRGDEVE	R				
RMVCRGNODE	R				
RMVCRSDMNK	R				
RMVDEVDMNE	R				
RMVDFRID	R				
RMVDSTQ		S	S		
RMVDSTRTE		S	S		
RMVDSTSYSN		S	S		
RMVDWDFN					
RMVEXITPGM	R				
RMVJRNCHG		S		S	
RMVJWDFN					
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			

Tabela 151. Autorizările profilurilor de utilizator livrate de IBM pentru comenzi restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
RMVTRCFTR	R				
RSTAUT	R				
RST[3]					
RSTCFG	R				
RSTDFROBJ	R				
RSTDLO	R				
RSTLIB	R				
RSTLICPGM	R				
RSTOBJ[3]					
RSTPFRCOL	R				
RSTPFRDTA					
RSTS36F	R				
RSTS36FLR	R				
RSTS36LIBM	R				
RSTS38AUT	R				
RSTUSFCNR[4]					
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				
SAVPFRCOL	R				
SAVPFRDTA					
SAVRSTCHG	R				
SAVRSTLIB	R				
SAVRSTOBJ	R				
SBMFNCJOB	R				
SBMNWSCMD	R				
SETMSTK	R				
SETMSTKEY					
SNDDSTQ		S	S		
SNDPRD		S	S	S	S
SNDPTF		S	S	S	S
SNDPTFORD				S	S

Tabela 151. Autorizările profilurilor de utilizator livrate de IBM pentru comenzi restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
SNDSMGOBJ		S	S	S	S
SNDSRVRQS				S	S
STRASPBAL	R				
STRBEST	R				
STRCHTSVR	R				
STRCLUNOD	R				
STRCMNTRC				S	
STRCRG	R				
STRDBG		S		S	S
STRDBGSVR		S	S	S	S
STRDW					
STRHOSTSVR		S	S	S	S
STRIDXMON	R				
STRIPSIFC		S	S	S	S
STRJW	R				
STRJOBTRC					
STRMGDSYS		S	S	S	S
STRMGRSRV		S	S	S	S
STRMSF[1]			S	S	S
STRNFSSVR	R				
STROBJCVN	R				
STRPEX		S		S	
STRPFRG	R				
STRPFRT	R				
STRPFRTRC	R			S	
STRRGZIDX	R				
STRSPLRCL	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				
STRWCH	R				
TRCASPBAL	R				
TRCCPIC	R				

Tabela 151. Autorizările profilurilor de utilizator livrate de IBM pentru comenzi restricţionate (continuare)

Nume comandă	QSECOFR	QPGMR	QSYSOPR	QSRV	QSRVBAS
TRCICF	R				
TRCINT		S		S	
TRCJOB		S	S	S	S
TRCTCPAPP				S	S
TRNPIN	R				
UPDPTFINF	R				
VFYCMN		S	S	S	S
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				
WRKJRN		S	S	S	
WRKLIB					
WRKLIBPDM					
WRKLICINF	R				
WRKNWSCFG	R				
WRKORDINF			S	S	
WRKPEXDFN		S		S	
WRKPEXFTR		S		S	
WRKPGMTBL	R				
WRKPRB		S	S	S	S
WRKPTFGRP		S	S	S	S
WRKPTFORD	R			S	S
WRKSRVPVD				S	S
WRKSYSACT	R				
WRKTRC	R				
WRKTXTIDX	R				
WRKUSRTBL	R				
WRKWCH	R				

[1] Profilul de utilizator QMSF este de asemenea autorizat la această comandă.

[2] QSRV poate să ruleze această comandă doar dacă nu se face un IPL.

[3] În plus la QSYS, profilul de utilizator QRDARS400 are autorizare.

[4] În plus la QSYS, profilul de utilizator QUMB are autorizare.

Anexa D. Autorizare necesară pentru obiecte folosite de comenzi

Tabelele din această secţiune arată ce autorizare este necesară pentru obiecte referite de comenzi.

De exemplu, in intrarea pentru comanda Modificare profil utilizator (CHGUSRPRF) tabela listează toate obiectele la 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 i5/OS (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.

Următoarele secţiuni sunt descrieri ale coloanelor din tabele.

Obiect referit

Obiectele listate în coloana *Obiect referit* sunt obiectele la care utilizatorul poate necesita autorizare la folosirea comenzii.

Autorizare necesară pentru obiect

Autorizările specificate în tabele arată autorizările de obiect şi autorizările de date care sunt necesare pentru obiect la folosirea comenzii.

Autorizare necesară 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.

Tip obiect

Valoarea se referă la tipul de obiect specificat în coloana Obiect referit.

Sistem de fişiere

Valoarea se referă la tipul de sistem de fişiere la care aparţine obiecte referit.

Pentru sistemul de fişiere integrat din sistemul de operare i5/OS, consultaţi Sistem de fişiere integrat.

Următoarea tabelă descrie autorizările care sunt 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.

Tabela 152. Descrierea tipurilor de autorizări

specială	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.

Tabela 152. Descrierea tipurilor de autorizări (continuare)

specială	Nume	Funcţii permise
*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. Modificarea atributelor pachetelor SQL. Mutarea bibliotecii sau folderului la un alt ASP.
*OBJREF	Object Reference - Referinţă la obiect	Specificaţi un fişier bază de date ca părinte într-o restricţie referenţiale. De exemplu, să presupunem că vreţi să definiţi o regulă că o înregistrare client trebuie să existe în fişierul CUSMAS înainte ca o comandă de la client să poate fi adăugată în fişierul CUSORD. Vă trebuie autorizarea *OBJREF pentru fişierul CUSMAS pentru a defini această regulă.
*AUTLMGT	Authorization List Management - Gestionare listă de autorizare	Adăugaţi şi înlăturaţi utilizatori şi autorizările lor din lista de autorizare.
Autorizări date:		
*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.

[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.

În afară de aceste valori, coloanele *Autorizare necesară* ale tabelei ar putea arăta subseturi definite de sistem ale acestor autorizări. Tabela următoare prezintă subseturile autorizărilor pentru obiect şi autorizărilor pentru date.

Tabela 153. Autorizare definită de sistem

specială	*ALL	*CHANGE	*USE	*EXCLUDE
Autorizări obiect				
*OBJOPR	X	X	X	
*OBJMGT	X			
*OBJEXIST	X			
*OBJALTER	X			
*OBJREF	X			
Autorizări pentru date				

Tabela 153. Autorizare definită de sistem (continuare)

specială	*ALL	*CHANGE	*USE	*EXCLUDE
*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 154. Autorizare definită de sistem

specială	*RWX	*RW	*RX	*R	*WX	*W	*X
Autorizări obiect							
*OBJOPR	X	X	X	X	X	X	X
*OBJMGT							
*OBJEXIST							
*OBJALTER							
*OBJREF							
Autorizări 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

Supoziţii folosire comandă

Există unele supoziţii implicite care trebuie să le luaţi în considerare înainte de a folosi orice comandă.

1. Autorizare *USE este necesară pentru a folosi orice comandă. Această autorizare nu este menţionată în tabele.
2. Pentru a introduce orice comandă de afişare, aveţi nevoie de autorizare operaţională asupra fişierului de afişare livrat de IBM, fişierul de ieşire imprimantă sau grupul panou care este folosit de comandă. Aceste fişiere şi grupuri de panouri sunt livrate cu autorizarea publică *USE.

Reguli generale pentru autorizările de obiect în comenzi

Această tabelă arată regulile generale pentru autorizările de obiect în comenzi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 prefix cale	*X	
	Directorul când este specificat modelul (* sau ?)	*R	

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
Creare obiect în director	Directoarele din prefix cale	*X	
	Directorul care va conţine obiecte noi	*WX	
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 de utilizator care va deţine obiectul creat (fie profilul de 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 dacă este 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
	Fişier format (QA*xxxxx*), dacă fişierul ieşire nu există	*OBJOPR	
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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 de 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 de 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 de utilizator care rulează comanda afişată devine proprietarul fişierului de ieşire nou creat, 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 autorizare specială *JOBCTL nu are nevoie de autorizare suplimentară asupra cozii de ieşire. Un utilizator cu autorizare specială *SPLCTL nu are nevoie de autorizare suplimentară asupra cozii 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 majoritatea obiectelor

Această tabelă listează comenzile care pot funcţiona pe majoritatea obiectelor în ordine alfabetică.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Tabela 155. Comenzi comune pentru majoritatea obiectelor

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ALCOBJ [1,2,11]	Obiect	*OBJOPR	*EXECUTE
ANZOBJCVN (Q) [20]			
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

Tabela 155. Comenzi comune pentru majoritatea obiectelor (continuare)

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
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 de utilizator vechi	*DLT	*EXECUTE
	Profil de 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 proprietate şi *OBJEXIST sau *ALLOBJ	*EXECUTE
	Profil de utilizator vechi	*DLT	
	Profil de 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 informaţiile 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 155. Comenzi comune pentru majoritatea obiectelor (continuare)

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
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]			
RCLDBXREF			
RCLOBJOWN (Q)			
RCLSTG (Q)			
RCLTMPSTG (Q)	Obiect	*OBJMGT	*EXECUTE
RMVDFRID (Q) [10]			
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	
RSTDFROBJ (Q) [10]	ieşire de imprimantă QSYS/QPSRLDSP, dacă OUTPUT(*PRINT) este specificat	*USE	*EXECUTE
	Fişier de ieşire, dacă este specificat	Vedeţi regulile generale	Vedeţi regulile generale
	fişier referinţă câmp QSYS/QASRRSTO pentru fişier de ieşire, dacă un fişier de ieşire este specificat şi nu există	*USE	*EXECUTE

Tabela 155. Comenzi comune pentru majoritatea obiectelor (continuare)

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
RSTOBJ (Q)[3,13, 31, 33]	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 medii	*USE	*EXECUTE
	Cozile de mesaje care sunt restaurate în biblioteca unde există deja	*OBJOPR, *OBJEXIST [8]	*EXECUTE, *ADD
	Profilul de utilizator deţine obiectele care sunt create	*ADD [8]	
	Program care adoptă autorizare	Proprietar sau autorizare specială *SECADM şi *ALLOBJ	*EXECUTE
	Bibliotecă destinaţie	*EXECUTE, *ADD [8]	
	Bibliotecă pentru obiect salvat dacă VOL(*SAVVOL) este specificat	*USE [8]	
	Fişier de salvare	*USE	*EXECUTE
RSTOBJ (Q)	Unitate de bandă sau unitate optică	*USE	*EXECUTE
	Fişier bandă (QSYSTAP) sau fişier dischetă (QSYSDKT)	*USE [8]	*EXECUTE
	Fişier optic (OPTFILE)[22]	*R	Neaplicabilă
	Director părinte sau fişier optic (OPTFILE)[22]	*X	Neaplicabilă
	Prefix cale OPTFILE[22]	*X	Neaplicabilă
	Volum optic[24]	*USE	Neaplicabilă
	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
	Descriere de dispozitiv ASP[25]	*USE	
RSTSYSINF	Fişier de salvare	*USE	*EXECUTE
	Unitate de bandă sau unitate optică	*USE	*EXECUTE
	Fişier optic (OPTFILE)[22]	*R	Neaplicabilă
	Director părinte sau fişier optic (OPTFILE)[22]	*X	Neaplicabilă
	Prefix de cale de OPTFILE[22]	*X	Neaplicabilă
	Volum optic[24]	*USE	Neaplicabilă
RVKPUBAUT [20]			
RTVOBJD [2, 29]	Obiect	O autorizare alta decât *EXCLUDE	*EXECUTE
RVKOBJAUT [3,5,15, 27]	Dispozitiv ASP (dacă este specificat)	*USE	

Tabela 155. Comenzi comune pentru majoritatea obiectelor (continuare)

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
SAVCHGOBJ [3, 32]	Obiect (8)	*OBJEXIST	*EXECUTE
	Unitate de bandă sau 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
	Spaţiu comenzi utilizator, dacă este specificat	*USE	*EXECUTE
SAVCHGOBJ	Fişier optic (OPTFILE)[22]	*RW	Neaplicabilă
	Director părinte sau fişier optic (OPTFILE)[22]	*WX	Neaplicabilă
	Prefix cale sau fişier optic (OPTFILE)[22]	*X	Neaplicabilă
	Director rădăcină (/) al volumului optic[22, 23]	*RWX	Neaplicabilă
	Volum 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
	Descriere de dispozitiv ASP[25]	*USE	
SAVOBJ [3, 32]	Obiect	*OBJEXIST [8]	*EXECUTE
	Definiţie medii	*USE	*EXECUTE
	Unitate de bandă sau 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
	Spaţiu comenzi utilizator, dacă este specificat	*USE	*EXECUTE
SAVOBJ	Fişier optic (OPTFILE) [22]	*RW	Neaplicabilă
	Director părinte sau fişier optic (OPTFILE)[22]	*WX	Neaplicabilă
	Prefix cale OPTFILE[22]	*X	Neaplicabilă
	Director rădăcină (/) al volumului optic[22, 23]	*RWX	Neaplicabilă
	Volum 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
	Descriere de dispozitiv ASP[25]	*USE	
SAVSTG [10]			
SAVSYS [10]	Unitate de bandă, unitate optică	*USE	*EXECUTE
	Director rădăcină (/) al volumului optic[22]	*RWX	Neaplicabilă
	Volum optic[24]	*CHANGE	Neaplicabilă

Tabela 155. Comenzi comune pentru majoritatea obiectelor (continuare)

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
SAVSYSINF	Definiţie medii	*USE	*EXECUTE
	Unitate de bandă sau 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
	Fişier optic (OPTFILE)[22]	*RW	Neaplicabilă
	Director părinte sau fişier optic (OPTFILE) [22]	*WX	Neaplicabilă
	Prefix cale OPTFILE[22]	*X	Neaplicabilă
	Director rădăcină (/) al volumului optic[22, 23]	*RWX	Neaplicabilă
	Volum optic[24]	*CHANGE	
SAVRSTCHG	Pe sistemul sursă, aceeaşi autorizare precum se cere prin comanda SAVCHGOBJ.		
	Pe sistemul destinaţie, aceeaşi autorizare precum se cere prin comanda RSTOBJ.		
	Descriere de dispozitiv ASP[25]	*USE	
SAVRSTOBJ	Pe sistemul sursă, aceeaşi autorizare precum se cere prin comanda SAVOBJ.		
	Pe sistemul destinaţie, aceeaşi autorizare precum se cere prin comanda RSTOBJ.		
	Descriere de dispozitiv ASP[25]	*USE	
SETOBJACC	Obiect	*OBJOPR	*EXECUTE
STROBJCVN (Q)[20]			
STRSAVSYNC[34]			
WRKOBJ [19]	Obiect	Orice autorizare	*USE
WRKOBJLCK	Obiect		*EXECUTE
	Dispozitiv ASP	*EXECUTE	
WRKOBJOWN [17]	Profil de utilizator	*READ	*EXECUTE
WRKOBJPGP [17]	Profil de utilizator	*READ	*EXECUTE
WRKOBJPVT[17]	Profil de 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.

Tabela 155. Comenzi comune pentru majoritatea obiectelor (continuare)

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
[6]	Trebuie să fiţi proprietarul sau să aveţi autorizarea specială *ALLOBJ pentru a garanta autorizarea *OBJMGT sau *AUTLMGT.		
[7]	Această comandă nu poate fi utilizată pentru profiluri de 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 de utilizator OWNER(*GRPPRF), proprietarul 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 autorizărilor pentru noul obiect, noul obiect creat este şters.		
[10]	Trebuie să aveţi autorizarea specială *SAVSYS.		
[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 autorizarea specială *ALLOBJ pentru a specifica altă valoare decât *NONE pentru parametrul ALWOBJDIF.		
[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 păstrător de autorizare asociată, autorizarea *ALL pentru păstrătorul de autorizare este cerută.		
[17]	Această comandă nu suportă sistemul fişier QOPT.		
[18]	Trebuie să aveţi autorizarea 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 de utilizator care rulează comanda. Dacă obiectul sursă are un grup primar, noul obiect se poate să nu aibă acelaşi grup primar, dar autorizarea pe care o are grupul primar pe obiectul sursă va fi duplicată pe 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 ştergeţi 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.		

Tabela 155. Comenzi comune pentru majoritatea obiectelor (continuare)

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
[26] Trebuie să aveţi autorizarea specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.			
[27] ***** Risc securitate ***** Revocarea specifică a tuturor 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.			
[30] Vedeţi comenzile CHGPGM, CHGSRVPGM şi CHGMOD pentru a determina autorizarea necesară pentru a converti programe, programe service şi module.			
[31] Trebuie să aveţi autorizare specială *ALLOBJ pentru a specifica *YES pentru parametrul PVTAUT.			
[32] Trebuie să aveţi autorizare specială *ALLOBJ sau *SAVSYS pentru a specifica *YES pentru parametrul PVTAUT.			
[33] Trebuie să aveţi autorizare specială *SAVSYS pentru a specifica un nume pentru parametrul DFRID.			
[34] Trebuie să aveţi autorizare specială *SAVSYS şi *JOBCTL.			

Comenzi recuperare cale acces

Această tabelă listează autorizările specifice necesare pentru comenzile de recuperare cale de acces

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Aceste comenzi nu necesită nici o autorizare obiect.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
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 autorizarea specială *JOBCTL pentru a folosi această comandă.			
[2] Trebuie să aveţi autorizarea specială *ALLOBJ pentru a folosi această comandă.			

Comenzi AFP

Această tabelă listează autorizările specifice necesare pentru comenzile AFP.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
ADDFNTTBLE	Tabel font DBCS	*CHANGE	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CHGCDEFNT	Resursă font	*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 font	*OBJEXIST	*EXECUTE
DLTFNTTBL	Tabel font DBCS	*CHANGE	*EXECUTE
DLTFORMDF	Definiţie formular	*OBJEXIST	*EXECUTE
DLTOVL	Suprapunere	*OBJEXIST	*EXECUTE
DLTPAGDFN	Definiţie de pagină	*OBJEXIST	*EXECUTE
DLTPAGSEG	Segment de pagină	*OBJEXIST	*EXECUTE
DSPCDEFNT	Resursă font	*USE	*EXECUTE
DSPFNTRSCA	Resursă font	*USE	*EXECUTE
DSPFNTTBL	Tabel font DBCS	*USE	*EXECUTE
RMVFNTTBLE	Tabel font DBCS	*CHANGE	*EXECUTE
WRKFNTRSC [1]	Resursă font	*USE	*USE
WRKFORMDF [1]	Definiţie formular	*USE	*USE
WRKOVL [1]	Suprapunere	*USE	*USE
WRKPAGDFN [1]	Definiţie de pagină	Orice autorizare	*USE
WRKPAGSEG [1]	Segment de pagină	*USE	Orice autorizare

1 Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea cerută de operaţii individuale.

Comenzi socket-uri AF_INET peste SNA

Această tabelă listează autorizările specifice necesare pentru comenzile socket-uri AF_INET peste SNA.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate pentru această comandă. Responsabilul cu securitatea poate acorda autorizare *USE altora.

Aceste comenzi nu necesită autorizări de obiect:

Aceste comenzi nu necesită autorizări de obiect:			
ADDIPSIFC[1] ADDIPSRTE[1] ADDIPSLOC[1] CFGIPS	CHGIPSIFC[1] CHGIPSLOC[1] CHGIPSTOS[1] CVTIPSIFC	CVTIPSLOC ENDIPSIFC (Q) PRTIPSCFG RMVIPSIFC[1]	RMVIPSLOC[1] RMVIPSRTE[1] STRIPSIFC (Q)
[1] Trebuie să aveţi autorizarea specială *IOSYSCFG pentru a folosi această comandă.			

Comenzi alertare

Această tabelă listează autorizările specifice necesare pentru comenzile de alertare.

		Autorizare necesară	
Comandă	**Obiect referit**	**Pentru obiect**	**Pentru bibliotecă**
ADDALRD	Tabelă alertă	*USE, *ADD	*EXECUTE
CHGALRD	Tabelă alertă	*USE, *UPD	*EXECUTE
CHGALRTBL (Q)	Tabelă alertă	*CHANGE	*EXECUTE
CRTALRTBL (Q)	Tabelă alertă		*READ, *ADD
DLTALR	Fişier fizic QAALERT	*USE, *DLT	*EXECUTE
DLTALRTBL (Q)	Tabelă alertă	*OBJEXIST	*EXECUTE
RMVALRD	Tabelă alertă	*USE, *DLT	*EXECUTE
WRKALR [1]	Fişier fizic QAALERT	*USE	*EXECUTE
WRKALRD [1]	Tabelă alertă	*USE	*EXECUTE
WRKALRTBL [1]	Tabelă alertă	*READ	*USE
[1] Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea cerută de operaţii individuale.			

Comenzi dezvoltare aplicaţie

Această tabelă listează autorizările specifice necesare pentru comenzile de dezvoltare de aplicaţii.

		Autorizare necesară	
Comandă	**Obiect referit**	**Pentru obiect**	**Pentru bibliotecă**
FNDSTRPDM	Parte sursă	*READ	*EXECUTE
MRGFORMD	Descriere formular	*READ	*EXECUTE
STRAPF [1]	Fişier sursă	*OBJMGT, *CHANGE	*READ, *ADD
	Comenzile CRTPF, CRTLF, ADDPFM, ADDLFM şi RMVM	*USE	*EXECUTE
STRBGU [1]	Grafic	*OBJMGT, *CHANGE	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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
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, 4]			
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).

[4] Această comandă cere autorizarea specială *ALLOBJ.

Comenzi păstrător de autorizare

Această tabelă listează autorizările specifice necesare pentru comenzile păstrătorului de autorizare.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
CRTAUTHLR (Q)	Obiect asociat dacă acesta există	*ALL	*EXECUTE
DLTAUTHLR	Păstrător autoritate	*ALL	*EXECUTE
DSPAUTHLR	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.

Comenzile listei de autorizare

Această tabelă prezintă autorizările specifice necesare pentru comenzile listei de autorizare.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru biblioteca 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
RMVAUTLE [1]	*AUTL	*AUTLMGT sau drept de proprietate	*EXECUTE
RTVAUTLE [2]	*AUTL	*AUTLMGT sau drept de proprietate	*EXECUTE
WRKAUTL [3,4,5]	*AUTL		

1 Trebuie să fiţi proprietar sau să aveţi autorizare gestionare listă de autorizare.

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 autorizarea necesară de operaţie.

4 Nu trebuie să fiţi exclus (*EXCLUDE) din lista autorizare.

5 O anumită autorizare pentru lista autorizare este cerută.

Comenzi director legare

Această tabelă listează autorizările specifice necesare pentru comenzile director legare.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 autorizare	*USE
WRKBNDDIRE [1]	Director legare	*READ, *OBJOPR	*USE

[1] Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea cerută de operaţie.

Comenzi modificare descriere cerere

Această tabelă listează autorizările specifice necesare pentru comenzile de modificare descriere cerere.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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	Modificare descriere cerere de modificare	*CHANGE	*EXECUTE
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 autorizarea necesară de operaţie.

Comenzi diagramă

Această tabelă listează autorizările specifice necesare pentru comenzile diagramă.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
DLTCHTFMT	Format grafic	*OBJEXIST	*EXECUTE
DSPCHT	Format grafic	*USE	*USE
	Fişier bază de date	*USE	*USE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
DSPGDF	Fişier bază de date	*USE	*USE
STRBGU (Opţiunea 3) [2]	Format grafic	*CHANGE, *OBJEXIST	*EXECUTE
WRKCHTFMT [1]	Format grafic	Orice autorizare	*USE

[1] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizarea necesară de operaţie.

[2] Opţiunea 3 din meniul BGU (afişat atunci când este rulat STRGBU) este opţiunea Modificare format diagramă.

Comenzi clasă

Această tabelă listează autorizările specifice necesare pentru comenzile clasă.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 autorizarea necesară de operaţie.

Comenzi clasă-de-service

Această tabelă listează autorizările specifice necesare pentru comenzile clasă-de-service.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CHGCOSD [3]	Descriere clasă de serviciu	*CHANGE, OBJMGT	*EXECUTE
CRTCOSD [3]	Descriere clasă de serviciu		
DLTCOSD	Descriere clasă de serviciu	*OBJEXIST	*EXECUTE
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 autorizarea cerută de operaţii individuale.

[2] E necesară aceeaşi autorizare pentru obiect.

[3] Pentru a folosi această comandă, trebuie să aveţi autorizarea specială *IOSYSCFG.

Comenzi cluster

Această tabelă listează autorizările specifice necesare pentru comenzi cluster.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul cu securitatea poate acorda *USE altora.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 de utilizator pentru rulare program de ieşire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
	Descriere controler	*USE, *OBJMGT	
	Descriere linie	*USE, *OBJMGT	
	Descriere server de reţea (NWS)	*USE, *OBJMGT	
ADDCRGNODE (Q)[1]	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil de 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 de utilizator pentru rulare program de ieşire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
	Coada de mesaje preluare la defectare	*OBJOPR, *ADD	*EXECUTE
	Descriere controler	*USE, *OBJMGT	
	Descriere linie	*USE, *OBJMGT	
	Descriere server de reţea (NWS)	*USE, *OBJMGT	

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
CHGCRGDEVE (Q)[1]	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil de utilizator pentru rulare program de ieşire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
	Descriere controler	*USE, *OBJMGT	
	Descriere linie	*USE, *OBJMGT	
	Descriere server de reţea (NWS)	*USE, *OBJMGT	
CHGCRGPRI (Q)[1]	Programul serviciu QCSTCRG2	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil de utilizator pentru rulare program de ieşire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
	Comanda VFYCFG (Vary configuration - Verificare configurare)	*USE	
	Descriere controler	*USE, *OBJMGT	
	Descriere linie	*USE, *OBJMGT	
	Descriere server de reţea (NWS)	*USE, *OBJMGT	
CRTADMDMN (Q)[1, 3]	Profil de utilizator QCLUSTER	*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 de 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
	Descriere controler	*USE, *OBJMGT	
	Descriere linie	*USE, *OBJMGT	
	Descriere server de reţea (NWS)	*USE, *OBJMGT	
DLTADMDMN (Q) [1]	Grup resursă cluster	*OBJEXIST, *USE	
	QUSRSYS	*EXECUTE	
	QCLUSTER	*USE	
DLTCLU (Q)[1]	Programul serviciu QCSTCTL	*USE	
DLTCRG[1]	Grup resursă cluster	*OBJEXIST, *USE	*EXECUTE (QUSRSYS)

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
DLTCRGCLU (Q)[1]	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*OBJEXIST, *USE	*EXECUTE (QUSRSYS)
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil de 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 autorizări	*CHANGE	
ENDCRG (Q)[1]	Programul serviciu QCSTCRG2	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE (QUSRSYS)
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil de 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 de utilizator pentru rulare program de ieşire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
	Descriere controler	*USE, *OBJMGT	
	Descriere linie	*USE, *OBJMGT	
	Descriere server de reţea (NWS)	*USE, *OBJMGT	
RMVCRGNODE (Q) [1]	Programul serviciu QCSTCRG1	*USE	
	Grup resursă cluster	*CHANGE, *OBJEXIST	*EXECUTE
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil de utilizator pentru rulare program de ieşire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
	Descriere controler	*USE, *OBJMGT	
	Descriere linie	*USE, *OBJMGT	
	Descriere server de reţea (NWS)	*USE, *OBJMGT	
RMVDEVDMNE (Q)[1]	Programul serviciu QCSTDD	*USE	
STRCHTSVR	Listă de autorizări	*CHANGE	
STRCLUNOD (Q)[1]	Programul serviciu QCSTCTL	*USE	

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
STRCRG (Q)[1]	Programul serviciu QCSTCRG2	*USE	
	Grup resursă cluster	*CHANGE	*EXECUTE
	Program ieşire	*EXECUTE[2]	*EXECUTE[2]
	Profil de utilizator pentru rulare program de ieşire	*USE	
	Descriere dispozitiv	*USE, *OBJMGT	
	Descriere controler	*USE, *OBJMGT	
	Descriere linie	*USE, *OBJMGT	
	Descriere server de reţea (NWS)	*USE, *OBJMGT	
WRKCLU[4]	Grup resurse cluster	*USE	*EXECUTE

[1] Trebuie să aveţi autorizarea specială *IOSYSCFG pentru a folosi această comandă.

[2] Se aplică pentru profil de utilizator apelator şi profil de utilizator rulare program de ieşire.

[3] Profilului de utilizator care apelează îi sunt garantate autorizări *CHANGE şi *OBJEXIST asupra grupului de resurse cluster.

[4] Trebuie să aveţi autorizare specială *SERVICE sau să fiţi autorizat la funcţia de urmărire service i5/OS prin Application Administration în System i Navigator. 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.

Comenzi *CMD

Această tabelă listează autorizările specifice necesare pentru comenzile legate de operaţiile din comandă.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
CHGCMD	Comandă	*OBJMGT	*EXECUTE
CHGCMDDFT	Comandă	*OBJMGT, *USE	*EXECUTE
CHGPRXCMD	Comandă proxy	*OBJMGT	*EXECUTE
CRTCMD	Fişier sursă	*USE	*EXECUTE
	Comandă: REPLACE(*NO)		*READ, *ADD
	Comandă: REPLACE(*YES)	Vedeţi regulile generale.	Vedeţi regulile generale.
CRTPRXCMD	Comandă proxy: REPLACE(*NO)		*READ, *ADD
	Comandă proxy: REPLACE(*YES)	Vedeţi regulile generale la pagina D-2	Vedeţi regulile generale la pagina D-2
DLTCMD	Comandă	*OBJEXIST	*EXECUTE
DSPCMD	Comandă	*USE	*EXECUTE
GENCMDDOC[3]	Comandă	*USE	*EXECUTE
	Grup de panouri (asociat)	*USE	*EXECUTE
	Fişier ieşire: REPLACE = (*YES)	*ALL	*CHANGE
SBMRMTCMD	Comandă	*OBJOPR	*EXECUTE
	Fişier DDM	*USE	*EXECUTE
SLTCMD [1]	Comandă	Orice autorizare	*USE
WRKCMD [2]	Comandă	Orice autorizare	*USE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă

[1] Drept de proprietate sau unele autorizări pentru obiect sunt necesare.

[2] Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea 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.

Comenzi de control comitere

Această tabelă listează autorizările specifice necesare pentru comenzile de control al comiterii.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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.

Comenzi de informaţii pe partea de comunicaţii

Această tabelă listează autorizările specifice necesare pentru comenzile pe partea de comunicaţii.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CHGCSI	Obiect CSI	*USE, *OBJMGT	*EXECUTE
	Descriere dispozitiv [1]	*CHANGE	
CRTCSI	Obiect CSI		*READ, *ADD
	Descriere dispozitiv [1]	*CHANGE	
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).

Comenzi de configuraţie

Această tabelă listează autorizările specifice necesare pentru comenzile de configurare.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

		Autorizare necesară	
Comandă	**Obiect referit**	**Pentru obiect**	**Pentru bibliotecă**
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 de utilizator deţine obiectele care sunt create	*ADD [1]	
	Unitate de 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 şi cea necesară pentru comanda SAVCFG.		
	Pe sistemul destinaţie, aceeaşi autorizare ca şi cea necesară pentru comanda RSTCFG.		
VRYCFG [3, 5, 6, 7]	Obiect	*USE, *OBJMGT	*EXECUTE
WRKCFGSTS [4]	Obiect	*OBJOPR	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă

[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 autorizarea specială *ALLOBJ pentru a specifica altă valoare decât *NONE pentru parametrul ALWOBJDIF, sau RESETSYS(*YES).

[6] Trebuie să aveţi autorizarea specială *IOSYSCFG pentru biblioteca mediu de stocare când starea e *ALLOCATE sau *DEALLOCATE.

[7] Trebuie să aveţi autorizările speciale *IOSYSCFG şi *SECADM pentru a specifica GENPTHCERT(*PWDGRP), USRPRF(*YES) sau OMITUSRPRF.

Comenzi listă de configurare

Această tabelă listează autorizările specifice necesare pentru comenzile listă de configurare.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 autorizarea specială *IOSYSCFG.

Comenzi listă conexiuni

Această tabelă listează autorizările specifice necesare pentru comenzile listă de conexiuni.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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.

Comenzi descriere controler

Această tabelă listează autorizările specifice necesare pentru comenzile descriere controler.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
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		

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 autorizarea specială *IOSYSCFG.

[3] Pentru a folosi această comandă trebuie să aveţi autorizările speciale *ALLOBJ şi *IOSYSCFG sau *AUDIT.

Comenzi criptografie

Această tabelă listează autorizările specifice necesare pentru comenzile de criptografie.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate pentru această comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ADDCKMKSFE	Fişier utilizator	*ADD, *OBJOPR, *READ	
	Bibliotecă utilizator		*EXECUTE
	Director utilizator	*X	
	Fişier flux utilizator	*R	
ADDCRSDMNK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
	Coada de mesaje QHST	*OBJOPR, *ADD	*EXECUTE
ADDMSTPART (Q) [1]			
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
CHKMSTKVV (Q) [1]			
CLRMSTKEY (Q) [1]			
CPHDTA (Q)			
CRTCKMKSF	Bibliotecă utilizator		*ADD, *EXECUTE
DSPCKMKSFE	Fişier utilizator	*OBJOPR, *READ	
	Bibliotecă utilizator		*EXECUTE
ENCCPHK (Q)			
ENCFRMMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *ADD	*EXECUTE
ENCTOMSTK (Q)	QUSRSYS/QACRKTBL *FILE	*OBJOPR, *READ	*EXECUTE
GENCKMKSFE	Fişier utilizator	*ADD, *OBJOPR, *READ	
	Bibliotecă utilizator		*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
RMVCKMKSFE	Fişier utilizator	*DLT, *OBJOPR	
	Bibliotecă utilizator		*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
SETMSTKEY (Q) [1]			

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
TRNCKMKSF	Fişier utilizator	*OBJOPR, *READ, *UPD	
	Bibliotecă utilizator		*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

[1] Trebuie să aveţi autorizările speciale *ALLOBJ şi *SECADM pentru a folosi această comandă.

Comenzi zonă de date

Această tabelă listează autorizările specifice necesare pentru comenzile zonă de date.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CHGDTAARA [1]	Zonă de date	*CHANGE	*EXECUTE
CRTDTAARA [1]	Zonă de date		*READ, *ADD
	Descriere dispozitiv APPC[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 autorizare	*USE

[1] Dacă comenzi de creare şi modificare zonă de date sunt rulate folosind funcţii de limbaj de nivel înalt, aceste autorizări sunt încă necesare chiar prin autorizarea comenzi nu este.

[2] Autorizarea este verificată în momentul rulării, dar nu şi la momentul compilării.

[3] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizarea necesară de operaţie.

[4] Autorizarea este verificată când este folosită zona de date.

Comenzi coadă de date

Această tabelă listează autorizările specifice necesare pentru comenzile coadă de date.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
[1] Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea cerută de operaţii individuale.			
[2] Autorizarea este verificată când este folosită zona de date.			

Comenzi descriere dispozitiv

Această tabelă listează autorizările specifice necesare pentru comenzi de descriere dispozitiv.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CFGDEVMLB [4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
CHGASPA (Q)			
CHGASPACT (Q)[7]	Descriere dispozitiv	*USE	
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
CHGDEVNWSH[4]	Descriere dispozitiv	*CHANGE, *OBJMGT	*EXECUTE
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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
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		
CRTDEVNWSH[4]	Descriere dispozitiv		*EXECUTE
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		
DLTDEVD [1]	Descriere dispozitiv	*OBJEXIST	*EXECUTE
DSPASPSTS	Descriere dispozitiv	*USE	
DSPCNNSTS	Descriere dispozitiv	*OBJOPR	*EXECUTE
DSPDEVD	Descriere dispozitiv	*USE	*EXECUTE
ENDASPBAL (Q)			
ENDDEVRCY	Descriere dispozitiv	*USE	*EXECUTE
HLDCMNDEV [2]	Descriere dispozitiv	*OBJOPR	*EXECUTE
PRTCMNSEC [4, 5]			
RLSCMNDEV	Descriere dispozitiv	*OBJOPR	*EXECUTE
RSMDEVRCY	Descriere dispozitiv	*USE	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
SETASPGRP[6]	Toate descrierile de dispozitive din grupul ASP	*USE	
	Toate bibliotecile specificate din lista de biblioteci înainte de spaţiul de nume al bibliotecii şi lista de biblioteci sunt modificate	*USE	
STRASPBAL (Q)			
TRCASPBAL (Q)			
WRKDEVD [3]	Descriere dispozitiv	*OBJOPR	*EXECUTE

[1] Pentru a înlătura o coadă de ieşire asociată, autorizare existenţă obiect (*OBJEXIST) asupra cozii de ieşire şi autorizare de execuţie (*EXECUTE) asupra bibliotecii QUSRSYS sunt necesare.

[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 autorizarea 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.

[6] Când *CURUSR este specificat pentru grupul ASP (ASPGRP) sau parametrul Biblioteci pentru firul de execuţie curent (USRLIBL), trebuie de asemenea să aveţi autorizare de citire (*READ) asupra descrierii de job care este listată în profilul de utilizator şi autorizare de execuţie (*EXECUTE) asupra bibliotecii unde este localizată descrierea jobului.

[7] Trebuie să aveţi autorizare specială *JOBCTL pentru a rula această comandă.

Comenzi emulare dispozitiv

Această tabelă listează autorizările specifice necesare pentru comenzile de emulare dispozitiv.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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
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	Fişier-sursă	*OBJOPR	*EXECUTE
TRMPRTEML	Descriere dispozitiv emulare	*OBJOPR	*EXECUTE

Comenzi director şi umbrire director

Această tabelă listează autorizările specifice necesare pentru comenzile director şi umbrire director.

Aceste comenzi nu necesită nici o autorizare obiect:			
ADDDIRE [2] ADDDIRSHD [1] CHGSYSDIRA [2] CHGDIRE [3]	CHGDIRSHD [1] CPYFRMDIR [1] CPYTODIR [1] DSPDIRE	ENDDIRSHD [4] RMVDIRE [1] RMVDIRSHD [1] RNMDIRE [2]	STRDIRSHD [4] WRKDIRE [3,5] WRKDIRLOC [1,5] 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 autorizarea specială *JOBCTL.

[5] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizarea necesară de operaţie.

Comenzi server de director

Această tabelă listează autorizările specifice necesare pentru comenzile server de director.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CHGDIRSRVA [1]			
CPYTOLDIF [2]	Fişier flux LDIF (dacă există deja)	*STMF	*W, *OBJEXIST, *OBJMGT
	Director părinte al fişierului flux LDIF	*DIR	*WX

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CPYFRMLDIF [2]	Fişier flux LDIF	*STMF	*R
	Director părinte al fişierului flux LDIF	*DIR	*X
DB2LDIF [2]	Fişier flux LDIF (dacă există deja)	*STMF	*W, *OBJEXIST, *OBJMGT
	Director părinte al fişierului flux LDIF	*DIR	*WX
LDIF2DB [2]	Fişier flux LDIF	*STMF	*R
	Directorul părinte al fişierului flux LDIF	*DIR	*X

[1] Trebuie să aveţi autorizare specială *ALLOBJ şi *IOSYSCFG.

[2] Pentru a folosi această comandă, trebuie să îndepliniţi una din următoarele condiţii:
- Să aveţi autorizări speciale *ALLOBJ şi *IOSYSCFG
- Să furnizaţi DN administrator şi parola
- Să fiţi un administrator de server de director

Comenzi disc

Această tabelă listează autorizările specifice necesare pentru comenzile de disc.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate 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.

Comenzi pass-through staţie de afişare

Această tabelă listează autorizările specifice necesare pentru comenzile pass-through staţie de afişare.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate pentru comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ENDPASTHR			

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 de 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.

Comenzi distribuire

Această tabelă listează autorizările specifice necesare pentru comenzile de distribuire.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate pentru această comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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)			

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
RMVDSTQ (Q)			
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.

Comenzi linie de distribuire

Această tabelă listează autorizările specifice necesare pentru comenzile listă de distribuire.

Aceste comenzi nu necesită nici o autorizare obiect:			
ADDDSTLE [1] CHGDSTL[1]	CRTDSTL DLTDSTL [1]	DSPDSTL RMVDSTLE [1]	RNMDSTL [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 autorizarea necesară de operaţie.

Comenzi obiect bibliotecă de documente

Această tabelă listează autorizările specifice necesare pentru comenzile obiect bibliotecă de documente.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 de utilizator vechi	*DLT	*EXECUTE
	Profil de 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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CHKDOC	Document	*CHANGE	*EXECUTE
	Dicţionar ajutător pentru corectare ortografică	*CHANGE	*EXECUTE
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 autorizări	*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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
QRYDOCLIB [2,6]	Fişier cerut	*USE	*EXECUTE
	Listă documente, dacă există	*CHANGE	*EXECUTE
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 (Q)[7, 8, 9]	Obiect bibliotecă de documene, dacă se înlocuieşte	*ALL[10]	*EXECUTE
	Folderul părinte, dacă DLO este nou	*CHANGE[10]	*EXECUTE
	Profilul de utilizator proprietar, dacă DLO este nou	*ADD[10]	*EXECUTE
	Fişier sursă, dacă este specificat	Vedeţi regulile generale.	Vedeţi regulile generale.
	Fişier de salvare	*USE	*EXECUTE
	Fişier optic (OPTFILE)[17]	*R	Neaplicabilă
	Prefix cale al fişierului optic (OPTFILE)[17]	*X	Neaplicabilă
	Volum optic[19]	*USE	Neaplicabilă
	Unitate de bandă sau 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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
SAVDLO [7,13]	Obiect bibliotecă document	*ALL[10]	*EXECUTE
	Unitate de bandă sau 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	Neaplicabilă
	Directorul părinte al fişierului optic (OPTFILE)[17]	*WX	Neaplicabilă
	Prefixul cale al fişierului optic (OPTFILE)[17]	*X	Neaplicabilă
	Directorul root (/) al volumului[17, 18]	*RWX	Neaplicabilă
	Volum optic[19]	*CHANGE	Neaplicabilă
SAVRSTDLO	Pe sistemul sursă, aceeaşi autorizare ca şi cea necesară pentru comanda SAVDLO.		
	Pe sistemul destinaţie, aceeaşi autorizare ca şi cea necesară pentru comanda RSTDLO.		
WRKDOC	Folder	*USE	
WRKFLR	Folder	*USE	

1 Trebuie să aveţi autorizarea 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 Trebuie să aveţi autorizare specială *SAVSYS, *ALLOBJ sau să fiţi înrolat în directorul de distribuţie sistem.

8 E necesară autorizarea specială *SAVSYS sau *ALLOBJ pentru a folosi următoarea combinaţie de parametri: RSTDLO DLO(*MAIL).

9 Trebuie să aveţi autorizarea specială *ALLOBJ pentru a specifica altă valoare decât *NONE pentru parametrul ALWOBJDIF.

10 Dacă aveţi autorizarea specială *SAVSYS, nu aveţi nevoie de autorizarea specificată.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
[11] Aveţi nevoie de autorizarea *ALL pentru document dacă îl înlocuiţi. Aveţi nevoie de autorizări operaţionale şi pentru toate datele pentru folder dacă restauraţi informaţii noi în aceste foldere, sau aveţi nevoie de autorizarea specială *ALLOBJ. [12] Dacă este folosit pentru dicţionar, este necesară doar autorizarea 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.			
[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).			

Comenzi DNS

Această tabelă listează autorizările specifice necesare pentru comenzi DNS.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CHKDNSCFG [1]	Fişier de configurare existent	*R	
	Calea la fişierul de configurare existent	*X	
	Fişier de ieşire existent	*W	
	Calea la fişierul de ieşire existent	*X	
	Părintele noului fişier de ieşire	*RX	
CHKDNSZNE [1]	Fişier de zonă existent	*R	
	Calea la fişierul de zonă existent	*X	
	Fişier de ieşire existent	*W	
	Calea la fişierul de ieşire existent	*X	
	Părintele noului fişier de ieşire	*RX	

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CRTRNDCCFG [1]	Fişier sursă entropie existent	*R	
	Calea la fişierul sursă entropie existent	*X	
	Fişier de ieşire existent	*W	
	Calea la fişierul de ieşire existent	*X	
	Părintele noului fişier de ieşire	*RX	
RUNDNSUPD	Fişier intrare batch existent	*R	
	Calea la fişierul de intrare batch existent	*X	
	Fişier de chei existent	*R	
	Calea la fişierul de chei existent	*X	
	Fişier de ieşire existent	*W	
	Calea la fişierul de ieşire existent	*X	
	Părintele noului fişier de ieşire	*RX	
RUNRNDCCMD	Fişier de configurare RNDC existent	*R	
	Calea la fişierul de configurare RNDC existent	*X	
	Fişier de chei existent	*R	
	Calea la fişierul de chei existent	*X	
	Fişier de ieşire existent	*W	
	Calea la fişierul de ieşire existent	*X	
	Părintele noului fişier de ieşire	*RX	
STRDIGQRY	Fişier intrare batch existent	*R	
	Calea la fişierul de intrare batch existent	*X	
	Fişier de chei de încredere existent	*R	
	Calea la fişierul de chei de încredere existent	*X	
	Fişier de chei existent	*R	
	Calea la fişierul de chei existent	*X	
	Fişier de ieşire existent	*W	
	Calea la fişierul de ieşire existent	*X	
	Părintele noului fişier de ieşire	*RX	
STRHOSTQRY	Fişier de ieşire existent	*W	
	Calea la fişierul de ieşire existent	*X	
	Părintele noului fişier de ieşire	*RX	

[1] Trebuie să aveţi autorizarea specială *IOSYSCFG pentru a rula această comandă.

Comenzi set de caractere pe doi octeţi

Această tabelă listează autorizările specifice necesare pentru comenzile set de caractere pe doi octeţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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

Comenzi editare descriere

Această tabelă listează autorizările specifice necesare pentru comenzile de editare descriere.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CRTEDTD	Descriere de editare		*EXECUTE, *ADD
DLTEDTD	Descriere de editare	*OBJEXIST	*EXECUTE
DSPEDTD	Descriere de editare	*OBJOPR	*EXECUTE
WRKEDTD [1]	Descriere de editare	Orice autorizare	*USE
[1] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizarea necesară de operaţie.			

Comenzi variabile de mediu

Această tabelă listează autorizările specifice necesare pentru comenzile 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.			

Comenzi configurare comunicaţie fără fir LAN

Această tabelă listează autorizările specifice necesare pentru comenzile extinse configurare comunicaţie fără fir LAN.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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

Comenzi fişiere

Această tabelă listează autorizările specifice necesare pentru comenzile fişiere.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate pentru această comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ADDICFDEVE	Fişier ICF	*OBJOPR, *OBJMGT	*EXECUTE
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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
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
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	Fişier de salvare	*OBJOPR şi (*OBJMGT sau *OBJALTER).	*EXECUTE
CHGSRCPF	Fişier fizic sursă	*OBJMGT sau *OBJALTER	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
CHGTAPF	Fişier bandă	*OBJOPR, *OBJMGT	*EXECUTE
	Dispozitivul dacă numele dispozitivului e specificat	*OBJOPR	*EXECUTE
CLRPFM	Fişier fizic	*OBJOPR, *OBJMGT sau *OBJALTER, *DLT	*EXECUTE
CLRSAVF	Fişier de salvare	*OBJOPR, *OBJMGT	*EXECUTE
CPYF	Fişier-sursă	*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	Fişier-sursă	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier dispozitiv)	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier fizic)	Vedeţi regulile generale.	Vedeţi regulile generale.
CPYFRMIMPF	Fişier-sursă	*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
	comanda CRTDDMF	*USE	*USE
CPYFRMQRYF [1]	Fişier-sursă	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier dispozitiv)	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier fizic)	Vedeţi regulile generale.	Vedeţi regulile generale.
CPYFRMSTMF	Fişier de flux	*R	
	Directoarele din prefix nume cale al fişierului flux	*X	
	Fişierul bază de date destinaţie, dacă se specifică MBROPT(*ADD)	*WX	*X
	Fişier bază de date destinaţie, dacă MBROPT(*REPLACE sau *NONE) este specificat	*WX, *OBJMGT	*X
	Fişierul bază de date destinaţie, dacă este creat un nou membru)	*WX	*X, *ADD
	Tabela de conversie *TBL folosită pentru a translata datele	*R	*X
	Fişierul de salvare destinaţie există	*RWX, *OBJMGT	*X
	Fişierul de salvare destinaţie este creat		*RWX
CPYFRMTAP	Fişier-sursă	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier dispozitiv)	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier fizic)	Vedeţi regulile generale.	Vedeţi regulile generale.
CPYSRCF	Fişier-sursă	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier dispozitiv)	*OBJOPR, *READ	*EXECUTE
	Fişier-destinaţie (fişier fizic)	Vedeţi regulile generale.	Vedeţi regulile generale.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
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	Fişier-sursă	*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
	comanda CRTDDMF	*USE	*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	
	Fişier bază de date şi fişier flux, dacă AUT(*FILE) sau AUT(*INDIRFILE) este specificat	*OBJMGT	
	Tabela de conversie *TBL folosită pentru a translata datele	*R	*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
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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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	Fişier de salvare		*READ, *ADD, *EXECUTE
CRTSRCPF	Fişier fizic sursă		*READ, *ADD, *EXECUTE
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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
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 constrângere 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	Fişier 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
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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
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-sursă	*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
	Fişier de salvare	*USE	*EXECUTE
	Fişier Salvare/Restaurare optic[8] (dacă cel anterior există)	*RW	Neaplicabilă
	Directorul părinte al OPTFILE[8]	*WX	Neaplicabilă
	Prefix cale al OPTFILE[8]	*X	Neaplicabilă
	Director rădăcină (/) volum optic [8,9]	*RWX	Neaplicabilă
	Volum optic[10]	*CHANGE	Neaplicabilă
SAVS36F	Fişier-sursă	*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.
	Fişier-sursă	*USE	*EXECUTE
	Fişier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
STRAPF [3]	Fişier sursă	*OBJMGT, *CHANGE	*READ, *ADD
	Comenzile CRTPF, CRTLF, ADDPFM, ADDLFM şi RMVM	*USE	*EXECUTE
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
	Fişier (dacă există opţiunea de afişare date)	*READ	*EXECUTE
UPDDTA	Fişier	*CHANGE	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 autorizarea cerută de operaţii individuale.

[4] Dacă se creează un nou fişier şi există un păstrător de autorizare pentru el, atunci utilizatorul trebuie să aibă autorizarea toate (*ALL) pentru păstrătorul de autorizare sau să fie posesorul acestuia. Dacă nu există un păstrător 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 autorizarea specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.

Comenzi filtru

Această tabelă listează autorizările specifice necesare pentru comenzile filtru.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ADDALRACNE	Filtrare	*USE, *ADD	*EXECUTE
ADDALRSLTE	Filtrare	*USE, *ADD	*EXECUTE
ADDPRBACNE	Filtrare	*USE, *ADD	*EXECUTE
ADDPRBSLTE	Filtrare	*USE, *ADD	*EXECUTE
CHGALRACNE	Filtrare	*USE, *UPD	*EXECUTE
CHGALRSLTE	Filtrare	*USE, *UPD	*EXECUTE
CHGFTR	Filtrare	*OBJMGT	*EXECUTE
CHGPRBACNE	Filtrare	*USE, *UPD	*EXECUTE
CHGPRBSLTE	Filtrare	*USE, *UPD	*EXECUTE
CRTFTR	Filtrare		*READ, *ADD
DLTFTR	Filtrare	*OBJEXIST	*EXECUTE
RMVFTRACNE	Filtrare	*USE, *DLT	*EXECUTE
RMVFTRSLTE	Filtrare	*USE, *DLT	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
WRKFTR [1]	Filtrare	Orice autorizare	*EXECUTE
WRKFTRACNE [1]	Filtrare	*USE	*EXECUTE
WRKFTRSLTE [1]	Filtrare	*USE	*EXECUTE
[1] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizarea necesară de operaţie.			

Comenzi finanţe

Această tabelă listează autorizările specifice necesare pentru comenzile de finanţe.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate pentru această comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 de utilizator QFNC trebuie să aibă această autorizare.			

Comenzi operaţii grafice i5/OS

Această tabelă listează autorizările specifice necesare pentru comenzi operaţii grafice i5/OS.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 de utilizator sursă copiere	*CHANGE	*EXECUTE
	Profilul de utilizator destinaţie copiere	*CHANGE	*EXECUTE
WRKFCNUSG			

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
[1] Obiectul staţie de lucru este un obiect intern care e creat când instalaţi opţiunea i5/OS 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.			

Comenzi set de simboluri grafice

Această tabelă listează autorizările specifice necesare pentru comenzile set de simboluri grafice.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 autorizări pentru obiect sunt necesare.			

Comenzi server gazdă

Această tabelă listează autorizările specifice necesare pentru comenzile server gazdă.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate pentru această comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Aceste comenzi nu necesită nici o autorizare obiect.			
ENDHOSTSVR (Q)		STRHOSTSVR (Q)	

Comenzi catalog imagini

Această tabelă listează autorizările specifice necesare pentru comenzile catalog de imagini.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate pentru această comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Tip obiect	Autorizare necesară	
			Pentru obiect	Pentru bibliotecă[1]
ADDIMGCLGE	Catalog de imagini	*IMGCLG	*CHANGE	*EXECUTE
	Prefix cale director catalog imagini	*DIR	*X	
	Numele dispozitivul când FROMDEV este specificat	*DEVD	*USE	
	Fişier imagine când FROMFILE este specificat	*STMF	*R, *OBJMGT	
	Prefix cale fişier imagine când FROMFILE este specificat	*DIR	*X	
	Director părinte fişier imagine când FROMFILE este specificat	*DIR	*RX	
CHGIMGCLG	Catalog imagini	*IMGCLG	*CHANGE	*EXECUTE
	Prefix cale director catalog imagini	*DIR	Vedeţi regulile generale.	
	Prefix cale catalog imagini nou când parametrul DIR este spedificat	*DIR	Vedeţi regulile generale.	
CHGIMGCLGE	Catalog imagini	*IMGCLG	*CHANGE	*EXECUTE
	Prefix cale director catalog imagini	*DIR	Vedeţi regulile generale.	
CRTIMGCLG	QUSRSYS	*LIB		*READ, *ADD
	Catalog imagini dacă se specifică DIR(*REFIMGCLG)	*IMGCLG	*USE	*OBJOPR, *READ, *ADD, *EXECUTE
	Prefix cale director catalog imagini [2]	*DIR	Vedeţi regulile generale.	
DLTIMGCLG	Catalog imagini	*IMGCLG	*OBJEXIST	*EXECUTE
	Prefix cale director catalog imagini	*DIR	Vedeţi regulile generale.	
LODIMGCLG	Catalog imagini	*IMGCLG	*USE	*EXECUTE
	Catalog imagini când se specifică WRTPTC(*ALL) sau WRTPTC(*NONE)	*IMGCLG	*CHANGE	*EXECUTE
	dispozitiv virtual	*DEVD	*USE	
	Prefix cale director catalog imagini	*DIR	Vedeţi regulile generale.	
LODIMGCLGE	Catalog imagini	*IMGCLG	*USE	*EXECUTE
	Prefix cale director catalog imagini	*DIR	Vedeţi regulile generale.	
RMVIMGCLGE	Catalog de imagini	*IMGCLG	*CHANGE	*EXECUTE
	Prefix cale director catalog imagini	*DIR	Vedeţi regulile generale.	
RTVIMGCLG	Catalog imagini	*IMGCLG	*USE	*EXECUTE
	Descrierea dispozitiv dacă parametrul DEV este specificat	*DEVD	*USE	
VFYIMGCLG	Catalog de imagini	*IMGCLG	*USE	*EXECUTE
	dispozitiv virtual	*DEVD	*USE	
	Prefix cale director catalog imagini	*DIR	Vedeţi regulile generale.	
WRKIMGCLG	Catalog de imagini	*IMGCLG	*USE	*EXECUTE
WRKIMGCLGE	Catalog de imagini	*IMGCLG	*USE	*EXECUTE

Comandă	Obiect referit	Tip obiect	Autorizare necesară	
			Pentru obiect	Pentru bibliotecă[1]

[1] Biblioteca în care se află catalogul de imagini este QUSRSYS.

[2] Dacă este creat un director, trebuie se asemenea autorizare de scriere (*W) asupra directorului pentru a conţine noul director.

Comenzi sistem de fişiere integrat

Această tabelă listează autorizările specifice necesare pentru comenzile sistem de fişiere integrat.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate pentru această comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]
ADDLNK	Obiect când NKTYPE(*HARD) este specificat	*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, *CRTOBJAUD	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	All	*OBJMGT
	Directorul care conţine obiecte când se specifică SUBTREE(*ALL)	Orice director	All	*RX
	Obiect la setarea următoarelor atribute: *CRTOBJSCAN sau *SCAN[26]	*DIR şi *STMF	QOpenSys, ″root″ (/), UDFS	
	Obiect la setarea următoarelor atribute: *SETUID, *SETGID, *RSTDRNMUNL	Orice	Toate exceptând QSYS.LIB şi QLDS	Drept de proprietate [15]
	*CRTOBJAUD[9]			
	Prefix cale [9]	Vedeţi regulile generale.		
CHGAUD [4]				

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]
CHGAUT	Obiect	All	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
	Directorul care conţine obiecte când se specifică SUBTREE(*ALL)	Orice director sau bibliotecă	All	*RX
CHGCURDIR	Obiect	Orice director		*R
	Volum optic	*DDIR	QOPT[8]	*X
	Prefix cale	Vedeţi regulile generale.		
CHGOWN [24]	Obiect	All	QSYS.LIB	*OBJEXIST
		*FILE, *LIB, *SBSD	QSYS.LIB	*OBJEXIST, *OBJOPR
		All	QOpenSys, ″root″ (/), UDFS	Drept de proprietate şi *OBJEXIST[15]
		All	QDLS	Drept de proprietate sau *ALLOBJ
			QOPT[11]	Drept de proprietate sau *ALLOBJ
CHGOWN [24]	Profilul de utilizator al vechiului proprietar—toate mai puţin QOPT, QDLS	*USRPRF	All	*DLT
	Profilul de utilizator al noului proprietar—toate mai puţin QOPT, QDLS	*USRPRF	All	*ADD
	Volum optic	*DDIR	QOPT[8]	*CHANGE
	Directorul care conţine obiecte când se specifică SUBTREE(*ALL)	Orice director sau bibliotecă	All	*RX

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]
CHGPGP	Obiect	All	QSYS.LIB	*OBJEXIST
		*FILE, *LIB, *SBSD	QSYS.LIB	*OBJEXIST, *OBJOPR
		All	QOpenSys, ″root″ (/), UDFS	Drept de proprietate[5, 15]
		All	QDLS	Drept de proprietate sau *ALLOBJ
			QOPT[11]	Drept de proprietate sau *ALLOBJ
CHGPGP	Profilul de utilizator al vechiului grup primar—toate exceptând QOPT, QDLS	*USRPRF	All	*DLT
	Profilul de utilizator al noului grup primar—toate exceptând QOPT, QDLS	*USRPRF	All	*ADD
	Volum optic	*DDIR	QOPT[8]	*CHANGE
	Directorul care conţine obiecte când se specifică SUBTREE(*ALL)	Orice director sau bibliotecă	All	*RX
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
	Directorul care conţine obiecte când se specifică SUBTREE(*ALL)	Orice director	All	*RX
	Prefix cale	Vedeţi regulile generale.		
CHKOUT	Obiect	*STMF	QOpenSys, ″root″ (/), UDFS	*W
		*DOC	QDLS	*W
	Directorul care conţine obiecte când se specifică SUBTREE(*ALL)	Orice director	All	*RX
	Prefix cale	Vedeţi regulile generale.		

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	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	Fără
		alte	QSYS.LIB	*RX, *OBJMGT
		*DSTMF	QOPT[11]	*R
	Obiect destinaţie când e specificat REPLACE(*YES) (dacă obiectul destinaţie există deja)	Orice	All[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 destinaţie	*DDIR	QOPT[8]	*CHANGE

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]
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 ţintă)	*LIB	QSYS.LIB	*WX
		*DIR	QOpenSys, ″root″ (/), UDFS	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
	Prefix cale (obiect origine)	*DDIR	QOPT[11]	*X
CPYFRMSTMF	Consultaţi “Comenzi fişiere” la pagina 379			
CPYTOSTMF	Consultaţi “Comenzi fişiere” la pagina 379			
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	All	QDLS	*ALL
		All	Toate celelalte	*OBJMGT sau drept de proprietate
		ALL	QOPT[11]	Fără
	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

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]
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
DSPF	Fişier bază de date	*FILE	QSYS.LIB	*USE
	Bibliotecă fişiere bază de date	*LIB	QSYS.LIB	*EXECUTE
	Fişier de flux	*STMF	QOpenSys, ″root″ (/), UDFS	*R
		*USRSPC	QSYS.LIB	*USE
	Prefix cale	Vedeţi regulile generale.		
DSPLNK	Orice	Orice	″root″ (/), QOpenSys, UDFS QSYS.LIB[27], QDLS, QOPT[11]	Fără
	Fişier, opţiunea 12 (Gestionare legături)	*STMF, *SYMLNK, *DIR, *BLKSF, *SOCKET	″root″ (/), QOpenSys, UDFS	*R
DSPLNK	Obiect legătură simbolic	*SYMLNK	″root″ (/), QOpenSys, UDFS	Fără
	Volum optic	*DDIR	QOPT[8]	*USE
	Directorul părinte al obiectului referinţă - fără model [13]	*DIR	″root″ (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]
DSPLNK	Directorul părinte al obiectului referinţă - model specificat[13]	*DIR	″root″ (/), QOpenSys, UDFS	*R
		*LIB, *FILE	QSYS.LIB[27]	*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[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Directorul părinte al obiectului referinţă - opţiunea 12 (Gestionare legături)	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*SYMLNK	″root″ (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*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[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Prefixul obiectului referinţă părinte - model specificat[13]	*DIR	″root″ (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]
DSPLNK	Prefixul obiectului referinţă părinte - opţiunea 8 (Afişare atribute)	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
DSPLNK	Prefixul obiectului referinţă părinte - opţiunea 12 (Gestionare legături)	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*SYMLNK	″root″ (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*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[27]	*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[27]	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
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[27]	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]
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[27]	*RX
		*FLR	QDLS	*RX
		*DDIR	QOPT[11]	*RX
		*DDIR		*R
DSPMFSINF	Obiect	Orice	Orice	Fără
	Prefix cale	Vedeţi regulile generale.		
EDTF	Fişier bază de date, membru existent	*FILE	QSYS.LIB	*CHANGE
	Bibliotecă fişiere bază de date	*LIB	QSYS.LIB	*EXECUTE
	Fişier bază de date, membru nou	*FILE	QSYS.LIB	*CHANGE, *OBJMGT
	Bibliotecă fişiere bază de date, membru nou	*LIB	QSYS.LIB	*EXECUTE, *ADD
	Fişier flux, fişier existent	*STMF	QOpenSys, ″root″ (/), UDFS	*R
	Spaţiu utilizator	*USRSPC	QSYS.LIB	*CHANGE
	Directorul părinte la crearea unui nou fişier flux	*DIR	QOpenSys, ″root″ (/), UDFS	*WX
	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
	Jurnal	*JRN	QSYS.LIB	*OBJMGT, *OBJOPR
	Prefix cale	Vedeţi regulile generale.		

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]
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	Fără
		alt	QSYS.LIB	Fără
		*STMF	QOPT[11]	*W
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	Neaplicabilă
		*DSTMF	QOPT[11]	*RW
MOV	Mutat în QSYS *MBR	*STMF	QOpenSys, ″root″ (/), UDFS	*R, *OBJMGT, *OBJEXIST
		*DOC	QDLS	*ALL
		*DSTMF	QOPT[11]	*RW

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]
MOV	Volum optic (sursă şi destinaţie)	*DDIR	QOPT[8]	*CHANGE
	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.		
RCLLNK[16]				
RLSIFSLCK [18]	obiect	*STMF	″root″ (/), QOpenSys, UDFS	*R
	Prefix cale	Vedeţi regulile generale.		
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
	Directorul care conţine obiecte când se specifică SUBTREE(*ALL)	Orice director	All	*RX
	Volum optic	*DDIR	QOPT[8]	*CHANGE
	Prefix cale	Vedeţi regulile generale.		
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

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]
RMVLNK	Director părinte	*FLR	QDLS	*X
		*FILE	QSYS.LIB	*X, *OBJEXIST
		*LIB	QSYS.LIB	*X
		*DIR	QOpenSys, ″root″ (/), UDFS	*WX
		*DDIR	QOPT[11]	*WX
	Volum optic	*DDIR	QOPT[8]	*CHANGE
	Prefix cale	Vedeţi regulile generale.		
RNM[19]	Obiect	*DIR	QOpenSys, ″root″ (/), UDFS	*OBJMGT, *W
		Non *DIR	QOpenSys, ″root″ (/), UDFS	*OBJMGT
		*DOC, *FLR	QDLS	*ALL
		*MBR	QSYS.LIB	Neaplicabilă
		*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

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]
RST (Q) [23, 28, 30]	Obiectul, dacă există[2]	Orice	QOpenSys, ″root″ (/), UDFS	*W, *OBJEXIST
			QSYS.LIB	Variază [10]
			QDLS	*ALL
	Prefix cale	Vedeţi regulile generale.		
	Director părinte creat de operaţia de restaurare datorită CRTPRNDIR(*YES)[2]	*DIR	QOpenSys, ″root″ (/), UDFS	*WX
	Proprietar director părinte specificat în parametrul PRNDIROWN[2, 6]	*USRPRF	QSYS.LIB	*ADD
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 de utilizator care deţine obiectul nou restaurat[2]	*USRPRF	QSYS.LIB	*ADD
	Unitete bandă, unitate optică sau fişier salvare	*DEVD, *FILE	QSYS.LIB	*RX
	Definiţie medii	*MEDDFN	QSYS.LIB	*USE
RST (Q)	Bibliotecă pentru descrierea dispozitivului, definiţia mediului de stocare, 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

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]
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[29]	Obiect[2]	Orice	QOpenSys, ″root″ (/), UDFS	*R, *OBJEXIST
			QSYS.LIB	Variază [10]
			QDLS	*ALL
	Prefix cale	Vedeţi regulile generale.		
	Unitate de bandă, unitate optică	*DEVD	QSYS.LIB	*RX
	Definiţie mediu de stocare	*MEDDFN	QSYS.LIB	*USE
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
	Bibliotecă pentru descrierea dispozitivului, definiţia mediului de stocare, sau fişierul de salvare sau coadă de mesaje salvare-când-este-activ	*LIB	QSYS.LIB	*EXECUTE
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

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]
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 şi cea necesară pentru comanda SAV.			
	Pe sistemul destinaţie, aceeaşi autorizare ca şi cea necesară pentru comanda RST.			
STATFS	Obiect	Orice	Orice	Fără
	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
	Jurnal	*JRN	QSYS.LIB	*OBJMGT, *OBJOPR
	Prefix cale	Vedeţi regulile generale.		
WRKAUT[6, 7]	Obiect	*DOC sau *FLR	QDLS	*ALL
		All	not QDLS	*OBJMGT sau drept de proprietate
		*DDIR şi *DSTMF	QOPT[11]	*NONE
	Volum optic	*DDIR	QOPT[8]	*USE
	Prefix cale	Vedeţi regulile generale.		

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]
WRKLNK	Orice	Orice	″root″ (/), QOpenSys, UDFS QSYS.LIB[27], QDLS, QOPT[11]	Fără
	Fişier, opţiunea 12 (Gestionare legături)	*STMF, *SYMLNK, *DIR, *BLKSF, *SOCKET	″root″ (/), QOpenSys, UDFS	*R
	Obiect legătură simbolic	*SYMLNK	″root″ (/), QOpenSys, UDFS	Fără
	Volum optic	*DDIR	QOPT[8]	*USE
WRKLNK	Directorul părinte al obiectului referinţă - fără model [13]	*DIR	″root″ (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*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[27]	*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[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Directorul părinte al obiectului referinţă - opţiunea 12 (Gestionare legături)	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*SYMLNK	″root″ (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]
WRKLNK	Directorul părinte al obiectului referinţă - fără model [13]	*DIR	″root″ (/), QOpenSys, UDFS	*X
		*LIB *FILE	QSYS.LIB[27]	*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[27]	*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[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R
WRKLNK	Prefixul obiectului referinţă părinte - opţiunea 12 (Gestionare legături)	*DIR	″root″ (/), QOpenSys, UDFS	*RX
		*SYMLNK	″root″ (/), QOpenSys, UDFS	*X
		*LIB, *FILE	QSYS.LIB[27]	*X
		*FLR	QDLS	*X
		*DDIR	QOPT[11]	*X
		*DDIR		*R

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	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[27]	*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[27]	*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[27]	*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[27]	*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 autorizare 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. Consultaţi descrierea QLIRNMO API . 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.

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]

[6] Dacă profilul care este specificat folosind parametrul PRNDIROWN nu este utilizatorul făcând operaţia de restaurare, este necesară autorizare specială *SAVSYS sau *ALLOBJ.

[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.

[9] Utilizatorul trebuie să aibă autorizare specială *AUDIT pentru a modifica atributul *CRTOBJAUD şi utilizatorul nu are nevoie de nicio autorizare normală prefix nume cale (*X şi *R).

[10] Autorizarea necesară variază cu comanda 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 autorizarea specială *ALLOBJ pentru a folosi această comandă.

[17] În tabela 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 autorizarea specială *IOSYSCFG.

[19] Dacă atributul redenumiri şi dezlegări restricţionate (cunoscut de asemenea ca bitul S_ISVTX) este activ pentru un director, va restricţiona dezlegarea obiectelor din acel director dacă niciuna din aceste autorizări nu este îndeplinită:

- Utilizatorul are autorizare specială toate obiectele (*ALLOBJ).
- Utilizatorul este proprietarul obiectului care este dezlegat.
- 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. De asemenea, trebuie să aveţi autorizare specială *SAVSYS sau *ALLOBJ pentru a specifica *UDFS ca valoare pentru parametrul RBDMFS.

[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.

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect[1]

[26] Utilizatorul trebuie să aibă autorizarea specială *ALLOBJ şi *SECADM pentru a specifica atributele *CRTOBJSCAN şi *SCAN.

[27] Când afişaţi conţinutul directorului /QSYS.LIB, obiectele profil de utilizator (*USRPRF) asupra cărora apelantul nu are nici o autorizare (cum ar fi *EXCLUDE) nu sunt returnate.

[28] Utilizatorul trebuie să aibă autorizare specială *ALLOBJ pentru a specifica *YES pentru parametrul PVTAUT.

[29] Utilizatorul trebuie să aibă autorizare specială *ALLOBJ sau *SAVSYS pentru a specifica *YES pentru parametrul PVTAUT.

[30] Trebuie să aveţi autorizare specială *SAVSYS sau *ALLOBJ pentru a specifica *UDFS ca valoare pentru parametrul RBDMFS.

Comenzi definiţie date interactive

Această tabelă listează autorizările specifice necesare pentru comenzile de definiţie de date interactive.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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
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 autorizarea 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.

Comenzi IPX

Această tabelă listează autorizările specifice necesare pentru comenzile IPX.

Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate pentru această comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
DLTIPXD	Descriere IPX	*OBJEXIST	*EXECUTE
DSPIPXD	Descriere IPX	*USE	*EXECUTE
WRKIPXD	Descriere IPX	*OBJOPR	*EXECUTE

Comenzi index căutare informaţii

Această tabelă listează autorizările specifice necesare pentru comenzile index de căutare informaţii.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ADDSCHIDXE	Index de căutare	*CHANGE	*USE
	Grup panou	*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

Comezi atribut IPL

Această tabelă listează autorizările specifice necesare pentru comenzile atribut IPL.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate pentru această 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.

Comenzi Java

Această tabelă listează autorizările specifice necesare pentru comenzile Java.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ANZJVM	Comandă QSYS/STRSRVJOB	*USE	
	Comandă QSYS/STRDBG	*USE	
DSPJVMJOB[1]	Joburi JVM		
GENJVMDMP [1]			

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
PRTJVMJOB [1]			
WRKJVMJOB [1]			

[1] Trebuie să aveţi autorizarea specială *JOBCTL pentru a folosi această comandă.

Comenzi job

Această tabelă listează autorizările specifice necesare pentru comenzile de job.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
BCHJOB	Descriere job [9,11]	*USE	*EXECUTE
	Bibliotecile din lista de biblioteci (sistem, curent şi utilizator)[7]	*USE	
	Profil de 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 coada de ieşire	*READ	*EXECUTE
	Tabelă secvenţă de sortare[7]	*USE	*EXECUTE
CHGPJ	Profil de utilizator pentru pornire program necesită specificarea *PGMSTRRQS	*USE	*EXECUTE
	Profil de utilizator şi descriere job	*USE	*EXECUTE
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]			

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
DMPUSRTRC	Buffer urmărire utilizator [15]	*OBJOPR	*EXECUTE
DSCJOB [1]			
DSPACTPJ	Descriere dispozitiv ASP	*USE	
	Bibliotecă program		*EXECUTE
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]			
ENDLOGSVR[6]			
ENDPJ [6]	Descriere dispozitiv ASP	*USE	
	Bibliotecă program		*EXECUTE
HLDJOB [1]			
RLSJOB [1]			
RRTJOB			
RTVJOBA			
SBMDBJOB	Fişier bază de date	*USE	*EXECUTE
	Coadă job	*READ	*EXECUTE
SBMDKTJOB	Coada de mesaje	*USE, *ADD	*EXECUTE
	Coadă de joburi şi descriere dispozitiv	*READ	*EXECUTE
SBMJOB [2, 12, 17, 18]	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 de utilizator [10,11]	*USE	
	Profil de 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	
SBMNETJOB	Fişier bază de date	*USE	*EXECUTE
STRLOGSVR[6]			
STRPJ [6]	Descriere subsistem	*USE	
	Program	*USE	*EXECUTE
	Descriere dispozitiv ASP	*USE	
TFRBCHJOB	Coadă job	*READ	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
TFRGRPJOB	Program primul grup	*USE	*EXECUTE
TFRJOB [8]	Coadă job	*USE	*EXECUTE
	Descrierea subsistemului la care e alocată coada de joburi	*USE	
TFRSECJOB			
WRKACTJOB			
WRKARMJOB[16]			
WRKASPJOB	Descriere dispozitiv	*USE	
WRKJOB [1]			
WRKJOBLOG			
WRKSBMJOB			
WRKSBSJOB			
WRKUSRJOB			

1 Orice utilizator poate rula aceste comenzi pentru joburi care rulează sub propriul său profil de 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 în care se află 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 autorizare specială toate obiectele (*ALLOBJ), trebuie să aveţi autorizare specială *ALLOBJ sau să fiţi autorizat asupra funcţiei Istoric job toate obiectele a i5/OS prin Application Administration din System i Navigator. 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 de 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 de utilizator sub care rulează jobul sunt verificate pentru autorizare pentru obiectul referinţă.

10 Utilizatorul care lansează jobul este verificat pentru autorizare pentru obiectul referinţă.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
[11] E folosită autorizarea adoptată a utilizatorului care lansează comanda CHGJOB sau SBMJOB.			
[12] Trebuie să fiţi autorizat pentru profilul de utilizator şi descrierea jobului; profilul de 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 de 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.			
[16] Pentru a lucra cu un anumit job sau pentru a afişa detaliile unui anumit job, una din următoarele condiţii trebuie să se aplice: • Comanda trebuie emisă din acel job. • Emitentul comenzii trebuie să ruleze sub un profil de utilizator care este acelaşi cu identitatea utilizator job a jobului. • Emitentul comenzii trebuie să ruleze sub un profil de utilizator care are autorizare specială control job (*JOBCTL).			
[17] Trebuie să aveţi autorizare de folosire (*USE) asupra comenzii Modificare cod de contabilitate (CHGACGCDE) pentru a specifica un cont de contabilitate valoare caracter în parametrul Cod de contabilitate (ACGCDE).			
[18] Trebuie să aveţi autorizare specială control job (*JOBCTL) pentru a folosi parametrul Lansat pentru (SBMFOR).			

Comenzi descriere de job

Această tabelă listează autorizările specifice necesare pentru comenzile descriere de job.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, "Comenzi livrate cu autorizare publică *EXCLUDE", la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
CHGJOBD	Descriere job	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Profil de utilizator (USER)	*USE	
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 de utilizator (USER)	*USE	
DLTJOBD	Descriere job	*OBJEXIST	*EXECUTE
DSPJOBD	Descriere job	*OBJOPR, *READ	*EXECUTE
PRTJOBDAUT [1]			
WRKJOBD	Descriere job	Orice	*USE
[1] Trebuie să aveţi autorizarea specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.			

Comenzi coadă de joburi

Această tabelă listează autorizările specifice necesare pentru comenzile coadă de joburi.

Comandă	Obiect referit	Parametri coadă de joburi [4]		Autorizare specială	Autorizare necesară	
		AUTCHK	OPRCTL		Pentru obiect	Pentru bibliotecă
CHGJOBQ	Coadă de joburi	*DTAAUT			*READ, *ADD, *DLT, *OBJMGMT	*EXECUTE
		*OWNER			Proprietar [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CLRJOBQ [1]	Coadă job	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
CRTJOBQ [1]	Coadă job					*READ, *ADD
DLTJOBQ	Coadă job				*OBJEXIST	*EXECUTE
HLDJOBQ [1]	Coadă job	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
PRTQAUT [5]						
RLSJOBQ [1]	Coadă job	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKJOBQ [1,3]	Coadă job	*DTAAUT			*READ	*EXECUTE
		*OWNER			Proprietar [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
WRKJOBQD	Coadă de joburi				*READ	*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 în care se află 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 autorizarea specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.

Comenzi planificare job

Această tabelă listează autorizările specifice necesare pentru comenzile de planificare job.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
ADDJOBSCDE	Planificare job	*CHANGE	*EXECUTE
	Descriere job [1]	*USE	*EXECUTE
	Coadă de joburi [1,2]	*READ	*EXECUTE
	Profil de 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
	Profil de 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

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.

Comenzi de jurnalizare

Această tabelă listează autorizările specifice necesare pentru comenzile de jurnal.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă sau director**
ADDRMTJRN	Jurnal sursă	*CHANGE, *OBJMGT	*EXECUTE
	Jurnal destinaţie		*EXEC, *ADD
APYJRNCHG (Q)	Jurnal	*USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
	Obiectele sistem de fişiere neintegrat 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)

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă sau director
APYJRNCHGX (Q)	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
CHGJRNA (Q) [10]			
CHGJRNOBJ [9]	Jurnal	*OBJOPR, *OBJMGT	
	Obiecte sistem de fişiere neintegrat	*READ, *OBJMGT	
	Obiecte sistem de fişiere integrat	*R, *OBJMGT	*X
	Cale arbore SUBTREE(*ALL)	*RX, *OBJMGT	
	Cale arbore SUBTREE(*NONE)	*R, *OBJMGT	
CHGRMTJRN	Jurnal sursă	*CHANGE, *OBJMGT	*EXECUTE
	Jurnal sursă	*USE, *OBJMGT	*EXECUTE
CMPJRNIMG	Jurnal	*USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
	Fişier	*USE	*EXECUTE
CPYAUDJRNE[8]	Fişierul de ieşire deja există	*OBJOPR, *OBJMGT, *ADD, *DLT	*EXECUTE
	Fişierul de ieşire nu există		*EXECUTE, *ADD
CRTJRN	Jurnal		*READ, *ADD
	Receptor jurnal	*OBJOPR, *OBJMGT, *READ	*EXECUTE
DLTJRN	Jurnal	*OBJOPR, *OBJEXIST	*EXECUTE
DSPAUDJRNE[8]			

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă sau director**
DSPJRN [6]	Jurnal	*USE	*EXECUTE
	Jurnal dacă FILE(*ALLFILE) este specificat, nicio selecţie de obiecte nu este specificată, obiectul specificat a fost şters din sistem, obiectul specificat nu a fost jurnalizat niciodată, *IGNFILSLT sau *IGNOBJSLT este specificat pentru orice coduri jurnal selectate sau când OBJJID este specificat sau jurnalul este un jurnal la distanţă.	*OBJEXIST, *USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
	Obiect non-IFS dacă se specifică	*USE	*EXECUTE
	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
	Obiect IFS dacă se specifică	*R (Poate fi *X ca şi cum obiectul este un director şi SUBTREE (*ALL) este specificat)	*X
DSPJRNMNU[1]			
ENDJRN	Vedeţi“Comenzi sistem de fişiere integrat” la pagina 390.		
ENDJRNAP	Jurnal	*OBJOPR, *OBJMGT	*EXECUTE
	Fişier	*OBJOPR, *OBJMGT	*EXECUTE
ENDJRNLIB	Jurnal	*OBJOPR, *OBJMGT	*EXECUTE
	Bibliotecă	*OBJOPR, *OBJMGT, *READ	
ENDJRNOBJ	Jurnal	*OBJOPR, *OBJMGT	*EXECUTE
	Obiect	*OBJOPR, *READ, *OBJMGT	*EXECUTE
ENDJRNPF	Jurnal	*OBJOPR, *OBJMGT	*EXECUTE
	Fişier	*OBJOPR, *OBJMGT, *READ	*EXECUTE
JRNAP [2]			
JRNPF [3]			

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă sau director**
RCVJRNE	Jurnal	*USE	*EXECUTE
	Jurnal dacă FILE(*ALLFILE) este specificat, nicio selecţie de obiecte nu este specificată, obiectul specificat a fost şters din sistem, obiectul specificat nu a fost jurnalizat niciodată, *IGNFILSLT sau *IGNOBJSLT este specificat pentru orice coduri jurnal selectate sau când OBJJID este specificat sau jurnalul este un jurnal la distanţă.	*OBJEXIST, *USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
	Obiect non-IFS dacă se specifică	*USE	*EXECUTE
	Obiect IFS dacă se specifică	*R (Poate fi *X ca şi cum obiectul este un director şi SUBTREE (*ALL) este specificat)	*X
	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
RTVJRNE	Jurnal	*USE	*EXECUTE
	Jurnal dacă FILE(*ALLFILE) este specificat, nicio selecţie de obiecte nu este specificată, obiectul specificat a fost şters din sistem, obiectul specificat nu a fost jurnalizat niciodată, *IGNFILSLT sau *IGNOBJSLT este specificat pentru orice coduri jurnal selectate sau când OBJJID este specificat sau jurnalul este un jurnal la distanţă.	*OBJEXIST, *USE	*EXECUTE
	Receptor jurnal	*USE	*EXECUTE
	Obiect non-IFS dacă se specifică	*USE	*EXECUTE
	Obiect IFS dacă se specifică	*R (Poate fi *X ca şi cum obiectul este un director şi SUBTREE (*ALL) este specificat)	*X
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“Comenzi sistem de fişiere integrat” la pagina 390.		
STRJRNAP	Jurnal	*OBJOPR, *OBJMGT	*EXECUTE
	Fişier	*OBJOPR, *OBJMGT	*EXECUTE
STRJRNLIB	Jurnal	*OBJOPR, *OBJMGT	*EXECUTE
	Bibliotecă	*OBJOPR, *OBJMGT, *READ	

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă sau director**
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	*USE	*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 sau RST.

5 Sune necesare autorizările *OBJOPR şi *OBJEXIST pentru receptori jurnal dacă opţiunea este aleasă pentru a şterge receptori.

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 autorizarea specială *AUDIT pentru a folosi această comandă.

9 Pentru a specifica PTLTNS(*ALWUSE), trebuie să aveţi autorizarea specială *ALLOBJ.

10 Trebuie să aveţi autorizarea specială *JOBCTL pentru a folosi această comandă.

Comenzi receptor jurnal

Această tabelă listează autorizările specifice necesare pentru comenzile receptor jurnal.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
WRKJRNRCV [1], [2], [3]	Receptor jurnal	Orice autorizare	*USE

[1] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizarea 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.

Comenzi Kerberos

Această tabelă listează autorizările specifice necesare pentru comenzile Kerberos.

Comandă	Obiect referit	Tip obiect	Autorizare necesară pentru obiect
ADDKRBKTE	Fiecare director din numele de cale care precede fişierul tabelă de chei destinaţie care va fi deschis.	*DIR	*X
	Directorul părinte al fişierului tabelă de chei destinaţie când este specificată adăugare, dacă fişierul nu există deja.	*DIR	*WX
	Fişierul tabelă de chei când este specificată listare.	*STMF	*R
	Fişierul tabelă de chei când este specificată adăugare sau ştergere.	*STMF	*RW
	Fiecare director din calea la fişierele de configuraţie.	*DIR	*X
	Fişier de configuraţie	*STMF	*R
ADDKRBTKT	Fiecare director din numele de cale care precede fişierul tabelă de chei	*DIR	*X
	Fişier tabelă de chei	*STMF	*R
	Fiecare director din numele de cale care precede fişierul cache acreditări	*DIR	*X
	Fişier cache acreditări	*STMF	*RW
	Directorul părinte al fişierului cache care va fi folosit, dacă este specificat de variabila de mediu KRB5CCNAME şi fişierul este creat	*DIR	*WX
	Fiecare director din numele de cale la fişierele de configuraţie	*DIR	*X
	Fişiere de configuraţie	*STMF	*R
CHGKRBPWD			

Comandă	Obiect referit	Tip obiect	Autorizare necesară pentru obiect
DLTKRBCCF	Firecare director din numele de cale care precede fişierul cache de acreditări, dacă fişierul cache de acreditări nu se află în directorul implicit.	*DIR	*X
	Directorul părinte al fişierul cache de acreditări, dacă fişierul cache de acreditări nu se află în directorul implicit.	*DIR	*WX
	Fişierul cache de acreditări, dacă fişierul cache de acreditări nu se află în directorul implicit.	*STMF	*RW, *OBJEXIST
	Firecare director din numele de cale la fişierele de acreditări, dacă fişierul cache de acreditări nu se află în directorul implicit.	*DIR	*X
	Fişiere de configurare, dacă fişierul cache de acreditări nu se află în directorul implicit.	*STMF	*R
DLTKRBCCF	Toate directoarele din numele de cale, dacă fişierul cache de acreditări nu se află în directorul implicit.	*DIR	*X
	Fişierul cache de acreditări, dacă fişierul cache de acreditări se află în directorul implicit.	*STMF	*RW
	Firecare director din numele de cale la fişierele de configurare, dacă fişierul cache de acreditări se află în directorul implicit.	*DIR	*X
	Fişiere de configurare, dacă fişierul cache de acreditări se află în directorul implicit.	*STMF	*R
DSPKRBCCF	Fiecare director din numele de cale care precede fişierul tabelă de chei	*DIR	*X
	Fişier tabelă de chei	*STMF	*R
	Fiecare director din numele de cale care precede fişierul cache acreditări	*DIR	*X
	Fişier cache acreditări	*STMF	*RW
DSPKRBKTE	Fiecare director din numele de cale care precede fişierul tabelă de chei destinaţie care va fi deschis.	*DIR	*X
	Directorul părinte al fişierului tabelă de chei destinaţie când este specificată adăugare, dacă fişierul nu există deja.	*DIR	*WX
	Fişierul tabelă de chei când este specificată listare.	*STMF	*R
	Fişierul tabelă de chei când este specificată adăugare sau ştergere.	*STMF	*RW
	Fiecare director din calea la fişierele de configuraţie.	*DIR	*X
	Fişiere de configurare	*STMF	*R

Comandă	Obiect referit	Tip obiect	Autorizare necesară pentru obiect
RMVKRBKTE	Fiecare director din numele de cale care precede fişierul tabelă de chei destinaţie care va fi deschis.	*DIR	*X
	Directorul părinte al fişierului tabelă de chei destinaţie când este specificată adăugare, dacă fişierul nu există deja.	*DIR	*WX
	Fişierul tabelă de chei când este specificată listare.	*STMF	*R
	Fişierul tabelă de chei când este specificată adăugare sau ştergere.	*STMF	*RW
	Fiecare director din calea la fişierele de configuraţie.	*DIR	*X
	Fişiere de configurare	*STMF	*R

Comenzi limbă

Această tabelă listează autorizările specifice necesare pentru comenzile de limbă.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CLOSE	Comanda de închidere	*USE	*EXECUTE
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
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
	Includere fişier	*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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
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
CRTCLMOD	Fişier sursă	*USE	*EXECUTE
	Includere fişier	*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
	Includere fişier	*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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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
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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
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
CRTSQLCI OS/400' (DB2 Query Manager şi SQL Development pentru programul licenţiat i5/OS) [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 i5/OS) [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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
CRTSQLCBLI (DB2 Query Manager şi SQL Development pentru programul licenţiat i5/OS) [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 OS/400' (DB2 Query Manager şi SQL Development pentru programul licenţiat i5/OS) [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
CRTSQLFTN (DB2 Query Manager şi SQL Development pentru programul licenţiat i5/OS) [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 OS/400' (DB2 Query Manager şi SQL Development pentru programul licenţiat i5/OS) [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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
CRTSQLRPG (DB2 Query Manager şi SQL Development pentru programul licenţiat i5/OS) [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 OS/400' (DB2 Query Manager şi SQL Development pentru programul licenţiat i5/OS) [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
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
INCLUDE	Fişier sursă	*USE	*EXECUTE
RTVCLDSRC	Obiect Locale	*USE	*EXECUTE
	În-fişier	Vedeţi regulile generale.	Vedeţi regulile generale.
RUNSQLSTM[1]	Fişier sursă	*OBJOPR, *READ	*EXECUTE
STRCBLDBG	Program	*CHANGE	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
STRREXPRC	Fişier sursă	*USE	*EXECUTE
	Program ieşire	*USE	*EXECUTE
STRSQL (DB2 Query Manager şi SQL Development pentru programul licenţiat i5/OS) [1]	Tabelă secvenţă de sortare	*USE	*EXECUTE
	Descriere dispozitiv imprimantă	*USE	*EXECUTE
	Coadă de ieşire imprimantă	*USE	*EXECUTE
	Fişier imprimantă	*USE	*EXECUTE

[1] Consultaţi Autorizare, privilegii şi drept de proprietate obiect pentru informaţii suplimentare despre cerinţe de securitate pentru instrucţiuni SQL.

Comenzi bibliotecă

Această tabelă listează autorizările specifice necesare pentru comenzile de bibliotecă.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru biblioteca pe care se acţionează
ADDLIBLE	Bibliotecă		*USE
CHGCURLIB	Bibliotecă curentă nouă		*USE
CHGLIB [8]	Bibliotecă		*OBJMGT
CHGLIBL	Fiecare bibliotecă pusă în lista de biblioteci		*USE
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	

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru biblioteca pe care se acţionează**
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
RSTLIB (Q)[7, 17, 19]	Definiţie medii	*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 de utilizator 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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru biblioteca pe care se acţionează**
RSTLIB (Q)	Fişier bandă (QSYSTAP) sau dischetă (QSYSDKT)	*USE [6]	*EXECUTE
	Ieşire imprimantă QSYS/QPSRLDSP, dacă s-a specificat OUTPUT(*PRINT)	*USE	*EXECUTE
	Fişier de salvare	*USE	*EXECUTE
	Fişier optic (OPTFILE)[12]	*R	Neaplicabilă
	Prefix cale al fişierului optic (OPTFILE)[12]	*X	Neaplicabilă
	Volum optic[11]	*USE	
	Descriere dispozitiv ASP[15]	*USE	
RSTS36LIBM	Fişier-sursă	*USE	*EXECUTE
	În-fişier	*CHANGE	*EXECUTE
	Bibliotecă destinaţie	*CHANGE	*EXECUTE
	Fişier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
RTVLIBD	Bibliotecă		O autorizare alta decât *EXCLUDE
SAVLIB[18]	Fiecare obiect din bibliotecă	*OBJEXIST [6]	*READ, *EXECUTE
	Definiţie medii	*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
	Spaţiu comenzi utilizator, dacă este specificat	*USE	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru biblioteca pe care se acţionează
SAVLIB	Fişier optic[12]	*RW	Neaplicabilă
	Directorul părinte al fişierului optic (OPTFILE)[12]	*WX	Neaplicabilă
	Prefix cale al fişierului optic (OPTFILE)[12]	*X	Neaplicabilă
	Director rădăcină (/) volum optic[12, 13]	*RWX	Neaplicabilă
	Volum optic[11]	*CHANGE	
	Descriere dispozitiv ASP[15]	*USE	
SAVRSTLIB	Pe sistemul sursă, aceeaşi autorizare precum se cere prin comanda SAVLIB.		
	Pe sistemul destinaţie, aceeaşi autorizare precum se cere prin comanda RSTLIB.		
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, 16]	Bibliotecă		*USE

[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 autorizarea specială *ALLOBJ pentru a specifica altă valoare decât *NONE pentru parametrul ALWOBJDIF.

[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.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru biblioteca pe care se acţionează
[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.			
[16] Această comandă cere autorizarea specială *ALLOBJ.			
[17] Trebuie să aveţi autorizare specială *ALLOBJ pentru a specifica *YES pentru parametrul PVTAUT.			
[18] Trebuie să aveţi autorizare specială *ALLOBJ sau *SAVSYS pentru a specifica *YES pentru parametrul PVTAUT.			
[19] Trebuie să aveţi autorizare specială *SAVSYS pentru a specifica un nume pentru parametrul DFRID.			

Comenzi cheie de licenţă

Această tabelă listează autorizările specifice necesare pentru comenzile cheie de licenţă.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ADDLICKEY (Q)	Fişier ieşire	*USE	*EXECUTE
DSPLICKEY (Q)	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
RMVLICKEY (Q)	Fişier ieşire	*CHANGE	*EXECUTE

Comenzi program licenţiat

Această tabelă listează autorizările specifice necesare pentru comenzile program licenţiat.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		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)			

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiecte	Pentru biblioteci
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 autorizarea cerută de operaţii individuale.

Comenzi descriere de linie

Această tabelă listează autorizările specifice necesare pentru comenzile de descriere de linie.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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
CRTLINDDI [2]	Descriere de linie		*READ, *ADD
	Descriere interfaţă de reţea (NWI)	*USE	*EXECUTE
	Descriere controler (NETCTL)	*USE	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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

1 Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea cerută de operaţii individuale.

2 Pentru a folosi această comandă, trebuie să aveţi autorizarea specială *IOSYSCFG.

3 Pentru a folosi această comandă, trebuie să aveţi autorizarea specială *ALLOBJ.

Comenzi reţea locală (LAN)

Această tabelă listează autorizările specifice necesare pentru comenzile reţea locală (LAN).

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Aceste comenzi nu necesită nici o autorizare obiect:			
ADDLANADPI CHGLANADPI	DSPLANADPP DSPLANSTS	RMVLANADPT (Q) RMVLANADPI	WRKLANADPT

Comenzi locale

Această tabelă listează autorizările specifice necesare pentru comenzile locale.

		Autorizare necesară	
Comandă	**Obiect referit**	**Pentru obiect**	**Pentru bibliotecă**
CRTLOCALE	Fişier sursă	*USE	*USE, *ADD
DLTLOCALE	Locale-ul	*OBJEXIST	*EXECUTE

Comenzi Cadru de lucru server mail

Această tabelă listează autorizările specifice necesare pentru comenzile cadru de lucru server mail.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Această comandă nu necesită nici o autorizare pentru obiect:			
ENDMSF (Q)	STRMSF (Q)		

Comenzi mediu

Această tabelă listează autorizările specifice necesare pentru comenzile de mediu.

		Autorizare necesară	
Comandă	**Obiect referit**	**Pentru obiect**	**Pentru bibliotecă**
ADDTAPCTG	Descriere bibliotecă bandă	*USE	*EXECUTE
CFGDEVMLB[1]	Descriere bibliotecă bandă	*CHANGE, *OBJMGT	*EXECUTE
CHGDEVMLB (Q)	Descriere bibliotecă bandă	*CHANGE, *OBJMGT	*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
CRTTAPCGY	Descriere bibliotecă bandă		

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
DLTDKTLBL	Descriere unitate de dischetă	*USE	*EXECUTE
DLTMEDDFN	Definiţie medii	*OBJEXIST	*EXECUTE
DLTTAPCGY	Descriere bibliotecă bandă		
DMPTAP (Q)[5]	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 autorizarea 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.

[5] Pentru a utiliza această comandă, trebuie să aveţi autorizare specială *ALLOBJ când TYPE(*HEX) este specificat sau banda are setat steagul volum asigurat sau fişier asigurat.

Comenzi meniu şi grup de panouri

Această tabelă listează autorizările specifice necesare pentru comenzile meniu şi grup de panouri.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CHGMNU	Meniu	*CHANGE	*USE
CRTMNU	Fişier sursă	*USE	*EXECUTE
	Meniu: REPLACE(*NO)		*READ, *ADD
	Meniu: REPLACE(*YES)	Vedeţi regulile generale.	*READ, *ADD

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
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
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 panou	*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 panou	Orice	*EXECUTE

1 Pentru a folosi o operaţie individuală, trebuie să aveţi autorizarea necesară de operaţie.

Comenzi mesaj

Această tabelă listează autorizările specifice necesare pentru comenzile mesaj.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
DSPMSG	Coada de mesaje	*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	Coada de mesaje	*USE	*EXECUTE
	Înlăturare mesaje din coada de mesaje	*USE, *DLT	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
RMVMSG	Coada de mesaje	*OBJOPR, *DLT	*EXECUTE
RTVMSG	Fişier de mesaje	*USE	*EXECUTE
SNDBRKMSG	Coada de mesaje care primeşte replica la mesajele de interogare	*OBJOPR, *ADD	*EXECUTE
SNDMSG	Coada de mesaje	*OBOPR, *ADD	*EXECUTE
	Coada de mesaje care primeşte replica la mesajul de interogare	*OBJOPR, *ADD	*EXECUTE
SNDPGMMSG	Coada de mesaje	*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	Coada de mesaje	*USE, *ADD	*EXECUTE
	Înlăturare mesaje din coada de mesaje	*USE, *ADD, *DLT	*EXECUTE
SNDUSRMSG	Coada de mesaje	*OBJOPR, *ADD	*EXECUTE
	Fişierul mesaj, când se trimite mesaj predefinit	*USE	*EXECUTE
WRKMSG	Coada de mesaje	*USE	*USE
	Coada de mesaje care primeşte replica la mesajul de interogare	*USE, *ADD	*USE
	Înlăturare mesaje din coada de mesaje	*USE, *DLT	*USE

Comenzi descriere mesaj

Această tabelă listează autorizările specifice necesare pentru comenzile de descriere mesaj.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 autorizarea cerută de operaţii individuale.

Comenzi fişier mesaj

Această tabelă listează autorizările specifice necesare pentru comenzile fişier mesaj.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CHGMSGF	Fişier de mesaje	*USE, *DLT	*EXECUTE
CRTMSGF	Fişier de mesaje		*READ, *ADD
DLTMSGF	Fişier de mesaje	*OBJEXIST	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 autorizare	*USE
[1] Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea cerută de operaţii individuale.			

Comenzi coadă de mesaje

Această tabelă listează autorizările specifice necesare pentru comenzile coadă de mesaje.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CHGMSGQ	Coada de mesaje	*USE, *DLT	*EXECUTE
CLRMSGQ	Coada de mesaje	*OBJOPR, *DLT	*EXECUTE
CRTMSGQ	Coada de mesaje		*READ, *ADD
DLTMSGQ	Coada de mesaje	*OBJEXIST, *USE, *DLT	*EXECUTE
DSPLOG			*EXECUTE
WRKMSGQ [1]	Coada de mesaje	Orice autorizare	*USE
[1] Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea cerută de operaţii individuale.			

Comenzi migrare

Această tabelă listează autorizările specifice necesare pentru comenzile de migrare.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
RCVMGRDTA	Fişier	*ALL	*READ, *ADD
	Dispozitiv	*CHANGE	*EXECUTE
SNDMGRDTA	Fişier	*ALL	*READ, *ADD
	Dispozitiv	*CHANGE	*EXECUTE
Aceste comenzi nu necesită nici o autorizare obiect. Aceste comenzi sunt livrate cu autorizarea publică *EXCLUDE. Trebuie să aveţi autorizare specială *ALLOBJ pentru a utiliza aceste comenzi.			

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ANZS34OCL ANZS36OCL CHGS34LIBM CHKS36SRCA CVTBASSTR CVTBASUNF CVTBGUDTA CVTS36FCT	CVTS36JOB CVTS38JOB GENS36RPT GENS38RPT MGRS36 MGRS36APF [1] MGRS36CBL MGRS36DFU [1]	MGRS36DSPF MGRS36ITM MGRS36LIB MGRS36MNU MGRS36MSGF MGRS36QRY [1] MGRS36RPG MGRS36SEC MGRS38OBJ	MIGRATE QMUS36 RESMGRNAM RSTS38AUT STRS36MGR STRS38MGR
[1] Trebuie să aveţi autorizarea specială *ALLOBJ şi să aveţi opţiunea 4 i5/OS instalată.			

Comenzi descriere mod

Această tabelă listează autorizările specifice necesare pentru comenzile de descriere mod.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CHGMODD [2]	Descriere mod	*CHANGE, *OBJMGT	*EXECUTE
CRTMODD [2]	Descriere mod		*READ, *ADD
CHGSSNMAX	Descriere dispozitiv	*OBJOPR	*EXECUTE
DLTMODD	Descriere mod	*OBJEXIST	*EXECUTE
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 autorizarea cerută de operaţii individuale. [2] Pentru a folosi această comandă, trebuie să aveţi autorizarea specială *IOSYSCFG.			

Comenzi modul

Această tabelă listează autorizările specifice necesare pentru comenzile modul.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 autorizare	*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 autorizarea cerută de operaţii individuale.

Comenzi descriere NetBIOS

Această tabelă listează autorizările specifice necesare pentru comenzile descriere NetBIOS.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 autorizarea cerută de operaţii individuale.

[2] Pentru a folosi această comandă, trebuie să aveţi autorizarea specială *IOSYSCFG.

Comenzi reţea

Această tabelă listează autorizările specifice necesare pentru comenzile de reţea.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ADDNETJOBE (Q)	Profil de utilizator în intrarea job reţea	*USE	
APING	Descriere dispozitiv	*CHANGE	
AREXEC	Descriere dispozitiv	*CHANGE	
CHGNETA (Q) [4]			
CHGNETJOBE (Q)	Profil de 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 de 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	Coada de mesaje	*OBJOPR, *ADD	*EXECUTE
VFYAPPCCNN	Descriere dispozitiv	*CHANGE	
WRKNETF [2,3]			
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.

Comenzi sistem de fişiere reţea

Această tabelă listează autorizările specifice necesare pentru comenzile sistem de fişiere reţea.

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare 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]	fără			

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect
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]	fără			
UNMOUNT [1]				

[1] Pentru a folosi această comandă, trebuie să aveţi autorizarea 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.

Comenzi descriere interfaţă reţea

Această tabelă listează autorizările specifice necesare pentru comenzile descriere interfaţă reţea.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CHGNWIFR [2]	Descriere interfaţă de reţea	*CHANGE, *OBJMGT	*EXECUTE
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 autorizarea specială *IOSYSCFG.

Comenzi server de reţea

Această tabelă listează autorizările specifice necesare pentru comenzile server de reţea.

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare 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)	*STMF	″root″ (/)	*RW
	Descriere server de reţea	*NWSD	QSYS.LIB	*CHANGE, *OBJMGT
CHGNWSSTG[2]	Cale (root şi /QFPNWSSTG)	*DIR	″root″ (/)	*WX
CHGNWSUSRA [4]	Profil de 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)	*STMF	″root″ (/)	*OBJEXIST
DLTWNTSVR[5]	Descriere server de reţea	*NWSD	QSYS.LIB	*OBJEXIST
	Descriere de linie	*LIND	QSYS.LIB	*OBJEXIST
	Configuraţie server de reţea	*NWSCFG	QSYS.LIB	*OBJEXIST
	Stocare server reţea - Cale (/QFPNWSSTG)	*DIR	″root″ (/)	*WX
	Director părinte (numele spaţiului de stocare)	*DIR	″root″ (/)	*RWX, *OBJEXIST
	Fişierele care compun spaţiul de stocare)	*STMF	″root″ (/)	*OBJEXIST
DSPNWSSTG	Prefix cale	Vedeţi regulile generale		
	Fişierele care compun spaţiul de stocare)	*STMF	″root″ (/)	*R
INSWNTSVR[6, 7]	Descriere server de reţea	*NWSD	Neaplicabilă	*USE
	Descriere de linie	*LIND	Neaplicabilă	*USE
	Configuraţie server de reţea	*NWSCFG	Neaplicabilă	*USE
	Stocare server reţea - Cale (/QFPNWSSTG)	*DIR	″root″ (/)	*WX
RMVNWSSTGL [2]	Cale (/QFPNWSSTG)	*DIR	″root″ (/)	*X
	Director părinte (numele spaţiului de stocare)	*DIR	″root″ (/)	*WX
	Fişierele care compun spaţiul de stocare)	*STMF	″root″ (/)	*RW
	Descriere server de reţea	*NWSD	QSYS.LIB	*CHANGE, *OBJMGT
WRKNWSSTG	Prefix cale	Vedeţi regulile generale		
	Fişierele care compun spaţiul de stocare)	*STMF	″root″ (/)	*R
Aceste comenzi nu necesită nici o autorizare obiect:				
ADDRMTSVR CHGNWSA [4](Q) CHGNWSALS CRTNWSALS DLTNWSALS DSPNWSA	DSPNWSALS DSPNWSSSN DSPNWSSTC DSPNWSUSRA SBMNWSCMD (Q) [3]		SNDNWSMSG WRKNWSALS WRKNWSENR WRKNWSSSN WRKNWSSTS	

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect
[1] Autorizarea necesară nu e folosită pentru comenzi ale serverului de reţea.				
[2] Pentru a folosi această comandă, trebuie să aveţi autorizarea 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.				
[5] Pentru a folosi această comandă, trebuie să aveţi autorizarea specială *ALLOBJ.				
[6] Pentru a folosi această comandă, aveţi nevoie de autorizările speciale *IOSYSCFG, *ALLOBJ şi *JOBCTL.				
[7] Trebuie să aveţi autorizarea specială *SECADM pentru a specifica altă valoare decât cea implicită pentru parametrii IPSECRULE, CHAPAUT sau SPCERTID.				

Comenzi configurare server de reţea

Această tabelă listează autorizările specifice necesare pentru comenzile de configurare server de reţea.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru biblioteca QUSRSYS
CHGNWSCFG[1, 3]	Configuraţie server de reţea	*CHANGE	*EXECUTE
CRTNWSCFG [1, 3]	Configuraţie server de reţea	*USE	*READ, *ADD
DLTNWSCFG[1, 3]	Configuraţie server de reţea	*OBJEXIST	*EXECUTE
DSPNWSCFG[1, 3]	Configuraţie server de reţea	*USE	*EXECUTE
INZNWSCFG[1, 2]	Configuraţie server de reţea	*CHANGE	*EXECUTE
WRKNWSCFG[1]	Configuraţie server de reţea	*USE	*EXECUTE
[1] Pentru a folosi această comandă, trebuie să aveţi autorizarea specială *IOSYSCFG.			
[2] Pentru a folosi această comandă, trebuie să aveţi autorizare specială *SECADM.			
[3] Pentru a specifica altă valoare decât cea implicită pentru parametrii IPSECRULE, CHAPAUT sau SPCERTID trebuie să aveţi autorizare de administrator (*SECADM).			

Comenzi descriere server de reţea

Această tabelă listează autorizările specifice necesare pentru comenzile descriere server de reţea.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru biblioteca 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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru biblioteca QSYS

[1] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizarea necesară de operaţie.

[2] Pentru a folosi această comandă, trebuie să aveţi autorizarea specială *IOSYSCFG.

Comenzi listă noduri

Această tabelă listează autorizările specifice necesare pentru comenzile listă noduri.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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.

Comenzi servicii birou

Această tabelă listează autorizările specifice necesare pentru comenzile servicii birou.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Aceste comenzi nu necesită nici o autorizare obiect.			
ADDACC (Q) DSPACC DSPACCAUT DSPUSRPMN	GRTACCAUT [2,3,6] (Q) GRTUSRPMN [1,2] RMVACC [1] (Q) RVKACCAUT [1]	RVKUSRPMN [1,2] WRKDOCLIB [4] WRKDOCPRTQ [5]	

[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.

Comenzi educaţie online

Această tabelă listează autorizările specifice necesare pentru comenzile educaţie online.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate pentru această comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

		Autorizare necesară	
Comandă	**Obiect referit**	**Pentru obiect**	**Pentru bibliotecă**
CVTEDU			
STREDU			

Comenzi asistent operaţional

Această tabelă listează autorizările specifice necesare pentru comenzile asistent operaţional.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

		Autorizare necesară	
Comandă	**Obiect referit**	**Pentru obiect**	**Pentru bibliotecă**
CHGBCKUP [1]	QUSRSYS/QEZBACKUPL *USRIDX	*CHANGE	*EXECUTE
CHGCLNUP[2]			
CHGPWRSCD [3]			
CHGPWRSCDE [3]			
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
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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
STRCLNUP[4]	Profil de utilizator QPGMR	*USE	
	Coadă job	*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 autorizarea specială *JOBCTL.

[5] Trebuie să aveţi autorizarea specială *ALLOBJ.

Comenzi optice

Această tabelă listează autorizările specifice necesare pentru comenzile optice.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară		
		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	Neaplicabilă	Neaplicabilă
	Dispozitiv optic	*USE	*EXECUTE	*CHANGE[3]
	CSI server	*USE	*EXECUTE	Neaplicabilă
CHKOPTVOL	Dispozitiv optic	*USE	*EXECUTE	*USE
	Directorul root (/) al volumului	*RWX	Neaplicabilă	Neaplicabilă
CPYOPT	Dispozitiv optic	*USE	*EXECUTE	*USE - Volum sursă
				*ALL - Volum destinaţie
	Fiecare director precedent în calea fişierului sursă	*X	Neaplicabilă	Neaplicabilă
	Fiecare director precedent din calea fişierului destinaţie	*X	Neaplicabilă	Neaplicabilă
	Fişier sursă (*DSTMF)[5]	*R	Neaplicabilă	Neaplicabilă
	Directorul părinte al fişierului destinaţie	*WX	Neaplicabilă	Neaplicabilă
	Părintele directorului părinte dacă se creează director	*WX	Neaplicabilă	Neaplicabilă

Comandă	Obiect referit	Autorizare necesară		
		Obiect	**Bibliotecă**	**Volum optic**[1]
CPYOPT	Fişierul destinaţie este înlocuit datorită SLTFILE(*ALL)	*W	Neaplicabilă	Neaplicabilă
	Fişierul destinaţie este înlocuit datorită SLTFILE(*CHANGED)	*RW	Neaplicabilă	Neaplicabilă
	Fiecare director din cale care precede directorul sursă	*X	Neaplicabilă	Neaplicabilă
	Fiecare director din cale care precede directorul destinaţie	*X	Neaplicabilă	Neaplicabilă
CPYOPT	Directorul care e copiat [5]	*R	Neaplicabilă	Neaplicabilă
	Directorul care e copiat dacă el conţine intrări	*RX	Neaplicabilă	Neaplicabilă
	Părintele directorului destinaţie	*WX	Neaplicabilă	Neaplicabilă
	Directorul destinaţie dacă e înlocuit datorită SLTFILE(*ALL)	*W	Neaplicabilă	Neaplicabilă
	Directorul destinaţie dacă e înlocuit datorită SLTFILE(*CHANGED)	*RW	Neaplicabilă	Neaplicabilă
	Directorul destinaţie dacă intrările urmează să fie create	*WX	Neaplicabilă	Neaplicabilă
CPYOPT	Fişiere sursă	*R	Neaplicabilă	Neaplicabilă
	Fişierul destinaţie este înlocuit datorită SLTFILE(*ALL)	*W	Neaplicabilă	Neaplicabilă
	Fişierul destinaţie este înlocuit datorită SLTFILE(*CHANGED)	*RW	Neaplicabilă	Neaplicabilă
CRTDEVOPT [4]	Dispozitiv optic		*EXECUTE	
CVTOPTBKU	Dispozitiv optic	*USE	*EXECUTE	*ALL
DSPOPT	Prefix cale când DATA (*SAVRST)[5]	*X	Neaplicabilă	Neaplicabilă
	Prefix fişier când (*SAVRST)[2]	*R	Neaplicabilă	Neaplicabilă
	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

Comandă	Obiect referit	Autorizare necesară		
		Obiect	**Bibliotecă**	**Volum optic**[1]
INZOPT	Directorul root (/) al volumului	*RWX	Neaplicabilă	Neaplicabilă
	Dispozitiv optic	*USE	*EXECUTE	*ALL
LODOPTFMW	Fişier de flux	*R	Neaplicabilă	Neaplicabilă
	Prefix cale	Vedeţi regulile generale.		
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 autorizare pentru lista care securizează curent volumul optic pentru a o modifica.

[4] Pentru a folosi această comandă, trebuie să aveţi autorizarea specială *IOSYSCFG.

[5] Această verificare de autorizare este făcută doar când formatul mediului de stocare optic este UDF (Universal Disk Format).

Comenzi coadă ieşire

Această tabelă listează autorizările specifice necesare pentru comenzile coadă de ieşire.

Comandă	Obiect referit	Parametri coadă ieşire		Autorizare specială	Autorizare necesară	
		AUTCHK	OPRCTL		Pentru obiect	Pentru bibliotecă
CHGOUTQ [1]	Coadă de date				*READ	*EXECUTE
	Coadă de ieşire	*DTAAUT			*OBJMGT, *READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar [2]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Coada de mesaje				*OBJOPR *ADD	*EXECUTE
	obiect de personalizare staţie de lucru				*USE	*EXECUTE
	Program transformare date utilizator				*OBJOPR *EXECUTE	*EXECUTE
	Program cu driver utilizator				*OBJOPR *EXECUTE	*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
	Coadă de ieşire				*OBJOPR *ADD	*EXECUTE
	obiect de personalizare staţie de lucru				*USE	*EXECUTE
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

Comandă	Obiect referit	Parametri coadă ieşire		Autorizare specială	Autorizare necesară	
		AUTCHK	OPRCTL		Pentru obiect	Pentru bibliotecă

[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 autorizarea specială *ALLOBJ pentru a folosi această comandă.

Comenzi pachet

Această tabelă listează autorizările specifice necesare pentru comenzile pachet.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 serviciu	*OBJOPR, *READ	*EXECUTE
STRSQL			

Comenzi performanţă

Această tabelă listează autorizările specifice necesare pentru comenzile de performanţă.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul cu securitatea poate acorda *USE altora.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ADDDWDFN (Q) [7]			
ADDJWDFN (Q) [7]			
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	

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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
ANZCMDPFR (Q)	Fişier comenzi	*USE	*EXECUTE
	Fişier ieşire	*USE	*EXECUTE, *ADD
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
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
CHGMGTCOL	MGTCOL	*OBJMGT	
	Bibliotecă utilizator		*EXECUTE
CHGPEXDFN (Q)[5]	Biblioteca 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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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
CPYPFRCOL (Q)	Bibliotecă sursă		*EXECUTE
	Bibliotecă destinaţie		*EXECUTE, *ADD
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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CRTPEXDTA (Q)[5]	Biblioteca *MGTCOL		*EXECUTE
	Bibliotecă de date[1]		*READ, *ADD [2]
CRTPFRDTA (Q)	Bibliotecă sursă		*EXECUTE
	Bibliotecă destinaţie		*ADD, *READ
	Bibliotecă sursă		*USE
CRTPFRSUM (Q)	Bibliotecă utilizator		*ADD, *READ
CVTPFRCOL (Q)	Bibliotecă sursă		*USE
	Bibliotecă destinaţie		*USE, *ADD
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
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]
DLTPFRCOL (Q)	Bibliotecă		*EXECUTE
DLTPFRDTA (Q)[4]	QPFR/QPTDLTCP *PGM	*USE	*EXECUTE
DMPMEMINF	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
DMPTRC (Q)[5]	Biblioteca în care vor fi memorate datele de urmărire		*EXECUTE, *ADD
	Fişier de ieşire (QAPTPAGD)	*CHANGE	*EXECUTE, *ADD
DSPHSTGPH (Q)[4]	QPFR/QPGCTRL *PGM	*USE	*EXECUTE
	Biblioteca date istorice		*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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
ENDDW (Q)[7]			
ENDJOBTRC (Q)[4]	QPFR/QPTTRCJ0 *PGM	*USE	*EXECUTE
ENDJW (Q)[7]			
ENDPEX (Q)[5]	Bibliotecă 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
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]	Bibliotecă de date[1]		*EXECUTE[2]
	Fişier ieşire	*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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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
RMVDWDFN (Q) [7]			
RMVJWDFN (Q) [7]			
RMVPEXDFN (Q)[5]			
RMVPEXFTR (Q)[5]			
RSTPFRCOL (Q)	Biblioteca asociată cu colecţia de restaurare	*EXECUTE,, *ADD [6]	
	Fişier de salvare	*USE	*EXECUTE
SAVPFRCOL (Q)	Biblioteca în care se află colecţia ce va fi salvată	*EXECUTE [6]	
	Fişier de salvare, dacă este gol	*USE, *ADD	*EXECUTE, *ADD
	Fişier de salvare, dacă există înregistrări în el	*OBJMGT, *USE, *ADD	*EXECUTE
STRBEST (Q)[4]	QPFR/QCYBMAIN *PGM	*USE	*EXECUTE
STRDBMON[3, 4]	Fişier ieşire	*OBJOPR, *ADD	*EXECUTE
STRDW (Q)[7]	Bibliotecă utilizator		*EXECUTE
STRJOBTRC (Q)	QPFR/QPTTRCJ1 *PGM	*USE	*EXECUTE
STRJW (Q) [7]	Bibliotecă utilizator		*EXECUTE
STRPEX (Q)[5]			
STRPFRCOL (Q)			
STRPFRG (Q)[4]	QPFR/QPGSTART *PGM	*USE	*EXECUTE
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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
Aceste comenzi nu necesită nici o autorizare 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 în care se află 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 autorizare specială *SERVICE sau trebuie să fiţi autorizat asupra funcţiei Urmă service a i5/OS prin Application Administration din Navigator System i. 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.

[6] Dacă aveţi autorizarea specială *SAVSYS, nu aveţi nevoie de autorizarea specificată.

[7] Pentru a folosi aceată comandă, trebuie să aveţi autorizare specială de service (*SERVICE) sau să fiţi autorizat asupra funcţiei Disk Watcher a sistemului de operare prin suportul Navigator System i Application Administration. Comanda Modificare folosire funcţie (CHGFCNUSG), cu un ID de funcţie de QIBM_SERVICE_DISK_WATCHER, poate fi de asemenea folosită pentru a modifica lista de utilizatori cărora le este permis să folosească unealta disk watcher.

Comenzi grup descriptori de tipărire

Această tabelă listează autorizările specifice necesare pentru comenzile grup descriptori de tipărire.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CHGPDGPRF	Profil de utilizator	*OBJMGT	
CRTPDG	Grup descriptor tipărire		*READ, *ADD
DLTPDG	Grup descriptor tipărire	*OBJEXIST	*EXECUTE
DSPPDGPRF	Profil de utilizator	*OBJMGT	
RTVPDGPRF	Profil de utilizator	*READ	

Comenzi configurare Facilitate service tipărire

Această tabelă listează autorizările specifice necesare pentru comenzile de configurare facilitate service tipărire.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
[1] Opţiunea PSF/400 este necesară pentru a folosi această comandă.			
[2] Este necesară autorizarea specială *IOSYSCFG pentru a folosi această comandă.			

Comenzi problemă

Această tabelă listează autorizările specifice necesare pentru comenzile problemă.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
ADDPRBACNE (Q)	Filtrare	*USE, *ADD	*EXECUTE
ADDPRBSLTE (Q)	Filtrare	*USE, *ADD	*EXECUTE
ANZPRB (Q)	Comanda SNDSRVRQS	*USE	*EXECUTE
CHGPRB (Q)			*EXECUTE
CHGPRBACNE (Q)	Filtrare	*USE, *UPD	*EXECUTE
CHGPRBSLTE (Q)	Filtrare	*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
[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 de 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.			

Comenzi program

Această tabelă listează autorizările specifice necesare pentru comenzile program.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
Autorizările pentru obiect necesare pentru comenzile CRT*xxx*PGM sunt afişate în tabela Limbaje din “Comenzi limbă” la pagina 423.			
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 serviciu	*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.	Păstrătorul [7], *USE, *OBJMGT	*USE, *ADD, *DLT
CLRTRCDTA [1]			
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
	Export sursă fişier	*OBJOPR *READ	*EXECUTE
	Director legare	*USE	*EXECUTE
CVTCLSRC	Fişier-sursă	*USE	*EXECUTE
	În-fişier	*OBJOPR, *OBJMGT, *USE, *ADD, *DLT	*READ, *ADD

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
DLTDFUPGM	Program	*OBJEXIST	*EXECUTE
	Fişier afişare	*OBJEXIST	*EXECUTE
DLTPGM	Program	*OBJEXIST	*EXECUTE
DLTSRVPGM	Program serviciu	*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 serviciu	*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
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	Programul tratare-tastă-atenţie	*EXECUTE	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
SETPGMINF	Fişiere baze 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
UPDSRVPGM	Program service	*OBJMGT, *OBJEXIST, *USE	*USE, *ADD
	Programul service specificat în parametrul BNDSRVPGM	*USE	*EXECUTE
	Modul	*USE	*EXECUTE
	Director legare	*USE	*EXECUTE
	Export sursă fişier	*OBJOPR *READ	*EXECUTE
WRKPGM [6]	Program	Orice autorizare	*USE
WRKSRVPGM [6]	Program serviciu	Orice autorizare	*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. Deoarece autorizarea pentru biblioteca în care se află programul este verificată în momentul apelării programului, autorizarea pentru bibliotecă nu este verificată din nou când comanda DMPCLPGM este rulată.

[4] Se aplică doar pentru programele ILE.

[5] Consultaţi Autorizare, privilegii şi drept de proprietate obiect pentru informaţii suplimentare despre cerinţe de securitate pentru instrucţiuni SQL.

[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.

Comenzi interpretor shell QSH

Această tabelă listează autorizările specifice necesare pentru comenzile interpretor shell QSH.

Comenzile listate în acest tabel nu necesită vreo autorizare pentru obiecte.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
STRQSH [1, 2]			
QSH[1, 2]			

[1] QSH este un alias pentru comanda CL STRQSH.

[2] Aveţi nevoie de autorizarea *RX pentru toate scripturile şi toate directoarele din calea scriptului.

Comenzi interogare

Această tabelă listează autorizările specifice necesare pentru comenzile de interogare.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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
RTVQMFORM	Formular Query Manager	*OBJEXIST	*EXECUTE
	Fişier sursă destinaţie	*ALL	*READ, *ADD, *EXECUTE
	Comenzile ADDPFM, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, OVRDBF, RMVM	*USE	*EXECUTE
RTVQMQRY	Interogare Query Manager	*USE	*EXECUTE
	Fişier sursă destinaţie	*ALL	*READ, *ADD
	Comenzile ADDPFM, CHGPFM, CLRPFM, CPYSRCF, CRTPRTF, CRTSRCPF, DLTF, DLTOVR, OVRDBF, RMVM	*USE	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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.
	Comenzile 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 instrucţiunile au ca rezultat un raport tipărit sau un obiect interogare.	*USE	*EXECUTE
STRQRY			*EXECUTE
WRKQMFORM [3]	Formular Query Management	Orice autorizare	*USE
WRKQMQRY [3]	Interogare Query Management	Orice autorizare	*USE
WRKQRY [3]			

[1] Pentru a rula STRQM, trebuie să aveţi autorizarea cerută de declaraţiile din interogare. De exemplu, pentru a insera o linie într-o tabelă este necesară autorizarea *OBJOPR, *ADD şi *EXECUTE pentru tabel.

[2] Drept de proprietate sau unele autorizări pentru obiect sunt necesare.

[3] Pentru a folosi operaţii individuale, trebuie să aveţi autorizarea cerută de operaţii individuale.

[4] Pentru a folosi comandă individuală, trebuie să aveţi autorizarea specială *JOBCTL.

Comenzi întrebare şi răspuns

Această tabelă listează autorizările specifice necesare pentru comenzile întrebare şi răspuns.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ANSQST (Q)	Fişier bază de date QAQA*xx*BQPY [1]	*READ	*READ
ASKQST	Fişier bază de date QAQA*xx*BBPY [1] sau QAQA*xx*BQPY [1]	*READ	*READ
CHGQSTDB (Q)	Fişier bază de date QAQA*xx*BQPY [1]	*READ	*READ

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CRTQSTDB [2] (Q)	Fişiere baze 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] sau 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 autorizarea 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 autorizarea necesară pentru aceste opţiuni.

Comenzi cititor

Această tabelă listează autorizările specifice necesare pentru comenzile cititor.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
STRDBRDR	Coada de mesaje	*OBJOPR, *ADD	*EXECUTE
	Fişier bază de date	*OBJOPR, *USE	*EXECUTE
	Coadă job	*READ	*EXECUTE
STRDKTRDR	Coada de mesaje	*OBJOPR, *ADD	*EXECUTE
	Coadă job	*READ	*EXECUTE
	Descriere dispozitiv	*OBJOPR, *READ	*EXECUTE
Aceste comenzi nu necesită vreo autorizare obiect:			
ENDRDR [1]	HLDRDR [1]	RLSRDR [1]	

[1] Trebuie să fiţi utilizatorul care a pornit cititorul sau să aveţi autorizarea specială (*ALLOBJ) sau control job (*JOBCTL).

Comenzi facilitate înregistrare

Această tabelă listează autorizările specifice necesare pentru comenzile facilitate înregistrare.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ADDEXITPGM (Q)			
RMVEXITPGM (Q)			
WRKREGINF			

Comenzi bază de date relaţională

Această tabelă listează autorizările specifice necesare pentru comenzile bază de date relaţională.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 autorizare obiect:			
RMVRDBDIRE WRKRDBDIRE			
[1] Autorizare verificată atunci când este folosită intrarea director RDB.			

Comenzi resurse

Această tabelă listează autorizările specifice necesare pentru comenzile resurse.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 autorizarea de a folosi comanda CRT corespunzătoare.			

Comenzi Intrare job la distanţă (RJE)

Această tabelă listează autorizările specifice necesare pentru comenzile Intrare job la distanţă (RJE).

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
ADDFCTE	Tabelă de control formulare	*DELETE, *USE, *ADD	*READ, *EXECUTE
	Fişier dispozitiv [1,2]	*USE	*READ, *EXECUTE
	Fişier fizic [1,2] (RJE generează membri)	*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 de 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 de 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 generează membri)	*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 de utilizator QUSER	*USE	*READ, *EXECUTE
CHGFCT	Tabelă de control formulare	*OBJOPR, *OBJMGT	*READ, *EXECUTE
CHGFCTE	Tabelă de control formulare	*USE	*READ, *EXECUTE
	Fişier dispozitiv [1,2]	*USE	*READ, *EXECUTE
	Fişier fizic [1,2] (RJE generează membri)	*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 de 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 de 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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
CHGRJEWTRE	Descriere sesiune	*USE	*READ, *EXECUTE
	Fişier dispozitiv [1,2]	*USE	*READ, *EXECUTE
	Fişier fizic [1,2] (RJE generează membri)	*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 de 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 de utilizator QUSER	*USE	*EXECUTE
CNLRJERDR	Descriere sesiune	*USE	*EXECUTE
	Coada de mesaje	*USE, *ADD	*EXECUTE
CNLRJEWTR	Descriere sesiune	*USE	*EXECUTE
	Coada de mesaje	*USE, *ADD	*EXECUTE
CRTFCT	Tabelă de control formulare		*READ, *ADD
CRTRJEBSCF	Fişier BSC		*READ, *EXECUTE, *ADD
	Fişier fizic sursă(DDS)	*READ	*EXECUTE
	Descriere dispozitiv	*READ	*EXECUTE
CRTRJECFG	Descriere sesiune		*READ, *ADD, *UPD, *OBJOPR
	Coadă job		*READ, *ADD
	Descriere job		*READ, *OBJOPR, *ADD
	Descriere subsistem		*READ, *OBJOPR, *ADD
	Coada de mesaje		*READ, *ADD
	Fişier CMN		*READ, *EXECUTE, *ADD
	Fişier BSC		*READ, *EXECUTE, *ADD
	Fişier imprimantă		*USE, *ADD

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
CRTRJECFG	Fişier fizic		*EXECUTE, *ADD
	Profil de utilizator QUSER [3]	*USE	*EXECUTE
	Coadă de ieşire	*READ	*EXECUTE
	Tabelă 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 de utilizator QUSER	*USE	*EXECUTE
CVTRJEDTA	Tabelă 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	Tabelă de control formulare	*OBJEXIST	*EXECUTE
DLTRJECFG	Descriere sesiune	*OBJEXIST	*EXECUTE
	Coadă job	*OBJEXIST	*EXECUTE
	Fişier BSC/CMN	*OBJEXIST, *OBJOPR	*EXECUTE
	Fişier fizic	*OBJEXIST, *OBJOPR	*EXECUTE
	Fişier imprimantă	*OBJEXIST, OBJOPR	*EXECUTE
	Coada de mesaje	*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	Tabelă de control formulare	*OBJOPR, *READ, *ADD, *DLT	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
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
	Coada de mesaje	*USE, *ADD	*EXECUTE
	Obiecte legate de job [7]		
SNDRJECMD	Descriere sesiune	*USE	*EXECUTE
STRRJECSL	Descriere sesiune	*USE	*EXECUTE
	Coada de mesaje	*USE	*EXECUTE
STRRJERDR	Descriere sesiune	*USE	*USE
STRRJESSN [5]	Descriere sesiune	*USE	*USE, *ADD
	Program	*USE	*EXECUTE
	Profil de utilizator QUSER	*USE	*EXECUTE
	Obiecte legate de job [7]		*EXECUTE
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 de utilizator QUSER	*USE	*READ, *EXECUTE
WRKFCT [8]	Tabelă de control formulare	*USE	*EXECUTE
WRKRJESSN [8]	Descriere sesiune	*USE	*EXECUTE
WRKSSND [8]	Descriere sesiune	*CHANGE	*EXECUTE

1 Profil de utilizator QUSER necesită autorizare pentru acest obiect.

2 Dacă obiectul nu este găsit sau nu este deţinută autorizarea necesară, un mesaj informaţional este trimis şi funcţia comenzii este încă realizată.

3 Această autorizare este necesară pentru a crea descrierea jobului QRJESSN.

4 Această autorizare este necesară doar când DLTCMN(*YES) este specificat.

5 Trebuie să aveţi autorizarea specială *JOBCTL.

6 Fişierele de intrare includ cele încorporate folosind instrucţiunea de control .. READFILE.

7 Examinaţi autorizările necesare pentru comanda SBMJOB.

8 Pentru a folosi o operaţie individuală, trebuie să aveţi autorizarea necesară de operaţie.

Comenzi atribute securitate

Această tabelă listează autorizările specifice necesare pentru comenzile atribute de securitate.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CHGSECA [1]			
CHGSECAUD [2,3]			
CFGSYSSEC [1,2,3]			
DSPSECA			
DSPSECAUD [3]			
PRTSYSSECA [4]			

[1] Trebuie să aveţi autorizarea specială *SECADM pentru a folosi această comandă.

[2] Trebuie să aveţi autorizarea specială *ALLOBJ pentru a folosi această comandă.

[3] Trebuie să aveţi autorizarea specială *AUDIT pentru a folosi această comandă.

[4] Trebuie să aveţi autorizarea specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.

Comenzi intrare autentificare server

Această tabelă listează autorizările specifice necesare pentru comenzile intrare autentificare server.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ADDSVRAUTE[1]			
CHGSVRAUTE[1]			
DSPSVRAUTE	Profil de utilizator	*READ	*EXECUTE
RMVSVRAUTE[1]			

[1] Dacă profilul de utilizator pentru această operaţie nu este *CURRENT sau utilizatorul curent pentru job, trebuie să aveţi autorizarea specială *SECADM şi autorizarea *USE pentru profil.

Comenzi service

Această tabelă listează autorizările specifice necesare pentru comenzile de service.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate pentru această comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ADDTRCFTR[11]			
APYPTF (Q)	Bibliotecă produs	*OBJMGT	
CHGSRVA [3] (Q)			
CHKCMNTRC [3] (Q)			*EXECUTE
CHKPRDOPT (Q)	Toate obiectele din opţiunea produs [4]		

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
CPYPTF[2](Q)	Fişier-sursă	*USE	*EXECUTE
	În-fişier[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
	Fişier-sursă	*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	
DMPJOB (Q)			*EXECUTE
DMPJOBINT (Q)			
DSPPTF (Q)	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
DSPSRVA (Q)			
DSPSRVSTS (Q)			
DSPSSTUSR [20]			
ENDCMNTRC [3] (Q)	NWID sau descriere de linie	*USE	*EXECUTE
ENDCPYSCN (Q)	Descriere dispozitiv	*USE	*EXECUTE
ENDSRVJOB (Q)			
ENDTRC (Q)	Bibliotecă	*ADD, *EXECUTE	
	Fişiere baze de date	*OBJOPR, *OBJMGMT, *ADD, *DLT	
	Comenzi: PTRTRC, DLTTRC	*USE	
EDNWCH[16] (Q)	Sesiune de urmărire urmărind un mesaj în intr-un jurnal job [18]		
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.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
PRTERRLOG (Q)	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
PRTINTDTA[12,13] (Q)			
PRTTRC[11](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)	CRTIMGCLG	*USE	
	QUSRSYS		*ADD, *READ
SNDSRVRQS (Q)			
STRCMNTRC [11] (Q)	NWID (ID reţea) sau descriere de linie	*USE	*EXECUTE
	Job observat[17]		
	Urmărire program	*OBJOPR şi *EXECUTE	*EXECUTE
	Coadă de mesaje	*USE	*USE
STRCPYSCN	Coadă job	*USE	*EXECUTE
	Descriere dispozitiv	*USE	*EXECUTE
	Fişier sursă, dacă este specificat	Vedeţi regulile generale.	Vedeţi regulile generale.
STRSRVJOB (Q)	Profil de utilizator al jobului	*USE	*EXECUTE
STRSST [3] (Q)			
STRTRC (Q)[11, 15]	Job observat[17]		
	Urmărire program	*OBJOPR şi *EXECUTE	*EXECUTE
	Coadă de mesaje	*USE	*USE
STRWCH[16] (Q)	Job observat[17]		
	Observare program	*OBJOPR şi *EXECUTE	*EXECUTE
	Coadă de mesaje	*USE	*USE
TRCCNN[11](Q)	Job observat[17]		
	Urmărire program	*OBJOPR şi *EXECUTE	*EXECUTE
	Coadă de mesaje	*USE	*USE
TRCCPIC (Q)			

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
TRCICF (Q)			
TRCINT[11] (Q)	Job observat[17]		
	Urmărire program	*OBJOPR şi *EXECUTE	*EXECUTE
	Coadă de mesaje	*USE	*USE
TRCJOB (Q)	Fişier sursă, dacă este specificat	Vedeţi regulile generale.	Vedeţi regulile generale.
	Program de ieşire, dacă există	*USE	*EXECUTE
TRCTCPAPP[11] (Q)	Descriere de linie	*USE	
	Interfaţă reţea	*USE	
	Interfaţă reţea	*USE	
	Job observat[17]		
	Urmărire program	*OBJOPR şi *EXECUTE	*EXECUTE
	Coadă de mesaje	*USE	*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)			
WRKPTFORD (Q)	QESCPTFO şi SNDPTFORD	*USE	
WRKSRVPVD (Q)			
WRKTRC[11] (Q)			
WRKWCH[19] (Q)			

1 Aveţi nevoie de autorizare pentru comanda PRTERRLOG pentru unele proceduri de analiză dacă înregistrările din istoricul de erori sunt salvate.

2 Se aplică de asemenea toate restricţiile pentru comanda RSTOBJ.

3 Trebuie să aveţi autorizare specială Service (*SERVICE) pentru a folosit această comandă.

4 Obiectele listate sunt folosite de comandă, dar autorizarea pentru obiecte nu este verificată. autorizarea pentru a folosi comanda este suficientă pentru a folosi obiectele.

5 Aveţi nevoie de autorizarea *USE pentru obiectele de comunicaţii pe care le verificaţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
[6] Trebuie să aveţi autorizarea specială *SPLCTL pentru a salva un fişier de spool. [7] Atunci când SAVAPARDTA este rulată pentru o problemă nouă, o bibliotecă unică APAR este creată pentru acea problemă. Dacă rulaţi din nou SAVAPARDTA pentru aceeaşi problemă pentru a colecta mai multe informaţii, trebuie să aveţi autorizarea 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 autorizări 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 autorizarea *USE pentru comanda SNDSRVRQS. Următoarele restricţii se aplică parametrului IMGDIR: • Trebuie să aveţi autorizare *X asupra fiecărui director din cale. • Trebuie să aveţi autorizare *WX asupra directorului care conţine imaginea optică.			
[11] Pentru a folosi această comandă, trebuie să aveţi autorizare specială *SERVICE sau trebuie să fiţi autorizat asupra funcţiei Urmărire service a i5/OS prin Application Administration din System i. Poate fi folosită de asemenea comanda Modificare informaţii de folosire funcţie (CHGFCNUSG), cu ID-ul de funcţie QIBM_SERVICE_TRACE, pentru a modifica lista de utilizatori care au permisunea de a realiza operaţii de urmărire. [12] Pentru a folosi această comandă, trebuie să aveţi autorizare specială *SERVICE sau trebuie să fiţi autorizat asupra funcţiei Dump serviciu a i5/OS prin Application Administration din System i. 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 jobul pentru care se tipăresc datele interne sau lansatorul comenzii trebuie să ruleze sub un profil de utilizator identic cu utilizatorul jobului pentru care sunt tipărite datele interne sau lansatorul comenzii trebuie să ruleze sub un profil de utilizator care are autorizarea 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. [15] Dacă specificaţi un nume generic de utilizator pentru parametrul Nume job (JOB), trebuie să aveţi autorizare specială toate obiectele (*ALLOBJ) sau să fiţi autorizat asupra funcţiei Urmărire orice utilizator a i5/OS prin Application Administration în System i Navigator. De asemenea, poate fi folosită comanda CHGFCNUSG (Change Function Usage - Modificare utilizare funcţie) cu ID-ul de funcţie QIBM_ACCESS_ALLOBJ_TRACE pentru a modifica lista de utilizatori cărora le este permis să realizeze operaţii de urmărire.			

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
[16] Pentru a folosi această comandă, trebuie să aveţi autorizare specială service (*SERVICE) sau trebuie să fiţi autorizat asupra funcţiei Urmărire service a i5/OS prin Application Administration din System i. De asemenea, poate fi folosită comanda CHGFCNUSG (Change Function Usage - Modificare utilizare funcţie) cu ID-ul de funcţie QIBM_ACCESS_ALLOBJ_SERVICE pentru a modifica lista de utilizatori cărora le este permis să pornească şi să oprească operaţii de urmărire.			
[17] Autorizare specială *JOBCTL este necesară dacă jobul rulează sub un alt utilizator din identitatea utilizator job a jobului observat. Autorizare specială *ALLOBJ este necesară dacă *ALL este specificat pentru numele jobului observat, sau este specificat un nume utilizator generic. Un utilizator care nu are autorizare specială *ALLOBJ poate realiza funcţia dacă este autorizat asupra funcţiei Urmărire orice job a i5/OS prin Application Administration în System i Navigator. De asemenea, poate fi folosită comanda CHGFCNUSG (Change Function Usage - Modificare utilizare funcţie) cu ID-ul de funcţie QIBM_ACCESS_ALLOBJ_SERVICE pentru a modifica lista de utilizatori cărora le este permis să pornească şi să oprească operaţii de urmărire.			
[18] Este necesară aceeaşi autorizare ca la comanda STRWCH.			
[19] Pentru a folosi această comandă, trebuie să aveţi autorizare specială service (*SERVICE) sau să fiţi autorizat asupra funcţiei de urmărire serviciu şi funcţiei urmărire serviciu a i5/OS prin Application Administration în System i Navigator. 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.			
[20] Trebuie să aveţi autorizări speciale Auditare (*AUDIT) şi Administrator securitate (*SECADM) pentru a folosi această comandă.			

Comenzi dicţionar ajutor ortigrafie

Această tabelă listează autorizările specifice necesare pentru comenzile dicţionar ajutor ortografie.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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 autorizare	*USE
[1] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizarea necesară de operaţie.			

Comenzi sferă de control

Această tabelă listează autorizările specifice necesare pentru comenzile sferă de control.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ADDSOCE	Sferă de control[1]	*USE, *ADD	*EXECUTE
DSPSOCSTS			
RMVSOCE	Sferă de control[1]	*USE, *DLT	*EXECUTE
WRKSOC	Sferă de control[1]	*USE	*EXECUTE
[1] Sfera de control este fişier fizic QUSRSYS/QAALSOC.			

Comenzi fişier spooled

Această tabelă listează autorizările specifice necesare pentru comenzile fişier spooled.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate pentru această comandă. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

		Parametri coadă ieşire				Autorizare necesară	
Comandă	**Obiect referit**	**DSPDTA**	**AUTCHK**	**OPRCTL**	**Autorizare specială**	**Pentru obiect**	**Pentru bibliotecă**
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 spool	*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 pentru DSP sau altă operaţie ce foloseşte fişierul ieşire (OUTPUT (*OUTFILE))	Vedeţi regulile generale pentru DSP sau altă operaţie ce foloseşte fişierul ieşire (OUTPUT (*OUTFILE))
	Fişier spool	*OWNER				Proprietar [6]	
	Coadă de ieşire[3]	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Proprietar [4]	
		*YES sau *NO		*YES	*JOBCTL		
DLTEXPSPLF (Q) [10]	Pool discuri independent [9]					*USE	
DLTSPLF [1]	Coadă de ieşire[3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Proprietar [4]	
				*YES	*JOBCTL		

Comandă	Obiect referit	Parametri coadă ieşire			Autorizare specială	Autorizare necesară	
		DSPDTA	AUTCHK	OPRCTL		Pentru obiect	Pentru bibliotecă
DSPSPLF [1]	Coadă de ieşire[3]	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Proprietar [4]	
		*YES sau *NO		*YES	*JOBCTL		
	Fişier spool	*OWNER				Proprietar [6]	
HLDSPLF [1]	Coadă de ieşire[3]		*DTAAUT			*READ, *ADD, *DLT	
			*OWNER			Proprietar [4]	
				*YES	*JOBCTL		
RCLSPLSTG (Q) [10]	Pool discuri independent [9]					*USE	
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 spool	*OWNER				Proprietar [6]	
SNDTCPSPLF [1,5]	Coadă de ieşire[3]	*YES				*READ	
		*NO	*DTAAUT			*READ, *ADD, *DLT	
		*NO	*OWNER			Proprietar [4]	
		*YES sau *NO		*YES	*JOBCTL		
	Fişier spool	*OWNER				Proprietar [6]	
STRSPLRCL (Q)[9, 10]	Pool discuri independent [9]					*USE	
WRKSPLF							

1 Utilizatorii sunt întotdeauna 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 de utilizator, trebuie să aveţi una din autorizările arătate în coada de ieşire sau să aveţi autorizarea 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 autorizarea *USE pentru coada de ieşire şi biblioteca de coadă de ieşire a destinatarului atunci când trimiteţi un fişier unui utilizator de pe acelaşi subsistem.

Comandă	Obiect referit	Parametri coadă ieşire			Autorizare specială	Autorizare necesară	
		DSPDTA	AUTCHK	OPRCTL		Pentru obiect	Pentru bibliotecă

[6] Trebuie să fiţi proprietarul fişierului spool.

[7] Dacă aveţi autorizarea specială *SPLCTL, nu aveţi nevoie de autorizare pentru coada de ieşire destinaţie dar trebuie să aveţi autorizarea *EXECUTE pentru bibliotecă.

[8] Când fişierul spool a fost reţinut cu HLDJOB SPLFILE(*YES) şi fişierul spool a fost de asemenea decuplat de la job, utilizatorul trebuie să aibă autorizarea *USE pentru comanda RLSJOB fie autorizarea specială *JOBCTL sau să fie proprietarul fişierului spool.

[9] Trebuie să aveţi autorizare *USE asupra tuturor pool-urilor de disc independente dintr-un grup de pool de discuri independente.

[10] Trebuie să aveţi autorizare *SPLCTL pentru a rula această comandă.

Comenzi descriere subsistem

Această tabelă listează autorizările specifice necesare pentru comenzi de descriere subsistem.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ADDAJE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job[9]	*OBJOPR, *READ	*EXECUTE
ADDCMNE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job[9]	*OBJOPR, *READ	*EXECUTE
	Profil de utilizator	*USE	
ADDJOBQE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
ADDPJE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Profil de utilizator	*USE	
	Descriere job[9]	*OBJOPR, *READ	*EXECUTE
ADDRTGE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
ADDWSE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job[9]	*OBJOPR, *READ	*EXECUTE
CHGAJE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job[9]	*OBJOPR, *READ	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CHGCMNE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job[9]	*OBJOPR, *READ	*EXECUTE
	Profil de utilizator	*USE	
CHGJOBQE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
CHGPJE	Descriere subsistem	*OBJOPR, *OBJMGT, *READ	*EXECUTE
	Profil de utilizator	*USE	
	Descriere job[9]	*OBJOPR, *READ	*EXECUTE
CHGRTGE	Descriere subsistem	*OJBOPR, *OBJMGT, *READ	*EXECUTE
CHGSBSD [5, 7]	Descriere subsistem	*OJBOPR, *OBJMGT, *READ	*EXECUTE
	fişier afişare semnare[4]	*USE	*EXECUTE
CHGWSE	Descriere subsistem	*OJBOPR, *OBJMGT, *READ	*EXECUTE
	Descriere job[9]	*OBJOPR, *READ	*EXECUTE
CRTSBSD [5] (Q)	Descriere subsistem		*READ, *ADD
	fişier afişare semnare[4]	*USE	*EXECUTE
	Descriere dispozitiv ASP[8]	*USE	
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
	Descriere dispozitiv ASP	*USE	
WRKSBS [2, 3]	Descriere subsistem	Orice autorizare	*USE
WRKSBSD [3]	Descriere subsistem	Orice autorizare	*USE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
[1] Trebuie să aveţi autorizare specială de control job (*JOBCTL) pentru a utiliza această comandă.			
[2] Necesită unele autorizări (orice în afară de *EXCLUDE)			
[3] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizarea necesară de operaţie.			
[4] Autorizarea este necesară pentru a realiza verificările de forma ale fişierului de afişare. Acest ajutor prezice că afişare va merge corect 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 autorizarea specială *SECADM sau *ALLOBJ pentru a specifica o anumită bibliotecă pentru biblioteca subsistem.			
[6] Trebuie să aveţi autorizarea specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.			
[7] Trebuie să aveţi autorizări speciale *ALLOBJ şi *SECADM pentru a modifica numele de grup ASP.			
[8] Pentru a specifica o descriere de dispozitiv ASP care nu există, trebuie să aveţi autorizare specială toate obiectele (*ALLOBJ).			
[9] Pentru a specifica o descriere de job care nu există, trebuie să aveţi autorizare specială toate obiectele (*ALLOBJ).			

Comenzi sistem

Această tabelă listează autorizările specifice necesare pentru comenzile sistem.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Subiectul Comenzile livrate cu autorizare publică *EXCLUDE arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul cu securitatea poate acorda autorizare *USE altora.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
PWRDWNSYS[1]	Catalog de imagini (dacă este specificat)	*USE	
RTVSYSINF (Q)[2]	Bibliotecă	*READ, *ADD, *EXECUTE	
Aceste comenzi nu necesită nici o autorizare obiect:			
CHGSHRPOOL DSPSYSSTS ENDSYS[1] PRTSYSINF (Q)	RCLACTGRP[1] RCLRSC RETURN RTVGRPA	SIGNOFF UPDSYSINF (Q)[3] WRKSHRPOOL	WRKSYSSTS
[1] Trebuie să aveţi autorizare specială de control job (*JOBCTL) pentru a utiliza această comandă.			
[2] Trebue să aveţi autorizare specială *SAVSYS pentru a folosi această comandă.			
[3] Trebuie să aveţi autorizări speciale *SECADM, *ALLOBJ, *AUDIT, *JOBCTL şi *SAVSYS pentru a folosi această comandă.			

Comenzi listă răspunsuri sistem

Această tabelă listează autorizările specifice necesare pentru comenzile listă de răspunsuri sistem.

Aceste comenzi nu necesită autorizări obiect:			
ADDRPYLE (Q)	CHGRPYLE (Q)	RMVRPYLE (Q)	WRKRPYLE

Comenzi valoare de sistem

Această tabelă listează autorizările specifice necesare pentru comenzile valoare de sistem.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Aceste comenzi nu necesită vreo autorizare 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.

Comenzi mediu System/36

Această tabelă listează autorizările specifice necesare pentru comenzile de mediu System/36.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

		Autorizare necesară	
Comandă	**Obiect referit**	**Pentru obiect**	**Pentru bibliotecă**
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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
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)	Fişier-sursă	*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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
RSTS36FLR [1,2,3] (Q)	Folder S/36	*USE	*EXECUTE
	În-fişier	*CHANGE	*EXECUTE
	Fişier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
RSTS36LIBM (Q)	Fişier-sursă	*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	Fişier-sursă	*USE	*EXECUTE
	În-fişier, atunci când este fişier fizic	*ALL	Vedeţi regulile generale.
	Fişier dispozitiv sau descriere dispozitiv	*USE	*EXECUTE
SAVS36LIBM	Fişier-sursă	*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 autorizarea *ALL pentru document dacă îl înlocuiţi. Aveţi nevoie de autorizări operaţionale şi pentru toate datele pentru folder dacă restauraţi informaţii noi în aceste foldere, sau aveţi nevoie de autorizarea specială *ALLOBJ.

2 Dacă este folosit pentru dicţionar, este necesară doar autorizarea pentru comandă.

3 Trebuie să fiţi înscris în directorul de distribuire sistem dacă folderul sursă este un folder document.

Comenzi tabelă

Această tabelă listează autorizările specifice necesare pentru comenzile tabelă.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CRTTBL	Tabelă		*READ, *ADD, *EXECUTE
	Fişier sursă	*USE	*EXECUTE
DLTTBL	Tabelă	*OBJEXIST	*EXECUTE
WRKTBL [1]	Tabelă	Orice autorizare	*USE

1 Pentru a folosi o operaţie individuală, trebuie să aveţi autorizarea necesară de operaţie.

Comenzi TCP/IP

Această tabelă listează autorizările specifice necesare pentru comenzile TCP/IP.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

		Autorizare necesară	
Comandă	**Obiect referit**	**Pentru obiect**	**Pentru bibliotecă**
ADDTCPSVR[1]	Program de apelat	*EXECUTE	*EXECUTE
CHGTCPSVR[1]	Program de apelat	*EXECUTE	*EXECUTE
CPYTCPHT [6]	Obiecte fişier		
CVTTCPCL (Q)	Obiecte fişier	*USE	*EXECUTE
ENDTCPPTP	Descriere de linie[4]	*USE	*EXECUTE
	Descriere controler[4]	*USE	*EXECUTE
	Descriere 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
STRTCPFTP	Obiecte tabel	*USE	*EXECUTE
	Obiecte fişier	*USE	*EXECUTE
STRTCPPTP	Descriere de linie[4]	*USE	*EXECUTE
	Descriere controler[4]	*USE	*EXECUTE
	Descriere dispozitiv[4]	*USE	*EXECUTE
	Obiecte fişier	*USE	*EXECUTE
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 autorizare obiect:			

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ADDCOMSNMP [1]	CFGRTG	CHGVTMAP	RMVTCPRSI [1]
ADDNETTBLE [1]	CFGTCPSMTP	DSPVTMAP	RMVTCPRTE [1]
ADDOSPFARA[1]	CFGTCPSNMP	ENDTCP (Q)	RMVTCPSVR [1]
ADDOSPFLNK[1]	CFGTCPTELN	ENDTCPCNN	RNMTCPHTE [1]
ADDOSPFIFC[1]	CHGCOMSNMP [1]	ENDTCPIFC (Q)	SETVTMAP
ADDOSPFRNG[1]	CHGFTPA [1]	MGRTCPHT [1]	STRTCP (Q)
ADDPCLTBLE [1]	CHGLPDA [1]	NETSTAT	STRTCPIFC (Q)
ADDRIPACP[1]	CHGOSPFA[1]	PING	VFYTCPCNN
ADDRIPFLT[1]	CHGOSPFARA[1]	RMVCOMSNMP [1]	WRKNAMSMTP [3]
ADDRIPIFC[1]	CHGOSPFIFC[1]	RMVNETTBLE [1]	WRKNETTBLE[1]
ADDRIPIGN[1]	CHGOSPFLNK[1]	RMVOSPFARA[1]	WRKPCLTBLE[1]
ADDSRVTBLE [1]	CHGOSPFRNG[1]	RMVOSPFIFC[1]	WRKSRVTBLE[1]
ADDTCPHTE [1]	CHGRIPA[1]	RMVOSPFLNK[1]	WRKTCPSTS
ADDTCPIFC [1]	CHGRIPFLT[1]	RMVOSPFRNG[1]	
ADDTCPPORT [1]	CHGRIPIFC[1]	RMVPCLTBLE [1]	
ADDTCPRSI [1]	CHGSMTPA [1]	RMVRIPACP[1]	
ADDTCPRTE [1]	CHGSNMPA [1]	RMVRIPFLT[1]	
CFGTCP	CHGTCPA [1]	RMVRIPIFC[1]	
CFGTCPAPP	CHGTCPHTE[1]	RMVRIPIGN[1]	
CFGTCPFTP [1]	CHGTCPIFC[1]	RMVSRVTBLE [1]	
CFGTCPLPD [1]	CHGTCPRTE [1]	RMVTCPHTE[1]	
	CHGTELNA [1]	RMVTCPIFC[1]	
		RMVTCPPORT [1]	

1 Trebuie să aveţi autorizarea specială *IOSYSCFG pentru a folosi această comandă.

2 Comanda SNDTCPSPLF şi comanda LPR folosesc aceleaşi combinaţii de autorizări obiect referit ca şi comanda SNDNETSPLF.

3 Trebuie să aveţi autorizarea specială *SECADM pentru a modifica tabela alias de sistem sau tabela alias a unui profil de utililizator.

4 Dacă aveţi autorizarea specială *JOBCTL, nu aveţi nevoie de autorizarea specificată pentru obiect.

5 Dacă aveţi autorizarea specială *JOBCTL, nu aveţi nevoie de autorizarea specificată pentru obiectul de pe sistemul la distanţă.

6 Pentru autorizările necesare, consultaţi descrierea Ecranului (DSP) sau alte operaţii folosind secţiunea fişier de ieşire (OUTPUT(*OUTFILE)) din subiectul Reguli generale pentru autorizările de obiect asupra comenzilor.

Comenzi descriere fus orar

Această tabelă listează autorizările specifice necesare pentru comenzile descriere fus orar.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă

[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 autorizarea *USE pentru fişierul de mesaje şi autorizarea *EXECUTE pentru biblioteca fişierului de mesaje pentru a vedea numele complete şi abreviate.

Modernizare comenzi date informaţii comandă

Această tabelă listează autorizările specifice necesare pentru comenzile de date informaţii comandă.

Aceste comenzi sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
WRKORDINF	Fişier QGPL/QMAHFILE	*CHANGE, *OBJALTER	*EXECUTE

Comenzi index utilizator, coadă utilizatori şi spaţiu utilizator

Această tabelă listează autorizările specifice necesare pentru comenzile index utilizator, coadă utilizatori şi spaţiu utilizator.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
DLTUSRIDX	Index utilizator	*OBJEXIST	*EXECUTE
DLTUSRQ	Coadă utilizator	*OBJEXIST	*EXECUTE
DLTUSRSPC	Spaţiu utilizator	*OBJEXIST	*EXECUTE

Comenzi sistem de fişiere definit de utilizator

Această tabelă listează autorizările specifice necesare pentru comenzile sistem de fişier definit de utilizator.

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare 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* sau /dev/IASPname	*DIR	″root″ (/)	*RWX
DLTUDFS [1,2,4,5,8,9,10] (Q)	/dev/QASP*xx* sau /dev/IASPname	*DIR	″root″ (/)	*RWX
	şi orice obiect sistem de fişiere integrat din UDFS		″root″ (/)	*OBJEXIST
	Orice obiect director care nu este gol	*DIR	″root″ (/)	*WX
DSPUDFS	unele_dirxx	*DIR	″root″ (/)	*RX

Comandă	Obiect referit	Tip obiect	Sistem de fişiere	Autorizare necesară pentru obiect
MOUNT [1,2,3]	dir_peste_care_ se_montează	*DIR	″root″ (/)	*W
	Prefix cale	Vedeţi regulile generale.		
RMVMFS [1]				
UNMOUNT [1]				

[1] Pentru a folosi această comandă, trebuie să aveţi autorizarea specială *IOSYSCFG.

[2] Există două convenţii de numire directoare, care depind de locaţia sistemului de fişiere definit de utilizator (UDFS). Folosiţi una din convenţiile următoare:

- - /dev/QASPxx unde *xx* este 01 pentru ASP-ul sistemului sau 02-32 pentru ASP-urile de bază utilizator.
- - /dev/IASPname unde *IASPname* este numele ASP-ului independent.

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] Un UDFS poate conţine un întreg subarbore de obiecte, astfel atunci 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 autorizarea *OBJEXIST pentru fiecare obiect din UDFS altfel nici un obiect nu este şters.

[6] Trebuie să aveţi autorizările speciale *ALLOBJ (toate obiectele) şi *SECADM (administrator securitate) pentru a specifica o valoare pentru parametrul CRTOBJSCAN (opţiunea Scanare pentru obiecte) alta decât *PARENT.

[7] autorizarea specială (*AUDIT) este necesară atunci când specificaţi o valoare alta decât *SYSVAL pentru valoare Auditare pentru parametrul (CRTOBJAUD) al obiectelor.

[8] Trebuie să aveţi autorizări de scriere (*W) şi execuţie (*X) asupra tuturor obiectelor director care nu sunt goale din UDFS.

[9] Dacă un obiect director care nu este gol din UDFS are atributul ″restricţie de redenumire şi dezlegare″ setat Yes (acest atribut este echivalent cu bitul de mod S_ISVTX), atunci una sau mai multe din următoarele condiţii trebuie să fie adevărate:

- Trebuie să fiţi proprietarul tuturor obiectelor conţinute în director.
- Trebuie să fiţi proprietarul directorului.
- Trebuie să aveţi autorizare specială *ALLOBJ.

[10] UDFS nu poate fi şters dacă conţine un obiect cu atributul *numai citire* setat la *yes* sau dacă conţine un obiect care este înregistrat la ieşire.

Comenzi profil de utilizator

Această tabelă listează autorizările specifice necesare pentru comenzile profil de utilizator.

Comenzile identificate cu (Q) sunt livrate cu autorizarea publică *EXCLUDE. Anexa C, “Comenzi livrate cu autorizare publică *EXCLUDE”, la pagina 325 arată care profiluri de utilizator livrate de IBM sunt autorizate asupra comenzii. Responsabilul de securitate poate acorda autorizarea *USE celorlalţi.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
ANZDFTPWD [3, 14, 15](Q)			
ANZPRFACT [3, 14, 15](Q)			
CHGACTPRFL [14](Q)			

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
CHGACTSCDE [3, 14, 15](Q)			
CHGDSTPWD [1]			
CHGEXPSCDE [3, 14, 15](Q)			
CHGPRF	Profil de 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 ieşire [2]	*USE	*EXECUTE
	Program de tratare tastă Attn[2]	*USE	*EXECUTE
	Bibliotecă curentă [2]	*USE	*EXECUTE
CHGPWD			
CHGUSRAUD [11](Q)			
CHGUSRPRF [3]	Profil de 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 ieşire [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	Profil de utilizator	*CHANGE	
CHKPWD			
CRTUSRPRF [3, 12, 17]	Program iniţial	*USE	*EXECUTE
	Meniu iniţial	*USE	*EXECUTE
	Descriere job	*USE	*EXECUTE
	Coada de mesaje	*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]	Profil de utilizator	*OBJEXIST, *USE	*EXECUTE
	Coadă de mesaje[5]	*OBJEXIST, *USE, *DLT	*EXECUTE

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
DMPUSRPRF [22](Q)	Profil de utilizator		
DSPACTPRFL [14](Q)			
DSPACTSCD [14](Q)			
DSPAUTUSR [6]	Profil de utilizator	*READ	
DSPEXPSCD [14](Q)			
DSPPGMADP	Profil de utilizator	*OBJMGT	
	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
DSPSSTUSR [23]			
DSPUSRPRF[19]	Profil de utilizator	*READ	*EXECUTE
	Fişier ieşire	Vedeţi regulile generale.	Vedeţi regulile generale.
DSPUSRPRTI	Profil de utilizator	*USE	
GRTUSRAUT [7]	Profil de utilizator referenţiat	*READ	
	Obiecte pentru care acordaţi autorizare	*OBJMGT	*EXECUTE
PRTPRFINT [14](Q)			
PRTUSRPRF [18]			
RSTAUT (Q) [8]			
RSTUSRPRF (Q) [8,10, 16]			
RTVUSRPRF[20]	Profil de utilizator	*READ	
RTVUSRPRTI	Profil de 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]	Profil de utilizator	Orice autorizare	

1 Această comandă poate rula doar dacă sunteţi înregistrat ca QSECOFR.

2 Aveţi nevoie de autorizare obiect doar pentru câmpurile pe care le modificaţi în profilul de utilizator.

3 autorizarea specială *SECADM este necesară.

4 Autorizarea *OBJMGT pentru profilul de utilizator nu poate veni de la autorizarea adoptată.

5 Coada de mesaje asociată cu profilul de utilizator este ştearsă dacă este deţinută de acel profil de utilizator. Pentru a şterge coada de mesaje, utilizatorul care rulează DLTUSRPRF trebuie să aibă autorizările specificate.

6 Afişare include doar profilurile de utilizator pe care utilizatorul care rulează comanda are autorizarea specificată.

7 Vedeţi autorizările necesare pentru comanda GRTOBJAUT.

8 Autorizarea specială *SAVSYS este necesară.

9 Dacă selectaţi opţiunea de a şterge obiectele deţinute de profilul de utilizator, trebuie să aveţi autorizarea necesară operaţiei de ştergere. Dacă selectaţi opţiunea de transfer proprietate către alt profil de utilizator, trebuie să aveţi autorizarea necesară pentru obiecte şi pentru profilul de utilizator destinaţie. Vedeţi informaţiile pentru comanda CHGOBJOWN.

10 Trebuie să aveţi autorizarea specială *ALLOBJ pentru a specifica altă valoare decât *NONE pentru parametrul ALWOBJDIF.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
[11] Trebuie să aveţi autorizarea specială *AUDIT.			
[12] Utilizatorului al cărui profil este creat îi sunt date aceste autorizări: *OBJMGT, *OBJOPR, *READ, *ADD, *DLT, *UPD, *EXECUTE.			
[13] Pentru a folosi o operaţie individuală, trebuie să aveţi autorizarea necesară de operaţie.			
[14] Trebuie să aveţi autorizarea specială *ALLOBJ pentru a folosi această comandă.			
[15] Trebuie să aveţi autorizarea specială *JOBCTL pentru a folosi această comandă.			
[16] Trebuie să aveţi autorizările speciale *ALLOBJ şi *SECADM pentru a specifica SECDTA(*PWDGRP), USRPRF(*ALL) sau OMITUSRPRF.			
[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 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.			
[18] Trebuie să aveţi autorizarea specială *ALLOBJ sau *AUDIT pentru a folosi această comandă.			
[19] Trebuie să aveţi ori autorizarea specială *ALLOBJ sau *AUDIT pentru a fi afişată valoarea curentă de auditare a obiectului şi a acţiunii afişate. 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. Altfel, este returnată valoarea *NOTAVL pentru a indica faptul că nu sunt disponibile valorile pentru extragere.			
[21] Pentru a folosi această comandă, trebuie să aveţi autorizare specială de service (*SERVICE) sau să fiţi autorizat asupra funcţiei Service Dump a sistemului de operare prin suportul Navigator System i Application Administration. Comanda Modificare folosire funcţie (CHGFCNUSG), cu un ID de funcţie de QIBM_SERVICE_DISK_DUMP, poate fi de asemenea folosită pentru a modifica lista de utilizatori cărora le este permis să realizez operaţii de dump.			
[22] Pentru a folosi această comandă, trebuie să aveţi autorizare specială *SERVICE sau să aveţi autorizare asupra liste de folosire funcţie QIBM_SERVICE_DUMP.			
[23] Trebuie să aveţi autorizare specială administrator de securitate (*SECADM) sau auditare (*AUDIT) pentru a folosi această comandă.			

Comenzi listă de validare

Această tabelă listează autorizările specifice necesare pentru comenzile listă de validare.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	**Pentru bibliotecă**
CRTVLDL	Listă de validări		*ADD, *READ
DLTVLDL	Listă de validări	*OBJEXIST	*EXECUTE

Comenzi personalizare staţie de lucru

Această tabelă listează autorizările specifice necesare pentru comenzile de personalizare staţie de lucru.

Comandă	Obiect referit	Autorizare necesară	
		Pentru obiect	Pentru bibliotecă
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

Comenzi scriitor

Această tabelă listează autorizările specifice necesare pentru comenzile scriitor

Comandă	Obiect referit	Parametri coadă ieşire		Autorizare specială	Autorizare necesară	
		AUTCHK	OPRCTL		Pentru obiect	Pentru bibliotecă
CHGWTR [2, 4]	Coadă de ieşire curentă[1]	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Proprietar [3]	
			*YES	*JOBCTL		
	Crearea unei noi cozi de ieşire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
ENDWTR [1]	Coadă de ieşire	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Proprietar [3]	
			*YES	*JOBCTL		
HLDWTR [1]	Coadă de ieşire	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Proprietar [3]	
			*YES	*JOBCTL		
RLSWTR [1]	Coadă de ieşire	*DTAAUT			*READ, *ADD, *DLT	
		*OWNER			Proprietar [3]	
			*YES	*JOBCTL		

Comandă	Obiect referit	Parametri coadă ieşire		Autorizare specială	Autorizare necesară	
		AUTCHK	OPRCTL		Pentru obiect	Pentru bibliotecă
STRDKTWTR [1]	Coadă de ieşire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar [3]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Coada de mesaje				*OBJOPR, *ADD	*EXECUTE
	Descriere dispozitiv				*OBJOPR, *READ	
STRPRTWTR [1]	Coadă de ieşire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar [3]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Coada de mesaje				*OBJOPR, *ADD	*EXECUTE
	obiect de personalizare staţie de lucru				*USE	*EXECUTE
	Program cu driver utilizator				*OBJOPR *EXECUTE	*EXECUTE
	Program transformare date utilizator				*OBJOPR *EXECUTE	*EXECUTE
	Program separare utilizator				*OBJOPR *EXECUTE	*EXECUTE
	Descriere dispozitiv				*OBJOPR, *READ	
STRRMTWTR [1]	Coadă de ieşire	*DTAAUT			*READ, *ADD, *DLT	*EXECUTE
		*OWNER			Proprietar [3]	*EXECUTE
			*YES	*JOBCTL		*EXECUTE
	Coada de mesaje				*OBJOPR, *ADD	*EXECUTE
	obiect de personalizare staţie de lucru				*USE	*EXECUTE
	Program cu driver utilizator				*OBJOPR *EXECUTE	*EXECUTE
	Program transformare date utilizator				*OBJOPR *EXECUTE	*EXECUTE
WRKWTR						

Comandă	Obiect referit	Parametri coadă ieşire		Autorizare specială	Autorizare necesară	
		AUTCHK	OPRCTL		Pentru obiect	Pentru bibliotecă

[1] Dacă aveţi autorizarea specială *SPLCTL, nu aveţi nevoie de nici o autorizare pentru coada de ieşire.

[2] Pentru modificarea cozii de ieşire pentru scriitor, aveţi nevoie de autorizările specificate pentru noua coadă de ieşire.

[3] Trebuie să fiţi proprietarul cozii de ieşire.

[4] Trebuie să aveţi autorizarea *EXECUTE pentru biblioteca noii cozi de ieşire chiar dacă utilizatorul are autorizarea specială *SPLCTL.

Anexa E. Operaţii obiecte şi auditare

Această colecţie de subiecte listează operaţiile care pot fi realizate asupra obiectelor din sistem şi dacă acele 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, inclusiv o valoare din profilul de utilizator al utilizatorului care execută acţiunea şi o valoare definită pentru obiect. “Planificarea auditării accesului la obiecte” la pagina 286 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 comune tuturor tipurilor de obiecte

Această listă descrie operaţiile pe care le puteţi realiza pe toate tipurile de obiecte şi dacă acele operaţii sunt auditate.

- Operaţie citire

CRTDUPOBJ
Creare obiect duplicat (dacă este specificat *ALL pentru *"from-object"*).

DMPOBJ
Abandon obiect

DMPSYSOBJ
Abandon obiect sistem

QSRSAVO
Salvare API obiect

QsrSave
Salvare Obiect API-ul director

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).

- Operaţia de modificare

APYJRNCHG
Aplicare modificări jurnalizate

CHGJRNOBJ
Modificare obiect jurnalizat

CHGOBJD
Modificare descriere obiect

CHGOBJOWN
Modificare proprietar obiect

CRTxxxxxx
Creare obiect

Observaţii:

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

Observaţii:

1. Dacă este specificat *ALL sau *CHANGE pentru biblioteca în care se află 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
Grant Object Authority

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

QSRRSTO
Restaurare API obiect

QsrRestore
Restaurare obiect în API-ul director

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 autorizare 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 [1]
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
Display Object Authority - Afişare autorizare obiect

EDTOBJAUT
Edit Object Authority

1. Apare un prompt care afişează valorile curente când este cerută avertizarea pentru o comandă. De exemplu, dacă tastaţi CHGURSPRF USERA şi apăsaţi F4 (prompt), ecranul Modificare profil de utilizator arată valorile curente pentru profilul de utilizator USERA.

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

RMVDFRID
Înlăturare ID amânare

RSTDFROBJ
Restaurare obiect amânat

RTVOBJD
Extragere descriere obiect

SAVSTG
Salvare spaţiu de stocare (auditare doar pentru comanda SAVSTG)

WRKOBJLCK
Gestionare blocare obiect

WRKOBJOWN
Lucru cu obiecte după proprietar

WRKxxx
Gestionare comenzi de obiecte

Operaţii pentru Timpi recuperare cale de acces

Această listă descrie operaţiile pe care le puteţi realiza pe obiectul Timpi recupere cale de acces şi dacă acele operaţii sunt auditate.

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 de 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

Operaţii pentru Tabelă alerte (*ALRTBL)

Această listă descrie operaţiile pe care le puteţi realiza pe Tabelă alerte (*ALRTBL) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Fără

- Operaţia 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

Operaţii pentru Listă de autorizare (*AUTL)

Această listă descrie operaţiile pe care le puteţi realiza pe Listă de autorizare (*AUTL) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Fără
- Operaţia de modificare

  ADDAUTLE
  Adăugare intrare listă de autorizare

  CHGAUTLE
  Modificare intrare listă de autorizare

  EDTAUTL
  Editare listă de autorizare

  RMVAUTLE
  Înlăturare intrare listă de autorizare
- Operaţiile care nu sunt auditate

  DSPAUTL
  Afişare listă de autorizare

  DSPAUTLOBJ
  Afişare obiecte listă de autorizare

  DSPAUTLDLO
  Afişare DLO listă de autorizare

  RTVAUTLE
  Extragere intrare de listă de autorizare

  QSYLATLO
  Obiecte listă securizate de API-ul *AUTL

  WRKAUTL
  Gestionare listă de autorizare

Operaţii pentru Păstrător de autorizare (*AUTHLR)

Această listă descrie operaţiile pe care le puteţi realiza pe Păstrător de autorizare (*AUTHLR) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Fără

- Operaţia de modificare

  Asociat
  Când este folosit pentru a securiza un obiect.

- Operaţiile care nu sunt auditate

  DSPAUTHLR
  Afişare păstrător de autorizare

Operaţii pentru Director de legare (*BNDDIR)

Această listă descrie operaţiile pe care le puteţi realiza pe Director de legare (*BNDDIR) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  CRTPGM
  Creare program

  CRTSRVPGM
  Creare program service

  RTVBNDSRC
  Extragere sursă legătură

  UPDPGM
  Actualizare program

  UPDSRVPGM
  Actualizare program service

- Operaţia 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 configuraţii (*CFGL)

Această listă descrie operaţiile pe care le puteţi realiza pe Listă de configuraţii (*CFGL) şi dacă acele operaţii sunt auditate.

- Operaţie citire

CPYCFGL
Copiere listă de configuraţie. O intrare este scrisă pentru *din-lista-configuraţie*

- Operaţia 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)

Această listă descrie operaţiile pe care le puteţi realiza pe Fişiere speciale (*CHRSF) şi dacă acele operaţii sunt auditate.

Vedeţi Operaţii pentru fişierul flux (*STMF) pentru auditare *CHRSF.

Operaţii pentru Format diagramă (*CHTFMT)

Această listă descrie operaţiile pe care le puteţi realiza pe Format diagramă (*CHTFMT) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  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
- Operaţia de modificare

  Fără
- Operaţiile care nu sunt auditate

  Fără

Operaţii pentru Descriere locale C (*CLD)

Această listă descrie operaţiile pe care le puteţi realiza pe Descriere locale C (*CLD) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  RTVCLDSRC
  Extragere sursă C Locale

Setlocale
Folosiţi obiectul C locale în timpul rulării programului C folosind funcţia Setare locale.

- Operaţia de modificare

  Fără

- Operaţiile care nu sunt auditate

  Fără

Operaţii pentru Modificare descriere cerere (*CRQD)

Această listă descrie operaţiile pe care le puteţi realiza pe Modificare descriere cerere (*CRQD) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  QFVLSTA
  API-ul Listare activităţi de modificare descriere cerere

  QFVRTVCD
  API-ul Extragere modificare descriere cerere

  SBMCRQ
  Lansare modificare cerere

- Operaţia 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

Operaţii pentru Clasă (*CLS)

Această listă descrie operaţiile pe care le puteţi realiza pe Clasă (*CLS) şi dacă acele operaţii sunt auditate.

- Operaţie citire

Fără

- Operaţia de modificare

CHGCLS
Modificare clasă

- Operaţiile care nu sunt auditate

Pornire job
Când este folosit de gestionarea de lucru pentru a porni un job

DSPCLS
Afişare clasă

WRKCLS
Gestionare clasă

Operaţii pentru Comandă (*CMD)

Această listă descrie operaţiile pe care le puteţi realiza pe Comandă (*CMD) şi dacă acele operaţii sunt auditate.

- Operaţie citire

Rulare Când comanda rulează

- Operaţia 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. Utilizarea acestor comenzi 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.		

Operaţii pentru Listă conexiuni (*CNNL)

Această listă descrie operaţiile pe care le puteţi realiza pe Listă conexiuni (*CNNL) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Fără

- Operaţia 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

Operaţii pentru Descriere clasă-de-serviciu (*COSD)

Această listă descrie operaţiile pe care le puteţi realiza pe Descriere clasă-de-serviciu (*COSD) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Fără

- Operaţia 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

Operaţii pentru Informaţii parte comunicaţii (*CSI)

Această listă descrie operaţiile pe care le puteţi realiza pe Informaţii parte comunicaţii (*CSI) şi dacă acele operaţii sunt auditate.

- Operaţie citire

DSPCSI
Afişare informaţii parte comunicaţii

Iniţializare
Iniţializare conversaţie

- Operaţia de modificare

CHGCSI
Modificare informaţii parte comunicaţii

- Operaţiile care nu sunt auditate

WRKCSI
Gestionare informaţii parte comunicaţii

Operaţii pentru Hartă produs sistem (*CSPMAP)

Această listă descrie operaţiile pe care le puteţi realiza pe Hartă produs sistem (*CSPMAP) şi dacă acele operaţii sunt auditate.

- Operaţie citire

Reference - Referinţă
Când este referit într-o aplicaţie CSP

- Operaţia de modificare

Fără

- Operaţiile care nu sunt auditate

DSPCSPOBJ
Afişare obiect CSP

WRKOBJCSP
Gestionare obiecte pentru CSP

Operaţii pentru Tabelă produse sistem (*CSPTBL)

Această listă descrie operaţiile pe care le puteţi realiza pe Tabelă produse sistem (*CSPTBL) şi dacă acele operaţii sunt auditate.

- Operaţie citire

Reference - Referinţă
Când este referit într-o aplicaţie CSP

- Operaţia de modificare

  Fără

- Operaţiile care nu sunt auditate

  DSPCSPOBJ
  Afişare obiect CSP

  WRKOBJCSP
  Gestionare obiecte pentru CSP

Operaţii pentru Descriere controler (*CTLD)

Această listă descrie operaţiile pe care le puteţi realiza pe Descriere controler (*CTLD) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  SAVCFG
  Salvare configuraţie

  VFYCMN
  Test legătură

- Operaţia 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

Operaţii pentru descriere dispozitiv (*DEVD)

Această listă descrie operaţiile pe care le puteţi realiza pe o descriere de dispozitiv (*DEVD) şi dacă acele operaţii sunt auditate.

- Operaţie citire

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

- Operaţia 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

Operaţii pentru Director (*DIR)

Această listă descrie operaţiile pe care le puteţi realiza pe Director (*DIR) şi dacă acele operaţii sunt auditate.

- Operaţii citire/căutare

  access, accessx, QlgAccess, QlgAccessx
  Determinaţi accesibilitate fişier

  CHGATR
  Modificare atribut

  CPY Copiere obiect

  DSPCURDIR
  Afişare director curent

  DSPLNK
  Afişare legături obiect

  faccessx
  Determinare accesabilitate fişier pentru o clasă de utilizatori după descriptor

  getcwd, qlgGetcwd
  API-ul de obţinere nume cale pentru directorul curent

  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 Salvare obiect

  WRKLNK
  Gestionare legături

- Operaţia de modificare

  CHGATR
  Modificare atribute

  CHGAUD
  Modificare valoare de auditare

  CHGAUT
  Modificare autorizare

  CHGOWN
  Modificare proprietar

CHGPGP
Modificare grup primar

chmod, QlgChmod
API-ul Modificare autorizări fişier

chown, QlgChown
API-ul Modificare grup şi proprietar

CPY Copiere obiect

CRTDIR
Creare director

fchmod
API-ul de modificare autorizări fişier după descriptor

fchown
API-ul de modificare grup şi proprietar după descriptor

mkdir, QlgMkdir
API-ul de creare director

MOV Mutare obiect

Qp0lRenameKeep, QlgRenameKeep
API-uri de redenumire fişier sau director, păstrare nou

Qp0lRenameUnlink, QlgRenameUnlink
API-uri 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 obiect

RST Restaurare obiect

utime, QlgUtime
API-ul de Setare acces fişier şi timpi de modificare

WRKAUT
Lucru cu autorizări

WRKLNK
Lucru cu legături obiect

- 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 duplicare descriptor fişier deschis

dup2 API-ul de duplicare descriptor fişier deschis 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 control fişier

fpathconf
API-uri de obţinere variabile nume cale configurabile

fstat, fstat64
API-uri de obţinere informaţii fişier după descriptor

givedescriptor
API-ul de acordare acces fişier

ioctl API-ul executare cerere control I/O

lseek, lseek64
API-uri de setare offset citire/scriere

lstat, lstat64, QlgLstat, QlgLstat64
API-uri de obţinere fişier sau informaţii de legătură

pathconf, QlgPathconf
API-ul de obţinere variabile 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 a descriptorilor fişier multipli

stat, QlgStat
API-ul de obţinere informaţii fişier

takedescriptor
API-ul de luare acces fişier

Operaţii pentru Server de director

Această listă descrie operaţiile pe care le puteţi realiza pe Server de director şi dacă acele operaţii sunt auditate.

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

  Add - Adăugare
  Adăugarea unor noi intrări director

  Modificare
  Modificarea detaliilor intrare director

  Delete - 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

Alimentare
Furnizarea datelor de intrare director folosind umbrirea de director

- Operaţiile care nu sunt auditate

Comenzile CL
Comenzile CL care lucrează pe 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

Listare 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 Obiect bibliotecă de documente (*DOC sau *FLR)

Această listă descrie operaţiile pe care le puteţi realiza pe obiecte bibliotecă de documente (*DOC sau *FLR) şi dacă acele operaţii sunt auditate.

- Operaţie citire

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 obţinere 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.

- Operaţia 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 [2]
Copiere document

Notă: O intrare de modificare este scrisă dacă documentul destinaţie există deja.

CRTFLR
Creare folder

CVTTOFLR [2]
Convertire la folder

DLTDLO [2]
Ştergere DLO

DLTSHF
Ştergere raft de cărţi

DTLDOCL [2]
Ştergere listă de documente

DLTDST [2]
Ştergere distribuţie

EDTDLOAUT
Editare autorizare DLO

EDTDOC
Editare document

FILDOC [2]
Document fişier

GRTACCAUT
Acordare autorizare cod acces

GRTUSRPMN
Acordare permisiune utilizator

MOVDOC [2]
Mutare document

2. O intrare de modificare este scrisă pentru document şi pentru folder dacă destinaţia operaţiei este într-un folder.

MRGDOC [2]
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 [2]
Cerere bibliotecă documente

Notă: O intrare de modificare este scrisă dacă un document existent rezultat dintr-o căutare este înlocuit.

RCVDST [2]
Primire distribuţie

RGZDLO
Reorganizare DLO

RMVACC
Înlăturare cod acces pentru orice DLO la care este ataşat codul de acces

RMVDLOAUT
Înlăturare autorizare DLO

RNMDLO [2]
Redenumire DLO

RPLDOC
Înlocuire document

RSTDLO [2]
Restaurare DLO

RSTSHF
Restaurare raft de cărţi

RTVDOC
Extragere document (verificare)

RVKACCAUT
Revocare autorizare cod acces

RVKUSRPMN
Revocare permisiune utilizator

SAVDLO [2]
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

Operaţii pentru Zonă de date (*DTAARA)

Această listă descrie operaţiile pe care le puteţi realiza pe Zonă de date (*DTAARA) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  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
- Operaţia 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

Operaţii pentru Utilitar interactiv definiţie date (*DTADCT)

Această listă descrie operaţiile pe care le puteţi realiza pe Utilitar interactiv definiţie date (*DTADCT) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Fără

- Operaţia de modificare

  Create - Creare
  Dicţionar de date şi definiţii de date

  Modificare
  Dicţionar de date şi definiţii de date

  Copiere
  Definiţii de date (înregistrate cu creare)

  Delete - 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

Operaţii pentru Coadă de date (*DTAQ)

Această listă descrie operaţiile pe care le puteţi realiza pe Coadă de date (*DTAQ) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  QMHRDQM
  API-ul de extragere mesaje din coada de date

- Operaţia 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 Editare descriere (*EDTD)

Această listă descrie operaţiile pe care le puteţi realiza pe Editare descriere (*EDTD) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  DSPEDTD
  Afişare descriere editare

  QECCVTEC
  API-ul de editare expansiune cod (prin rutina QECEDITU)

- Operaţia de modificare

  Fără

- 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)

Această listă descrie operaţiile pe care le puteţi realiza pe Înregistrare ieşire (*EXITRG) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  QUSRTVEI
  API-ul Extragere informaţii ieşire

  QusRetrieveExitInformation
  API-ul Extragere informaţii ieşire

- Operaţia 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

  Fără

Operaţii pentru Tabelă de control furmulare (*FCT)

Această listă descrie operaţiile pe care le puteţi realiza pe Tabelă control furmulare (*FCT) şi dacă acele operaţii sunt auditate.

- Nici o operaţie de citire sau modificare nu este auditată pentru tipul de obiect *FCT.

Operaţii pentru Fişier (*FILE)

Această listă descrie operaţiile pe care le puteţi realiza pe Fişier (*FILE) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  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

- Operaţia 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 constrângere 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

CHGPFTRG
Modificare declanşator fişier fizic

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 Fişiere FIFO (*FIFO)

Această listă descrie operaţiile pe care le puteţi realiza pe obiecte FIFO (*FIFO) şi dacă acele operaţii sunt auditate.

Vedeţi Operaţii pentru fişier flux (*STMF) pentru auditare *FIFO.

Operaţii pentru Folder (*FLR)

Această listă descrie operaţiile pe care le puteţi realiza pe obiecte folder (*FLR) şi dacă acele operaţii sunt auditate.

Vedeţi operaţiile pentru “Operaţii pentru Obiect bibliotecă de documente (*DOC sau *FLR)” la pagina 513

Operaţii pentru Resursă font (*FNTRSC)

Această listă descrie operaţiile pe care le puteţi realiza pe Resursă font (*FNTRSC) şi dacă acele operaţii sunt auditate.

- Operaţie citire

Tipărire
Tipărirea unui fişier spool care referă la o resursă font

- Operaţia de modificare

  Fără

- Operaţiile care nu sunt auditate

  WRKFNTRSC
  Gestionare resurse font

  Tipărire
  Referirea la resursa font la crearea unui fişier spool

Operaţii pentru Definiţie formular (*FORMDF)

Această listă descrie operaţiile pe care le puteţi realiza pe Definiţie formular (*FORMDF) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Tipărire
  Tipărirea unui fişier spool care referă la o definiţie de formular

- Operaţia de modificare

  Fără

- Operaţiile care nu sunt auditate

  WRKFORMDF
  Gestionare definiţii de formular

  Tipărire
  Referirea la definiţia de formular la crearea unui fişier spool

Operaţii pentru Obiect filtru (*FTR)

Această listă descrie operaţiile pe care le puteţi realiza pe Obiect filtru (*FTR) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Fără

- Operaţia 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

Operaţii pentru Set simboluri grafice (*GSS)

Această listă descrie operaţiile pe care le puteţi realiza pe Set simboluri grafice (*GSS) şi dacă acele operaţii sunt auditate.

- Operaţie citire

Încărcat
Când este încărcat

Font Când este folosit ca font dintr-o imprimantă descrisă extern

- Operaţia de modificare

Nici una.

- Operaţiile care nu sunt auditate

WRKGSS
Gestionare setul de simboluri grafice

Operaţii pentru Dicţionar set de caractere pe doi octeţi (*IGCDCT)

Această listă descrie operaţiile pe care le puteţi realiza pe Dicţionar set de caractere pe doi octeţi (*IGCDCT) şi dacă acele operaţii sunt auditate.

- Operaţie citire

DSPIGCDCT
Afişare dicţionar IGC

- Operaţia de modificare

EDTIGCDCT
Editare dicţionar IGC

Operaţii pentru Sortare set de caractere pe doi octeţi (*IGCSRT)

Această listă descrie operaţiile pe care le puteţi realiza pe Sortare set de caractere pe doi octeţi (*IGCSRT) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  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)
- Operaţia de modificare

  CPYIGCSRT
  Copiere sortare IGC (*la-obiectul-*ICGSRT*)

  Conversie
  Conversia la formatul V3R1, dacă este necesar

  Create - Creare
  Crearea unui caracter definit de utilizator (opţiune 1 din meniul CGU)

  Delete - Ştergere
  Ştergerea unui caracter definit de utilizator (opţiune 2 din meniul CGU)

  Update - 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 Tabelă set de caractere pe doi octeţi (*IGCTBL)

Această listă descrie operaţiile pe care le puteţi realiza pe Tabelă set de caractere pe doi octeţi (*IGCTBL) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  CPYIGCTBL
  Copiere tabelă IGC

  STRFMA
  Pornire ajutor gestionare fonturi
- Operaţia de modificare

  STRFMA
  Pornire ajutor gestionare fonturi
- Operaţiile care nu sunt auditate

  CHKIGCTBL
  Verificare tabelă IGC

Operaţii pentru Descriere job (*JOBD)

Această listă descrie operaţiile pe care le puteţi realiza pe Descriere job (*JOBD) şi dacă acele operaţii sunt auditate.

- Operaţie citire

Fără

- Operaţia 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 Coadă de joburi (*JOBQ)

Această listă descrie operaţiile pe care le puteţi realiza pe Coadă de joburi (*JOBQ) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Fără
- Operaţia de modificare

  Intrare
  Când o intrare este plasată sau înlăturată din coadă

  CHGJOBQ
  Modificare coadă de joburi

  CLRJOBQ
  Curăţare coadă joburi

  HLDJOBQ
  Blocare coadă joburi

  RLSJOBQ
  Eliberare coadă joburi
- Operaţiile care nu sunt auditate

  ADDJOBQE “Descrierile de subsistem” la pagina 205
  Adăugare intrare coadă joburi

  CHGJOB
  Modificare job dintr-un JOBQ în alt JOBQ

  CHGJOBQE “Descrierile de subsistem” la pagina 205
  Modificare intrare coadă joburi

  QSPRJOBQ
  Extragere informaţii coadă joburi

  RMVJOBQE “Descrierile de subsistem” la pagina 205
  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

WRKJOBQD
Descrierea Lucru cu coadă de joburi

Operaţii pentru Obiect planificator joburi (*JOBSCD)

Această listă descrie operaţiile pe care le puteţi realiza pe Obiect planificator joburi (*JOBSCD) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Fără

- Operaţia 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

  Lucru cu ...
  Gestionare joburi lansate anterior din intrarea de planificare job

  QWCLSCDE
  API-ul de listare intrare planificare job

Operaţii pentru Jurnal (*JRN)

Această listă descrie operaţiile pe care le puteţi realiza pe Jurnal (*JRN) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  CMPJRNIMG
  Comparaţie imagini jurnal

  DSPJRN
  Afişare intrare jurnal pentru jurnale utilizator

  QJORJIDI
  Extragere informaţii de identificator jurnal (JID)

3. O înregistrare de auditare este scrisădacă auditarea obiectelor este specificată pentru descrierea subsistemului (*SBSD).

QjoRetrieveJournalEntries
Extragere intrări jurnal

RCVJRNE
Primire intrare jurnal

RTVJRNE
Extragere intrare jurnal

- Operaţia 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 Receptor jurnal (*JRNRCV)

Această listă descrie operaţiile pe care le puteţi realiza pe Receptor jurnal (*JRNRCV) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Fără

- Operaţia 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)

Această listă descrie operaţiile pe care le puteţi realiza pe Bibliotecă (*LIB) şi dacă acele operaţii sunt auditate.

- Operaţie 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

  Notă:

  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 OBJ(AR/WRK*) OBJTYPE(*FILE)
     ```

     Dacă o bibliotecă numită “AR” nu conţine nume de fişiere care încep cu “WRK”, nu este scrisă nici o înregistrare de auditare pentru acea bibliotecă.

Listă de biblioteci
Adăugare bibliotecă la lista de biblioteci

- Operaţia de modificare

  CHGLIB
  Modificare bibliotecă

  CLRLIB
  Curăţare bibliotecă

  MOVOBJ
  Mutare obiect

  RNMOBJ
  Redenumire obiect

  Add - Adăugare
  Adăugare obiect la bibliotecă

  Delete - Ştergere
  Ştergere obiect din bibliotecă

- Operaţiile care nu sunt auditate

  Fără

Operaţii pentru Descriere de linie (*LIND)

Această listă descrie operaţiile pe care le puteţi realiza pe Descriere de linie (*LIND) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  SAVCFG
  Salvare configuraţie

  RUNLPDA
  Rulare comenzi operaţionale LPDA-2

  VFYCMN
  Test legătură

  VFYLNKLPDA
  Test legătură LPDA-2

- Operaţia 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

Operaţii pentru Servicii mail

Această listă descrie operaţiile pe care le puteţi realiza pe Servicii Mail şi dacă acele operaţii sunt auditate.

Notă: Acţiunile servicii mail sunt auditate dacă valoarea de sistem acţiune de auditare (QAUDLVL) sau parametrul de auditare acţiune (AUDLVL) din profilul de 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 de 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

  Fişier 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.

  Recepţie
  Primire element mail

  Răspuns
  Răspuns unui element mail

Trimitere
Trimitere element mail

View Vizualizare element mail

Operaţii pentru Meniu (*MENU)

Această listă descrie operaţiile pe care le puteţi realiza pe Meniu (*MENU) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Afişare
  Afişarea unui meniu cu comanda GO MENU sau cu comanda din caseta de dialog UIM
- Operaţia de modificare

  CHGMNU
  Modificare meniu
- Operaţiile care nu sunt auditate

  Retur Întoarcerea la un meniu din stiva de meniuri care a fost deja afişată

  DSPMNUA
  Afişare atribute meniu

  WRKMNU
  Lucru cu meniu

Operaţii pentru Descriere mod (*MODD)

Această listă descrie operaţiile pe care le puteţi realiza pe Descriere mod (*MODD) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Fără
- Operaţia 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 Obiect modul (*MODULE)

Această listă descrie operaţiile pe care le puteţi realiza pe Obiect modul (*MODULE) şi dacă acele operaţii sunt auditate.

- Operaţie 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

- Operaţia de modificare

  CHGMOD
  Modificare modul
- Operaţiile care nu sunt auditate

  DSPMOD
  Afişare modul

  RTVBNDSRC
  Extragere sursă legătură

  WRKMOD
  Gestionare module

Operaţii pentru Fişier mesaj (*MSGF)

Această listă descrie operaţiile pe care le puteţi realiza pe Fişier mesaj (*MSGF) şi dacă acele operaţii sunt auditate.

- Operaţie 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
- Operaţia 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 Coadă de mesaje (*MSGQ)

Această listă descrie operaţiile pe care le puteţi realiza pe Coadă de mesaje (*MSGQ) şi dacă acele operaţii sunt auditate.

- Operaţie 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.

- Operaţia 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

Program
Programare operaţii coadă de mesaje

Operaţii pentru Grup de noduri (*NODGRP)

Această listă descrie operaţiile pe care le puteţi realiza pe Grup de noduri (*NODGRP) şi dacă acele operaţii sunt auditate.

- Operaţie citire

DSPNODGRP
Afişare grup de noduri

- Operaţia de modificare

CHGNODGRPA
Modificare grup de noduri

Operaţii pentru Listă de noduri (*NODL)

Această listă descrie operaţiile pe care le puteţi realiza pe Listă de noduri (*NODL) şi dacă acele operaţii sunt auditate.

- Operaţie citire

QFVLSTNL
Listare intrări listă de noduri

- Operaţia 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)

Această listă descrie operaţiile pe care le puteţi realiza pe Descriere NetBIOS (*NTBD) şi dacă acele operaţii sunt auditate.

- Operaţie citire

SAVCFG
Salvare configuraţie

- Operaţia 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 Interfaţă de reţea (*NWID)

Această listă descrie operaţiile pe care le puteţi realiza pe Interfaţă de reţea (*NWID) şi dacă acele operaţii sunt auditate.

- Operaţie citire

SAVCFG
Salvare configuraţie

- Operaţia 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 Descriere server de reţea (*NWSD)

Această listă descrie operaţiile pe care le puteţi realiza pe Descriere server de reţea (*NWSD) şi dacă acele operaţii sunt auditate.

- Operaţie citire

SAVCFG
Salvare configuraţie

- Operaţia 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 Coadă de ieşire (*OUTQ)

Această listă descrie operaţiile pe care le puteţi realiza pe Coadă de ieşire (*OUTQ) şi dacă acele operaţii sunt auditate.

- Operaţie citire

STRPRTWTR
Pornire scriitor imprimantă la o coadă de ieşire

STRRMTWTR
Pornire scriitor la distanţă la o coadă de ieşire

- Operaţia de modificare

Plasare
Când o intrare este plasată sau înlăturată din coadă

CHGOUTQ
Modificare coadă de ieşire

CHGSPLFA [4]
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 [4]
Ştergere fişier spool

HLDOUTQ
Reţinere coadă de ieşire

RLSOUTQ
Eliberare coadă de ieşire

- Operaţiile care nu sunt auditate

CHGSPLFA [4]
Modificare atribute fişier spool

CPYSPLF [4]
Copiere fişier spool

Creare [4]
Creare fişier spool

DSPSPLF [4]
Afişare fişier spool

HLDSPLF [4]
Reţinere fişier spool

QSPROUTQ
Extragere informaţii coadă de ieşire

RLSSPLF [4]
Eliberare fişier spool

SNDNETSPLF [4]
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)

Această listă descrie operaţiile pe care le puteţi realiza pe Suprapunere (*OVL) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Tipărire
  Tipărire fişier spool care referă o suprapunere
- Operaţia de modificare

  Fără
- Operaţiile care nu sunt auditate

  WRKOVL
  Gestionare suprapuneri

  Tipărire
  Referirea la suprapunere când se creează un fişier spool

Operaţii pentru Definiţie pagină (*PAGDFN)

Această listă descrie operaţiile pe care le puteţi realiza pe Definiţie pagină (*PAGDFN) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Tipărire
  Tipărirea unui fişier spool care referă la o definiţie de pagină

4. Aceasta este de asemenea auditată dacă auditarea de acţiuni (valoarea sistem QAUDLVL sau valoarea profil de utilizator AUDLVL) include *SPLFDTA.

- Operaţia de modificare

  Fără
- 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)

Această listă descrie operaţiile pe care le puteţi realiza pe Segment de pagină (*PAGSEG) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Tipărire
  Tipărirea unui fişier spool care referă la un segment de pagină
- Operaţia de modificare

  Fără
- Operaţiile care nu sunt auditate

  WRKPAGSEG
  Gestionare segmente de pagină

  Tipărire
  Referirea la segmentul de pagină la crearea unui fişier spool

Operaţii pentru Grup descriptor tipărire (*PDG)

Această listă descrie operaţiile pe care le puteţi realiza pe Grup descriptor tipărire (*PDG) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Deschidere
  Când grupul de descriptori tipărire este deschis pentru citire de către un API PrintManager sau verb CPI.
- Operaţia 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)

Această listă descrie operaţiile pe care le puteţi realiza pe Program (*PGM) şi dacă acele operaţii sunt auditate.

- Operaţie 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

- Operaţia 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 Grup panouri (*PNLGRP)

Această listă descrie operaţiile pe care le puteţi realiza pe Grup panouri (*PNLGRP) şi dacă acele operaţii sunt auditate.

- 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

  Fără
- Operaţiile care nu sunt auditate

  WRKPNLGRP
  Gestionare grupuri de panouri

Operaţii pentru Disponibilitate produs (*PRDAVL)

Această listă descrie operaţiile pe care le puteţi realiza pe Disponibilitate produs (*PRDAVL) şi dacă acele operaţii sunt auditate.

- Operaţia de modificare

  WRKSPTPRD
  Gestionare produse suportate, când este adăugat sau înlăturat suportul
- Operaţiile care nu sunt auditate

  Read - Citire
  Nici o operaţie de citire nu este auditată

Operaţii pentru Definiţie produs (*PRDDFN)

Această listă descrie operaţiile pe care le puteţi realiza pe Definiţie produs (*PRDDFN) şi dacă acele operaţii sunt auditate.

- Operaţia de modificare

  ADDPRDLICI
  Adăugare informaţii de licenţă produs

WRKSPTPRD
Gestionare produse suportate, când este adăugat sau înlăturat suportul

- Operaţiile care nu sunt auditate

Read - Citire
Nici o operaţie de citire nu este auditată

Operaţii pentru Încărcare produs (*PRDLOD)

Această listă descrie operaţiile pe care le puteţi realiza pe Încărcare produs (*PRDLOD) şi dacă acele operaţii sunt auditate.

- 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

Read - Citire
Nici o operaţie de citire nu este auditată

Operaţii pentru Formular Query Manager (*QMFORM)

Această listă descrie operaţiile pe care le puteţi realiza pe Formular Query Manager (*QMFORM) şi dacă acele operaţii sunt auditate.

- 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

Folosiţi
Accesaţi formularul folosind opţiunea 2, 5, 6 sau 9 sau funcţia F13 din DB2 Query Manager şi SQL Development Kit pentru i5/OS.

- 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 interogare Query Manager (*QMQRY)

Această listă descrie operaţiile pe care le puteţi realiza pe interogare Query Manager (*QMQRY) şi dacă acele operaţii sunt auditate.

- 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

  Folosiţi
  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

  Conversie
  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

  Activ Orice operaţie cerere care este făcută pentru cererea 'activă'.

Operaţii pentru Definiţie interogare (*QRYDFN)

Această listă descrie operaţiile pe care le puteţi realiza pe Definiţie interogare (*QRYDFN) şi dacă acele operaţii sunt auditate.

- 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 interogare folosind opţiunea 3 din ecranul “Lucrul cu interogări”

  Create - Creare
  Creaţi o interogare folosind opţiunea 1 din ecranul “Lucrul cu interogări”

  Delete - Ştergere
  Ştergeţi o interogare folosind opţiunea 4 din ecranul “Lucrul cu interogări”

  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 Tabelă de translatare cod referinţă (*RCT)

Această listă descrie operaţiile pe care le puteţi realiza pe Tabelă translatare cod referinţă (*RCT) şi dacă acele operaţii sunt auditate.

- Operaţie citire

Fără

- Operaţia de modificare

  Fără

- Operaţiile care nu sunt auditate

  Fără

Operaţii pentru Listă de răspunsuri

Această listă descrie operaţiile pe care le puteţi realiza pe List de răspunsuri şi dacă acele operaţii sunt auditate.

Notă: Acţiunile listei de răspuns sunt auditate dacă valoarea sistem de auditare acţiune (QAUDLVL) sau parametrul de auditare acţiune (AUDLVL) din profilul de 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

  Fără

Operaţii pentru Descriere subsistem (*SBSD)

Această listă descrie operaţiile pe care le puteţi realiza pe Descriere subsistem (*SBSD) şi dacă acele operaţii sunt auditate.

- 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

Operaţii pentru Index de căutare informaţii (*SCHIDX)

Această listă descrie operaţiile pe care le puteţi realiza pe Index căutare informaţii (*SCHIDX) şi dacă acele operaţii sunt auditate.

- 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

Operaţii pentru Socket local (*SOCKET)

Această listă descrie operaţiile pe care le puteţi realiza pe Socket local (*SOCKET) şi dacă acele operaţii sunt auditate.

- 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
Modificare auditare

CHGAUT
Modificare autorizare

CHGOWN
Modificare proprietar

CHGPGP
Modificare grup primar

CHKIN
Înregistrare

CHKOUT
Debifare

chmod API-ul Modificare autorizări fişier

chown API-ul Modificare grup şi proprietar

givedescriptor
API-ul de acordare acces fişier

legătură
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
Lucru cu autorizări

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
  Afişare 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 sincronizare 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

citire 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

scriere API-ul de scriere în fişier

writev API-ul de scriere în fişier (Vector)

Operaţii pentru Dicţionar ajutor verificare ortografie (*SPADCT)

Această listă descrie operaţiile pe care le puteţi realiza pe Dicţionare ajutor verificare ortografie (*SPADCT) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Verificare
  Funcţia verificare ortografică

  Ajutor Funcţia de ajutor ortografie

  Despărţire
  Funcţia de despărţire

  Legare Funcţia de legare

  Sinonime
  Funcţia sinonim

  Bază Folosire dicţionar ca bază la crearea unui alt dicţionar

  Verificare
  Folosire 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 ajutor ortografie
- Operaţiile care nu sunt auditate

  Fără

Operaţii pentru Fişier spooled

Această listă descrie operaţiile pe care le puteţi realiza pe Fişiere spooled şi dacă acele operaţii sunt auditate.

Notă: Acţiunile fişierului spool sunt auditate dacă valoarea sistem de auditare a acţiunii (QAUDLVL) sau parametrul de auditare acţiune (AUDLVL) din profilul de 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 cu CHGSPLFA:
  - COPIES
  - DEV
  - FORMTYPE
  - RESTART
  - PAGERANGE
  - OUTQ
  - DRAWER
  - PAGDFN
  - FORMDF
  - USRDFNOPT
  - USRDFNOBJ
  - USRDFNDTA
  - EXPDATE
  - SAVE

  Modificarea oricăruia din următoarele atribute fişier spool cu CHGSPLFA:

  Create - Creare

  Crearea unui fişier spool folosind operaţiile de tipărire

  Crearea unui fişier spool folosind API-ul QSPCRTSP

  Delete - Ştergere

  Ştergerea unui fişier spool folosind oricare din următoarele operaţii:
  - 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
  - Ştergerea fişierelor spool care au expirat folosind comanda DLTEXPSPLF
  - Ştergerea fişierelor spool prin funcţia operaţională curăţare asistată

  Reţinere

  Reţinerea unui fişier spool prin oricare din următoarele operaţii:
  - 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

Read - Citire
Citirea unui fişier spool de pe o imprimantă sau scriitor de dischetă

Eliberare
Eliberarea unui fişier spool

Restaurare
Restaurare fişier spool

Salvare
Salvare fişier spool

Operaţii pentru Pachet SQL (*SQLPKG)

Această listă descrie operaţiile pe care le puteţi realiza pe Pachet SQL (*SQLPKG) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Rulare Când este rulat obiectul *SQLPKG
- Operaţia de modificare

  Fără
- Operaţiile care nu sunt auditate

  PRTSQLINF
  Tipărire informaţii SQL

Operaţii pentru Program service (*SRVPGM)

Această listă descrie operaţiile pe care le puteţi realiza pe Program service (*SRVPGM) şi dacă acele operaţii sunt auditate.

- 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 sesiune (*SSND)

Această listă descrie operaţiile pe care le puteţi realiza pe Descriere sesiune (*SSND) şi dacă acele operaţii sunt auditate.

Nici o operaţie de citire sau modificare nu este auditată pentru tipul de obiect *SSND.

Operaţii pentru Spaţiu de stocare server (*SVRSTG)

Această listă descrie operaţiile pe care le puteţi realiza pe Spaţiu de stocare server (*SVRSTG) şi dacă acele operaţii sunt auditate.

Nici o operaţie de citire sau modificare nu este auditată pentru tipul de obiect *SVRSTG.

Operaţii pentru Fişier flux (*STMF)

Această listă descrie operaţiile pe care le puteţi realiza pe Fişier flux (*STMF) şi dacă acele operaţii sunt auditate.

- Operaţie citire

CPY Copiere obiect

DSPLNK
Afişare legături obiect

givedescriptor
API-ul de acordare acces fişier

MOV Mutare obiect

open, open64, QlgOpen, QlgOpen64, Qp0lOpen
API-uri de deschidere fişier

SAV Salvare obiect

WRKLNK
Lucru cu legături obiect

- Operaţia de modificare

ADDLNK
Adăugare legătură

CHGAUD
Modificare auditare

CHGAUT
Modificare autorizare

CHGOWN
Modificare proprietar

CHGPGP
Modificare grup primar

CHKIN
Obiect înregistrat la intrare

CHKOUT
Obiect înregistrat la ieşire

chmod, QlgChmod
API-uri de modificare autorizări fişier

chown, QlgChown
API-uri de modificare proprietar şi grup

CPY Copiere obiect

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 obiect

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 obiect

RST Restaurare obiect

unlink, QlgUnlink
API-uri de înlăturare legătură la fişier

utime, QlgUtime
API-uri de Setare acces fişier şi timpi de modificare

WRKAUT
Lucru cu autorizări

WRKLNK
Gestionare legături

- Operaţiile care nu sunt auditate

close 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 sincronizare 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

citire 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

scriere API-ul de scriere în fişier

writev API-ul de scriere în fişier (Vector)

Operaţii pentru Legătură simbolică (*SYMLNK)

Această listă descrie operaţiile pe care le puteţi realiza pe Legătură simbolică (*SYMLNK) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  CPY Copiere obiect

  DSPLNK
  Afişare legături obiect

  MOV Mutare obiect

  readlink
  API-ul de citire valoare a legăturii simbolice

  SAV Salvare obiect

  WRKLNK
  Lucru cu legături obiect
- Operaţia de modificare

  CHGOWN
  Modificare proprietar

  CHGPGP
  Modificare grup primar

  CPY Copiere obiect

  MOV Mutare obiect

  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 obiect

  RST Restaurare obiect

  symlink, QlgSymlink
  API-uri realizare legătură simbolică

  unlink, QlgUnlink
  API-uri de înlăturare legătură la fişier

  WRKLNK
  Lucru cu legături obiect
- Operaţiile care nu sunt auditate

  lstat, lstat64, QlgLstat, QlgLstat64
  API-uri legătură stare

Operaţii pentru Descriere maşină S/36 (*S36)

Această listă descrie operaţiile pe care le puteţi realiza pe Descriere maşină S/36 (*S36) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Fără

- 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)

Această listă descrie operaţiile pe care le puteţi realiza pe Tabelă (*TBL) şi dacă acele operaţii sunt auditate.

- 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 - Citire
  Folosirea Tabelei de secvenţe sortare când se rulează orice comandă care poate specifica o secvenţă de sortare

- Operaţia de modificare

  Fără

- Operaţiile care nu sunt auditate

WRKTBL
Gestionare tabelă

Operaţii pentru Index utilizatori (*USRIDX)

Această listă descrie operaţiile pe care le puteţi realiza pe Index utilizatori (*USRIDX) şi dacă acele operaţii sunt auditate.

- 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 instrucţiunile 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

Operaţii pentru Profil de utilizator (*USRPRF)

Această listă descrie operaţiile pe care le puteţi realiza pe Profil de utilizator (*USRPRF) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  RCLOBJOWN
  Recuperare obiecte după proprietar
- Operaţia de modificare

  CHGPRF
  Modificare profil

  CHGPWD
  Modificare parolă

  CHGUSRPRF
  Modificare profil de utilizator

  CHKPWD
  Verificare parolă

  DLTUSRPRF
  Ştergere profil de utilizator

  GRTUSRAUT
  Acordare autorizare utilizator (*la-profil-utilizator*)

  QSYCHGPW
  API-ul de modificare parolă

  RSTUSRPRF
  Restaurare profil de utilizator
- Operaţiile care nu sunt auditate

DSPPGMADP
Afişare programe care adoptă

DSPUSRPRF
Afişare profil de utilizator

GRTUSRAUT
Acordare autorizare utilizator (*de-la-profil-utilizator*)

PRTPRFINT
Tipărire valori interne profil

PRTUSRPRF
Tipărire profil de 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 de utilizator

WRKOBJOWN
Gestionare obiecte deţinute

WRKUSRPRF
Lucru cu profiluri de utilizator

Operaţii pentru Coadă utilizatori (*USRQ)

Această listă descrie operaţiile pe care le puteţi realiza pe Coadă utilizatori (*USRQ) şi dacă acele operaţii sunt auditate.

- 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 instrucţiunile 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)

Această listă descrie operaţiile pe care le puteţi realiza pe Spaţiu utilizator (*USRSPC) şi dacă acele operaţii sunt auditate.

- 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 instrucţiunile 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 Listă de validare (*VLDL)

Această listă descrie operaţiile pe care le puteţi realiza pe Listă de validare (*VLDL) şi dacă acele operaţii sunt auditate.

- 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

Operaţii pentru Obiect personalizare staţie de lucru (*WSCST)

Această listă descrie operaţiile pe care le puteţi realiza pe Obiect personalizare staţie de lucru (*WSCST) şi dacă acele operaţii sunt auditate.

- Operaţie citire

  Alimentare
  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

  Fără
- Operaţiile care nu sunt auditate

  Fără

Anexa F. Dispunerea intrărilor de jurnal de auditare

Această secţiune conţine informaţii de dispunere pentru toate tipurile de intrări cu codul de jurnal T în jurnalul de auditare (QAUDJRN). Aceste intrări sunt controlate de auditarea de acţiune şi de obiect pe care o definiţi dumneavoastră.

Dispunerilor intrărilor de jurnal descrise în această anexă sunt similare cu modul de definire al unui fişier fizic folosind DDS. De exemplu, Binary (4) este definit pentru a păstraîntre 1 şi 4 cifre de informaţii cu cerinţă de spaţiu de stocare de doi octeţi, în timp ce Binary (5) păstrează între 1 şi 5 cifre de informaţii cu cerinţă de spaţiu de stocare de 4 octeţi. Limbajele precum RPG folosesc şi forţează aceste definiţii. Sistemul scrie intrări suplimentare în jurnalul de auditare pentru evenimente ca un IPL sistem sau salvarea receptorului de jurnal. Dispunerile pentru aceste tipuri de intrări pot fi găsite în subiectul Gestionare jurnal.

"Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 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.

"Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 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.

Notă: Formatele de ieşire TYPE2 şi *TYPE4 nu mai sunt actualizate; deci, este recomandat să încetaţi să folosiţi formatele *TYPE2 şi *TYPE4 şi să folosiţi doar formate *TYPE5.

"Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" 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.

"Intrări jurnal AD (Modificare auditare)" la pagina 568 la "Intrări jurnal ZR (citire obiect)" la pagina 695 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 bază de date model. Puteţi folosi comanda DSPJRN pentru a copia intrările copiate din jurnalul de auditare în fişierul de ieşire pentru analiză. "Analizarea intrărilor jurnalului de auditare cu o interogare sau cu un program" la pagina 296 furnizează exemple de folosire a fişierelor de ieşire de bază de date de modele. Vedeţi de asemenea subiectul Gestionare jurnal.

Notă: În aceste tabele de intrări jurnal, aţi putea vedea o coloană goală sub offset, JE sau J4, coloană. Înseamnă că nu există niciun fişier de ieşire model pentru acel tip de jurnal de auditare.

Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)

Această tabelă listează toate valorile posibile pentru câmpurile care sunt comune tuturor tipurilor de intrări când OUTFILFMT(*TYPE5) este specificat în comanda DSPJRN.

Tabela 156. Câmpuri antet standard pentru intrări jurnal auditare. Format înregistrare QJORDJE5 (*TYPE5)

Offset	Field	Format	Descriere
1	Lungime intrare	Zoned(5,0)	Lungimea totală 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)	Vedeti “Tipurile de intrări Jurnal auditare (QAUDJRN)” la pagina 566 pentru o listă de tipuri 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 de utilizator asociat cu jobul [1].
75	Număr de job	Zoned(6,0)	Număr job.
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 condiţii: • Numele programului nu se aplica 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 de utilizator	Char(10)	Numele profilului de utilizator curent. [1].
197	Nume sistem	Char(8)	Numele sistemului.
205	Identificator jurnal	Char(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
215	Restricţie referenţială	Char(1)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
216	Declanşator	Char(1)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
217	Date incomplete	Char(1)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.

Tabela 156. Câmpuri antet standard pentru intrări jurnal auditare (continuare). Format înregistrare QJORDJE5 (*TYPE5)

Offset	Field	Format	Descriere
218	Ignorat de APY/ RMVJRNCHG	Char(1)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
219	ESD minimizat	Char(1)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
220	Indicator de obiect	Char(1)	Folosit pentru obiecte jurnalizate. 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-ului care conţine receptorul care 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.
311	Adresă la distanţă	Char(46)	Adresa la distanţă asociată cu intrarea de jurnal.
357	Unitate logică de lucru.	Char(39)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
396	ID tranzacţie	Char(140)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
536	Rezervat	Char(20)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
556	Indicatori de valoare de nul	Char(50)	Folosit pentru obiecte jurnalizate. 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 de utilizator de la offset 187 au aceeaşi valoare. Pentru joburi prestart, câmpul nume profil de utilizator conţine numele utilizatorului care porneşte tranzacţia. Pentru unele joburi, ambele câmpuri conţin QSYS ca nume utilizator. Câmpul nume profil de utilizator din datele specifice intrării conţine utilizatorul care a provocat intrarea. Dacă este folosit un API pentru a schimba profiluri de utilizator, câmpul Nume profil de utilizator conţine numele noului profil de utilizator (cu care se face schimb).

Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)

Această tabelă listează toate valorile posibile pentru câmpurile care sunt comune tuturor tipurilor de intrări când OUTFILFMT(*TYPE4) este specificat în comanda DSPJRN.

Tabela 157. Câmpuri antet standard pentru intrări jurnal auditare. Format înregistrare QJORDJE4 (*TYPE4)

Offset	Field	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)	Vedeti “Tipurile de intrări Jurnal auditare (QAUDJRN)” la pagina 566 pentru o listă de tipuri 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 de utilizator asociat cu jobul [1].
65	Număr de job	Zoned(6,0)	Număr job.
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 aplica 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 de utilizator	Char(10)	Numele profilului de utilizator curent. [1].
142	Nume sistem	Char(8)	Numele sistemului.
150	Identificator jurnal	Char(10)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
160	Restricţie referenţială	Char(1)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
161	Declanşator	Char(1)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
162	(Zonă rezervată)	Char(8)	
170	Indicatori de valori de nul	Char(50)	Folosit pentru obiecte jurnalizate. Nu este folosit pentru intrări de jurnal de auditare.
220	Lungime date specifice intrării	Binary (4)	Lungimea datelor specifice intrării.

Tabela 157. Câmpuri antet standard pentru intrări jurnal auditare (continuare). Format înregistrare QJORDJE4 (*TYPE4)

Offset	Field	Format	Descriere
	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 de utilizator de la offset 132 au aceeaşi valoare. Pentru joburi prestart, câmpul nume profil de utilizator conţine numele utilizatorului care porneşte tranzacţia. Pentru unele joburi, ambele câmpuri conţin QSYS ca nume utilizator. Câmpul nume profil de utilizator din datele specifice intrării conţine utilizatorul care a provocat intrarea. Dacă este folosit un API pentru a schimba profiluri de utilizator, câmpul Nume profil de utilizator conţine numele noului profil de utilizator (cu care se face schimb).		

Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)

Această tabelă listează toate valorile posibile pentru câmpurile care sunt comune tuturor tipurilor de intrări când OUTFILFMT(*TYPE2) este specificat în comanda DSPJRN.

Tabela 158. Câmpuri antet standard pentru intrări jurnal auditare. Format de înregistrare QJORDJE2 (*TYPE2)

Offset	Field	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)	Vedeti “Tipurile de intrări Jurnal auditare (QAUDJRN)” la pagina 566 pentru o listă de tipuri de intrări şi 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 intrării.
41	Nume utilizator	Char(10)	Numele profilului de utilizator asociat cu jobul [1].
51	Număr de job	Zoned(6,0)	Număr job.
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 adevărată una din următoarele: • 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 intrări 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.

Tabela 158. Câmpuri antet standard pentru intrări jurnal auditare (continuare). Format de înregistrare QJORDJE2 (*TYPE2)

Offset	Field	Format	Descriere
118	Profil de utilizator	Char(10)	Numele profilului de utilizator curent. [1].
128	Nume sistem	Char(8)	Numele sistemului.
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 de utilizator* de la offset-ul 118 au aceeaşi valoare. Pentru joburi prestart, câmpul *nume profil de utilizator* conţine numele utilizatorului care porneşte tranzacţia. Pentru unele joburi, ambele câmpuri conţin QSYS ca nume utilizator. Câmpul *nume profil de utilizator* din datele specifice intrării conţine utilizatorul care a provocat intrarea. Dacă este folosit un API pentru a schimba profiluri de utilizator, câmpul *Nume profil de utilizator* conţine numele noului profil de utilizator (cu care se face schimb).

Tipurile de intrări Jurnal auditare (QAUDJRN)

Această tabelă prezintă toate tipurile de intrări disponibile pentru jurnalul de auditare.

Tabela 159. Tipurile de intrări 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 de 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
IM	Monitorizare intruziuni
IP	Comunicaţie între procese
IR	Acţiuni reguli IP
IS	Gestionare securitate internet
JD	Modificare parametru utilizator pentru o descriere job
JS	Acţiuni care afectează joburile
KF	Fişierul inel de chei

Tabela 159. Tipurile de intrări Jurnal auditare (QAUDJRN) (continuare)

Tip intrare	Descriere
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	Schimbare profil
PW	Parolă nevalidă
RA	Modificare autorizare în timpul restaurării
RJ	Restaurare descriere job cu profil de utilizator specificat
RO	Modificare proprietar obiect în timpul restaurării
RP	Restaurare program cu autorizare adoptată
RQ	Restaurare obiect *CRQD
RU	Restaurare autorizare profil de 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 gestionare 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

Tabela 159. Tipurile de intrări Jurnal auditare (QAUDJRN) (continuare)

Tip intrare	Descriere
VR	Acces resursă reţea
VS	Pornire sau terminare sesiune server
VU	Modificare profil reţea
VV	Modificare stare serviciu
X0	Autentificare reţea
X1	Jeton de identificare
XD	Extensie server de director
YC	Obiect DLO accesat (modificare)
YR	Obiect DLO accesat (citire)
ZC	Obiect accesat (modificare)
ZR	Obiect accesat (citire)

Intrări jurnal AD (Modificare auditare)

Această tabelă furnizează formatul intrărilor de jurnal AD (modificare auditare).

Tabela 160. Intrări jurnal AD (Modificare auditare). Fişier descriere câmp QASYADJE/J4/J5

Offset			Field	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Consultaţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561,“Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563, şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru listarea câmpurilor.
156	224	610	Tip intrare.	Char(1)	**D** comanda CHGDLOAUD **O** Comanda CHGOBJAUD sau 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.
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 auditare pentru acest utilizator.

Tabela 160. Intrări jurnal AD (Modificare auditare) (continuare). Fişier descriere câmp QASYADJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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 gestionare sisteme.
207	275	661	CHGUSRAUD *OPTICAL	Char (1)	Y = Scriere o înregistrare de auditare când acest utilizator accesează dispozitive optice.
208	276	662	CHGUSRAUD *AUTFAIL	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator are o eşuare de autorizare.
		663	CHGUSRAUD *JOBBAS	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator realizează o funcţie de bază job.
		664	CHGUSRAUD *JOBCHGUSR	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator modifică profilul de utilizator activ al unui fir de execuţie sau fişierul de grup.
		665	CHGUSRAUD *NETBAS	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator realizează funcţiei de bază de reţea.
		666	CHGUSRAUD *NETCLU	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator realizează funcţii de grup cluster sau resurse cluster.
		667	CHGUSRAUD *NETCMN	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator realizează funcţii de comunicaţie de reţea.
		668	CHGUSRAUD *NETFAIL	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator are o eşuare de reţea.
		669	CHGUSRAUD *NETSCK	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator realizează taskuri socket.
		670	CHGUSRAUD *PGMFAIL	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator are o eşuare de program.
		671	CHGUSRAUD *PRTDTA	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator realizează o funcţie de tipărire cu parametrul SPOOL(*NO).

Tabela 160. Intrări jurnal AD (Modificare auditare) (continuare). Fişier descriere câmp QASYADJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
		672	CHGUSRAUD *SECCFG	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator realizează configuraţie de securitate.
		673	CHGUSRAUD *SECDIRSRV	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator realizează modificări sau actualizări folosind funcţii de service director.
		674	CHGUSRAUD *SECIPC	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator realizează modificări asupra comunicaţiilor interprocese.
		675	CHGUSRAUD *SECNAS	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator realizează acţiuni serviciu autentificare reţea.
		676	CHGUSRAUD *SECRUN	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator realizează funcţii runtime de securitate.
		677	CHGUSRAUD *SECSCKD	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator realizează funcţii de descriere socket.
		678	CHGUSRAUD *SECVFY	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator foloseşte funcţii de verificare.
		679	CHGUSRAUD *SECVLDL	Char(1)	Y = Scriere o înregistare de auditare când acest utilizator manipulează liste de validare.
		680	(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 set de caractere codat pentru numele obiectului.
334	402	788	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
336	404	790	ID-ul limbaj 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 obiect fişier[1,2]	Char(16)	ID-ul fişier al obiectului.
374	442	828	Nume obiect[1]	Char(512)	Numele obiectului.
	954	1340	ID fişier obiect[1]	Char(16)	ID-ul fişier al obiectului.
	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[1]	Binary(5)	Identificatorul set de caractere codat pentru numele căii.

Tabela 160. Intrări jurnal AD (Modificare auditare) (continuare). Fişier descriere câmp QASYADJE/J4/J5

Offset					
JE	**J4**	**J5**	**Field**	**Format**	**Descriere**
	989	1375	ID regiune sau ţară nume cale [1]	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	991	1377	ID limbă nume cale[1]	Char(3)	ID-ul de limbă pentru numele de cale.
	994	1380	Lungime nume cale[1]	Binary(4)	Lungimea numelui căii.
	996	1382	Indicator nume cale[1]	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	997	1383	ID fişier înrudit [1,3]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri în format hexazecimal.[3]
	1013	1399	Nume cale[1, 4]	Char(5002)	Numele căii obiectului.

[1] Aceste câmpuri sunt folosite pentru obiectele din ″root″ (/), QOpenSys şi sisteme 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] Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.

[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.

Intrări jurnal AF (eşuare autorizare)

Această tabelă furnizează formatul intrărilor de jurnal AF (eşuare autorizare).

Tabela 161. Intrări jurnal AF (eşuare autorizare). Fişier descriere câmp QASYAFJE/J4/J5

Offset					
JE	**J4**	**J5**	**Field**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Consultaţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561,“Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563, şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru listarea câmpurilor.

Tabela 161. Intrări jurnal AF (eşuare autorizare) (continuare). Fişier descriere câmp QASYAFJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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 autorizare 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 **K** Violare specială a autorizării **N** Jetonul profil nu este un jeton regenerabil **O** Eşuare autorizare obiect optic **P** Eroare de schimbare 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 de profil nu este valid pentru schimb **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, 12, 17]	Char(10)	Numele obiectului.
167	235	621	Numele bibliotecii[13]	Char(10)	Numele bibliotecii în care este obiectul sau numărul corecţiei de LIC care a eşuat la aplicare.[11]
177	245	631	Tip obiect[14, 17]	Char(8)	Tipul obiectului.

Tabela 161. Intrări jurnal AF (eşuare autorizare) (continuare). Fişier descriere câmp QASYAFJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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 i5/OS. **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 de job	Zoned(6,0)	Număr job.
212	280	666	Nume program	Char(10)	Numele programului.

Tabela 161. Intrări jurnal AF (eşuare autorizare) (continuare). Fişier descriere câmp QASYAFJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
222	290	676	Biblioteca program	Char(10)	Numele bibliotecii unde este găsit programul.
232	300	686	Profil de 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. **AAC** Nu sunteţi autorizat pentru a folosi comanda de analiză avansată SST. **HCA** Profilul de 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[15, 16]	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 set de caractere codat pentru numele obiectului.
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	IF fişier obiect[3,4]	Char(16)	ID-ul fişier al obiectului.
439	507	893	Nume obiect[3,6]	Char(512)	Numele obiectului.

Tabela 161. Intrări jurnal AF (eşuare autorizare) (continuare). Fişier descriere câmp QASYAFJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	1019	1405	ID fişier obiect [3]	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[3]	Binary(5)	Identificatorul set de caractere codat pentru numele căii.
	1054	1440	ID regiune sau ţară nume cale [3]	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	1056	1442	ID limbă nume cale [3]	Char(3)	ID-ul de limbă pentru numele de cale.
	1059	1445	Lungime nume cale[3]	Binary(4)	Lungimea numelui căii.
	1061	1447	Indicator nume cale[3]	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	1062	1448	ID fişier director înrudit [3, 8]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri hexazecimale.[8]
	1078	1464	Nume cale[3, 9]	Char(5002)	Numele căii obiectului.
		6466	Nume bibliotecă program ASP	Char(10)	Numele ASP pentru biblioteca program
		6476	Nume bibliotecă program ASP	Char(5)	Numărul ASP pentru biblioteca program

[1] Când tipul de violare este descrierea G, numele obiectului conţine numele *SRVPGM care a conţinut ieşirea care a detectat eroarea. Pentru mai multe detalii despre tipurile de violări, vedeţi “Intrări jurnal auditare securitate” la pagina 269.

[2] Acest câmp conţine numele utilizatorului care a cauzat intrarea. QSYS ar putea fi utilizator pentru următoarele intrări:
- 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 pentru obiectele din ″root″ (/), QOpenSys şi sisteme de fişiere definite de utilizator.

[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 de violare este T, numele obiectului conţine portul TCP/IP pe care utilizatorul nu este autorizat să îl folosească. Valoarea este lăsată aliniată la stânga şi goală. Câmpurile bibliotecă obiect şi tip obiect vor fi goale.

Tabela 161. Intrări jurnal AF (eşuare autorizare) (continuare). Fişier descriere câmp QASYAFJE/J4/J5

Offset			Field	Format	Descriere
JE	J4	J5			
[6]			Când tipul de violare este O, numele obiectului 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 Javacare este creat nu poate extinde clasa sa de bază deoarece clasa de bază are atribute de sistem Java.		
[8]			Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.		
[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 tipul de violare este X şi valoarea de cod Violare operaţie este LIC, aceasta indică că o corecţie LIC nu a fost aplicată datorită unei violări de semnătură. Acest câmp va conţine numărul corecţiei LIC a cărei aplicare a eşuat.		
[12]			Când tipul de violare este K, numele obiectului conţine numele comenzii sau programului care a detectat eroarea. Dacă comanda are mai multe nume alternative, numele comenzii în înregistrarea de auditare s-ar putea să nu se potrivească cu numele specific al comenzii folosit dar va fi unul dintre alternativele echivalente. O valoare specială a *INSTR indică faptul că o instrucţiune de maşină a detectat eroarea.		
[13]			Când tipul de violare este K, numele bibliotecii conţine numele bibliotecii programului sau *N pentru biblioteca comenzii care a detectat eroarea.		
[14]			Când tipul de violare este K, tipul obiectului conţine tipul obiectului comenzii sau programului care a detectat eroarea.		
[15]			Când tipul de violare este K, calea folderului ar putea conţine numele complet de API al API-ul sau numele punctului de ieşire care a detectat eroarea.		
[16]			Când tipul de violare este X şi codul de violare operaţie este AAC, calea de foldere poate conţine numele de comandă AAC de 30 caractere.		
[17]			Când tipul de obiect este *LIC şi biblioteca obiectului este *N, numele obiectului este o nume LIC Ru.		

Intrări jurnal AP (autorizare adoptată)

Această tabelă furnizează formatul intrărilor de jurnal AP (autorizare adoptată).

Tabela 162. intrări jurnal AP (autorizare adoptată). Fişier descriere câmp QASYAPJE/J4/J5

Offset			Field	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Consultaţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561,“Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563, şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru listarea câmpurilor.
156	224	610	Tip intrare.	Char(1)	**S** Pornire **E** Oprire **A** Autorizarea adoptată folosită în timpul activării program

Tabela 162. intrări jurnal AP (autorizare adoptată) (continuare). Fişier descriere câmp QASYAPJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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 de utilizator	Char(10)	Numele profilului de utilizator a cărui autorizare este adoptată.
195	263	649	ID fişier obiect	Char(16)	ID-ul fişier al obiectului.
	279	665	ASP Name[1]	Char(10)	Numele dispozitivului ASP.
	289	675	ASP Number[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.

Intrări jurnal AU (modificări atribut)

Această tabelă furnizează formatul intrărilor de jurnal AU (modificări atribut).

Tabela 163. Intrări jurnal AU (modificări atribut). Fişier descriere câmp QASYAUJ5

Offset			
J5	**Field**	**Format**	**Descriere**
610	Tip intrare	Char(1)	Tipul intrării. **E** Atribute de configuraţie EIM
611	Acţiunea	Char(3)	Acţiunea **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-ul de limbă al noii valori	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-ul de limbă al vechii valori	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.

Intrări jurnal CA (modificări autorizare)

Această tabelă furnizează formatul intrărilor de jurnal CA (modificări autorizare).

Tabela 164. Intrări jurnal CA (modificări autorizare). Fişier descriere câmp QASYCAJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Consultaţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561,“Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563, şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru listarea câmpurilor.
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 unde este stocat obiectul.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Nume utilizator	Char(10)	Numele profilului de utilizator a cărui autorizare este revocată.
195	263	649	Nume listă de autorizare	Char(10)	Numele listei de autorizare.
					Autorizările acordate sau înlăturate:
205	273	659	Object Existence - Existenţă obiect	Char(1)	**Y** *OBJEXIST
206	274	660	Management Obiect	Char(1)	**Y** *OBJMGT
207	275	661	Obiect Operaţional	Char(1)	**Y** *OBJOPR
208	276	662	Authorization List Management - Gestionare listă de autorizare	Char(1)	**Y** *AUTLMGT
209	277	663	Listă de autorizare	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

Tabela 164. Intrări jurnal CA (modificări autorizare) (continuare). Fişier descriere câmp QASYCAJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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		(Zonă rezervată)	Char(10)	
		689	Atribut obiect	Char(10)	Atributul obiectului.
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)	
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 set de caractere codat pentru numele obiectului.
378	446	832	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
380	448	834	ID-ul limbaj 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 obiect fişier[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.

Tabela 164. Intrări jurnal CA (modificări autorizare) (continuare). Fişier descriere câmp QASYCAJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	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.
	1033	1419	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	1035	1421	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
	1038	1424	Lungime nume cale	Binary(4)	Lungimea numelui căii.
	1040	1426	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	1041	1427	ID fişier director relativ[3]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri în format hexazecimal.[3]
	1057	1443	Nume cale[4]	Char(5002)	Numele căii obiectului.

[1] Aceste câmpuri sunt folosite pentru obiectele din ″root″ (/), QOpenSys şi sisteme 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] Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.

[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.

Intrări jurnal CD (şir comandă)

Această tabelă furnizează formatul intrărilor de jurnal CD (şir comandă).

Tabela 165. Intrări jurnal CD (şir comandă). Fişier descriere câmp QASYCDJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Consultaţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561,"Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563, şi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 pentru listarea câmpurilor.
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 unde este stocat obiectul.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253	639	Rulaţi 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 de comenzi	Char(10)	Nume ASP pentru biblioteca de comenzi
		6650	Numărul ASP pentru biblioteca de comenzi	Char(5)	Numărul ASP pentru biblioteca de comenzi

Intrări jurnal CO (creare obiect)

Această tabelă furnizează formatul intrărilor de jurnal CO (creare obiect).

Tabela 166. Intrări jurnal CO (creare obiect). Fişier descriere câmp QASYCOJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Consultaţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561,"Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563, şi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 pentru listarea câmpurilor.

Tabela 166. Intrări jurnal CO (creare obiect) (continuare). Fişier descriere câmp QASYCOJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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		(Zonă rezervată)	Char(20)	
		639	Atribut obiect	Char(10)	Atributul obiectului.
		649	(Zonă rezervată)	Char(10)	
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 set de caractere codat pentru numele obiectului.
332	400	786	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
334	402	788	ID-ul limbaj 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 obiect fişier[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.
	987	1373	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	989	1375	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
	992	1378	Lungime nume cale	Binary(4)	Lungimea numelui căii.

Tabela 166. Intrări jurnal CO (creare obiect) (continuare). Fişier descriere câmp QASYCOJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	994	1380	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	995	1381	ID fişier director relativ[3]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri în format hexazecimal.[3]
	1011	1397	Nume cale[4]	Char(5002)	Numele căii obiectului.

[1] Aceste câmpuri sunt folosite pentru obiectele din ″root″ (/), QOpenSys şi sisteme 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] Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.

[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.

Intrări jurnal CP (modificări profil de utilizator)

Această tabelă furnizează formatul intrărilor de jurnal CP (modificări profil de utilizator).

Tabela 167. Intrări jurnal CP (modificări profil de utilizator). Fişier descriere câmp QASYCPJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Consultaţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561,“Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563, şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru listarea câmpurilor.
156	224	610	Tip intrare.	Char(1)	Tipul intrării. **A** Modificare la un profil de utilizator
157	225	611	Nume profil de utilizator	Char(10)	Numele profilului de utilizator care a fost modificat.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.

Tabela 167. Intrări jurnal CP (modificări profil de utilizator) (continuare). Fişier descriere câmp QASYCPJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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
194	262	648	Autorizare specială administrator securitate	Char(1)	**Y** Autorizarea 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 de 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.

Tabela 167. Intrări jurnal CP (modificări profil de utilizator) (continuare). Fişier descriere câmp QASYCPJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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	Capabilităţi limitate	Char(10)	Valoarea 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 de 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-ul pentru utilizator.
493	561	947	Identificare grup	Char(10)	gid pentru utilizator.
503	571	957	Gestionare parole locale	Char(10)	Valoarea parametrului LCLPWDMGT.
		967	Parolă compusă conform regulilor	Char(10)	Indică dacă noua parolă este compusă conform regulilor de compunere a parolelor. ***PASSED** Verificată şi este în concordanţă. ***SYSVAL** Verificată dar nu este în concordanţă din cauza unei reguli bazate pe valori sistem. ***EXITPGM** Verificată dar nu este în concordanţă din cauza unui răspuns de ieşire al unui program. ***NONE** Neverificată; drept noua parolă a fost specificat *NONE. ***NOCHECK** Neverificată; parola a fost schimbată. Acest câmp are semnificaţie numai când câmpul Parolă schimbată conţine un *Y*.
		977	Interval de expirare parolă	Char(7)	Specifică valoarea la care a fost schimbat intervalul de expirare a parolei. ***NOMAX** Fără interval de expirare. ***SYSVAL** Valoarea QPWDEXPITV a sistemului este folosită. **number** Dimensiunea intervalului de expirare în zile.

Tabela 167. Intrări jurnal CP (modificări profil de utilizator) (continuare). Fişier descriere câmp QASYCPJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
		984	Blocare modificare parolă	Char(10)	Specifică valoarea la care a fost modificată blocarea modificării de parolă. ***SYSVAL** Valoarea de sistem QPWDCHGBLK este folosită. ***NONE** Nicio blocare. **1-99** Ore blocate.

Intrări jurnal CQ (modificări *CRQD)

Această tabelă furnizează formatul intrărilor de jurnal CQ (modificări *CRQD).

*Tabela 168. Intrări jurnal CQ (modificări *CRQD).* Fişier descriere câmp QASYCQJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Consultaţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561,“Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563, şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru listarea câmpurilor.
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

Intrări jurnal CU (operaţii cluster)

Această tabelă furnizează formatul intrărilor de jurnal CU (operaţii cluster).

Tabela 169. Intrări jurnal CU (operaţii cluster). Fişier descriere câmp QASYCUJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561 şi “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 pentru menţionarea de câmp.

Tabela 169. Intrări jurnal CU (operaţii cluster) (continuare). Fişier descriere câmp QASYCUJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	224	610	Tip intrare.	Char(1)	Tipul intrării. **M** Operaţie control cluster **R** operaţie de gestionare grup resurse cluster (*GRP)
	225	611	Acţiune intrare	Char(3)	Tipul acţiunii. **ADD** Add - Adăugare **CRT** Create - Creare **DLT** Delete - Ştergere **DST** Distribuire **END** Oprire **FLO** Preluare la eroare **LST** Listare informaţii **RMV** Înlăturare **STR** Pornire **SWT** Switch **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.
	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 cluster-ului.
	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 de coadă de utilizator.
		693	Nume ASP	Char(10)	Numele ASP pentru biblioteca de coadă utilizator.
		703	Număr ASP	Char(5)	Număr ASP pentru biblioteca de coadă utilizator.

Intrări jurnal CV (verificare conexiune)

Această tabelă furnizează formatul intrărilor de jurnal CV (verificare conexiune).

Tabela 170. Intrări jurnal CV (verificare conexiune). Fişier descriere câmp QASYCVJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561 şi "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 pentru menţionarea de câmp.
	224	610	Tip intrare.	Char(1)	Tipul intrării. **C** Conexiune stabilită **E** Conexiune terminată **R** Conexiune refuzată
	225	611	Acţiunea	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. Folosită pentru Tipul de intrare E sau R. **C** Nici un răspuns de la serverul de autentificare. Folosită pentru Tipul de intrare R. **L** Eroare de configurare LCP. Folosită pentru Tipul de intrare R. **N** Eroare de configuraţie NCP. Folosită pentru Tipul de intrare R. **P** Parola nu este validă. Folosită pentru Tipul de intrare E sau R. **R** Autentificarea a fost refuzată 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)	Nume profil point-to-point.
	236	622	Protocol	Char(10)	Tipul intrării. **L2TP** Protocolul de tunelare nivel 2 **PPP** Protocol punct la punct. **SLIP** Protocol internet linie serială.

Tabela 170. Intrări jurnal CV (verificare conexiune) (continuare). Fişier descriere câmp QASYCVJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	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 bibliotecă obiect *VLDL.
	286	672	Nume utililizator *VLDL	Char(100)	Nume utilizator *VLDL.
	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.

Tabela 170. Intrări jurnal CV (verificare conexiune) (continuare). Fişier descriere câmp QASYCVJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	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. Folosită pentru Tipul de intrare E sau R.
	637	1023	Rezervat	Binary(4)	Întotdeauna zero
		1025	Nume ASP	Char(10)	Numele ASP pentru biblioteca listei de validare
		1035	Număr ASP	Char(5)	Numărul ASP pentru biblioteca listei de validare

Intrări jurnal CY (configurare criptografică)

Această tabelă furnizează formatul intrărilor de jurnal CY (configuraţie criptografică).

Tabela 171. Intrări jurnal CY (configurare criptografică). Fişier descriere câmp QASYCYJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.

Tabela 171. Intrări jurnal CY (configurare criptografică) (continuare). Fişier descriere câmp QASYCYJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	224	610	Tip intrare.	Char(1)	Tipul intrării. **A** Funcţie de control acces coprocesor Cryptographic **F** Funcţie de control facilitate coprocesor Cryptographic **K** Funcţie cheie master servicii Cryptographic **M** Funcţie cheie master coprocesor Cryptographic
	225	611	Acţiunea	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. **LOD** Încărcare cheie master. **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. **TST** Testare cheie master.
	228	614	Profil card	Char(8)	Numele profilului de card.[2]
	236	622	Rol card	Char(8)	Rolul profilului de card.[2]
	244	630	Nume dispozitiv	Char(10)	Numele dispozitivului cryptographic.[2]

Tabela 171. Intrări jurnal CY (configurare criptografică) (continuare). Fişier descriere câmp QASYCYJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
		640	ID cheie master[1]	Binary(4)	Id cheie master servicii criptografice[3]. Valori posibile sunt după cum urmează: **-2** Cheie master salvare/restaurare **-1** Cheie master ASP **1** Cheie master 1 **2** Cheie master 2 **3** Cheie master 3 **4** Cheie master 4 **5** Cheie master 5 **6** Cheie master 6 **7** Cheie master 7 **8** Cheie master 8
		644	Criptare cheie master	Char(1)	Cheia master criptată cu cheia master implicită S/R. **Y** Cheia master a fost setată şi criptată cu cheia master implicită de salvare/restaurare. **N** Cheia master a fost setată şi criptată cu o cheie master salvare/restaurare setată de utilizator.
		645	Versiune cheie master	Char(8)	Versiunea cheii master care a fost curăţată. **NEW** Noua versiune a fost curăţată. **CURRENT** Versiunea curentă a fost curăţată. **OLD** Versiunea veche a fost curăţată. **PENDING** Versiunea în aşteptare a fost curăţată.

[1] Când tipul intrării (J5 offset 610) este K, profilul card (J5 offset 614), rolul cardului (J5 offset 622) şi numele dispozitivului (J5 offset 630) este făcut câmp gol.

[2] Când tipul de intrare este K, acest câmp este blanc.

[3] Când tipul de intrare nu este K, acest câmp este blanc.

Intrări jurnal DI (server de director)

Această tabelă furnizează formatul intrărilor de jurnal DI (server de director).

Tabela 172. Intrări jurnal DI (server de director). Fişier descriere câmp QASYDIJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.
	224	610	Tip intrare.	Char(1)	Tipul intrării. **L** Operaţie LDAP
	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. **CI** Creare instanţă **CO** Creare obiect. **CP** Modificare parolă. **DI** Ştergere instanţă **DO** Obiect ştergere. **EX** Exportare director LDAP. **IM** Importare director LDAP. **OM** Obiect gestionare (redenumire). **OW** Modificare drept de proprietate. **PO** Modificare politică. **PW** Parolă eşuată. **RM** Gestionarea replicărilor **UB** Dezlegare cu succes. **ZC** Obiect modificare. **ZR** Obiect citire.

Tabela 172. Intrări jurnal DI (server de director) (continuare). Fişier descriere câmp QASYDIJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	227	613	Cod eşuare autorizare	Char(1)	Cod pentru eşuările de autorizare. Acest câmp este folosit doar dacă tipul operaţiei (J5 offset 611) 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) **G** Încercare de gestionare replicare neautorizată. **I** Încercare de importare neautorizată. **M** Încercare de modificare neautorizată. **P** Încercare neautorizată de modificare politică. **R** Încercare de citire neautorizată (căutare). **U** Încercare neautorizată de citire configuraţie de auditare. **X** Încercare neautorizată de autorizare proxy.
	228	614	Modificare configuraţie	Char(1)	Modificări configuraţie. Acest câmp este folosit doar dacă tipul operaţiei (J5 offset 611) este CF. **A** Modificare ND administrator. **C** Modificare istoric pornit/oprit. **L** Modificare nume bibliotecă backend. **P** Modificare agent de publicare. **R** Modificare server replică. Dacă tipul operaţiei este (J5 offset 611) RM următoarele valori pot fi prezente: **U** Suspendare replicare. **V** Reluare replicare. **W** Replicare modificări aflate în aşteptare acum. **X** Ocolire una sau mai multe modificări aflate în aşteptare. **Y** Dezactivare context replicare. **Z** Dezactivare context replicare.

Tabela 172. Intrări jurnal DI (server de director) (continuare). Fişier descriere câmp QASYDIJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	229	615	Cod modificare configuraţie	Char(1)	Cod pentru modificările configuraţiei. Acest câmp este folosit doar dacă tipul operaţiei (J5 offset 611) este CF. **A** Element adăugat la configuraţie **D** Element şters din configuraţie **M** Element modificat
	230	616	Propagare steguleţ	Char(1)	Indică setarea nouă a proprietarului sau valorii de propagare ACL. Acest câmp este folosit doar dacă tipul operaţiei (J5 offset 611) este CA sau OW. **T** Adevărat **F** Fals
	231	617	Alegere autentificare legătură	Char(20)	Alegerea de autentificare legătură. Acest câmp este folosit doar dacă tipul operaţiei (J5 offset 611) 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.

Tabela 172. Intrări jurnal DI (server de director) (continuare). Fişier descriere câmp QASYDIJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	4343	4729	CCSID nume proprietar	Bin(5)	Identificatorului de set de caractere codat al numelui proprietarului. Acest câmp este folosit doar dacă tipul operaţiei (J5 offset 611) este OW.
	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 (J5 offset 611) 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 (J5 offset 611) este OM, OW, PO, ZC, AF+M, sau AF+P. • 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 operaţii PO, ZC, AF+M, sau AF+P, 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 (J5 offset 611) este OM, OW, PO, ZC, AF+M, sau AF+P. • 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 PO, ZC, AF+M,sau AF+P,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 (J5 offset 611) este OM, OW, PO, ZC, AF+M sau AF+P. • 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 PO, ZC, AF+M sau AF+P, acest câmp va conţine lungimea listei 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)	CCSID-ul numelui căii.
	8394	8780	ID regiune sau ţară nume cale[2]	Char(2)	ID-ul de ţară sau regiune al numelui de cale.
	8396	8782	ID limbă nume cale[2]	Char(3)	ID-ul de limbă al numelui de cale.

Tabela 172. Intrări jurnal DI (server de director) (continuare). Fişier descriere câmp QASYDIJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	8399	8785	Lungime nume cale[2]	Bin(4)	Lungimea numelui căii.
	8401	8787	Indicator nume cale[2]	Char(1)	Indicator nume cale. **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	8402	8788	ID fişier director relative[2,3]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri în format hexazecimal.[3]
	8418	8804	Nume cale[1,2]	Char(5002)	Numele căii obiectului.
		13806	Profil de utilizator local	Char(10)	Numele profil de utilizator local care este mapat la numele utilizator LDAP (J5 offset 719). Spaţiul gol indică faptul că nici un profil de 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.
		13817	Proxy ID CCSID	Bin(5)	identificator set de caractere codate (CCSID) al ID-ului proxy.
		13821	Lungime ID proxy	Bin(4)	Lungimea ID-ului proxy.
		13823	ID proxy[1]	Char(2002)	Numele ID-ului proxy. Acest câmp este folosit când controlul autorizaţiei proxy est folosit pentru a cere ca o operaţie să fie făcută sub autorizarea ID-ului proxy sau pentru un bind SASL în care clientul a specificat un ID de autorizare diferit de ID-ul bind.
		15825	Impunere grup	Char(1)	Impunere apartenenţă grup **0** Grupurile nu au fost specificate de către client. **1** Grupurile au fost specificate de client.
		15826	Referinţă încrucişată	Char(36)	Şir referinţă încrucişată folosit pentru a corela această intrare cu intrările XD care listează grupurile.
		15862	Nume instanţă	Char(8)	Nume instanţă
		15870	CCSID rută	Bin(5)	CCSID-ul rutei
		15874	Lungime rută	Bin(4)	Lungimea rutei
		15876	Rută	Char(502)	Rută cerere

Tabela 172. Intrări jurnal DI (server de director) (continuare). Fişier descriere câmp QASYDIJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
[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 (J5 offset 611) este EX sau IM.					
[3] Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.					

Intrări jurnal DO (operaţie de ştergere)

Această tabelă furnizează formatul intrărilor de jurnal DO (operaţie de ştergere).

Tabela 173. Intrări jurnal DO (operaţie de ştergere). Fişier descriere câmp QASYDOJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.
156	224	610	Tip intrare.	Char(1)	Tipul intrării. **A** Obiectul a fost şters sub controlul comiterii **C** A fost comisă ştergere în aşteptare a obiectului **D** O creare în aşteptare a obiectului a fost rulată înapoi. **I** Iniţializare spaţiu variabilă de mediu **P** Ştergerea obiectului este în curs (ştergerea a fost realizată sub controlul comiterii) **R** O ştergere în curs de obiect a fost rulată înapoi.
157	225	611	Nume obiect	Char(10)	Numele obiectului.
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii unde este stocat obiectul.
177	245	631	Tip obiect	Char(8)	Tipul obiectului.
185	253		(Zonă rezervată)	Char(20)	
		639	Atribut obiect	Char(10)	Atributul obiectului.
		649	(Zonă rezervată)	Char(10)	
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.

Tabela 173. Intrări jurnal DO (operaţie de ştergere) (continuare). Fişier descriere câmp QASYDOJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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 obiect [1]	Binary(4)	Lungimea numelui obiectului.
328	396	782	CCSID nume obiect [1]	Binary(5)	Identificatorul set de caractere codat pentru numele obiectului.
332	400	786	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
334	402	788	ID-ul limbaj 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 obiect fişier[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.
	987	1373	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	989	1375	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
	992	1378	Lungime nume cale	Binary(4)	Lungimea numelui căii.
	994	1380	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	995	1381	ID fişier director relativ[3]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri în format hexazecimal.[3]
	1011	1397	Nume cale[4]	Char(5002)	Numele căii obiectului.

Tabela 173. Intrări jurnal DO (operaţie de ştergere) (continuare). Fişier descriere câmp QASYDOJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
[1]	Aceste câmpuri sunt folosite pentru obiectele din ″root″ (/), QOpenSys şi sisteme 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]	Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.				
[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 în bibliotecă, acestea sunt informaţiile ASP pentru obiect.				

Intrări jurnal DS (Resetare ID utilizator unelte de service livrate de IBM)

Această tabelă furnizează formatul intrărilor de jurnal DS (resetare ID utilizator unelte de service livrate de IBM).

Tabela 174. Intrări jurnal DS (Resetare ID utilizator unelte de service livrate de IBM). Fişier descriere câmp QASYDSJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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.

Tabela 174. Intrări jurnal DS (Resetare ID utilizator unelte de service livrate de IBM) (continuare). Fişier descriere câmp QASYDSJE/J4/J5

Offset					
JE	**J4**	**J5**	**Field**	**Format**	**Descriere**
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.

Intrări jurnal EV (variabilă de mediu)

Această tabelă furnizează formatul intrărilor de jurnal EV (variabilă de mediu).

Tabela 175. Intrări jurnal EV (variabilă de mediu). Fişier descriere câmp QASYEVJ4/J5

Offset					
JE	**J4**	**J5**	**Field**	**Format**	**Descriere**
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561, "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 şi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 pentru menţionarea câmpului.
	224	610	Tip intrare.	Char(1)	Tipul intrării. **A** Add - Adăugare **C** Modificare **D** Delete - Ştergere **I** Iniţializare spaţiu variabilă mediu
	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.

Tabela 175. Intrări jurnal EV (variabilă de mediu) (continuare). Fişier descriere câmp QASYEVJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	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.

Intrări jurnal GR (înregistrare generică)

Această tabelă furnizează formatul intrărilor de jurnal GR (înregistrare generică).

Tabela 176. Intrări jurnal GR (înregistrare generică). Fişier descriere câmp QASYGRJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561 şi "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 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	Acţiunea	Char(2)	Acţiune executată. **ZC** Modificare **ZR** Read - Citire
	227	613	Nume utilizator	Char(10)	Nume profil de 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.
	241	627	Lungime câmp 1	Binary (4)	Lungimea datelor din câmpul 1.

Tabela 176. Intrări jurnal GR (înregistrare generică) (continuare). Fişier descriere câmp QASYGRJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	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:** A fost anulată înregistrarea funcţiei ***CHGUSAGE:** Informaţiile de folosire funcţie au fost modificate ***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** Anulare înregistrare 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 176. Intrări jurnal GR (înregistrare generică) (continuare). Fişier descriere câmp QASYGRJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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 176. Intrări jurnal GR (înregistrare generică) (continuare). Fişier descriere câmp QASYGRJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	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 valori: ***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 autorizări 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 de 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 de 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 valori: ***REGISTER** ***REREGISTER**

[1] Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea câmpului.

Intrări jurnal GS (acordare descriptor)

Această tabelă furnizează formatul intrărilor de jurnal GS (acordare descriptor).

Tabela 177. Intrări jurnal GS (acordare descriptor). Fişier descriere câmp QASYGSJE/J4/J5

Offset					
JE	**J4**	**J5**	**Field**	**Format**	**Descriere**
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561, "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 şi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 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 de job	Zoned (6,0)	Numărul jobului.
183	251	637	Nume profil de utilizator	Char (10)	Numele profilului de utilizator.
	261	647	JUID	Char (10)	Identitatea utilizator job al jobului destinaţie. (Această valoare se aplică doar la înregistrările de auditare subtipul G)

Intrări jurnal IM (monitorizare intruziuni)

Această tabelă furnizează formatul intrărilor de jurnal IM (monitorizare intruziuni).

Tabela 178. Intrări jurnal IM (monitorizare intruziuni). QASYIMJE/J4/J5 Fişier descriere de câmp

Offset					
JE	**J4**	**J5**	**Field**	**Format**	**Descriere**
		1			Câmpurile antet comune pentru toate tipurile de intrări.
		610	Tip intrare.	Char(1)	Tipul intrării. **P** Detectare potenţial eveniment de intruziune
		611	Timpul evenimentului	TIMESTAMP	Timpul la care a fost detectat evenimentul, în format apremntă de timp SAA.
		637	Identificator punct de detectare	Char(4)	Un identificator unic pentru locaţia de procesare care a detectat evenimentul de intruziune. Acest câmp este creat pentru a fi folosit de către personalul de serviciu.
		641	Familie adrese locale	Char(1)	Familie adrese IP locale asociată cu evenimentul detectat.

Tabela 178. Intrări jurnal IM (monitorizare intruziuni) (continuare). QASYIMJE/J4/J5 Fişier descriere de câmp

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
		642	Număr port local	Zone(5, 0)	Număr port local asociat cu evenimentul detectat.
		647	Adresă IP locală	Char(46)	Adresă IP locală asociată cu evenimentul detectat.
		693	Adresă de familie la distanţă	Char(1)	Adresă de familie la distanţă asociată cu evenimentul detectat.
		694	Număr port la distanţă	Zoned(5, 0)	Număr port la distanţă asociat cu evenimentul detectat.
		699	Adresă IP la distanţă	Char(46)	Adresă IP la distanţă asociată cu evenimentul detectat.
		745	Identificator de tip Probe	Char(6)	Identifică tipul de probe folosit pentru a detecta potenţiale intruziuni. Valori posibile sunt după cum urmează: **ATTACK** Eveniment detectat de acţiunea Attack **TR-TCP** Acţiune Regulare trafic a detectat eveniment peste TCP **TR-UDP** Acţiune Regulare trafic a detectat eveniment peste UDP **SCANE** Eveniment detectat de acţiunea Scan **SCANG** Eveniment detectat de acţiunea scanare globală (global Scan) **XATTACK** Posibil atac intruziune **XTRTCP** Eveniment de ieşire TR detectat (TCP) **XTRUDP** Eveniment de ieşire TR detectat (UDP) **XSCAN** Eveniment de scanare de ieşire detectat
		751	Corelator de evenimente	Char(4)	Identificator unic pentru acest eveniment specific de intruziune. Acest identificator poate fi folosit pentru a corela această înregistrare de auditare cu alte informaţii despre detectarea intruziunilor.

Tabela 178. Intrări jurnal IM (monitorizare intruziuni) (continuare). QASYIMJE/J4/J5 Fişier descriere de câmp

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
		755	Tip eveniment	Char(8)	Identifică tipul de intruziune potenţială care a fost detectată. Valorile posibile sunt după cum urmează: **ACKSTORM** TCP ACK storm **ADRPOISN** Address poisoning **FLOOD** Eveniment inundaţie (flood) **FRAGGLE** Fraggle attack **ICMPRED** redirecţionare ICMP (Internet Control Message Protocol) **IPFRAG** fragment IP **MALFPKT** Pachet format greşit **OUTRAW** Outbound Raw **PERPECH** Ecou continuu **PNGDEATH** Pingul morţii **RESTOPT** Opţiuni IP restricţionate **RESTPROT** Protocol IP restricţionat **SMURF** Atac smurf
		763	Protocol	Char(3)	Număr protocol
		766	Condiţie	Char(4)	Număr condiţie din fişierul de politică IDS
		770	Throttling	Char(1)	• 0 = inactiv • 1 = activ
		771	Pachete ignorate	Zoned(5,0)	Număr de pachete ignorate la throttle
		776	Stiva TCP/IP destinaţie	Char(1)	**P** Stivă producţie **S** Stivă servicii
		777	Rezervat	Char(6)	Rezervat pentru folosire viitoare
		783	Pachet suspectat	Char(1002)[1]	Un câmp de lungime variabilă care poate conţine până la primii 1000 de octeţi ai pachetului IP asociat cu evenimentul detectat. Acest câmp conţine date binare şi ar trebui tratat ca şi cum ar avea un CCSID de 65535.

[1] Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea informaţiei pachetului suspectat.

Intrări jurnal IP (comunicaţie interprocese)

Această tabelă furnizează formatul intrărilor de jurnal IM (comunicaţie interprocese).

Tabela 179. Intrări jurnal IP (comunicaţie interprocese). Fişier descriere câmp QASYIPJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.
156	224	610	Tip intrare.	Char(1)	Tipul intrării. **A** Modificări de autorizare şi/sau proprietate **C** Create - Creare **D** Delete - 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** Coada de mesaje **S** Semafor
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
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

Tabela 179. Intrări jurnal IP (comunicaţie interprocese) (continuare). Fişier descriere câmp QASYIPJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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 două caractere conţin lungimea numelui semaforului.

Intrări jurnal IR (acţiuni reguli IP)

Această tabelă furnizează formatul intrărilor de jurnal IR (acţiuni reguli IP).

Tabela 180. Intrări jurnal IR (acţiuni reguli IP). Fişier descriere câmp QASYIRJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561 şi "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 pentru menţionarea de câmp.
	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** Regulile 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.
	245	631	Rezervat	Char(18)	
	263	649	Lungime nume fişier	Binary (4)	Lungimea numelui fişier.

Tabela 180. Intrări jurnal IR (acţiuni reguli IP) (continuare). Fişier descriere câmp QASYIRJ4/J5

Offset					
JE	**J4**	**J5**	**Field**	**Format**	**Descriere**
	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.
|	896	1282	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
|	898	1284	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
|	901	1287	Lungime nume cale	Binary(4)	Lungimea numelui căii.
	903	1289	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	904	1290	ID fişier director relativ[3]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri în format hexazecimal.[3]
	920	1306	Nume cale[4]	Char(5002)	Numele căii obiectului.

\| [1] Aceste câmpuri sunt folosite pentru obiectele din ″root″ (/), QOpenSys şi sisteme de fişiere definite de utilizator.

[2] Dacă ID-ul are bitul cel mai din stânga setat şi restul biţilor zero, ID-ul nu este setat.

[3] Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.

[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.

Intrări jurnal IS (gestionare securitate internet)

Această tabelă furnizează formatul intrărilor de jurnal IS (gestionare securitate internet).

Tabela 181. Intrări jurnal IS (gestionare securitate internet). Fişier descriere câmp QASYISJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561 şi “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 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[1]	Char(15)	Adresă IP locală.
	240	626	Port ID client local	Char(5)	Port ID client local.
	245	631	Adresă IP la distanţă[1]	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	Familie de adresă IP locale	Char (1)	Familie de adresă IP locale **4** IPv4 **6** IPv6
		652	Adresă IP locală	Char (46)	Adresă IP locală
		698	Familie de adresă IP la distanţă	Char (1)	Familie de adresă IP la distanţă **4** IPv4 **6** IPv6
		699	Adresă IP la distanţă	Char (46)	Adresă IP la distanţă
		745	Rezervat	Char (162)	Rezervat
	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 i5/OS VPN Key Manager

Tabela 181. Intrări jurnal IS (gestionare securitate internet) (continuare). Fişier descriere câmp QASYISJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	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 **5** Adresă IP versiunea 6 **6** Subreţea IP versiunea 6 **7** Interval adresă IP versiunea 4 **8** Interval de adrese IP versiunea 6 **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
	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 **5** Adresă IP versiunea 6 **6** Subreţea IP versiunea 6 **7** Interval adresă IP versiunea 4 **8** Interval de adrese IP versiunea 6 **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)
[1] Acest câmp suportă doar adrese IPv4.					

Intrări jurnal JD (modificare descriere job)

Această tabelă furnizează formatul intrărilor de jurnal JD (modificare descriere job).

Tabela 182. Intrări jurnal JD (modificare descriere job). Fişier descriere câmp QASYJDJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561, "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 şi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 pentru menţionarea câmpului.
156	224	610	Tip intrare.	Char(1)	Tipul intrării. **A** Profilul de 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 unde este stocat 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 de 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

Intrări jurnal JS (modificare job)

Această tabelă furnizează formatul intrărilor de jurnal JS (modificare job).

Tabela 183. Intrări jurnal JS (modificare job). Fişier descriere câmp QASYJSJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561, "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 şi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 pentru menţionarea câmpului.

Tabela 183. Intrări jurnal JS (modificare job) (continuare). Fişier descriere câmp QASYJSJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
156	224	610	Tip intrare.	Char(1)	Tipul intrării. **A** comanda ENDJOBABN **B** Lansare **C** Modificare **E** Oprire **H** Reţinere **I** Deconectare **J** Jobul curent încearcă să întrerupă alt job **K** Jobul curent este pe cale să fie întrerupt **L** Întreruperea jobului curent este completă **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 183. Intrări jurnal JS (modificare job) (continuare). Fişier descriere câmp QASYJSJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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** Interogare **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 de 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 de utilizator efectiv[2]	Char(10)	Numele profilului de 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	Nume 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.

Tabela 183. Intrări jurnal JS (modificare job) (continuare). Fişier descriere câmp QASYJSJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	934	1320	Câmp JUID	Char(10)	Conţine valoarea JUID
	944	1330	Profil de utilizator real	Char(10)	Numele profilului de utilizator real pentru firul de execuţie.
	954	1340	Profil de utilizator salvat	Char(10)	Numele profilului de utilizator salvat pentru firul de execuţie.
	964	1350	Profil grup real	Char(10)	Numele profilului de grup real pentru firul de execuţie.
	974	1360	Profil grup salvat	Char(10)	Numele profilului de grup salvat pentru firul de execuţie.
	984	1370	Utilizator real modificat[3]	Char(1)	Profilul de utilizator real a fost modificat. **Y** Da **N** Nu
	985	1371	Utilizator efectiv modificat[3]	Char(1)	Profilul de utilizator efectiv a fost modificat. **Y** Da **N** Nu
	986	1372	Utilizator salvat modificat[3]	Char(1)	Profilul de 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
		3656	Nume fus orar	Char(10)	Nume descriere fus orar
		3666	Nume job ieşire	Char(10)	Numele jobului care a întrerupt jobul curent sau numele jobului care a fost întrerupt de către jobul curent

Tabela 183. Intrări jurnal JS (modificare job) (continuare). Fişier descriere câmp QASYJSJE/J4/J5

Offset			Field	Format	Descriere
JE	J4	J5			
		3676	Utilizator job ieşire	Char(10)	Numele utilizatorului care a întrerupt jobul curent sau numele jobului care a fost întrerupt de către jobul curent
		3686	Număr job ieşire [6, 7]	Char(6)	Numărul jobului care a întrerupt jobul curent sau numele jobului care a fost întrerupt de către jobul curent
		3692	Nume program ieşire [6]	Char(10)	Programul de ieşire întrerupea jobul
		3702	Bibliotecă program ieşire [6]	Char(10)	Numele de bibliotecă al programului de ieşire întrerupea jobul
		3712	Nume APS bibliotecă JOBQ	Char(10)	Nume ASP pentru biblioteca JOBQ
		3722	Număr ASP bibliotecă JOBQ	Char(5)	Numărul ASP al bibliotecii JOBQ

[1] Acest câmp este gol dacă jobul este în coada de mesaje şi nu rulează.

[2] Când înregistrarea 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 610) este M sau T.

[4] Acest câmp este folosit doar dacă numărul de biblioteci din lista de biblioteci depăşeşte dimensiunea câmpului la offset-ul 729.

[5] Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea datelor din câmp.

[6] Acest câmp este folosit doar când tipul intrării (offset 610) este J, K sau L.

[7] Când tipul intrării este J, acest câmp conţine informaţii despre jobul care va fi întrerupt. Când tipul intrării este K sau L acest câmp conţine informaţii despre jobul care a cerut întreruperea jobului curent.

Intrări jurnal KF (fişier inel de chei)

Această tabelă furnizează formatul intrărilor de jurnal KF (fişier inel de chei).

Tabela 184. Intrări jurnal KF (fişier inel de chei). Fişier descriere câmp QASYKFJ4/J5

Offset			Field	Format	Descriere
JE	J4	J5			
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561 şi "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 pentru menţionarea de câmp.
	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

Tabela 184. Intrări jurnal KF (fişier inel de chei) (continuare). Fişier descriere câmp QASYKFJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	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 director părinte inel de chei
	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 sursă sau destinaţie.

Tabela 184. Intrări jurnal KF (fişier inel de chei) (continuare). Fişier descriere câmp QASYKFJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	830	1216	CCSID nume obiect	Binary(5)	CCSID nume fişier sursă sau destinaţie.
	834	1220	ID regiune sau ţară nume obiect	Char(2)	ID ţară sau regiuni nume fişier sursă sau destinaţie.
	836	1222	ID limbă nume obiect	Char(3)	ID limbă nume fişier sursă sau destinaţie.
	839	1225	Rezervat	Char(3)	
	842	1228	ID fişier părinte	Char(16)	ID fişier director părinte sursă sau destinaţie.
	858	1244	ID fişier obiect	Char(16)	ID fişier director sursă sau destinaţie.
	874	1260	Nume obiect	Char(512)	Nume fişier sursă sau destinaţie.
	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 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.
|	2449	2835	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
|	2451	2837	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
|	2454	2840	Lungime nume cale	Binary(4)	Lungimea numelui căii.
	2456	2842	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine nume de cale absolut complet pentru fişierul inel de chei. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
|	2457	2843	ID fişier director relativ[2]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri hexazecimale.[2]
	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 de fişier al fişierului sursă sau destinaţie.
	7491	7877	Nume ASP	Char(10)	Nume ASP fişier sursă sau destinaţie
	7501	7887	Număr ASP	Char(5)	Număr ASP fişier sursă sau destinaţie

Tabela 184. Intrări jurnal KF (fişier inel de chei) (continuare). Fişier descriere câmp QASYKFJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	7506	7892	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele căii.
	7510	7896	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	7512	7898	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
	7515	7901	Lungime nume cale	Binary(4)	Lungimea numelui căii.
	7517	7903	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine nume de cale absolut complet pentru fişierul sursă sau destinaţie. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	7518	7904	ID fişier director relativ[3]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri hexazecimale.[2]
	7534	7920	Nume cale absolută[1]	Char(5002)	Numele de cale absolută a fişierului sursă sau destinaţie.

[1] Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui căii.

[2] Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.

[3] Când indicatorul de nume de cale (offset 7517) este N, acest câmp va conţine ID-ul relativ de fişier al numelui de cale absolut de la offset 7534. Când indicatorul de nume de cale este Y, acest câmp va conţine 16 octeţi de zerouri hexazecimale.

[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.

Intrări jurnal LD (legare, dezlegare, căutare director)

Această tabelă furnizează formatul intrărilor de jurnal LD (legare, dezlegare, căutare director).

Tabela 185. Intrări jurnal LD (legare, dezlegare, căutare director). Fişier descriere câmp QASYLDJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561, "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 şi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 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 set de caractere codat pentru numele obiectului.
181	249	635	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
183	251	637	ID-ul limbaj 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.
205	273	659	ID obiect fişier[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.
	836	1222	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	838	1224	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
	841	1227	Lungime nume cale	Binary(4)	Lungimea numelui căii.

Tabela 185. Intrări jurnal LD (legare, dezlegare, căutare director) (continuare). Fişier descriere câmp QASYLDJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	843	1229	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	844	1230	ID fişier înrudit [1]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri hexazecimale.[1]
	860	1246	Nume cale[2]	Char(5002)	Numele căii obiectului.

[1] Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.

[2] Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui căii.

Intrări jurnal ML (Acţiuni mail)

Această tabelă furnizează formatul intrărilor de jurnal ML (acţiuni mail).

Tabela 186. Intrări jurnal ML (Acţiuni mail). Fişier descriere câmp QASYMLJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.
156	224	610	Tip intrare.	Char(1)	Tipul intrării. **O** Istoric de poştă deschis
157	225	611	Profil de utilizator	Char(10)	Nume profil de utilizator.
167	235	621	ID utilizator	Char(8)	Identificator utilizator
175	243	629	Adresă	Char(8)	Adresă utilizator

Intrări jurnal NA (modificare atribut)

Această tabelă furnizează formatul intrărilor de jurnal NA (modificare atribut).

Tabela 187. Intrări jurnal NA (modificare atribut). Fişier descriere câmp QASYNAJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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	Valoarea nouă atribut	Char(250)	Valoarea atributului după ce a fost modificat.
417	485	871	Valoarea veche atribut	Char(250)	Valoarea atributului înainte de a fi modificat.

Intrări jurnal ND (filtru căutare director APPN)

Această tabelă furnizează formatul intrărilor de jurnal ND (filtru căutare director APPN).

Tabela 188. Intrări jurnal ND (filtru căutare director APPN). Fişier descriere câmp QASYNDJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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.

Tabela 188. Intrări jurnal ND (filtru căutare director APPN) (continuare). Fişier descriere câmp QASYNDJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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 Filtru căutare director APPN şi Punct final APPN, consultaţi Protejarea sistemului într-un mediu APPN şi HPR pentru detalii.

Intrări jurnal NE (filtru punct final APPN)

Această tabelă furnizează formatul intrărilor de jurnal NE (filtru punct final APPN).

Tabela 189. Intrări jurnal NE (filtru punct final APPN). Fişier descriere câmp QASYNEJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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 Filtru căutare director APPN şi Punct final APPN, consultaţi Protejarea sistemului într-un mediu APPN şi HPR pentru detalii.

Intrări jurnal OM (modificare gestionare obiect)

Această tabelă furnizează formatul intrărilor de jurnal OM (modificare gestionare obiect).

Tabela 190. Intrări jurnal OM (modificare gestionare obiect). Fişier descriere câmp QASYOMJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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 se află vechiul obiect.
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		(Zonă rezervată)	Char(20)	
		659	Atribut obiect	Char(10)	Atributul obiectului.
		669	(Zonă rezervată)	Char(10)	
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.
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)	

Tabela 190. Intrări jurnal OM (modificare gestionare obiect) (continuare). Fişier descriere câmp QASYOMJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	497	883	Lungime nume cale	Binary (4)	Lungimea câmpului nume obiect vechi.
431	499	885	CCSID nume obiect [1]	Binary(5)	Identificatorul set de caractere codat pentru numele obiectului.
435	503	889	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
437	505	891	ID-ul limbaj 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 vechi obiect[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 obiect fişier[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.
	1618	2004	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	1620	2006	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
	1623	2009	Lungime nume cale	Binary(4)	Lungimea numelui căii.
	1625	2011	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	1626	2012	ID fişier director relativ[3]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri în format hexazecimal.[3]
	1642	2028	Nume cale absolută [5]	Char(5002)	Numele cale absolută vechi al obiectului.

Tabela 190. Intrări jurnal OM (modificare gestionare obiect) (continuare). Fişier descriere câmp QASYOMJE/J4/J5

Offset					
JE	**J4**	**J5**	**Field**	**Format**	**Descriere**
	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.
	6675	7061	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele căii.
	6679	7065	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	6681	7067	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
	6684	7070	Lungime nume cale	Binary(4)	Lungimea numelui căii.
	6686	7072	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	6687	7073	ID fişier director relativ[4]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri în format hexazecimal.[3]
	6703	7089	Nume cale absolută[5]	Char(5002)	Numele cale absolută nou al obiectului.

[1] Aceste câmpuri sunt folosite pentru obiectele din ″root″ (/), QOpenSys şi sisteme 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] Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.

[4] Când indicatorul de nume de cale (offset 6686) este N, acest câmp va conţine ID-ul relativ de fişier al numelui de cale absolut de la offset 6703. Când indicatorul de nume de cale este Y, acest câmp va conţine 16 octeţi de zerouri hexazecimale.

[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.

Intrări jurnal OR (restaurare obiect)

Această tabelă furnizează formatul intrărilor de jurnal OR (restaurare obiect).

Tabela 191. Intrări jurnal OR (restaurare obiect). Fişier descriere câmp QASYORJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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.
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	Comanda 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)	Indicatorul 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)	Indicatorul mod SETGID. **Y** Bitul mod SETGID pentru obiectul restaurat este activ. **N** Bitul mod SETGID pentru obiectul restaurat nu este activ.

Tabela 191. Intrări jurnal OR (restaurare obiect) (continuare). Fişier descriere câmp QASYORJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	277	663	Stare semnătură	Char(1)	Starea semnăturii pentru obiectul restaurat. **B** Semnătura nu a fost în format i5/OS **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
	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		(Zonă rezervată)	Char(14)	
		665	Atribut obiect	Char(10)	Atributul obiectului.
		675	(Zonă rezervată)	Char(4)	
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		(Zonă rezervată)	Char(18)	

Tabela 191. Intrări jurnal OR (restaurare obiect) (continuare). Fişier descriere câmp QASYORJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
		865	Restaurare autorizări private	Char(1)	Autorizările private cerute să fie restaurate (PVTAUT(*YES) specificate în comanda de restaurare) **Y** PVTAUT(*YES) specificat în comanda de restaurare **N** PVTAUT(*NO) specificat în comanda de restaurare
		866	Autorizări private salvate[8]	Binary(5)	Număr de autorizări private salvate
		870	Autorizări private restaurate[8]	Binary(5) [8]	Număr de autorizări private restaurate
		874	(Zonă rezervată)	Char(9)	
	497	883	Lungime nume cale	Binary (4)	Lungimea câmpului Nume obiect vechi.
431	499	885	CCSID nume obiect [3]	Binary(5)	CCSID pentru numele obiectului.
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	IF 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.
	1122	1508	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	1124	1510	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
	1127	1513	Lungime nume cale	Binary(4)	Lungimea numelui căii.

Tabela 191. Intrări jurnal OR (restaurare obiect) (continuare). Fişier descriere câmp QASYORJE/J4/J5

Offset			Field	Format	Descriere
JE	J4	J5			
	1129	1515	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	1130	1516	ID fişier înrudit [5]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri hexazecimale.[5]
	1146	1532	Nume cale[6]	Char(5002)	Numele căii 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 pentru obiectele din ″root″ (/), QOpenSys şi sisteme de fişiere definite de utilizator.

[4] Un ID care are bitul cel mai din stânga setat şi restul biţilor 0 indică faptul că ID -ul NU este setat.

[5] Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.

[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.

[8] Acest câmp este zero dacă Restaurare autorizări private (offset 865) este N.

Intrări jurnal OW (modificare drept de proprietate)

Această tabelă furnizează formatul intrărilor de jurnal OW (modificare drept de proprietate).

Tabela 192. Intrări jurnal OW (modificare drept de proprietate). Fişier descriere câmp QASYOWJE/J4/J5

Offset			Field	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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.

Tabela 192. Intrări jurnal OW (modificare drept de proprietate) (continuare). Fişier descriere câmp QASYOWJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii unde este stocat 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)	
	414	800	Lungime nume cale	Binary (4)	Lungimea numelui obiect nou.
348	416	802	CCSID nume obiect [1]	Binary(5)	Identificatorul set de caractere codat pentru numele obiectului.
352	420	806	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
354	422	808	ID-ul limbaj 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 obiect fişier[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.
	1007	1393	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	1009	1395	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
	1012	1398	Lungime nume cale	Binary(4)	Lungimea numelui căii.

Tabela 192. Intrări jurnal OW (modificare drept de proprietate) (continuare). Fişier descriere câmp QASYOWJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	1014	1400	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	1015	1401	ID fişier director relativ[3]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri în format hexazecimal.[3]
	1031	1417	Nume cale[4]	Char(5002)	Numele căii obiectului.

[1] Aceste câmpuri sunt folosite pentru obiectele din ″root″ (/), QOpenSys şi sisteme 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] Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.

[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.

Intrări jurnal O1 (acces optic)

Această tabelă furnizează formatul intrărilor de jurnal O1 (acces optic).

Tabela 193. Intrări jurnal O1 (acces optic). fişier descriere câmp QASY01JE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.
156	224	610	Tip intrare.	Char(1)	R-Citire U-Actualizare D-Ştergere C-Creare director X-Eliberare fişier reţinut

Tabela 193. Intrări jurnal O1 (acces optic) (continuare). fişier descriere câmp QASY01JE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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					

Intrări jurnal O2 (acces optic)

Această tabelă furnizează formatul intrărilor de jurnal O2 (acces optic).

Tabela 194. Intrări jurnal O2 (acces optic). Fişier descriere câmp QASY02JE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.

Tabela 194. Intrări jurnal O2 (acces optic) (continuare). Fişier descriere câmp QASY02JE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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
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

Intrări jurnal O3 (acces optic)

Această tabelă furnizează formatul intrărilor de jurnal O3 (acces optic).

Tabela 195. Intrări jurnal O3 (acces optic). fişier descriere câmp QASY03JE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561,“Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru listarea câmpului.
156	224	610	Tip intrare.	Char(1)	**A** Modificare atribute volum **B** Volum copie de rezervă **C** Conversie volum copie de rezervă la volum primar **E** Exportare **I** Iniţializare **K** Verificare Volum **L** Modificare listă autorizări **M** Importare **N** Redenumire **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
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 autoriz veche [2]	Char(10)	Listă de autorizare veche
259	327	713	Listă auth nouă [3]	Char(10)	Listă de autorizare 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 de autorizare, Modificare atribute volum şi Citire sector.

[2] Folosit doar pentru Importare, Exportare şi Modificare listă de autorizare.

[3] Folosit doar pentru Modificare listă de autorizare.

[4] Folosit doar pentru Citire sector.

Intrări jurnal PA (adoptare program)

Această tabelă furnizează formatul intrărilor de jurnal PA (adoptare program).

Tabela 196. Intrări jurnal PA (adoptare program). Fişier de descriere câmp QASYPAJE/J4/J5

Offset					
JE	**J4**	**J5**	**Field**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561, "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 şi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 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)	
	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	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
	289	675	ID-ul limbaj 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.

Tabela 196. Intrări jurnal PA (adoptare program) (continuare). Fişier de descriere câmp QASYPAJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	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 set de caractere codat pentru numele căii.
	886	1272	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	888	1274	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
	891	1277	Lungime nume cale	Binary(4)	Lungimea numelui căii.
	893	1279	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	894	1280	ID fişier director relativ[4]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri hexazecimale.[4]
	910	1296	Nume cale[5]	Char(5002)	Numele căii obiectului.

Tabela 196. Intrări jurnal PA (adoptare program) (continuare). Fişier de descriere câmp QASYPAJE/J4/J5

Offset			Field	Format	Descriere
JE	J4	J5			
[1]			Aceste câmpuri sunt folosite pentru obiectele din ″root″ (/), QOpenSys şi sisteme 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 tipul de intrare este J, câmpurile nume program şi nume bibliotecă vor conţine *N. În plus, câmpurile ID fişier părinte şi ID fişier obiect vor conţine zerouri binare.		
[4]			Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.		
[5]			Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui căii.		
[6]			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.		

Intrări jurnal PG (modificare grup primar)

Această tabelă furnizează formatul intrărilor de jurnal PG (modificare grup primar).

Tabela 197. Intrări jurnal PG (modificare grup primar). Fişier descriere câmp QASYPGJE/J4/J5

Offset			Field	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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	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.[5]
195	263	649	Grup primar nou	Char(10)	Grupul primar nou pentru obiect.
					Autorizările pentru grupul primar nou:
205	273	659	Object Existence - Existenţă obiect	Char(1)	**Y** *OBJEXIST
206	274	660	Management Obiect	Char(1)	**Y** *OBJMGT
207	275	661	Obiect Operaţional	Char(1)	**Y** *OBJOPR
208	276	662	Object Alter - Modificare obiect	Char(1)	**Y** *OBJALTER

Tabela 197. Intrări jurnal PG (modificare grup primar) (continuare). Fişier descriere câmp QASYPGJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
209	277	663	Object Reference - Referinţă la obiect	Char(1)	**Y** *OBJREF
210	278	664	(Zonă rezervată)	Char(10)	
220	288	674	Authorization List Management - Gestionare listă de autorizare	Char(1)	**Y** *AUTLMGT
221	289	675	Autorizare citire	Char(1)	**Y** *READ
222	290	676	Autorizare adăugare	Char(1)	**Y** *ADD
223	291	677	Autorizare actualizare	Char(1)	**Y** *UPD
224	292	678	Autorizare ştergere	Char(1)	**Y** *DLT
225	293	679	Autorizare execuţie	Char(1)	**Y** *EXECUTE
226	294	680	(Zonă rezervată)	Char(10)	
236	304	690	Autorizare excludere	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 office	Char(10)	Numele utilizatorului 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 folder	Char(63)	Calea folderului.
351	419	805	Office în numele utilizatorului	Char(10)	Utilizator care lucrează în numele unui alt utilizator.
361			(Zonă rezervată)	Char(20)	
	429	815	(Zonă rezervată)	Char(18)	
	447	833	Lungime nume obiect [1]	Binary (4)	Lungimea numelui obiectului.
381	449	835	CCSID nume obiect [1]	Binary(5)	Identificatorul set de caractere codat pentru numele obiectului.
385	453	839	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
387	455	841	ID-ul limbaj nume obiect [1]	Char(3)	ID-ul limbă pentru numele obiectului.
390	458	844	(Zonă rezervată)	Char(3)	
393	461	847	ID fişier părinte[1,2]	Char(16)	ID-ul fişierului directorului părinte.

Tabela 197. Intrări jurnal PG (modificare grup primar) (continuare). Fişier descriere câmp QASYPGJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
409	477	863	ID obiect fişier[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 căii.
	1040	1426	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	1042	1428	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
	1045	1431	Lungime nume cale	Binary(4)	Lungimea numelui căii.
	1047	1433	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	1048	1434	ID fişier director relativ[3]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri în format hexazecimal.[3]
	1064	1450	Nume cale[4]	Char(5002)	Numele căii obiectului.

[1] Aceste câmpuri sunt folosite pentru obiectele din ″root″ (/), QOpenSys şi sisteme 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] Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.

[4] Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui căii.

[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 despre biblioteca obiectului. Dacă obiectul nu este într-o bibliotecă, acestea sunt informaţiile ASP despre obiect.

Intrări jurnal PO (ieşire imprimantă)

Această tabelă furnizează formatul intrărilor de jurnal PO (ieşire imprimantă).

Tabela 198. Intrări jurnal PO (ieşire imprimantă). Fişier descriere câmp QASYPOJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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 de job	Zoned(6,0)	A treia parte a numelui de job calificat.
184	252	638	Profil de utilizator	Char(10)	Profilul de 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	Nume fişier spool	Char(10)	Numele fişierului spool[1]
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.

Tabela 198. Intrări jurnal PO (ieşire imprimantă) (continuare). Fişier descriere câmp QASYPOJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	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)	Timp 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 bibliotecă coadă ieşire.
		1189	Numărul ASP coadă de ieşire	Char(5)	Numărul ASP pentru bibliotecă coadă de ieşire.
		1194	Dată UTC creare fişier spooled	Char(7)	Data de creare fişier spooled în UTC (Aceasta este aceeaşi dată ca Dată creare fişier spool (offset 1151) doar în UTC).
		1201	Oră UTC creare fişier spooled	Char(6)	Oră de creare fişier spooled în UTC (Aceasta este aceeaşi oră ca Oră creare fişier spool (offset 1158) doar în UTC).

[1] Acest câmp este gol dacă tipul ieşirii este direct tipărit.

[2] Acest câmp este gol dacă tipul ieşirii este tipărit la distanţă.

Intrările de jurnal PS (Profile Swap - Schimbare profil)

Această tabelă prezintă formatul intrărilor de jurnal PS (Profile Swap - Schimbare profil).

Tabela 199. Intrările de jurnal PS (Profile Swap - Schimbare profil). Fişier descriere câmp QASYPSJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.

Tabela 199. Intrările de jurnal PS (Profile Swap - Schimbare profil) (continuare). Fişier descriere câmp QASYPSJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
156	224	610	Tip intrare.	Char(1)	Tipul intrării. **A** Schimbare 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** Jetonul profil generat pentru utilizator. **R** Toate jetoanele profil pentru un utilizator au fost înlăturate. **S** Pornire lucru în numele relaţiei **V** Profil de utilizator autentificat
157	225	611	Profil de utilizator	Char(10)	Nume profil de utilizator.
167	235	621	Locaţie sursă	Char(8)	Locaţie sursă pass-through.
175	243	629	Profil de 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 de profil este valid.

Intrări jurnal PW (parolă)

Această tabelă furnizează formatul intrărilor de jurnal PW (parolă).

Tabela 200. Intrări jurnal PW (parolă). Fişier descriere câmp QASYPWJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.
156	224	610	Tip intrare violare	Char(1)	Tipul violării **A** Eşuare legătură APPC. **C** Autentificare utilizator când comanda CHKPWD a eşuat. **D** ID-ul utilizator unelte de service nu este valid. **E** Parola ID utilizator unelte de service nu este validă. **P** Parola nu este validă. **Q** Încercarea de autentificare utilizator a eşuat deoarece este dezactivat profilul de utilizator. **R** Încercarea de autentificare utilizator a eşuat deoarece parola a fost expirată. Această înregistrare de auditare ar putea să nu aibă loc pentru unele mecanisme de autentificare utilizator. Unele mecanisme de autentificare nu verifică pentru parole expirate. **S** Parola de decriptare SQL nu este validă. **U** Numele utilizator nu este valid. **X** ID-ul utilizator unelte de service este dezactivat. **Y** ID-ul utilizator unelte de service nu este valid. **Z** Parola ID utilizator unelte de 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.

Tabela 200. Intrări jurnal PW (parolă) (continuare). Fişier descriere câmp QASYPWJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
		685[2]	Nume obiect	Char(10)	Numele obiectului care este decriptat.
		695	Bibliotecă obiect	Char(10)	Biblioteca pentru obiectul care este decriptat.
		705	Tip obiect	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.

Intrări jurnal RA (modificare autorizare pentru obiect restaurat)

Această tabelă furnizează formatul intrărilor de jurnal RA (modificare autorizare pentru obiect restaurat).

Tabela 201. Intrări jurnal RA (modificare autorizare pentru obiect restaurat). Fişier descriere câmp QASYRAJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561, "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 şi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 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 unde este stocat obiectul.
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 înlăturată.
197	265	651	AUTL înlăturată	Char(1)	**Y** Lista de autorizare înlăturat din obiect.
198	266	652	(Zonă rezervată)	Char(20)	
218	286	672	Nume DLO	Char(12)	Numele obiectului bibliotecă de documente.
230	298	684	(Zonă rezervată)	Char(8)	
238	306	692	Cale folder	Char(63)	Directorul care conţine obiectul bibliotecă de documente.

Tabela 201. Intrări jurnal RA (modificare autorizare pentru obiect restaurat) (continuare). Fişier descriere câmp QASYRAJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
301			(Zonă rezervată)	Char(20)	
	369	755	(Zonă rezervată)	Char(18)	
	387	773	Lungime nume cale	Binary(4)	Lungimea numelui obiectului.
321	389	775	CCSID nume obiect [1]	Binary(5)	Identificatorul set de caractere codat pentru numele obiectului.
325	393	779	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
327	395	781	ID-ul limbaj nume obiect [1]	Char(3)	ID-ul limbă pentru numele obiectului.
330	398	784	(Zonă rezervată)	Char(3)	
333	401	787	ID fişier părinte[1,2]	Char(16)	ID-ul fişierului directorului părinte.
349	417	803	ID obiect fişier[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 căii.
	980	1366	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	982	1368	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
	985	1371	Lungime nume cale	Binary(4)	Lungimea numelui căii.
	987	1373	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	988	1374	ID fişier director relativ[3]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri în format hexazecimal.[3]
	1004	1390	Nume cale[4]	Char(5002)	Numele căii obiectului.

Tabela 201. Intrări jurnal RA (modificare autorizare pentru obiect restaurat) (continuare). Fişier descriere câmp QASYRAJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
			[1] Aceste câmpuri sunt folosite pentru obiectele din ″root″ (/), QOpenSys şi sisteme 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] Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii. [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.		

Intrări jurnal RJ (Restaurare descriere job)

Această tabelă furnizează formatul intrărilor de jurnal RJ (restaurare descriere job).

Tabela 202. Intrări jurnal RJ (Restaurare descriere job). Fişier descriere câmp QASYRJJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.
156	224	610	Tip intrare.	Char(1)	Tipul intrării. **A** restaurarea unei descrieri job care a avut specificat un profil de 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 de 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

Intrări jurnal RO (modificare drept de proprietate pentru obiect restaurat)

Această tabelă furnizează formatul intrărilor de jurnal RO (modificare drept de proprietate pentru obiect restaurat).

Tabela 203. Intrări jurnal RO (modificare drept de proprietate pentru obiect restaurat). Fişier descriere câmp QASYROJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.
156	224	610	Tip intrare.	Char(1)	Tipul intrării. **A** Restaurarea obiectelor care au dreptul de proprietate modificat când sunt restaurate
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)	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 folder	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)	Identificatorul set de caractere codat pentru numele obiectului.
332	400	786	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
334	402	788	ID-ul limbaj 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 obiect fişier[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.

Tabela 203. Intrări jurnal RO (modificare drept de proprietate pentru obiect restaurat) (continuare). Fişier descriere câmp QASYROJE/J4/J5

Offset					
JE	**J4**	**J5**	**Field**	**Format**	**Descriere**
	987	1373	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	989	1375	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
	992	1378	Lungime nume cale	Binary(4)	Lungimea numelui căii.
	994	1380	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	995	1381	ID fişier director relativ[3]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri în format hexazecimal.[3]
	1011	1397	Nume cale[4]	Char(5002)	Numele căii obiectului.

[1] Aceste câmpuri sunt folosite pentru obiectele din ″root″ (/), QOpenSys şi sisteme 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] Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.

[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.

Intrări jurnal RP (restaurarea programelor care adoptă autorizare)

Această tabelă furnizează formatul intrărilor de jurnal RP (restaurarea programelor care adoptă autorizare).

Tabela 204. Intrări jurnal RP (restaurarea programelor care adoptă autorizare). Fişierul descriere câmp QASYRPJE/J4/J5

Offset					
JE	**J4**	**J5**	**Field**	**Format**	**Descriere**
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.

Tabela 204. Intrări jurnal RP (restaurarea programelor care adoptă autorizare) (continuare). Fişierul descriere câmp QASYRPJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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	Biblioteca program	Char(10)	Numele bibliotecii unde 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 regiunii sau ţării pentru numele obiectului.
	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 fişierului directorului părinte.
	311	697	ID obiect fişier[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 căii.
	874	1260	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	876	1262	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
	879	1265	Lungime nume cale	Binary(4)	Lungimea numelui căii.
	881	1267	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.

Tabela 204. Intrări jurnal RP (restaurarea programelor care adoptă autorizare) (continuare). Fişierul descriere câmp QASYRPJE/J4/J5

Offset			Field	Format	Descriere
JE	J4	J5			
	882	1268	ID fişier director relativ[3]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri în format hexazecimal.[3]
	898	1284	Nume cale[4]	Char(5002)	Numele căii obiectului.

[1] Aceste câmpuri sunt folosite pentru obiectele din ″root″ (/), QOpenSys şi sisteme de fişiere definite de utilizator.

[2] Dacă un ID are bitul cel mai din stânga setat şi restul biţilor zero, ID-ul nu este setat.

[3] Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.

[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.

Intrări jurnal RQ (restaurare obiect descriptor cerere modificare)

Această tabelă furnizează formatul intrărilor de jurnal RQ (restaurare obiect descriptor cerere modificare).

Tabela 205. Intrări jurnal RQ (restaurare obiect descriptor cerere modificare). Fişier descriere câmp QASYRQJE/J4/J5

Offset			Field	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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

Intrări jurnal RU (restaurare autorizare pentru profil de utilizator)

Această tabelă furnizează formatul intrărilor de jurnal RU (restaurare autorizare pentru profil de utilizator).

Tabela 206. Intrări jurnal RU (restaurare autorizare pentru profil de utilizator). Fişier de descriere câmp QASYRUJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.
156	224	610	Tip intrare.	Char(1)	Tipul intrării. **A** Restaurare autorizare pentru profilurile de utilizator
157	225	611	Nume utilizator	Char(10)	Numele profilului de 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

Intrări jurnal RZ (modificare grup primar pentru obiect restaurat)

Această tabelă furnizează formatul intrărilor de jurnal RZ (modificare grup primar pentru obiect restaurat).

Tabela 207. Intrări jurnal RZ (modificare grup primar pentru obiect restaurat). Fişier descriere câmp QASYRZJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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.

Tabela 207. Intrări jurnal RZ (modificare grup primar pentru obiect restaurat) (continuare). Fişier descriere câmp QASYRZJE/J4/J5

Offset					
JE	**J4**	**J5**	**Field**	**Format**	**Descriere**
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 folder	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)	Identificatorul set de caractere codat pentru numele obiectului.
332	400	786	ID regiune sau ţară nume obiect [1]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
334	402	788	ID-ul limbaj 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 obiect fişier[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.
	983	1369	CCSID nume cale	Binary(5)	Identificatorul set de caractere codat pentru numele căii.
	987	1373	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	989	1375	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
	992	1378	Lungime nume cale	Binary(4)	Lungimea numelui căii.
	994	1380	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	995	1381	ID fişier director relativ[3]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri în format hexazecimal.[3]

Tabela 207. Intrări jurnal RZ (modificare grup primar pentru obiect restaurat) (continuare). Fişier descriere câmp QASYRZJE/J4/J5

Offset			Field	Format	Descriere
JE	J4	J5			
	1011	1397	Nume cale[4]	Char(5002)	Numele căii obiectului.

[1] Aceste câmpuri sunt folosite pentru obiectele din ″root″ (/), QOpenSys şi sisteme 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] Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.

[4] Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui căii.

Intrări jurnal SD (modificare director distribuţie sistem)

Această tabelă furnizează formatul intrărilor de jurnal SD (modificare director distribuţie sistem).

Tabela 208. Intrări jurnal SD (modificare director distribuţie sistem). Fişier de descriere câmp QASYSDJE/J4/J5

Offset			Field	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.
156	224	610	Tip intrare.	Char(1)	Tipul intrării. **S** Modificare director sistem
157	225	611	Tip modificare	Char(3)	**ADD** Adăugare intrare director **CHG** Modificare intrare director **COL** Intrare colector **DSP** Afişare intrare director **IEŞIRE** Cerere fişier ieşire **PRT** Tipărire intrare director **RMV** Înlăturare 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

Tabela 208. Intrări jurnal SD (modificare director distribuţie sistem) (continuare). Fişier de descriere câmp QASYSDJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
172	240	626	Profil de utilizator	Char(10)	Profilul de 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** Iniţializare offline **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

Intrări jurnal SE (modificare intrare rutare subsistem)

Această tabelă furnizează formatul intrărilor de jurnal SE (modificare intrare rutare subsistem).

Tabela 209. Intrări jurnal SE (modificare intrare rutare subsistem). Fişier descriere câmp QASYSEJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.
156	224	610	Tip intrare.	Char(1)	Tipul intrării. **A** Intrare de rutare subsistem modificată
157	225	611	Nume subsistem	Char(10)	Numele obiectului
167	235	621	Nume bibliotecă	Char(10)	Numele bibliotecii unde este stocat 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 de ordine	Char(4)	Numărul de secvenţă

Tabela 209. Intrări jurnal SE (modificare intrare rutare subsistem) (continuare). Fişier descriere câmp QASYSEJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
209	277	663	Nume 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	Numele ASP pentru biblioteca program	Char(10)	Numele ASP pentru biblioteca program
		691	Numărul ASP pentru biblioteca program	Char(5)	Numărul ASP pentru biblioteca program

Intrări jurnal SF (acţiune fişier spooled)

Această tabelă furnizează formatul intrărilor de jurnal SF (acţiune fişier spooled).

Tabela 210. Intrări jurnal SF (acţiune fişier spooled). Fişier descriere câmp QASYSFJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.

Tabela 210. Intrări jurnal SF (acţiune fişier spooled) (continuare). Fişier descriere câmp QASYSFJE/J4/J5

Offset					
JE	**J4**	**J5**	**Field**	**Format**	**Descriere**
156	224	610	Tip acces	Char(1)	Tipul intrării **A** Fişier spooled citit de altcineva decât proprietarul fişierului spooled. **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 **S** Fişier spool salvat. **T** Fişier spool restaurat. **U** Modificare atribute cu relevanţă pentru securitate fişier spool. **V** Modificare doar atribute fără relevanţă pentru securitate fişier spool.
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 membrului de fişier.
205	273	659	Nume 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

Tabela 210. Intrări jurnal SF (acţiune fişier spooled) (continuare). Fişier descriere câmp QASYSFJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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.
	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.

Tabela 210. Intrări jurnal SF (acţiune fişier spooled) (continuare). Fişier descriere câmp QASYSFJE/J4/J5

Offset					
JE	**J4**	**J5**	**Field**	**Format**	**Descriere**
	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.
	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).

Tabela 210. Intrări jurnal SF (acţiune fişier spooled) (continuare). Fişier descriere câmp QASYSFJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
		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 bibliotecă coadă ieşire.
		1645	Numărul ASP coadă de ieşire	Char(5)	Numărul ASP pentru bibliotecă coadă de ieşire.
		1650	Nume ASP nou coadă de ieşire	Char(10)	Nume ASP pentru bibliotecă coadă de ieşire nouă.
		1660	Număr ASP nou pentru coada de ieşire	Char(5)	Număr ASP pentru bibliotecă coadă de ieşire nouă.
		1665	Stare fişier spool vechi	Char(3)	Stare fişier spool vechi
		1668	Stare nouă fişier spool	Char(3)	Stare nouă fişier spool
		1671	Data originală de creaţie	Char(7)	Data originală de creaţie.
		1678	Timpul original de creaţie	Char(6)	Timpul original de creaţie.
		1684	Data de expirare fişier spool vechi	Char(7)	Data de expirare fişier spool vechi
		1687	Data de expirare fişier spool nou	Char(7)	Data de expirare fişier spool nou
		1694	Dată UTC creare fişier spooled	Char(7)	Data de creare fişier spooled în UTC (Aceasta este aceeaşi dată ca Dată creare fişier spool (offset 1097) dar în UTC).
		1701	Oră UTC creare fişier spooled	Char(6)	Oră de creare fişier spooled în UTC (Aceasta este aceeaşi oră ca Oră creare fişier spool (offset 1104) dar în UTC).

[1] Acest câmp este gol când tipul intrării este I (tipărire inline).

Intrări jurnal SG (semnale asincrone)

Această tabelă furnizează formatul intrărilor de jurnal SG (semnale asincrone).

Tabela 211. Intrări jurnal SG (semnale asincrone). Fişier descriere câmp QASYSGJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561 şi “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 pentru menţionarea de câmp.
	224	610	Tip intrare.	Char(1)	Tipul intrării. **A** Semnal asincron i5/OS 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.
	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 de utilizator 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.

Intrări jurnal SK (conexiuni socket-uri securizate)

Această tabelă furnizează formatul intrărilor de jurnal SK (conexiuni socket-uri securizate).

Tabela 212. Intrări jurnal SK (conexiuni socket-uri securizate). Fişier de descriere câmp QASYSKJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561 şi “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 pentru menţionarea de câmp.
	224	610	Tip intrare	Char(1)	**A** Acceptare **C** Conectare **D** Adresă DHCP alocată **F** Poştă filtrată **P** Port nedisponibil **R** Refuzare poştă **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.
	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)	Numele de gazdă al clientului care face cererea.

[1] Acesta este un câmp de 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.

Intrări jurnal SM (modificare gestionare sisteme)

Această tabelă furnizează formatul intrărilor de jurnal SM (modificare gestionare sisteme).

Tabela 213. Intrări jurnal SM (modificare gestionare sisteme). Fişier de descriere câmp QASYSMJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561, "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 şi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 pentru menţionarea câmpului.
156	224	610	Tip intrare.	Char(1)	Funcţie accesată **B** Listă copie de rezervă modificată **C** Opţiuni de curăţare automată **D** DRDA **F** Sistem de fişiere HFS **N** Operaţie fişier reţea **O** Opţiuni copie de rezervă modificate **P** Planificare oprire/pornire alimentare **S** Listă răspunsuri sistem **T** Timpi de recuperare cale de acces modificaţi
157	225	611	Tip acces	Char(1)	**A** Add - Adăugare **C** Modificare **D** Delete - Ştergere **R** Înlăturare **S** Afişare **T** Extragere sau primire
158	226	612	Număr de ordine	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

Tabela 213. Intrări jurnal SM (modificare gestionare sisteme) (continuare). Fişier de descriere câmp QASYSMJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
243	311	697	Proprietar fişier reţea	Char(10)	Numele profilului de utilizator care deţine fişierul reţea
253	321	707	Utilizatorul care a generat fişierul reţea	Char(8)	Numele profilului de utilizator care a generat fişierul reţea
261	329	715	Adresa care a generat fişierul reţea	Char(8)	Adresa care a generat fişierul reţea

Intrări jurnal SO (acţiuni informaţii utilizator securitate server)

Această tabelă furnizează formatul intrărilor de jurnal SO (acţiuni informaţii utilizator securitate server).

Tabela 214. Intrări jurnal SO (acţiuni informaţii utilizator securitate server). Fişier descriere câmp QASYSOJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561, "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 şi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 pentru menţionarea câmpului.
156	224	610	Tip intrare.	Char(1)	Tipul intrării **A** Adăugare intrare **C** Modificare intrare **R** Înlăturare intrare **T** Extragere intrare
157	225	611	Profil de utilizator	Char(10)	Numele profilului de utilizator.
	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)	

Tabela 214. Intrări jurnal SO (acţiuni informaţii utilizator securitate server) (continuare). Fişier descriere câmp QASYSOJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	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 un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea câmpului.

Intrări jurnal ST (acţiune unelte service)

Această tabelă furnizează formatul intrărilor de jurnal ST (acţiuni unelte service).

Tabela 215. Intrări jurnal ST (acţiune unelte service). Fişier descriere câmp QASYSTJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561, "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 şi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 pentru menţionarea câmpului.
156	224	610	Tip intrare.	Char(1)	Tipul intrării **A** Înregistrare service
157	225	611	Unealtă service	Char(2)	Tipul intrării. **AN** ANZJVM **AR** Urmărire diagnostic ARM (consultaţi comanda ARMSRV QShell) **CD** QTACTLDV, QTADMPDV **CE** QWTCTLTR **CS** STRCPYSCN **CT** DMPCLUTRC **DC** DLTCMNTRC **DD** DMPDLO **DF** QWTDMPFR, QWTDMPLF **DI** QSCDIRD **DJ** DMPJVM, QPYRTJVM **DM** DMPMEMINF **DO** DMPOBJ

Tabela 215. Intrări jurnal ST (acţiune unelte service) (continuare). Fişier descriere câmp QASYSTJE/J4/J5

Offset			Field	Format	Descriere	
JE	J4	J5				
					DS	DMPSYSOBJ, QTADMPTS, QTADMPDV, QWTDMPLF
					DU	DMPUSRPRF
					DW	STRDW, ENDDW, ADDDWDFN, RMVDWDFN
					EC	ENDCMNTRC
					ER	ENDRMTSPT
					GS	QSMGSSTD
					HD	QYHCHCOP (DASD)
					HL	QYHCHCOP (LPAR)
					JW	STRJW, ENDJW, ADDJWDFN, RMVJWDFN
					LC	EPT creat
					LD	EPT şters
					LE	EPT pentru job a fost modificat
					LF	EPT sistem a fost reparat
					LG	Intrările din EPT au fost modificate
					LH	EPT comparat
					LI	Intrări EPT afişate
					MC	QWTMAINT (modificare)
					MD	QWTMAINT (dump)
					MP	Terminare job sistem
					MQ	Repornire job sistem
					OP	Consola de operaţii
					PC	PRTCMNTRC
					PE	PRTERRLOG, QTADMPDV
					PI	PRTINTDTA, QTADMPDV
					PS	QP0FPTOS
					SC	STRCMNTRC
					SE	QWTSETTR

Tabela 215. Intrări jurnal ST (acţiune unelte service) (continuare). Fişier descriere câmp QASYSTJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
					SF QWCCDSIC, QWVRCSTK (afişare intrare stivă internă) **SJ** STRSRVJOB **SN** QPZSYNC **SR** STRRMTSPT **SS** QFPHPSF **ST** STRSST **SV** QSRSRV **TA** TRCTCPAPP
					TC TRCCNN (specificat *FORMAT) **TE** ENDTRC, ENDPEX, TRCJOB(specificat *OFF sau *END) **TI** TRCINT sau TRCCNN cu SET(*ON), SET(*OFF) sau SET(*END) **TO** QTOBSRV **TQ** QWCTMQTM **TS** STRTRC, STRPEX, TRCJOB(specificat *ON)
					UD QTAUPDDV **WE** ENDWCH, QSCEWCH **WS** STRWCH, QSCSWCH **WT** WRKTRC **WW** WRKWCH
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 de job	Zoned(6,0)	A treia parte a numelui de job calificat
213	281	667	Nume obiect	Char(30)	Numele obiectului pentru DMPSYSOBJ
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 folder[8]	Char(63)	Directorul care conţine obiectul bibliotecă de documente
	432	818	Câmp JUID	Char(10)	JUID-ul jobului destinaţie

Tabela 215. Intrări jurnal ST (acţiune unelte service) (continuare). Fişier descriere câmp QASYSTJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	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 dezactivată şi informaţiile de urmărire şterse.
	452	838	Opţiune de urmărire aplicaţie[2]	Char(1)	Opţiunea de urmărire specificată în TRCTCPAPP. **A**[6] Activare **D**[6] Dezactivare **Y**[7] Colecţia de informaţii de urmărire pornită **N**[7] Colecţia de informaţii de urmărire oprită şi informaţiile de urmărire scrise în fişierul spool **E**[7] Colecţia de informaţii de urmărire terminată şi toate informaţiile de urmărire şterse (nici o ieşire creată)
	453	839	Urmărit de aplicaţie[2]	Char(10)	Numele aplicaţiei care este urmărită.
	463	849	Profiluri unelte de 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
		907	Tip de consolă [4]	Char(10)	Tipul consolei. Valorile posibile sunt: • *DIRECT • *LAN • *HMC
		917	Acţiune consolă [4]	Char(10)	Acţiune consolă. Valorile posibile sunt: • *RECOVERY • *TAKEOVER

Tabela 215. Intrări jurnal ST (acţiune unelte service) (continuare). Fişier descriere câmp QASYSTJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
		927	Familia de adrese[4]	Char(10)	Familia de adrese. • *IPv4 • *IPv6
		937	Adrese IP precedente [4]	Char(46)	Adresele IP ale dispozitivului consolă precedent pentru *LAN.
		938	ID-ul dispozitivului precedent [4]	Char(10)	ID-ul dispozitivului unealtă de service ale dispozitivului consolă precedent pentru *LAN.
		993	Adresă IP curentă [4]	Char(46)	Adresa IP a dispozitivului curent consolă pentru *LAN.
		1039	ID-ul dispozitivului curent [4]	Char(10)	ID-ul dispozitivului unealtă de service ale dispozitivului consolă precedent pentru *LAN.
		1049	Urmăreşte sesiune[5]	Char(10)	ID urmărire sesiune.
		1059	Intrare[9]	Char(10)	Numele intrării din tabele punct intrare care a fost modificată.
		1069	Obiect înrudit[10]	Char(10)	Numele obiectului înrudit. • Pentru valoarea LC unelte de service, acest câmp conţine numele tabelei punct de intrare de bază. • Pentru valoarea LG unelte de service, acest câmp conţine numele programului de înlocuire. • Pentru valoarea LH unelte de service, acest câmp conţine numele unei tabele punct de intrare de comparat.
		1079	Bibliotecă de obiecte înrudită[10]	Char(10)	Numele bibliotecii de obiecte înrudită. • Pentru valoarea LC unelte de service, acest câmp conţine numele bibliotecii tabelă punct de intrare de bază. • Pentru valoarea LG unelte de service, acest câmp conţine numele bibliotecii programului de înlocuire. • Pentru valoarea LH unelte de service, acest câmp conţine numele bibliotecii tabelei punct de intrare de comparat.

[1] Acest câmp este folosit doar când valoarea Unelte de service (offset 611) este CE.

[2] Acest câmp este folosit doar când valoarea Unelte de service (offset 611) este AR sau TA.

[3] Acest câmp este folosit doar când valoarea Unelte de service (offset 611) este ST sau OP.

[4] Acest câmp este folosit doar când valoarea Unelte de service (offset 611) este OP.

[5] Acest câmp este folosit doar când tipul intrării (offset 611) este WS sau WE.

Tabela 215. Intrări jurnal ST (acţiune unelte service) (continuare). Fişier descriere câmp QASYSTJE/J4/J5

Offset			Field	Format	Descriere
JE	J4	J5			
[6] Acest câmp este folosit doar când valoarea Unelte de service (offset 611) este AR.					
[7] Acest câmp este folosit doar când valoarea Unelte de service (offset 611) este TA.					
[8] Calea de foldere va conţine numele de 30 caractere Comandă analiză avansată când valoarea Unelte de service (offset 611) este GS.					
[9] Acest câmp este folosit doar când valoarea Unelte de service (offset 611) este LG.					
[10] Acest câmp este folosit doar când valoarea Unelte de service (offset 611) este LC, LG sau LH.					

Intrări jurnal SV (acţiune la valoare de sistem)

Această tabelă furnizează formatul intrărilor de jurnal SV (acţiune la valoare de sistem).

Tabela 216. Intrări jurnal SV (acţiune la valoare de sistem). Fişier descriere câmp QASYSVJE/J4/J5

Offset			Field	Format	Descriere
JE	J4	J5			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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 **D** Ajustare la UTC **E** Modificare la opţiune **F** Modificaţi la atributul de jurnal sistem
157	225	611	Valoare sistem sau atribut service	Char(10)	**JRNRCVCNT** Valoare număr recuperare jurnal modificat **MAXCCHWAIT** Timp aşteptare cache maxim jurnal modificat **QINPIDCO** Modificaţi opţiunea de configuraţie disc instalare curentă cu API-ul QINPIDCO.
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.

Tabela 216. Intrări jurnal SV (acţiune la valoare de sistem) (continuare). Fişier descriere câmp QASYSVJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
917	985	1371	Continuarea valorii vechi	Char(250)	Continuarea valorii valorii de sistem sau a atributului de service înainte să fie modificate.
		1621	Extensie continuată valoare nouă	Char(1000)	A doua continuare a valorii la care a fost modificată valoarea de sistem sau atributul de service.
		2621	Extensie continuată valoare veche	Char(1000)	A doua continuare a valorii valorii de sistem sau atributului de service înainte să fie modificate.

Intrări jurnal VA (modificare listă de control acces)

Această tabelă furnizează formatul intrărilor de jurnal VA (modificare listă de control acces).

Tabela 217. Intrări jurnal VA (modificare listă de control acces). Fişier descriere câmp QASYVAJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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)	Data 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.

Intrări jurnal VC (începere şi terminare conexiune)

Această tabelă furnizează formatul intrărilor de jurnal VC (începere şi terminare conexiune).

Tabela 218. Intrări jurnal VC (începere şi terminare conexiune). Fişier descriere câmp QASYVCJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.
156	224	610	Acţiune de conectare.	Char(1)	Acţiunea de conectare care a apărut. **S** Pornire **E** Oprire **R** Refuzare
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)	Data 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 conexiunii: **A** Deconectarea automată (timeout), partajare înlăturată 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.

Intrări jurnal VF (închidere fişier server)

Această tabelă furnizează formatul intrărilor de jurnal VF (închidere fişier server).

Tabela 219. Intrări jurnal VF (închidere fişier server). Fişier descriere câmp QASYVFJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561, "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 şi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 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.
173	241	627	Timp server	Zoned(6,0)	Data 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.

Intrări jurnal VL (limita de conturi depăşită)

Această tabelă furnizează formatul intrărilor de jurnal VL (limita de conturi depăşită).

Tabela 220. Intrări jurnal VL (limita de conturi depăşită). fişier descriere câmp QASYVLJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561, "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 şi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 pentru menţionarea câmpului.

Tabela 220. Intrări jurnal VL (limita de conturi depăşită) (continuare). fişier descriere câmp QASYVLJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
156	224	610	Motivul	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)	Data 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.

Intrările de jurnal VN (Logare şi delogare în reţea)

Această tabelă prezintă formatul intrărilor de jurnal VN (Logare şi delogare în reţea).

Tabela 221. Intrările de jurnal VN (Logare şi delogare în reţea). Fişier descriere câmp QASYVNJE/J4/J5

Offset			Câmp	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561, "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 şi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 pentru menţionarea câmpului.
156	224	610	Tip logare	Char(1)	Tipul evenimentului care a apărut: **F** Cerere delogare **O** Cerere logare **R** Logare refuzată
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)	Data 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.

Tabela 221. Intrările de jurnal VN (Logare şi delogare în reţea) (continuare). Fişier descriere câmp QASYVNJE/J4/J5

Offset			Câmp	Format	Descriere
JE	**J4**	**J5**			
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

Intrări jurnal VO (Listă de validare)

Această tabelă furnizează formatul intrărilor de jurnal VO (Listă de validare).

Tabela 222. Intrări jurnal VO (Listă de validare). Fişier descriere câmp QASYVOJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561 şi “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 pentru menţionarea de câmp.
	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** Înlăturare 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
	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

Tabela 222. Intrări jurnal VO (Listă de validare) (continuare). Fişier descriere câmp QASYVOJ4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	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)	Valoare 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

Intrări jurnal VP (eroare parolă reţea)

Această tabelă furnizează formatul intrărilor de jurnal VP (eroare parolă reţea).

Tabela 223. Intrări jurnal VP (eroare parolă reţea). Fişier descriere câmp QASYVPJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561, "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 şi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 pentru menţionarea câmpului.
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 a fost reţinut în istoric evenimentul pe serverul reţea.
173	241	627	Timp server	Zoned(6,0)	Data 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.

Intrări jurnal VR (acces resursă reţea)

Această tabelă furnizează formatul intrărilor de jurnal VR (acces resursă reţea).

Tabela 224. Intrări jurnal VR (acces resursă reţea). Fişier descriere câmp QASYVRJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)" la pagina 561, "Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)" la pagina 563 şi "Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)" la pagina 565 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 a fost reţinut în istoric evenimentul pe serverul reţea.
173	241	627	Timp server	Zoned(6,0)	Data 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.

Tabela 224. Intrări jurnal VR (acces resursă reţea) (continuare). Fişier descriere câmp QASYVRJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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 resursei folosite.

Intrări jurnal VS (sesiune server)

Această tabelă furnizează formatul intrărilor de jurnal VS (sesiune server).

Tabela 225. Intrări jurnal VS (sesiune server). Fişier descriere câmp QASYVSJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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.

Tabela 225. Intrări jurnal VS (sesiune server) (continuare). Fişier descriere câmp QASYVSJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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 înlăturată sau lipsă de permisiuni administrative **E** Eroare, deconectare sesiune sau parolă incorectă **N** Deconectare normală sau limită de nume utilizator **R** Restricţie cont

Intrări jurnal VU (modificare profil reţea)

Această tabelă furnizează formatul intrărilor de jurnal VU (modificare profil reţea).

Tabela 226. Intrări jurnal VU (modificare profil reţea). Fişier descriere câmp QASYVUJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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 de 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 a fost reţinut în istoric evenimentul pe serverul reţea.
173	241	627	Timp server	Zoned(6,0)	Data la care a fost reţinut în istoric evenimentul pe serverul reţea.
179	247	633	Nume calculator	Char(8)	Numele calculatorului care cere modificarea profilului de utilizator.

Tabela 226. Intrări jurnal VU (modificare profil reţea) (continuare). Fişier descriere câmp QASYVUJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
187	255	641	Utilizator	Char(10)	Numele utilizatorului care cere modificarea profilului de utilizator.
197	265	651	Acţiunea	Char(1)	Acţiune cerută: **A** Adăugare **C** Modificare **D** Ştergere **P** Parolă incorectă
198	266	652	Nume resursă	Char(260)	Numele resursei.

Intrări jurnal VV (modificare stare serviciu)

Această tabelă furnizează formatul intrărilor de jurnal VV (modificare stare serviciu).

Tabela 227. Intrări jurnal VV (modificare stare serviciu). Fişier descriere câmp QASYVVJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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 a fost reţinut în istoric evenimentul pe serverul reţea.
173	241	627	Timp server	Zoned(6,0)	Data 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.

Tabela 227. Intrări jurnal VV (modificare stare serviciu) (continuare). Fişier descriere câmp QASYVVJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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.
286	354	740	Valoare retur	Char(4)	Valoarea retur din operaţia de modificare.
290	358	744	Serviciu	Char(20)	Serviciul care fost modificat.

Intrări jurnal X0 (autentificare reţea)

Această tabelă furnizează formatul intrărilor de jurnal X0 (modificare stare serviciu).

Tabela 228. Intrări jurnal X0 (autentificare reţea). Fişier descriere câmp QASYX0JE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.

Tabela 228. Intrări jurnal X0 (autentificare reţea) (continuare). Fişier descriere câmp QASYX0JE/J4/J5

Offset					
JE	**J4**	**J5**	**Field**	**Format**	**Descriere**
156	224	610	Tip intrare.	Char(1)	Tipul intrării: **1** Tichet serviciu 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** Eşuare decriptare autentificator **7** Regiunea nu este în regiunile locale client **8** Tichetul este o încercare de repunere în funcţiune. **9** Tichetul nu este încă valid. **A** Decriptare eroare 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 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 canal **N** Context expirat desfăşurare GSS sau verificare GSS **O** Decriptare/decodificare desfăşurare GSS sau verificare GSS **P** Eroare sumă de control desfăşurare GSS sau verificare GSS **Q** Eroare secvenţială desfăşurare GSS sau 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

Tabela 228. Intrări jurnal X0 (autentificare reţea) (continuare). Fişier descriere câmp QASYX0JE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	539	925	Indicator adrese criptate	Char(1)	Indicator adrese IP criptate **Y** toate adresele incluse **N** nu toate adresele incluse **X** nefurnizat
	540	926	Steguleţe tichet	Char(8)	Steguleţe 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)

Tabela 228. Intrări jurnal X0 (autentificare reţea) (continuare). Fişier descriere câmp QASYX0JE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	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)
	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 server 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

Tabela 228. Intrări jurnal X0 (autentificare reţea) (continuare). Fişier descriere câmp QASYX0JE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
	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

Intrări jurnal X1 (jeton identitate)

Această tabelă furnizează formatul intrărilor de jurnal X1 (jeton identitate).

Tabela 229. Intrări jurnal X1 (jeton identitate). Fişier descriere câmp QASYX1JE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
		1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.
		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
		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

Tabela 229. Intrări jurnal X1 (jeton identitate) (continuare). Fişier descriere câmp QASYX1JE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
		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>receiver_eimID </EIMID> <APPID>RECEIVER_appID </APPID> <TIMESTAMP>receiver_timestamp </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 Datele din acest câmp vor fi în formatul: <EIMID>sender_eimID </EIMID> <APPID>sender_appID </APPID> <TIMESTAMP>sender_timestamp </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>initiator_eimID </EIMID> <APPID>initiator_appID </APPID> <TIMESTAMP>initiator_timestamp </TIMESTAMP>.
		2162	Lungime lanţ	Binary(5)	Lungimea datelor din câmpul lanţ.
		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 va fi trunchiat dacă lanţul este mai lung decât lungimea acestui câmp. Datele din acest câmp va 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 ar putea fi mai mare decât numărul de intrări din câmp dacă câmpul lanţ este trunchiat.
		4210	Lungime registru sursă	Binary(5)	Lungimea datelor din câmpul registru sursă.
		4214	Registru sursă	Char(508)	Registrul sursă specificat în jetonul identitate.
		4722	Lungime utilizator registru sursă	Binary(5)	Lungimea datelor din câmpul utilizator registru sursă.
		4726	Utilizator registru sursă	Char(508)	Utilizatorul registru sursă specificat în jetonul identitate.
		5234	Lungime registru destinaţie	Binary(5)	Lungimea datelor din câmpul registru destinaţie.

Tabela 229. Intrări jurnal X1 (jeton identitate) (continuare). Fişier descriere câmp QASYX1JE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
		5238	Registru destinaţie	Char(508)	Registru destinaţie specificat.
		5746	Lungime utilizator registru destinaţie	Binary(5)	Lungimea datelor din câmpul utilizator registru destinaţie.
		5750	Utilizator registru destinaţie	Char(508)	Utilizatorul registru destinaţie spre care indică jetonul identitate.

Intrări jurnal XD (extensie server de director)

Această tabelă furnizează formatul intrărilor de jurnal XD (extensie server de director).

Tabela 230. Intrări jurnal XD (extensie server de director). Fişier descriere câmp QASYXDJ5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
		1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.
		610	Tip intrare.	Char(1)	Tipul intrării: **G** Nume de grup. Câmpurile de la 1 la 5 conţin nume de grupuri.
		611	Referinţă încrucişată	Char(36)	Şir referinţă încrucişată folosit pentru a corela această intrare cu intrarea DI care foloseşte aceste grupuri. Mai multe intrări DI pot referi această intrare XD dacă mai multe cereri LDAP folosesc acelaşi set de grupuri.
		647	Rezervat	Char(100)	
		747	Câmp 1 CCSID	Bin(5)	Valoarea CCSID pentru câmpul 1.
		751	Lungime câmp 1	Bin(4)	Lungimea datelor din câmpul 1.
		753	Câmp 1	Char(2002)	Date câmp 1 Pentru tipul de intrare G, acest câmp va conţine un nume de grup dintr-o presupunere de apartenenţă de grup.
		2755	Câmpul 2 CCSID	Bin(5)	Valoarea CCSID pentru câmpul 2.
		2759	Lungime câmp 2	Bin(4)	Lungimea datelor din câmpul 2.
		2761	Câmpul 2	Char(2002)	Date câmp 2 Pentru tipul de intrare G, acest câmp va conţine un nume de grup dintr-o presupunere de apartenenţă de grup.

Tabela 230. Intrări jurnal XD (extensie server de director) (continuare). Fişier descriere câmp QASYXDJ5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
		4763	Câmpul 3 CCSID	Bin(5)	Valoarea CCSID pentru câmpul 3.
		4767	Lungime câmp 3	Bin(4)	Lungimea datelor din câmpul 3.
		4769	Câmp 3	Char(2002)	Date câmp 3 Pentru tipul de intrare G, acest câmp va conţine un nume de grup dintr-o presupunere de apartenenţă de grup.
		6771	Câmp 4 CCSID	Bin(5)	Valoarea CCSID pentru câmpul 4.
		6775	Lungime câmp 4	Bin(4)	Lungimea datelor din câmpul 4.
		6777	Câmp 4	Char(2002)	Date câmp 4 Pentru tipul de intrare G, acest câmp va conţine un nume de grup dintr-o presupunere de apartenenţă de grup.
		8779	CCSID 5 câmp	Bin(5)	Valoarea CCSID pentru câmpul 5.
		8783	Lungime câmp 5	Bin(4)	Lungimea datelor în câmpul 5.
		8785	Câmpul 5	Char(2002)	Date câmp 5 Pentru tipul de intrare G, acest câmp va conţine un nume de grup dintr-o presupunere de apartenenţă de grup.

Intrări jurnal YC (modificare la obiect DLO)

Această tabelă furnizează formatul intrărilor de jurnal YC (modificare la obiect DLO).

Tabela 231. Intrări jurnal YC (modificare la obiect DLO). Fişier descriere câmp QASYYCJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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 de utilizator al utilizatorului office
195	263	649	Nume document sau director	Char(12)	Numele documentului sau directorului

Tabela 231. Intrări jurnal YC (modificare la obiect DLO) (continuare). Fişier descriere câmp QASYYCJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
207	275	661	(Zonă rezervată)	Char(8)	
215	283	669	Cale folder	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 “Coduri numerice pentru tipuri de acces” la pagina 697 pentru o listă de coduri pentru tipurile de acces.					

Intrări jurnal YR (citire obiect DLO)

Această tabelă furnizează formatul intrărilor de jurnal YR (citire obiect DLO).

Tabela 232. Intrări jurnal YR (citire obiect DLO). Fişier descriere câmp QASYYRJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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 de 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 folder	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 “Coduri numerice pentru tipuri de acces” la pagina 697 pentru o listă de coduri pentru tipurile de acces.					

Intrări jurnal ZC (modificare la obiect)

Această tabelă furnizează formatul intrărilor de jurnal ZC (modificare la obiect).

Tabela 233. Intrări jurnal ZC (modificare la obiect). Fişier descriere câmp QASYZCJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 pentru menţionarea câmpului.
156	224	610	Tip intrare.	Char(1)	Acces obiect **C** Modificarea unui obiect **U** Modernizare a 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 233. Intrări jurnal ZC (modificare la obiect) (continuare). Fişier descriere câmp QASYZCJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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. Când tipul obiectului este un obiect sistem de fişiere integrat, acest câmp conţine informaţii suplimentare identificând cererea de modificare. Consultaţi fişierul de includere QSYSINC, QP0LJRNL.H pentru valorile posibile.
238			(Zonă rezervată)	Char(20)	
	306	692	(Zonă rezervată)	Char(18)	
	324	710	Lungime nume obiect [2]	Binary (4)	Lungimea numelui obiectului.

Tabela 233. Intrări jurnal ZC (modificare la obiect) (continuare). Fişier descriere câmp QASYZCJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
258	326	712	CCSID nume obiect [2]	Binary(5)	Identificatorul set de caractere codat pentru numele obiectului.
262	330	716	ID regiune sau ţară nume obiect [2]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
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 fişierului 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 căii.
	917	1303	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	919	1305	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
	922	1308	Lungime nume cale	Binary(4)	Lungimea numelui căii.
	924	1310	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	925	1311	ID fişier director relativ[4]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri hexazecimale.[4]
	941	1327	Nume cale[5]	Char(5002)	Numele căii obiectului.

Tabela 233. Intrări jurnal ZC (modificare la obiect) (continuare). Fişier descriere câmp QASYZCJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
[1] Vedeţi “Coduri numerice pentru tipuri de acces” la pagina 697 pentru o listă de coduri pentru tipurile de acces. [2] Aceste câmpuri sunt folosite pentru obiectele din ″root″ (/), QOpenSys şi sisteme de fişiere definite de utilizator. [3] Un ID care are bitul cel mai din stânga setat şi restul biţilor 0 indică faptul că ID -ul NU este setat. [4] Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii. [5] Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui căii. [6] 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.					

Intrări jurnal ZR (citire obiect)

Această tabelă furnizează formatul intrărilor de jurnal ZR (citire obiect).

Tabela 234. Intrări jurnal ZR (citire obiect). Fişier descriere câmp QASYZRJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
1	1	1			Câmpurile antet comune pentru toate tipurile de intrări. Vedeţi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE5 (*TYPE5)” la pagina 561, “Câmpuri antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE4 (*TYPE4)” la pagina 563 şi “Câmpurile antet standard pentru intrări jurnal auditare Format înregistrare QJORDJE2 (*TYPE2)” la pagina 565 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 234. Intrări jurnal ZR (citire obiect) (continuare). Fişier descriere câmp QASYZRJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
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)	Identificatorul set de caractere codat pentru numele obiectului.
262	330	716	ID regiune sau ţară nume obiect [2]	Char(2)	ID-ul regiunii sau ţării pentru numele obiectului.
264	332	718	ID limbă nume obiect[2]	Char(3)	ID-ul limbă pentru numele obiectului.
267	335	721	(Zonă rezervată)	Char(3)	

Tabela 234. Intrări jurnal ZR (citire obiect) (continuare). Fişier descriere câmp QASYZRJE/J4/J5

Offset			Field	Format	Descriere
JE	**J4**	**J5**			
270	338	724	ID fişier părinte[2,3]	Char(16)	ID-ul fişierului directorului părinte.
286	354	740	ID fişier obiect[2,3]	Char(16)	ID-ul fişier al obiectului.
302	370	756	Nume Object[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 căii.
	917	1303	ID regiune sau ţară nume cale	Char(2)	ID-ul de ţară sau regiune pentru numele de cale.
	919	1305	ID limbă nume cale	Char(3)	ID-ul de limbă pentru numele de cale.
	922	1308	Lungime nume cale	Binary(4)	Lungimea numelui căii.
	924	1310	Indicator nume cale	Char(1)	Indicator nume cale: **Y** Câmpul Nume cale conţine numele căii absolute complete pentru obiect. **N** Câmpul Nume cale nu conţine un numede cale absolut pentru obiect, în schimb conţine un nume de cale relativ. Câmpul ID fişier director înrudit este valid şi poate fi folosit pentru a forma un nume de cale absolut cu acest nume de cale relativ.
	925	1311	ID fişier director relativ[4]	Char(16)	Când câmpul indicator nume cale este ″N″, acest câmp va conţine ID-ul de fişier al directorului care conţine obiectul identificat în câmpul Nume cale. Altfel conţine zerouri hexazecimale.[4]
	941	1327	Nume cale[5]	Char(5002)	Numele căii obiectului.

[1] Vedeţi “Coduri numerice pentru tipuri de acces” pentru o listă de coduri pentru tipurile de acces.

[2] Aceste câmpuri sunt folosite pentru obiectele din ″root″ (/), QOpenSys şi sisteme de fişiere definite de utilizator.

[3] Un ID care are bitul cel mai din stânga setat şi restul biţilor 0 indică faptul că ID -ul NU este setat.

[4] Dacă câmpul indicator nume cale este N, dar ID-ul fişier înrudit conţine doar zerouri hexazecimale, atunci a avut loc o eroare la determinarea informaţiilor despre numele căii.

[5] Acesta este un câmp de lungime variabilă. Primii 2 octeţi conţin lungimea numelui căii.

Coduri numerice pentru tipuri de acces

Această tabelă listează codurile de acces folosite pentru intrările jurnal de auditare obiecte din fişierele QASYYCJE/J4/J5, QASYYRJE/J4/J5, QASYZCJE/J4/J5 şi QASYZRJE/J4/J5.

Tabela 235. Coduri numerice pentru tipuri de acces

Cod	Tip acces	Cod	Tip acces	Cod	Tip acces
1	Add - Adăugare	26	Încărcare	51	Trimitere
2	Activare program	27	Listare	52	Pornire

Tabela 235. Coduri numerice pentru tipuri de acces (continuare)

Cod	Tip acces	Cod	Tip acces	Cod	Tip acces
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	Interogare	57	Lucru
8	Verificare	33	Revendicare	58	Atribut DLO citire/modificare
9	Închidere	34	Recepţie	59	Securitate DLO citire/modificare
10	Curăţare	35	Read - Citire	60	Conţinut DLO citire/modificare
11	Comparaţie	36	Reorganizare	61	Toate părţile DLO citire/modificare
12	Anulare	37	Eliberare	62	Adăugare constrângere
13	Copiere	38	Înlăturare	63	Modificare constrângere
14	Create - Creare	39	Redenumire	64	Înlăturare constrângere
15	Conversie	40	Înlocuire	65	Pornire procedură
16	Depanare	41	Continuare	66	Obţinere acces la **OOPOOL
17	Delete - Ştergere	42	Restaurare	67	Semnare obiect
18	Dump	43	Extragere	68	Înlăturarea 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. Comenzi şi meniuri pentru comenzi de securitate

Meniul SECTOOLS (Unelte de securitate), meniul SECBATCH (Lansare sau planificare rapoarte securitate în batch), comenzile Configurare securitate sistem (CFGSYSSEC) şi Revocare autorizare publică (RVKPUBAUT) sunt patru unelte de securitate pe care le puteţi folosi pentru a configura securitatea sistemului.

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 speciificat.

Opţiuni din meniul Unelte de securitate

Puteţi folosi meniul Unelte de securitate (SECTOOLS) pentru a simplifica gestionarea şi controlul securităţii sistemului cu multele opţiuni şi comenzi pe care le furnizează.

Această figură arată partea meniului SECTOOLS care se leagă de profiluri de utilizator.

Pentru a accesa acest meniu, tastaţi GO SECTOOLS.

```
SECTOOLS                      Security Tools

Select one of the following:

  Work with profiles
     1. Analyze default passwords

     2. Display active profile list
     3. Change active profile list
     4. Analyze profile activity

     5. Display activation schedule
     6. Change activation schedule entry

     7. Display expiration schedule
     8. Change expiration schedule entry
     9. Print profile internals
```

Tabela 236 descrie aceste opţiuni de meniuri şi comenzile asociate:

Tabela 236. Comenzi unealtă pentru profiluri de utilizator

Opţiune meniu[1]	Nume comandă	Descriere	Fişier bază de date folosit
1	ANZDFTPWD	Folosiţi comanda Analizare parole implicite pentru a raporta şi a lua acţiuni pe profilurile de utilizatori care au o parolă egală cu cea a numelui profilului de utilizator.	QASECPWD[2]
2	DSPACTPRFL	Folosiţi comanda Afişare listă de profiluri active pentru a afişa sau tipări lista de profiluri de utilizatori care sunt exceptaţi de la procesarea ANZPRFACT.	QASECIDL[2]

Tabela 236. Comenzi unealtă pentru profiluri de utilizator (continuare)

Opţiune meniu[1]	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 de utilizator care este în lista de profiluri active este permanent 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 de 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 de utilizator de a fi dezactivate.	QASECIDL[2]
5	DSPACTSCD	Folosiţi comanda Afişare planificare activare pentru a afişa sau tipări informaţii despre planficarea pentru activarea şi dezactivarea de profiluri de utilizator specifice. Puteţi crea planificarea cu comanda 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 de 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 de utilizator sunt setate pentru a expira în acea zi. Folosiţi comanda DSPEXPSCD pentru a afişa profilurile de 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 intrări într-un obiect profil de utilizator (*USRPRF).	

Tabela 236. Comenzi unealtă pentru profiluri de utilizator (continuare)

Opţiune meniu[1]	Nume comandă	Descriere	Fişier bază de date folosit
Observaţii: 1. Opţiuni sunt din meniul SECTOOLS. 2. Acest fişier este în biblioteca QUSRSYS.			

Puteţi apăsa pe pagină jos în meniu pentru a vedea opţiunile suplimentare. Tabela 237 descrie opţiunile meniu şi comenzile asociate pentru auditarea securităţii:

Tabela 237. Comenzi unealtă pentru auditarea securităţii

Opţiune meniu[1]	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 gestionarea primitorilor jurnalului de auditare. Altfel, 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.	
12	CPYAUDJRNE	Folosiţi comanda copiere intrări jurnal auditat pentru a copia intrările jurnalului de auditare de securitate în fişiere de ieşire.	QASYxxJ5[2]

[1] Opţiuni sunt din meniul SECTOOLS.

[2] 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, “Dispunerea intrărilor de jurnal de auditare”, la pagina 561 a acestei colecţii de subiecte.

Cum să folosiţi meniul Batch securitate

Puteţi folosi meniul batch securitate pentru a lansa unul sau mai multe din rapoartele Unelte de securitate într-o coadă de joburi pentru a rula ulterior ca un job batch. Puteţi de asemenea alege să planificaţi oricare din rapoartele Unelte de securitate ca joburi batch pentru a fi lansate o dată sau să fie lansate la intervale regulate. Exemplele din acest subiect demonstrează cum să folosiţi meniul batch de securitate.

Următoarea este prima parte a meniului SECBATCH:

```
SECBATCH         Submit or Schedule Security Reports To Batch
                                                                  System:
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. Autorizarea pentru fişier
    12. File private authority
    13. Folder authority
```

Atunci când selectaţi o opţiune din acest meniu, vedeţi ecranul Lansare job (SBMJOB), după cum urmează:

```
                            Submit Job (SBMJOB)
Type choices, press Enter.

Command to run . . . . . > PRTADPOBJ USRPRF(*ALL)
_____________________________________________
_____________________________________________
_____________________________________________...
Job name . . . . . .   *JOBD          Name, *JOBD
Job description  . . . . . .   *USRPRF       Name, *USRPRF
  Library  . . . . . .                 Name, *LIBL, *CURLIB
Job queue  . . . . . .   *JOBD          Name, *JOBD
  Library  . . . . . .                 Name, *LIBL, *CURLIB
Job priority (on JOBQ) . . . . .   *JOBD          1-9, *JOBD
Output priority (on OUTQ)  . . .   *JOBD          1-9, *JOBD
Print device . . . . . .   *CURRENT      Name, *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
                                                                System:
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. Autorizarea pentru director
```

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:

```
                    Add Job Schedule Entry (ADDJOBSCDE)

Type choices, press Enter.

Job name . . . . . _____                    Name, *JOBD
Command to run . . . . . > PRTADPOBJ USRPRF(*ALL)
_____________________________________________
_____________________________________________
_____________________________________________
_____________________________________________...
Frequency  . . . . . *ONCE, *WEEKLY, *MONTHLY
Schedule date, or  . . . . . *CURRENT      Date, *CURRENT, *MONTHST
Schedule day . . . . . *NONE         *NONE, *ALL, *MON, *TUE.
+ for more values
Schedule time  . . . . . *CURRENT      Time, *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.

Opţiuni din meniul batch de securitate

Această tabelă descrie opţiunile de meniu şi comenzile asociate pentru rapoarte 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 de utilizator şi securitate relevantă. De aceea, raportul descriere de job (PRTJOBDAUT)tipăreşte descrieri de job din biblioteca specificată numai dacă autorizarea publică pentru descrierea de job nu este *EXCLUDE *şi* dacă descrierea de job specifică nu nume profil de 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 speciifică un profil de utilizator.

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

Tabela 238. Comenzi pentru rapoarte de securitate

Opţiunea meniu[1]	**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[6]	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 238. Comenzi pentru rapoarte de securitate (continuare)

Opţiunea meniu[1]	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. Acest raport 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 de utilizator 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 238. Comenzi pentru rapoarte de securitate (continuare)

Opţiunea meniu[1]	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 informaţii 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 aceeaşi 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 aceeaşi 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 comanda Tipărire autorizare coadă pentru a tipări setările de securitate pentru cozile de ieşire şi cozile de joburi din sistem. Aceste setări controlează cine poate vizualiza şi modifica intrări din coada de ieşire sau coada de joburi. 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 238. Comenzi pentru rapoarte de securitate (continuare)

Opţiunea meniu[1]	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 are 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 de utilizator care îndeplinesc criteriile specificate. Puteţi selecta profilurile de 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 de utilizator (*USRPRF).	

Tabela 238. Comenzi pentru rapoarte de securitate (continuare)

Opţiunea meniu[1]	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.	

[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 ale modelului sunt descrise în Anexa F, “Dispunerea intrărilor de jurnal de auditare”, la pagina 561 din această colecţie de subiecte.

[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 autorizările publice şi QPVPGM pentru autorizările 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.

[6] Comanda DSPAUDJRNE nu poate procesa toate tipuri de înregistrări de auditare securitate şi comanda nu listează toate câmpurile pentru înregistrările pe care le suportă.

Comenzi pentru personalizarea securităţii

Această tabelă descrie comenzile pe care le puteţi folosi pentru a personaliza securitate din sistem, care sunt în meniul SECTOOLS.

Tabela 239. Comenzi perntru personalizarea sistemului

Opţiune meniu[1]	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 de asemenea auditarea de securitate pe sistemul dumneavoastră. “Valorile care sunt setate de comanda Configurare securitate sistem” descrie ce face comanda.	
61	RVKPUBAUT	Folosiţi comanda Revocare autorizare publică pentru a seta autorizarea publică la *EXCLUDE pentru un set de comenzi sensibile la securitate pe sistemul dumneavoastră. “Ce face comanda Revocare autorizare publică” la pagina 710listează acţiunile pe care le realizează comanda RVKPUBAUT.	

[1] Opţiuni sunt din meniul SECTOOLS.

Valorile care sunt setate de comanda Configurare securitate sistem

Această tabelă listează valorile de sistem care sunt setate când rulaţi comanda Configurare securitate sistem (CFGSYSSEC) care rulează un program care este numit QSYS/QSECCFGS.

Tabela 240. Valori setate de comanda CFGSYSSEC

Nume valoare de sistem	Setare	Descriere valoare de 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 autorizare 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 de utilizator atunci când limita QMAXSIGN este atinsă.
QPWDEXPITV	60	Cât de des trebuie să-şi modifice utilizatorii parolele
QPWDMINLEN	6 (Vedeţi nota 3 şi 5)	Lungime minimă pentru parole
QPWDMAXLEN	8 (Vedeţi nota 4 şi 5)	Lungime maximă pentru parole
QPWDPOSDIF	1 (Da) (Vedeţi nota 5)	Dacă fiecare poziţie dintr-o parolă trebuie să difere de aceeaşi poziţie din vechea parolă
QPWDLMTCHR	Vedeţi nota 2 şi 5	Caractere care nu sunt permise în parolă
QPWDLMTAJC	1 (Da) (Vedeţi nota 5)	Dacă numere adiacente sunt interzise în parole
QPWDLMTREP	2 (Nu poate fi repetat consecutiv) (Vedeţi nota 5)	Dacă sunt interzise caractere repetate în parole
QPWDRQDDGT	1 (Da) (Vedeţi nota 5)	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
QPWDRULES	• *MINLEN6 • *MAXLEN10 • *LMTSAMPOS • *LMTPRFNAME • *DGTMIN1 • *CHRLMTAJC • *DGTLMTAJC • *DGTLMTFST • *DGTLMTLST • *SPCCHRLMTAJC • *SPCCHRLMTFST • *SPCCHRLMTLST (vedeţi nota 6)	Reguli pentru formarea unei parole valide.

Tabela 240. Valori setate de comanda CFGSYSSEC (continuare)

Nume valoare de sistem	Setare	Descriere valoare de sistem
QPWDVLDPGM	*NONE	Programul ieşire utilizator pe care sistem îl apelează pentru a valida parolele
QRMTSIGN	*FRCSIGNON	Cum manipulează sistemul o încercare de semnare la distanţă (passthrough sau TELNET).
QRMTSVRATR	0 (Off)	Permite ca sistemul să fie analizat la distanţă.
QSECURITY	50	Nivelul de securitate care este impus
QVFYOBJRST	3	Verificare obiect la restaurare

Observaţii:

1. Dacă rulaţi momentan cu o valoare QSECURITY de 30 sau mai puţin, asiguraţi-vă că examinaţi informaţiile din Capitolul 2, “Folosirea valorii de sistem QSecurity”, la pagina 9 înainte de a modifica la un nivel mai mare de securitate.
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) ca să modificaţi caracterele restricţionate.
3. Dacă lungimea minimă pentru parole este deja mai mare decât 6, valoarea de sistem QPWDMINLEN nu va fi modificată.
4. Dacă lungimea minimă pentru parole este deja mai mare decât 8, valoarea de sistem QPWDMAXLEN nu va fi modificată.
5. Această valoare de sistem este modificată doar când valoarea de sistem QPWDRULES specifică în mod curent o valoare de *PWDSYSVAL.
6. Această valoare de sistem nu va fi modificată dacă valoarea sa curentă este *PWDSYSVAL.

Comanda CFGSYSSEC setează de asemenea parola la *NONE pentru următoarele profiluri de utilizator livrate de IBM:

- QSYSOPR
- QPGMR
- QUSER
- QSRV
- QSRVBAS

În sfârşit, comanda CFGSYSSEC setează auditarea securităţii conform cu valorile pe care le-aţi specificat folosind comanda Modificare auditare securitate (CHGSECAUD).

Modificarea programului

Dacă unele valori de sistem ale setărilor nu sunt corespunzătoare pentru instalare, puteţi crea propria versiune a programului care procesează comanda Configurare securitate sistem (CFGSYSSEC).

Pentru a modifica programul, realizaţi următorii paşi:

1. Folosiţi Extragere sursă CL (RTVCLSRC) pentru a copia sursa pentru programul care rulează când folosiţi comanda CFGSYSSEC. Programul pentru extragere este QSYS/QSECCFGS. Atunci când îl extrageţi, daţi-i un nume diferit.
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 trebui să aibă un nume diferit.
3. Folosiţi comanda Modificare comandă (CHGCMD) pentru a modifica parametrul PGM pentru comanda CFGSYSSEC. Setaţi valoarea PGM la numele programului dumneavoastră. De exemplu, dacă creaţi un program în biblioteca QGPL care este numit MYSECCFG, trebuie să tastaţi următoarea comandă:

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

   Observaţii:

a. Dacă modificaţi programul QSYS/QSECCFGS, IBM nu poate garanta sau sugera fiabilitatea, capabilitatea de service, performanţa sau funcţia programului. Garanţiile implicate pentru fabricare sau potrivirea cu un anumit scop nu sunt acordate explicit.

b. Dacă modificaţi comanda RVKPUBAUT pentru a folosi un program de procesare comandă diferit, atunci semnătura digitală a acestei comenzi nu va mai fi validă.

Ce face comanda Revocare autorizare publică

Puteţi folosi comanda Revocare autorizare publică (RVKPUBAUT) pentru a seta autorizarea publică la *EXCLUDE pentru un set de comenzi şi programe.

Comanda RVKPUBAUT rulează un program care este numit QSYS/QSECRVKP. La livrare, QSECRVKP revocă autorizarea publică (prin setarea la *EXCLUDE) pentru comenzile care sunt listate în Tabela 241 şi interfeţele programabile pentru aplicaţii (API) care sunt listate în Tabela 242. Atunci când soseşte sistemul dumneavoastră, aceste comenzi şi API-uri au autorizarea publică setată la *USE.

Comenzile care sunt listate în Tabela 241 şi API-urile care sunt listate în Tabela 242 realizează pe sistemul dumneavoastră funcţii care pot oferi posibilitatea de a face rău. 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 în care se află aceste comenzi. Biblioteca implicită este QSYS. Dacă aveţi mai multe limbi naţionale pe sistem, trebuie să rulaţi comanda pentru fiecare bibliotecă QSYSxxx.

Tabela 241. Comenzile a căror autorizare publică este setată de comanda RVKPUBAUT

ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGE
ADDPJE	CHGWSE	RMVWSE
ADDRTGE	CPYCFGL	RSTLIB
ADDWSE	CRTCFGL	RSTOBJ
CHGAJE	CRTCTLAPPC	RSTS36F
CHGCFGL	CRTDEVAPPC	RSTS36FLR
CHGCFGLE	CRTSBSD	RSTS36LIBM
CHGCMNE	ENDRMTSPT	STRRMTSPT
CHGCTLAPPC	RMVAJE	STRSBS
CHGDEVAPPC	RMVCFGLE	WRKCFGL

API-urile din Tabela 242 sunt toate în biblioteca QSYS:

Tabela 242. Programe ale căror autorizare publică este setată de comanda RVKPUBAUT

QTIENDSUP		
QTISTRSUP		
QWTCTLTR		
QWTSETTR		
QY2FTML		

Începând cu V3R7, când rulaţi comanda RVKPUBAUT, sistemul setează autorizarea publică pentru directorul rădăcină la *USE (dacă nu este deja *USE sau mai puţin).

Modificarea programului

Dacă unele valori de sistem ale setărilor nu sunt corespunzătoare pentru instalare, puteţi crea propria versiune a programului care procesează comanda Revocare autorizare publică (RVKPUBAUT).

Pentru a modifica programul, realizaţi următorii paşi:

1. Folosiţi comanda Extragere sursă CL (RTVCLSRC) pentru a copia sursa pentru programul care rulează când folosiţi comanda RVKPUBAUT. Programul pentru a fi extras este QSYS/QSECRVKP. Atunci când îl extrageţi, daţi-i *un nume diferit*.
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.
3. Folosiţi comanda Modificare comandă (CHGCMD) pentru a modifica parametrul PGM pentru comanda RVKPUBAUT. Setaţi valoarea PGM la numele programului dumneavoastră. De exemplu, dacă creaţi un program în biblioteca QGPL care este numit MYRVKPGM, trebuie să tastaţi următoarea comandă:

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

   Observaţii:

   a. 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.
   b. Dacă modificaţi comanda RVJPUDAUT pentru a folosi un program de procesare comandă diferit, atunci semnătura digitală a acestei comenzi nu va mai fi validă.

Anexa H. Informaţii înrudite pentru Referinţă securitate i5/OS

Aici sunt prezentate manuale de produse, publicaţii IBM Redbooks (în format PDF), situri web şi subiecte din centrul de informare care conţin informaţii referitoare la securitate. Puteţi vizualiza sau tipări oricare PDF.

Manuale

- Recuperarea sistemului (aproximativ 8,42 MB), furnizează informaţii despre planificarea unei strategii de salvare de rezervă şi recuperare, salvarea informaţiilor din sistem şi recuperarea sistemului, pool de memorie auxiliară şi opţiuni protecţie disc.
- Instalarea, modernizarea sau ştergerea i5/OS şi a software-ului înrudit (3.053 KB), furnizează proceduri pas-cu-pas pentru instalarea iniţială, instalarea programelor licenţiate, corecţii temporare de program (PTF-uri) şi limbaje secundare de la IBM.
- Remote Workstation Support (1.636 KB), furnizează informaţii despre cum să setaţi şi să folosiţi suportul de staţie de lucru la distanţă, cum ar fi staţia de afişare pass-through, facilitatea de comandă gazdă distribuită şi ataşament la distanţă 3270.
- Cryptographic Support/400 (448 KB), descrie capabilităţile de securitate a datelor ale programului licenţiat Cryptographic Facility. Se explică cum se foloseşte facilitatea şi se oferă informaţii de referinţă pentru programatori.
- Local Device Configuration (763 KB), furnizează informaţii despre cum să faceţi o configuraţie iniţială şi cum să modificaţi acea configuraţie. Conţine de asemenea informaţii conceptuale despre configurarea dispozitivelor.
- *SNA Distribution Services*, SC41-5410 (2.259 KB), furnizează informaţii despre configurarea unei reţele pentru SNADS şi puntea VM/MVS. În plus, sunt discutate funcţiile de distribuire a obiectelor, serviciile pentru biblioteca de documente şi serviciile pentru directorul de distribuţie sistem. (Acest manual nu este inclus în această ediţie a centrului de informare i5/OS. Însă ar putea fi o resursă utilă pentru dumneavoastră. Manualul este disponibil la IBM Publications Center ca o copie tipărită, pe care o puteţi comanda, sau în format online, pe care îl puteţi descărca gratuit.)
- *ADTS for AS/400: Source Entry Utility*, SC09-2605 (460 KB), furnizează informaţii despre folosirea utilitarului intrare sursă (SEU - source entry utility) 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. (Acest manual nu este inclus în această ediţie a centrului de informare i5/OS. Însă ar putea fi o resursă utilă pentru dumneavoastră. Manualul este disponibil la IBM Publications Center ca o copie tipărită, pe care o puteţi comanda, sau în format online, pe care îl puteţi descărca gratuit.)

IBM Redbooks

- AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet (2,1 MB) Această publicaţie IBM Redbook discută problemele de securitate şi riscurile asociate cu conectarea produsului System i la Internet. Vi se oferă exemple, recomandări, sugestii şi tehnici pentru aplicaţii.
- Cool Title About the AS/400 and Internet (7,36 MB) Această publicaţie IBM Redbook vă poate ajuta să înţelegeţi şi apoi să folosiţi Internetul (sau propriul intranet) de pe produsul System i. Vă ajută să înţelegeţi cum se folosesc funcţiile şi caracteristicile. Această carte vă iniţiază în folosirea e-mail-ului, transferul de fişiere, emularea de terminal, gopher, HTTP şi 5250 la gateway HTML.

Situri web

- Lotus Documentation (http://www-10.lotus.com/ldd/doc)

Acest sit web furnizează informaţii despre Lotus Notes, Domino şi IBM Domino for i5/OS. De pe acest sit 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.

Alte informaţii

- Planificarea şi setarea securităţii sistemului furnizează un set de sugestii practice pentru folosirea caracteristicilor de securitate ale iSeries şi pentru stabilirea procedurilor de operare care sunt conştiente de securitate. Această carte descrie de asemenea cum să setaţi şi să folosiţi uneltele de securitate care fac parte din i5/OS.
- *Implementing AS/400 Security, 4th Edition* (October 15, 2000) by Wayne Madden and Carol Woodbury. Loveland, Colorado: 29th Street Press. Oferă îndrumări şi indicaţii practice pentru planificarea, setarea şi gestionarea securităţii sistemului.

  Număr de comandă ISBN
  1583040730
- System i Access pentru Windows furnizează informaţii tehnice despre programele System i Access pentru Windows pentru toate versiunile de System i Access pentru Windows
- Setarea TCP/IP furnizează informaţii care descriu cum să folosiţi şi să configuraţi TCP/IP.
- Aplicaţiile, protocoalele şi serviciile TCP/IP furnizează informaţii care descriu cum să folosiţi aplicaţiile TCP/IP, cum ar fi FTP, SMTP şi TELNET.
- Operaţiile de sistem de bază furnizează informaţii despre cum să porniţi şi să opriţi sistemul şi să gestionaţi problemele de sistem.
- Sistemul de fişiere integrat oferă o privire generală asupra sistemului de fişiere integrat, explicându-se ce este, cum poate fi folosit şi ce interfeţe sunt disponibile.
- iSeries şi securitatea în Internet vă ajută să rezolvaţi problemele potenţiale de securitate pe care le puteţi avea la conectarea iSeries la Internet. Pentru informaţii suplimentare, vizitaţi pagină acasă following IBM I/T (Information Technology) Security, la http://www.ibm.com/security. Stocarea optică furnizează informaţii despre funcţiile care sunt unice pentru *suportul optic*. 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.
- Tipărirea furnizează informaţii despre elementele şi conceptele tipăririi, fişierul de imprimantă şi suport spool de tipărire pentru operarea tipăririi şi conectivitatea tipăririi.
- Limbajul de control furnizează o discuţie largă de subiecte de programare, inclusiv o discuţie generală de obiecte şi biblioteci, programare CL, controlarea fluxului şi comunicaţiilor între programe, lucru cu obiect în programe CL şi crearea 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.

  Furnizează de asemenea o descriere a limbajului de control (CL) iSeries şi a comenzilor i5/OS. Comenzile i5/OS sunt utilizate pentru a accesa funcţii ale programului licenţiat i5/OS (5722-SS1). Toate comenzile CL non-i5/OS — cele asociate cu celelalte programe cu licenţă, incluzând toate limbile şi diversele utilitare — sunt descrise în alte cărţi care suportă acele programe cu licenţă.
- Programarea furnizează informaţii despre multe dintre limbajele şi utilitarele disponibile pe iSeries. Sunt prezentate rezumativ:
  - Toate comenzile CL iSeries (în programul i5/OS şi în toate celelalte programe licenţiate), în diverse forme.
  - Informaţii 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.
  - Obiectele livrate de IBM, cum ar fi bibliotecile.
  - Valorile de sistem livrate de IBM.
  - Cuvintelor cheie DDS pentru fişiere fizice, logice, de afişare, de imprimantă şi ICF.
  - Instrucţiunile REXX şi funcţiile încorporate.
  - Alte limbaje (cum ar fi RPG) şi utilitare (cum ar fi SEU şi SDA).

- Gestionarea sistemelor include informaţii despre colectarea datelor de performanţă, gestionarea valorilor de sistem şi gestionarea spaţiului de stocare.
- Concepte privind fişierul de bază de date furnizează o privire generală asupra modului în care puteţi să proiectaţi, să scrieţi, să rulaţi şi să testaţi instrucţiunile DB2 Query Manger şi SQL Development Kit pentru i5/OS. 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. Furnizează de asemenea informaţii despre:
  - 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

Salvarea fişierului PDF

Pentru a salva un PDF pe staţia de lucru pentru vizualizare sau tipărire:

1. Faceţi clic dreapta pe fişierul PDF în browser-ul dumneavoastră (faceţi clic dreapta pe legătura de mai sus).
2. Faceţi clic pe opţiunea de salvare locală a PDF-ului.
3. Navigaţi la directorul în care doriţi să salvaţi PDF-ul.
4. Faceţi clic pe **Save**.

Descărcarea programului Adobe Reader

Pentru a vizualiza sau tipări aceste PDF-uri, trebuie să aveţi instalat pe sitem Adobe Reader. Puteţi descărca o copie gratuită de pe situl Web Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Anexa I. Observaţii

Aceste informaţii au fost elaborate pentru produse şi servicii oferite în S.U.A.

Este posibil ca IBM să nu ofere în alte ţări produsele, serviciile sau 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 se sugerează faptul că poate fi folosit numai acel produs, program sau serviciu IBM. Poate fi folosit în loc orice produs, program sau serviciu care este echivalent din punct de vedere funcţional şi care nu încalcă dreptul de proprietate intelectuală al IBM. Însă evaluarea şi verificarea modului în care funcţionează un produs, program sau serviciu non-IBM ţine de responsabilitatea utilizatorului.

IBM poate avea brevete sau aplicaţii în curs de brevetare care să acopere subiectele descrise în acest document. Prin furnizarea acestui document nu vi se acordă nicio licenţă pentru aceste brevete. Puteţi trimite întrebări cu privire la licenţe, în scris, la:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pentru întrebări privind licenţa pentru informaţiile DBCS (pe doi octeţi), contactaţi departamentul IBM de proprietate intelectuală din ţara dumneavoastră sau trimiteţi întrebările 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 Marii Britanii sau al altor ţări unde asemenea prevederi nu sunt în concordanţă cu legile locale: INTERNATIONAL BUSINESS MACHINES CORPORATION OFERĂ ACEASTĂ PUBLICAŢIE “CA ATARE”, FĂRĂ NICI UN FEL DE GARANŢIE, EXPRESĂ SAU PRESUPUSĂ, INCLUSIV, DAR NU NUMAI, GARANŢIILE IMPLICITE DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME, DE VANDABILITATE SAU DE POTRIVIRE PENTRU UN ANUMIT SCOP. Unele state nu permit declinarea responsabilităţii pentru garanţiile exprese sau implicite în anumite tranzacţii şi de aceea este posibil ca aceste clauze să nu fie valabile în cazul dumneavoastră.

Aceste informaţii pot conţine greşeli tehnice sau erori de tipar. Se efectuează modificări periodice la informaţiile incluse aici; aceste modificări vor fi încorporate în noi ediţii ale publicaţiei. IBM poate aduce îmbunătăţiri şi/sau modificări produsului (produselor) descris în această publicaţie în orice moment, fără notificare.

Referirile din aceste informaţii la adrese de situri Web non-IBM sunt făcute numai pentru a vă ajuta, fără ca prezenţa lor să însemne un gir acordat acestor situri Web. Materialele de pe siturile Web respective nu fac parte din materialele pentru acest produs IBM, iar utilizarea acestor situri Web se face pe propriul risc.

IBM poate utiliza sau distribui oricare dintre informaţiile pe care le furnizaţi, în orice mod considerat adecvat, fără ca aceasta să implice vreo obligaţie pentru dumneavoastră.

Posesorii de licenţe pentru acest program care doresc să obţină informaţii despre el în scopul de a permite: (I) schimbul de informaţii între programe create independent şi alte programe (inclusiv acesta) şi (II) utilizarea mutuală a informaţiilor care au fost schimbate, trebuie să contacteze:

IBM Corporation
Software Interoperability Coordinator, Department YBWA

3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Aceste informaţii pot fi disponibile cu respectarea termenilor şi condiţiilor corespunzătoare, iar în unele cazuri cu plata unei taxe.

Programul licenţiat la care se referă aceste informaţii şi toate materialele licenţiate disponibile pentru ele sunt furnizate de IBM în conformitate cu termenii din IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code sau din alt acord echivalent încheiat 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. Este posibil ca unele măsurători să fi fost realizate pe sisteme de nivel evoluat şi nu există nici o garanţie că aceste măsurători vor fi identice pe sisteme general disponibile. Mai mult, unele măsurători pot fi estimări obţinute 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 prezentate sunt preţurile cu amănuntul sugerate de IBM, sunt actuale şi pot fi modificate fără notificare. Preţurile dealer-ului pot fi diferite.

Aceste informaţii sunt doar pentru 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 ca IBM să pretindă vreo plată, când o faceţi în scopul dezvoltării, folosirii, promovării şi distribuirii programelor de aplicaţii conform 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 fiabilitatea, suportul pentru service sau funcţionarea acestor programe.

Fiecare copie sau porţiune din aceste exemple de program sau orice lucrare derivată din acestea trebuie să includă un anunţ de copyright de genul următor:

© (numele companiei dumneavoastră) (anul). Unele porţiuni din acest cod sunt derivate din programele exemplu oferite de IBM Corp. © Copyright IBM Corp. _introduceţi anul sau anii_. Toate drepturile rezervate.

Dacă vizualizaţi aceste informaţii folosind o copie electronică, fotografiile şi ilustraţiile color s-ar putea să nu apară.

Informaţii despre interfaţa de programare

Această publicaţie, Referinţă securitate, conţine informaţii despre interfeţele de programare menite să permită beneficiarului să scrie programe pentru a obţine serviciile IBM i5/OS.

Mărci comerciale

Următorii termeni sunt mărci comerciale deţinute de International Business Machines Corporation în Statele Unite, în alte ţări sau ambele:

AIX
i5/OS
IBM
IBM (logo)
System i
z/OS

Intel, Intel Inside (logo-uri), MMX şi Pentium sunt mărci comerciale deţinute de Intel Corporation în Statele Unite, în alte ţări sau ambele.

Microsoft, Windows, Windows NT şi logo-ul Windows sunt mărci comerciale deţinute de Microsoft Corporation în Statele Unite, în alte ţări sau ambele.

Java şi toate mărcile comerciale bazate pe Java sunt mărci comerciale deţinute de Sun Microsystems, Inc. în Statele Unite, în alte ţări sau ambele.

Linux este o marcă comercială înregistrată deţinută de Linus Torvalds în Statele Unite, în alte ţări sau ambele.

UNIX este o marcă comercială înregistrată deţinută de The Open Group în Statele Unite şi în alte ţări.

Alte nume de companii, produse şi servicii pot fi mărci comerciale sau mărci de serviciu ale altora.

Windows

Termenii şi condiţiile

Permisiunile pentru utilizarea acestor publicaţii sunt acordate în conformitate cu următorii termeni şi condiţii.

Utilizare personală: Puteţi reproduce aceste publicaţii pentru utilizarea personală, necomercială, cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi distribui, afişa sau realiza obiecte derivate din aceste publicaţii sau dintr-o porţiune a lor fără consimţământul explicit al IBM.

Utilizare comercială: Puteţi reproduce, distribui şi afişa aceste publicaţii doar în cadrul întreprinderii dumneavoastră, cu condiţia ca toate anunţurile de proprietate să fie păstrate. Nu puteţi să realizaţi lucrări derivate din aceste informaţii, nici să reproduceţi, să distribuiţi sau să afişaţi aceste informaţii sau o porţiune a lor în afara întreprinderii dumneavoastră fără consimţământul explicit al IBM.

Cu excepţia a ceea ce este acordat explicit prin această permisiune, nu sunt acordate alte permisiuni, licenţe sau drepturi, explicit sau implicit, pentru publicaţii sau alte informaţii, date, software sau altă proprietate intelectuală conţinută în acestea.

IBM îşi rezervă dreptul de a retrage permisiunile acordate aici oricând consideră că folosirea publicaţiilor este în detrimentul intereselor sale sau când personalul IBM constată că instrucţiunile de mai sus nu sunt urmate corespunzător.

Nu puteţi descărca, exporta sau reexporta aceste informaţii decât în deplină conformitate cu legile şi regulamentele aplicabile, inclusiv toate legile şi regulamentele de export ale Statelor Unite.

IBM NU ACORDĂ NICIO GARANŢIE PENTRU CONŢINUTUL ACESTOR PUBLICAŢII. ACESTE PUBLICAŢII SUNT FURNIZATE ″CA ATARE″, FĂRĂ NICIUN FEL DE GARANŢIE, EXPLICITĂ SAU IMPLICITĂ,

INCLUZÂND, DAR NU NUMAI, GARANŢIILE IMPLICITE DE VANDABILITATE, DE NEÎNCĂLCARE A UNOR DREPTURI SAU NORME ŞI DE POTRIVIRE PENTRU UN ANUMIT SCOP.

Index

Caractere speciale

A

B

C

D

E

F

G

H

I

Î

J

M

N

O

P

Q

R

S

U

V

W

Z

Printed in USA

SA12-6497-10